値を更新し、

第2のインデックス変数jの配列要素S[j]を第2のシフト数ローテイトシフトした値と内部変数kとの算術加算結果に基づき内部変数kの値を更新し、

S[i]＋S[j]による配設要素S[(S[i]＋S[j])]を第3のシフト数ローテイトシフトした値と内部変数kとの算術加算結果に基づき、鍵ストリームを出力し、

前記鍵ストリームを生成するために参照した配列要素S[(S[i]＋S[j])]を、鍵ストリーム出力の直後に内部変数kと配列要素S[i]を用いて更新する第2の処理部と、

を備えている、ことを特徴とする請求項1記載の暗号装置。

[11] 初期設定配列aを用い、配列aの並べ替えを行って攪拌し、前記一時変数をなす内部変数kを、対応する配列要素aをローテイトシフトしたものと算術加算して求め、前記擬似乱数列の生成に用いる内部状態として配列Sを、配列aの要素をローテイトシフトしたものと配列Sの要素との所定の演算によって求める第1の処理部と、

前記擬似乱数(以下、「鍵ストリーム」と称する)を生成するにあたり、第1、第2のインデックス変数i、jに関して配列Sの参照結果S[j]と内部変数kとを算術加算し、S[i]＋S[j]による配設Sの参照結果と内部変数kに基づき、鍵ストリームを出力し、

鍵ストリームを生成するために参照したSのエントリを、鍵ストリーム出力直後に内部変数kを用いて更新する第2の処理部と、

を備えている、ことを特徴とする請求項1記載の暗号装置。

[12] 秘密鍵に基づき擬似乱数列を生成し、前記擬似乱数列を平文に作用させることにより暗号文を生成する暗号装置を構成するコンピュータに、

前記擬似乱数列の生成に用いる内部状態として、有限個の数値の列の並び替えを基礎とする状態に基づく内部状態を用い、

前記擬似乱数列の生成に用いる一時変数の少なくとも一つを、

前記内部状態のうちの一つ、又は、複数個の数値を使用した、線形、又は、非線形、線形及び非線形の組み合わせの結果に基づき、内部状態の数より小さい数に依存し、あらかじめ定められた、左又は右ローテイトシフトを実行した結果を値とする一時変数とし、

前記擬似乱数を、前記内部状態のうちの1つ又は複数個の数値と、前記一時変数

WAVELYNX EX. 1003, Pg. 978
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

との予め定められた所定の演算によって生成する、処理

を実行させるプログラム。

[13] 請求項12記載のプログラムにおいて、

前記有限個の数値の列の並び替えを基礎とする状態に基づく内部状態に関して、

前記内部状態の更新を、並び替え以外の、線形演算、および、非線形演算を用いて行う、ことを特徴とするプログラム。

[14] 請求項12記載のプログラムにおいて、

前記有限個の数値の列の並び替えを基礎とする状態に基づく内部状態に関して、

前記内部状態の更新として、並び替え以外の、線形演算及び非線形演算を用いて行い、前記内部状態の状態数を、単調増加と単調減少のうちの一方にしたがって変化させる、ことを特徴とするプログラム。

[15] 請求項12記載のプログラムにおいて、

前記有限個の数値の列の並び替えを基礎とする状態に基づく内部状態に関して、

前記内部状態の更新として、並び替え以外の線形演算及び非線形演算を用いて行い、内部状態の状態数を振動させる、ことを特徴とするプログラム。

[16] 請求項12記載のプログラムにおいて、

前記内部状態の更新を、

前記擬似乱数列の出力ごとに行う、

前記擬似乱数列の出力よりも多く行う、

前記擬似乱数列の出力よりも少なく行う、

のうちの選択されたいずれか一つで行う、ことを特徴とする、プログラム。

[17] 請求項12記載のプログラムにおいて、

前記ローテイトシフトの方向及び／又はシフト数を、前記内部状態の数値に依存して動的に変更する、ことを特徴とする、プログラム。

[18] 請求項12記載のプログラムにおいて、

前記ローテイトシフトの方向及びシフト数を、あらかじめ定められたテーブルの値に従って変更する、ことを特徴とする、プログラム。

[19] 前記擬似乱数列の生成に用いる内部状態として、配列Sの要素の並び替えと算術

WAVELYNX EX. 1003, Pg. 979
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

加算を繰り返すことで配列Sの要素を攪拌し配列Sの初期状態を作成し、その際、前記一時変数をなす内部変数kの初期値を配列Sの要素から求める第1の処理と、

前記擬似乱数（以下、「鍵ストリーム」と称する）を生成する処理として、

第1、第2のインデックス変数iとjに関して配列Sの要素S[j]と内部変数kの算術加算結果をローテイトシフトした値で内部変数kの値を更新し、

S[i]＋S[j]による配設Sの参照結果S[(S[i]＋S[j])]と内部変数kとの算術加算結果に基づき、鍵ストリームを出力し、

前記鍵ストリームを生成するために参照した配列Sの要素S[(S[i]＋S[j])]を、鍵ストリーム出力の直後に内部変数kと配列要素S[i]を用いて更新する第2の処理と、

を前記コンピュータに実行させる請求項12記載のプログラム。

[20] 前記擬似乱数列の生成に用いる内部状態として、配列Sの要素の並び替えと算術加算を繰り返すことで配列Sの要素を攪拌し配列Sの初期状態を作成し、その際、前記一時変数をなす内部変数kの初期値を配列Sの要素から求める第1の処理と、

前記擬似乱数（以下、「鍵ストリーム」と称する）を生成する処理として、

第1のインデックス変数iの配列要素S[i]を第1のシフト数ローテイトシフトした値と、第2のインデックス変数jとを算術加算した結果に基づき、第2のインデックス変数jの値を更新し、

第2のインデックス変数jの配列要素S[j]を第2のシフト数ローテイトシフトした値と内部変数kとの算術加算結果に基づき内部変数kの値を更新し、

S[i]＋S[j]による配設要素S[(S[i]＋S[j])]を第3のシフト数ローテイトシフトした値と内部変数kとの算術加算結果に基づき、鍵ストリームを出力し、

前記鍵ストリームを生成するために参照した配列要素S[(S[i]＋S[j])]を、鍵ストリーム出力の直後に内部変数kと配列要素S[i]を用いて更新する第2の処理と、

を前記コンピュータに実行させる請求項12記載のプログラム。

[21] 初期設定配列aを用い、配列aの並べ替えを行って攪拌し、前記一時変数をなす内部変数kを、対応する配列要素aをローテイトシフトしたものと算術加算して求め、前記擬似乱数列の生成に用いる内部状態として配列Sを、配列aの要素をローテイトシフトしたものと配列Sの要素との所定の演算によって求める第1の処理と、

WAVELYNX EX. 1003, Pg. 980
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

前記擬似乱数（以下、「鍵ストリーム」と称する）を生成する処理として、

第1、第2のインデックス変数i、jに関して配列Sの参照結果S[j]と内部変数kとを算術加算し、

S[i]＋S[j]による配設Sの参照結果と内部変数kに基づき、鍵ストリームを出力し、

鍵ストリームを生成するために参照したSのエントリを、鍵ストリーム出力直後に内部変数kを用いて更新する第2の処理と、

を前記コンピュータに実行させる請求項12記載のプログラム。

[22] コンピュータを用いて擬似乱数列を生成する方法であって、

擬似乱数列の生成に用いる内部状態として、有限個の数値の列の並び替えを基礎とする状態に基づく内部状態を用い、

前記擬似乱数列の生成に用いる一時変数の少なくとも一つを、

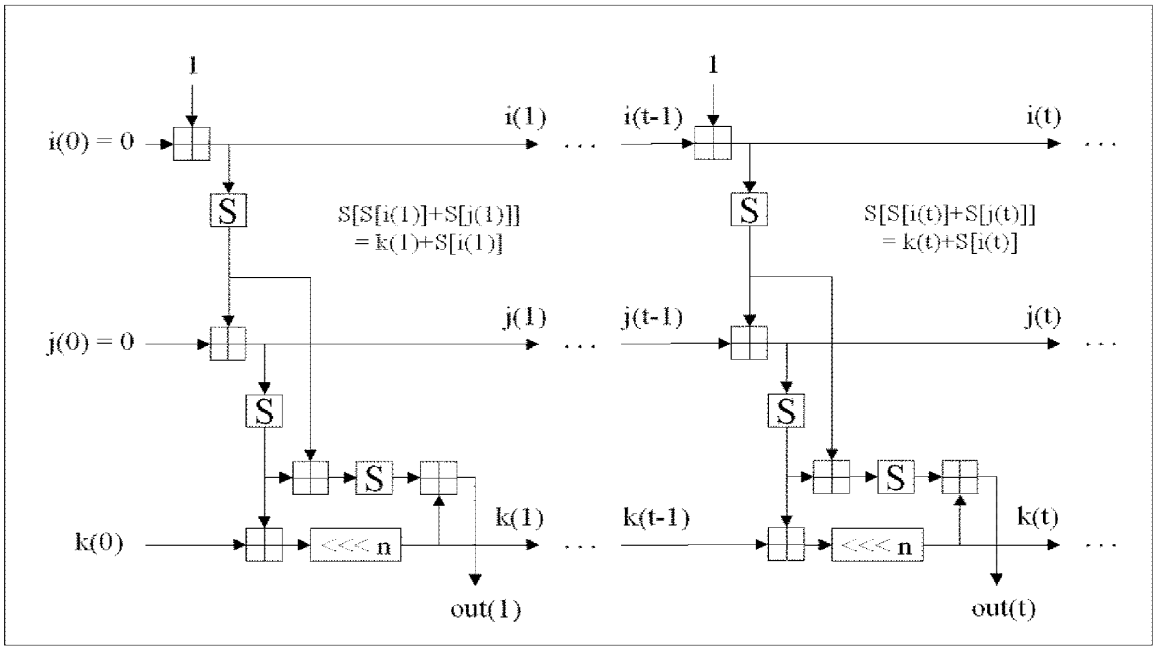
前記内部状態のうちの一つ、又は、複数個の数値を用いた、線形、又は、非線形、線形及び非線形の組み合わせの結果に基づき、内部状態の数より小さい数に依存し、あらかじめ定められた、左又は右ローテイトシフトを実行した結果を値とする一時変数とし、

前記擬似乱数を、前記内部状態のうちの1つ又は複数個の数値と、前記一時変数との予め定められた所定の演算によって生成する、

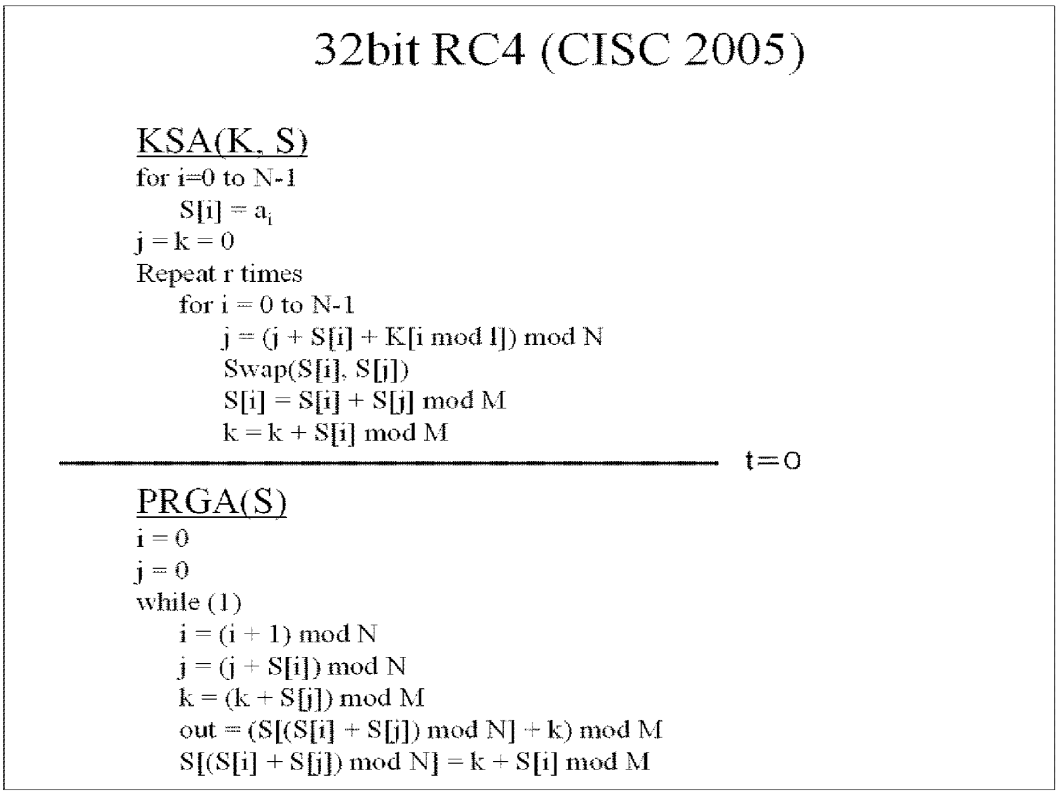
ことを特徴とする擬似乱数列の生成方法。

WAVELYNX EX. 1003, Pg. 981
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

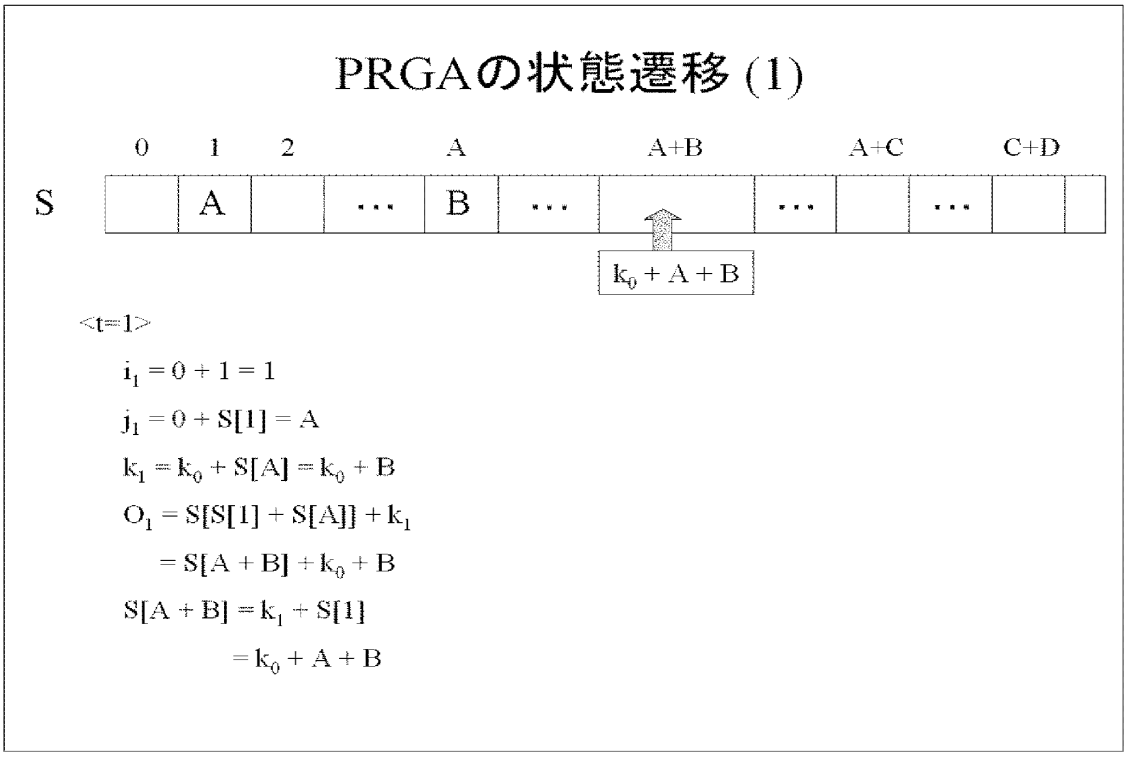
[図1]


1
i(0) = 0
i(1)
i(t-1)
i(t)
S
S[S[i(1)]+S[j(1)]]
= k(1)+S[i(1)]
S[S[i(t)]+S[j(t)]]
= k(t)+S[i(t)]
j(0) = 0
j(1)
j(t-1)
j(t)
k(0)
k(1)
k(t-1)
k(t)
<<< n
out(1)
out(t)

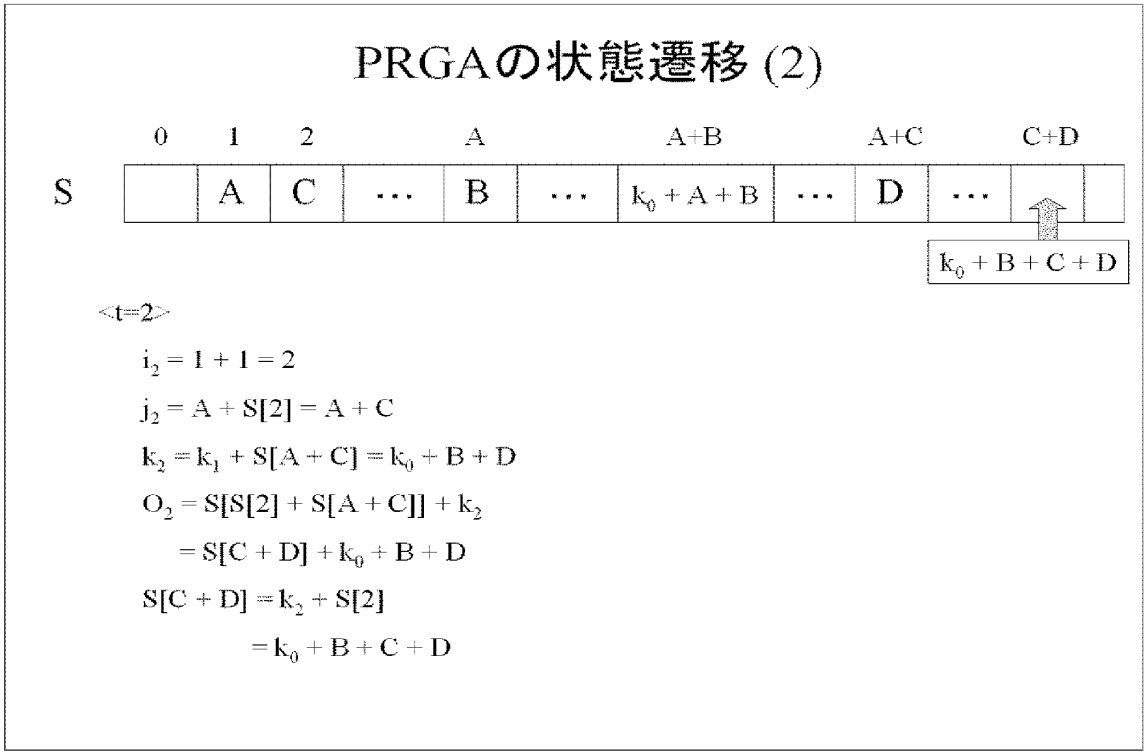
[図2]


32bit RC4 (CISC 2005)
KSA(K, S)
for i=0 to N-1
S[i] = a_i
j = k = 0
Repeat r times
for i = 0 to N-1
j = (j + S[i] + K[i mod l]) mod N
Swap(S[i], S[j])
S[i] = S[i] + S[j] mod M
k = k + S[i] mod M
t=0
PRGA(S)
i = 0
j = 0
while (1)
i = (i + 1) mod N
j = (j + S[i]) mod N
k = (k + S[j]) mod M
out = (S[(S[i] + S[j]) mod N] + k) mod M
S[(S[i] + S[j]) mod N] = k + S[i] mod M

[図3]

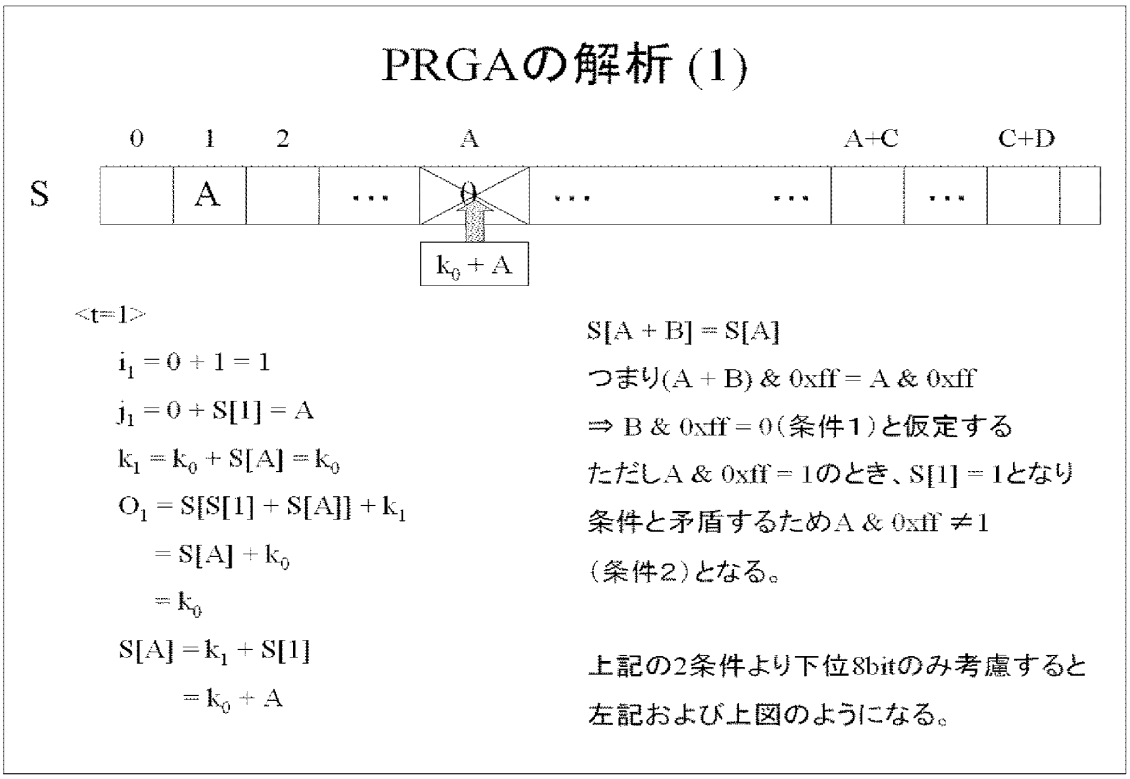


[図4]

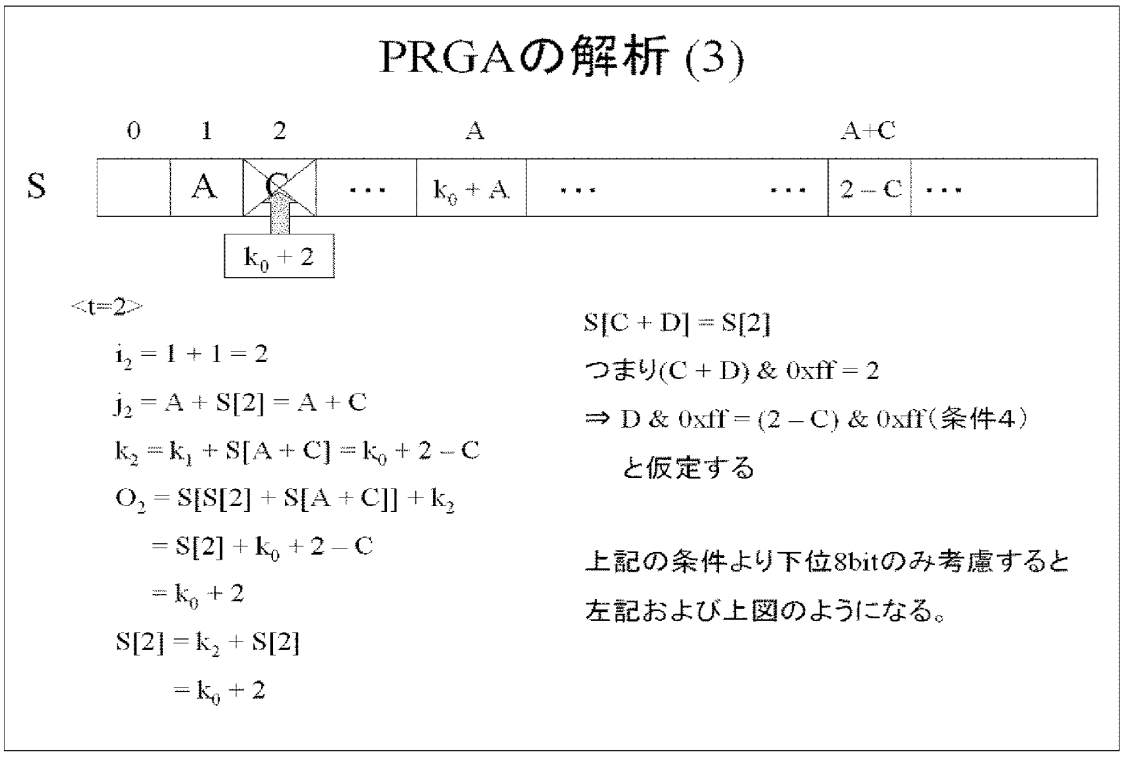


WAVELYNX EX. 1003, Pg. 983
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

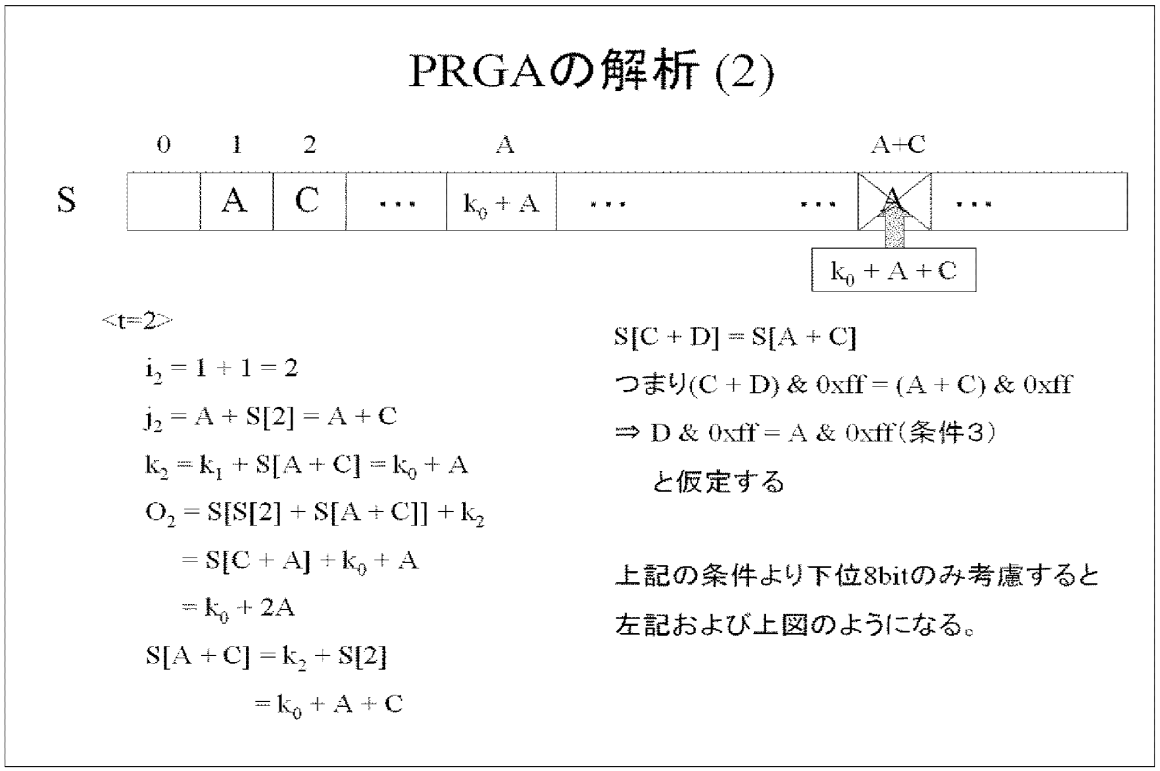
[図5]


PRGAの解析 (1)
0
1
2
A
A+C
C+D
S
A
0
$k_0 + A$
<t=1>
$i_1 = 0 + 1 = 1$
$j_1 = 0 + S[1] = A$
$k_1 = k_0 + S[A] = k_0$
$O_1 = S[S[1] + S[A]] + k_1$
$= S[A] + k_0$
$= k_0$
$S[A] = k_1 + S[1]$
$= k_0 + A$
S[A + B] = S[A]
つまり(A + B) & 0xff = A & 0xff
⇒ B & 0xff = 0（条件1）と仮定する
ただしA & 0xff = 1のとき、S[1] = 1となり
条件と矛盾するためA & 0xff ≠1
（条件2）となる。
上記の2条件より下位8bitのみ考慮すると
左記および上図のようになる。

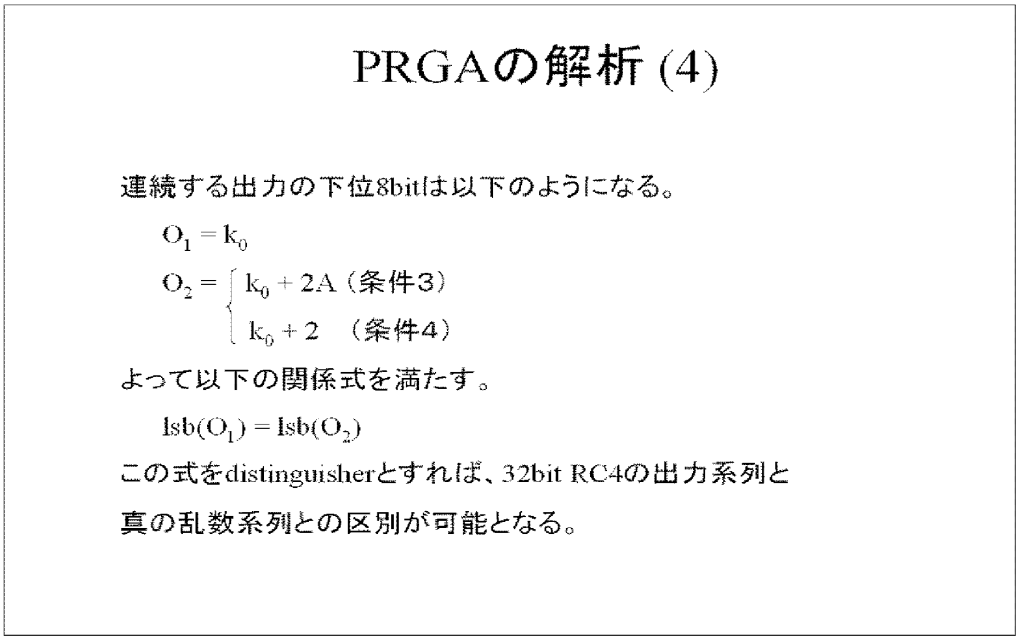
[図6]


PRGAの解析 (3)
0
1
2
A
A+C
S
A
C
$k_0 + A$
$2 - C$
$k_0 + 2$
<t=2>
$i_2 = 1 + 1 = 2$
$j_2 = A + S[2] = A + C$
$k_2 = k_1 + S[A + C] = k_0 + 2 - C$
$O_2 = S[S[2] + S[A + C]] + k_2$
$= S[2] + k_0 + 2 - C$
$= k_0 + 2$
$S[2] = k_2 + S[2]$
$= k_0 + 2$
S[C + D] = S[2]
つまり(C + D) & 0xff = 2
⇒ D & 0xff = (2 − C) & 0xff（条件4）
と仮定する
上記の条件より下位8bitのみ考慮すると
左記および上図のようになる。

[図7]



[図8]



WAVELYNX EX. 1003, Pg. 985
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[図9]

解読に必要なデータ量（理論値）

初期処理によってS-boxエントリが一様にランダムで出力均等と仮定すると、

$p1 = 1/256$

$p2 = 255/256$

$p3 = 1/256 \cdot 1/256 + 255/256 \cdot 2/256 = 511/256^2$

となる。条件を満たさない場合にdistinguisherが成り立つ確率は1/2とすると

任意にdistinguisherが成り立つ確率は、

$$\Pr\{lsb(O_1) = lsb(O_2)\}$$
$$= \Pr\{lsb(O_1) = lsb(O_2) \mid 条件OK\} + \Pr\{lsb(O_1) = lsb(O_2) \mid 条件NG\}$$
$$= p1 \cdot p2 \cdot p3 \cdot 1 + \{1 - p1 \cdot p2 \cdot p3\} \cdot 2^{-1}$$
$$= 2^{-1} \cdot (1 + 1/256 \times 255/256 \times 511/256^2)$$
$$\fallingdotseq 2^{-1} \cdot (1 + 2^{-15.008})$$

解読に必要なデータ量は理論的に以下のようになる。

$O(q^{-2}) = O(2^{30.02})$

[図10]

解読に必要なデータ量（実験値）

実験で得られた確率は以下のとおり。

$p1 \cdot p2 \cdot p3 = 2^{-14.404}$

となる。条件を満たさない場合にdistinguisherが成り立つ確率は1/2とすると

任意にdistinguisherが成り立つ確率は、

$$\Pr\{lsb(O_1) = lsb(O_2)\}$$
$$= \Pr\{lsb(O_1) = lsb(O_2) \mid 条件OK\} + \Pr\{lsb(O_1) = lsb(O_2) \mid 条件NG\}$$
$$= p1 \cdot p2 \cdot p3 \cdot 1 + \{1 - p1 \cdot p2 \cdot p3\} \cdot 2^{-1}$$
$$\fallingdotseq 2^{-1} \cdot (1 + 2^{-14.404})$$

解読に必要なデータ量は実験的に以下のようになる。

$O(q^{-2}) = O(2^{28.81})$

WAVELYNX EX. 1003, Pg. 986
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[図11]

実験結果 (distinguisher)

データ量N	棄却率
2^{24}	42 %
2^{25}	53 %
2^{26}	45 %
2^{27}	67 %
2^{28}	85 %
2^{29}	96 %

[図12]

元アルゴリズム

PRGA(S)
i = 0
j = 0
while (1)
    i = (i + 1) mod N
    j = (j + S[i]) mod N
    k = (k + S[j]) mod M
    out = (S[(S[i] + S[j]) mod N] + k) mod M
    S[(S[i] + S[j]) mod N] = k + S[i] mod M

($N = 2^n$, $M = 2^m$)

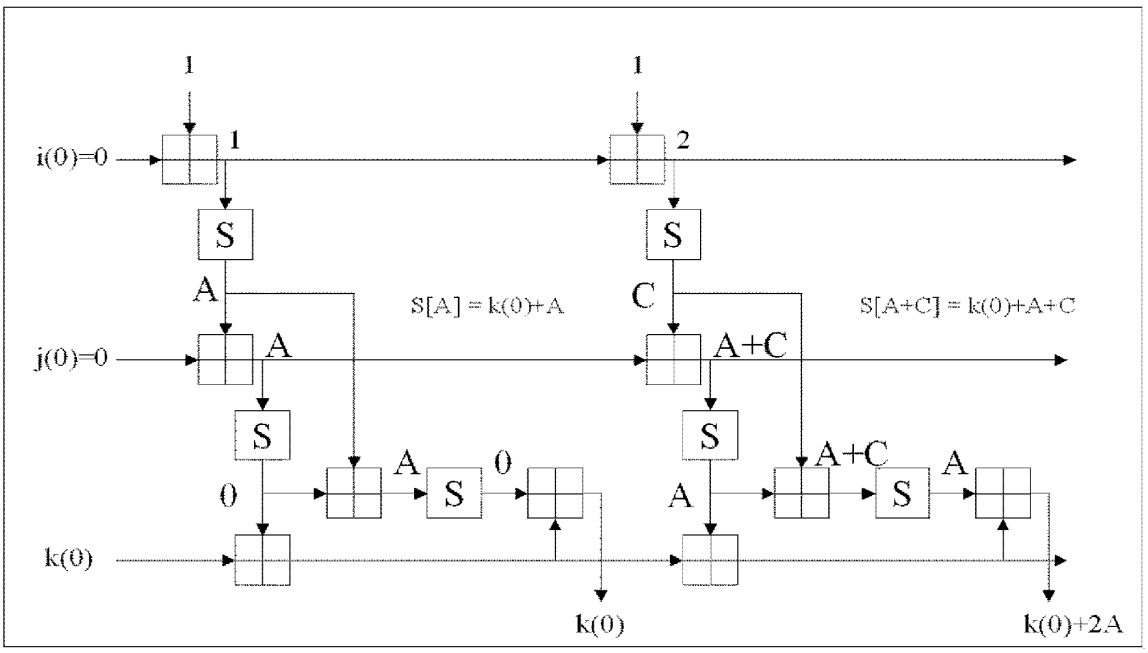
[図13]

変更アルゴリズム

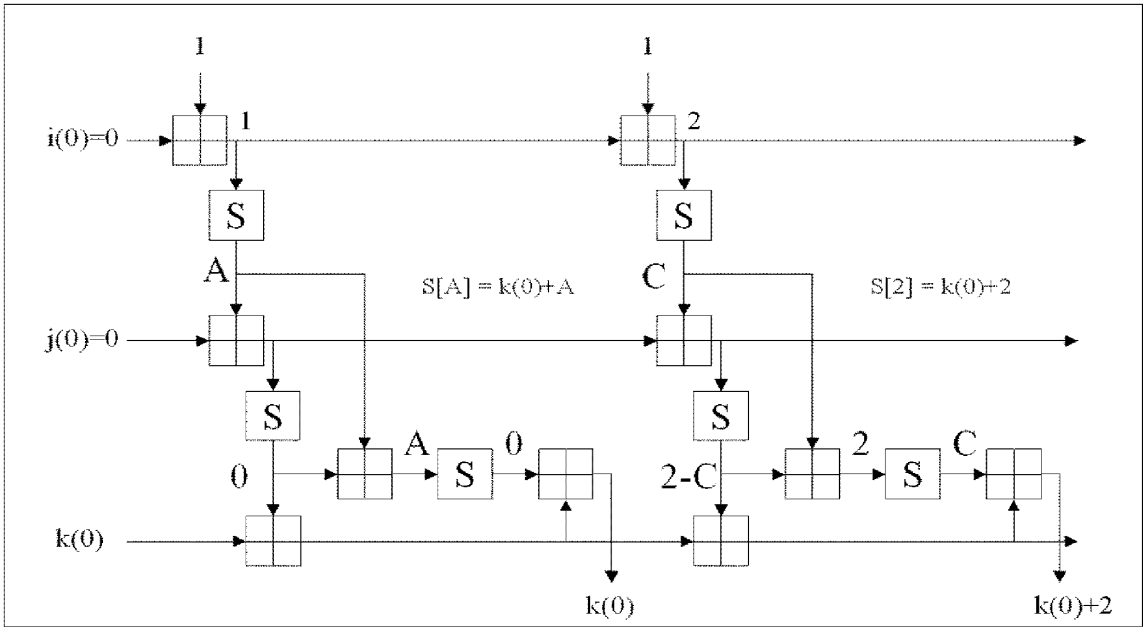
PRGA(S)
i = 0
j = 0
while (1)
    i = (i + 1) mod N
    j = (j + S[i]) mod N
    k = ((k + S[j]) <<< n) mod M
    out = (S[(S[i] + S[j]) mod N] + k) mod M
    S[(S[i] + S[j]) mod N] = k + S[i] mod M

(N = 2^n, M = 2^m)

[図14]



[図15]



[図16]

```
KSA(K, S)
for i=0 to N-1
    a[i] = i
j = k = 0
for r = 0 to 3
    for i = 0 to N-1
        j = (j + a[i] + K[i mod l]) mod N
        Swap(a[i], a[j])
        k = k + (a[i] <<< 8×r)
    for i = 0 to N-1
        S[i] = S[i] ⊕ (a[i] <<< 8×(3-r))
```

[図17]

```
PRGA(S)
i = 0
j = 0
while (1)
    i = (i + 1) mod N
    j = (j + (S[i] >>> 24)) mod N
    k = (k + (S[j] >>> 16)) mod M
    out = ((S[(S[i] + S[j]) mod N] >>> 8) + k) mod M
    S[(S[i] + S[j]) mod N] = k + S[i] mod M
```

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/063797

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/22(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Gong et al."Towards a General RC4-like Keystream Generator", [online], Guang Gong's Home Page, [retrieved on 2007-08-28], Retrieved from the Internet: <URL:http://calliope.uwaterloo.ca/~ggong/publication/CISC141.pdf>	1-22
A	Wu,"Cryptanalysis of a 32-bit RC4-like Stream Cipher", [online], Cryptology ePrint Archive, 2005/219, [retrieved on 2007-08-28], Retrieved from the Internet: <URL:http://eprint.iacr.org/2005/219.pdf >	1-22

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 August, 2007 (28.08.07)	04 September, 2007 (04.09.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/063797

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Tsunoo et al."The Most Efficient Distinguishing Attack on VMPC and RC4", [online], eSTREAM, the ECRYPT Stream Cipher Project, [retrieved on 2007-08-28], Retrieved from the Internet: <URL: http://www.ecrypt.eu.org/stream/papersdir/037.pdf >	1-22

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０６３７９７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/22(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/22

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	Gong et al.” Towards a General RC4-like Keystream Generator”, [online], Guang Gong's Home Page, [retrieved on 2007-08-28], Retrieved from the Internet : <URL:http://calliope.uwaterloo.ca/~ggong/publication/CISC141.pdf>	１－２２

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２８．０８．２００７	国際調査報告の発送日 ０４．０９．２００７
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３８５７ 石田　信行 電話番号　０３－３５８１－１１０１　内線　３５４６

WAVELYNX EX. 1003, Pg. 993
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	Wu,” Cryptanalysis of a 32-bit RC4-like Stream Cipher”, [online],Cryptology ePrint Archive, 2005/219, [retrieved on 2007-08-28], Retrieved from the Internet : <URL : http://eprint.iacr.org/2005/219.pdf >	１－２２
A	Tsunoo et al.” The Most Efficient Distinguishing Attack on VMPC and RC4”, [online], eSTREAM, the ECRYPT Stream Cipher Project, [retrieved on 2007-08-28], Retrieved from the Internet : <URL: http://www.ecrypt.eu.org/stream/papersdir/037.pdf >	１－２２

WAVELYNX EX. 1003, Pg. 994
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 043 687 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
22.11.2006 Bulletin 2006/47

(51) Int Cl.:
G06T 1/00 *(2006.01)*

(21) Application number: **00400949.4**

(22) Date of filing: **06.04.2000**

(54) **Method for inserting a watermark and associated decoding method**

Verfahren zum Einfügen eines Wasserzeichens und dazugehöriges Dekodierverfahren

Méthode pour insérer un filigranne et méthode associée de décodage

(84) Designated Contracting States:
DE FR GB

(30) Priority: **09.04.1999 FR 9904461**
09.04.1999 FR 9904462
25.06.1999 FR 9908187

(43) Date of publication of application:
11.10.2000 Bulletin 2000/41

(73) Proprietor: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

(72) Inventors:
- **Donescu, Ioana**
  35000 Rennes (FR)
- **Nguyen, Eric**
  35000 Rennes (FR)
- **Onno, Patrice**
  35000 Rennes (FR)

(74) Representative: **Santarelli**
14, avenue de la Grande Armée,
B.P. 237
75822 Paris Cedex 17 (FR)

(56) References cited:
- **MENG AND CHANG: "EMBEDDING VISIBLE VIDEO WATERMARKS IN THE COMPRESSED DOMAIN" INTERNATIONAL CONFERENCE ON IMAGE PROCESSING ICIP98, vol. 1, 4 - 7 October 1998, pages 474-477, XP002124674 NEW-YORK NY US**
- **SWANSON E.A.: "OBJECT-BASED TRANSPARENT VIDEO WATERMARKING" IEEE FIRST WORKSHOP ON MULTIMEDIA SIGNAL PROCESSING, 23 - 25 June 1997, pages 369-374, XP002124675 NEW-YORK NY US**
- **PODILCHUK C I ET AL: "IMAGE-ADAPTIVE WATERMARKING USING VISUAL MODELS" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,US,IEEE INC. NEW YORK, vol. 16, no. 4, 1 May 1998 (1998-05-01), pages 525-539, XP000765113 ISSN: 0733-8716**
- **TAO B ET AL: "ADAPTIVE WATERMARKING IN THE DCT DOMAIN" IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING (ICASSP),US,LOS ALAMITOS,CA: IEEE COMP. SOC. PRESS, 1997, pages 2985-2988, XP000788033 ISBN: 0-8186-7920-4**
- **RUANAIDH J J K O ET AL: "WATERMARKING DIGITAL IMAGES FOR COPYRIGHT PROTECTION" IEE PROCEEDINGS: VISION, IMAGE AND SIGNAL PROCESSING,GB, INSTITUTION OF ELECTRICAL ENGINEERS, vol. 143, no. 4, 1 August 1996 (1996-08-01), pages 250-256, XP000613938 ISSN: 1350-245X**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 1 043 687 B1

Description

[0001] The present invention concerns a method of inserting a watermark and an associated method of decoding a watermarking signal.

[0002] Correlatively, it concerns a device for inserting a watermarking signal and a device for decoding a watermarking signal.

[0003] The present invention lies in general terms in the technical field of watermarking of digital images, and more particularly still images.

[0004] Watermarking digital data makes it possible to protect these data, for example by associating copyright information with them.

[0005] In its general principe, watermarking consists of inserting an indelible watermark in digital data, which can be likened to encoding additional information in the data.

[0006] Decoding this additional information makes it possible to check the additional information which has been inserted.

[0007] This inserted watermark must consequently be both imperceptible, robust to certain distortions applied to the digital image and reliable to detect.

[0008] Conventionally, a usual technique of inserting a watermarking signal in a digital image consists of using a linear modulation model in which at least one subset of coefficients representing the digital image is modulated according to this linear model using a weighting coefficient.

[0009] By denoting as $X = \{X_i, 1 \leq i \leq N\}$ a set of the coefficients representative at least of part of a digital image, and as $w = \{w_j, 1 \leq j \leq P\}$ a watermark of size $P \leq N$, a pseudo-random signal with known distribution and average of zero, the linear insertion formula is :

$$X'_j = X_j + b\,\alpha_j\,w_j, \text{ with } 1 \leq j \leq P,$$

in which $\{X_j, 1 \leq j \leq P\}$ i s a subset of the set of coefficients X, b is an information bit, and α_j is a weighting coefficient, also called modulation amplitude.

[0010] The detection of the watermark then consists in detecting whether or not the pseudo-random sequence w has been inserted into a set of coefficients. This detection is carried out without using the original image and can be based on a standardised statistical test which makes it possible to calculate a probability of correct detection.

[0011] Such an insertion technique makes it possible, by insertion of a watermark, to insert a single information bit since the response from the detector is binary (yes/no).

[0012] In order to insert a larger number of information bits into the digital image, in particular when a code of Q bits is wanted, indicating, for example, the name or the address of the owner or of the author of the image, it is necessary to reiterate the previously described insertion method as many times as there are information bits to be inserted. Typically, in order to insert a binary signal, either b = 1, or b = -1 is used.

[0013] Put another way, Q subsets of coefficients have to be chosen and the modulation of these subsets has to be carried out by choosing Q watermarks.

[0014] Separate subsets of coefficients are preferably chosen such that the modulation operations are not superimposed on one another, which could disturb the detection or cause troublesome visual effects.

[0015] It is a matter, consequently, of choosing a partition of the coefficients representative of the digital image into Q separate subsets, each carrying one information bit.

[0016] Numerous known methods use a technique of inserting a watermarking signal of given size by spectrum spreading. The disadvantage of these methods, describe for example in the article entitled "Secure spread spectrum watermarking for multimedia" by I.J. COX et al, in Proc. ICIP, pages 243-246, Sept. 1996 and in the article entitled "Digital watermarking of raw and compressed video" by F. HARTUNG et al, in Proc. SPIE 2952 : Digital Compression Technologies and Systems for Video Communication, pages 205-213, October 1996, is that they use an arbitrary partitioning of the image into blocks of fixed size without any guarantee of detectability of the modulations effected on each of the blocks.

[0017] The aim of the present invention is to propose a method of inserting a watermark wherein a partitioning of a digital image is adapted to the image, ensuring detectability of the bits inserted for a technique of insertion by modulation.

[0018] ' The present invention thus relates to a method of inserting a watermarking signal in a digital image by modulation of coefficients of distinct regions representing said digital image, comprising a step of determining a partitioning into distinct regions of the digital image.

[0019] In accordance with the invention, this partitioning into regions is effected by an adaptive partitioning as a function of a criterion of statistical detectability of an information bit inserted in each region.

WAVELYNX EX. 1003, Pg. 996
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0020] In this way an adaptive partitioning is performed which has the advantage of adapting to the content of the image signal and guaranteeing detectability of the inserted watermarking signal, unlike the choice of an arbitrary partitioning into fixed blocks.

[0021] This spatial adaptivity is necessary so as the content of the image is not spatially homogenous.

[0022] This is because, for a given modulation amplitude, the greater the length of the sequence of the watermarking signal inserted, and consequently the greater the size of the region and therefore the number of modulatable coefficients, the more reliable is the detection.

[0023] It can in fact be shown that, when a correlation calculation is used for effecting the detection, the response of the detector is proportional to $P^{1/2}$ where P is the length of the sequence of the watermarking signal.

[0024] Moreover, the response of the detector is also dependent on the image signal itself. The greater the variance in the coefficients representing the image, the weaker the response of the detector.

[0025] In conclusion, for a given modulation amplitude and image, there exists a minimum length of the watermarking signal necessary for ensuring a given detection probability, this minimum length also depending on the local content of the image signal in the region in which the watermarking signal is inserted.

[0026] The adaptive partitioning effected by the method according to the invention guarantees the detectability of the watermarking signal inserted in the different regions determined by this partitioning.

[0027] Preferably, the detectability criterion is calculated using a maximum value of the weighting coefficient ensuring imperceptibility of the watermarking signal for the modulation of the set of coefficients representing said digital image.

[0028] This is because, the greater the modulation amplitude, that is to say the value of the weighting coefficient, the more reliable is the detection in that a better probability of detection can be obtained. Nevertheless, the greater this modulation amplitude, the more this modulation may be visible in the watermarked image.

[0029] It is therefore judicious to choose a modulation amplitude equal to a maximum amplitude, generally denoted JND (Just Noticeable Difference), beyond which the modulation becomes visibly perceptible in the image.

[0030] It can be shown that this maximum amplitude also depends on the length of the sequence of the watermarking signal and that it decreases with this length.

[0031] By choosing a maximum value of the weighting coefficient ensuring imperceptibility of the watermarking signal for the modulation of the set of coefficients representing said digital image, the value of the weighting coefficient on each region of the partitioning, and with a size less than the cardinal number of all the coefficients representing the image, will be much less than the maximum modulation amplitude which guarantees imperceptibility of the modulation on this region.

[0032] The partitioning thus performed also ensures invisibility of the modulation effected on each of the regions obtained by the partitioning.

[0033] According to an advantageous characteristic of the invention, the detectability criterion is calculated using, for each coefficient to be modulated, a weighting coefficient according to a law of the form $\alpha_i = k_i.\alpha_v$, where k_i is a modulation factor dependent on the coefficients situated in a vicinity of the coefficient considered on said region and α_v is equal to said maximum value of the weighting coefficient.

[0034] It is thus possible to exploit the possibilities of visual "masking" of the modulation by the image signal itself. Typically, use is made of the fact that, the greater the activity of the image signal, in the sense for example of a significant local variance in the coefficients, the less visible will be the modulation.

[0035] It is thus possible to locally increase the weighting coefficient and therefore the modulation amplitude, to the benefit of detectability, without impairing the imperceptibility of the inserted modulation.

[0036] According to another preferred characteristic of the invention, the method of inserting a watermark includes a step of applying a distortion before calculating the detectability criterion.

[0037] According to another preferred characteristic of the invention, the method of inserting a watermark includes a prior step of comparing the size of each region of the partitioning with a minimum size corresponding to the minimum size of a statistically significant sample for detecting a watermarking signal inserted in said region.

[0038] Indeed, because of the calculations of a statistical nature performed when the watermarking signal is detected, notably when standardised hypothesis tests are used, it is necessary to consider a minimum boundary for the size of each region of the partitioning guaranteeing the validity of the detection tests.

[0039] According to one particularly practical embodiment of the invention, for each region of the partitioning, all the coefficients of said region are modulated by inserting the watermarking signal, a detectability amplitude is calculated from said detectability criterion and said detectability criterion is validated by comparing said detectability amplitude with a predetermined threshold value.

[0040] The detectability amplitude can be the result of a calculation of correlation between the set of modulated coefficients and the watermarking signal or the result of a standardised statistical test such as the one described in the article entitled "A method for signature casting on digital images" by I. PITAS, in Proc. ICIP, pages 215-218, September 1996.

[0041] Practically, the detectability criterion can be validated if a minimum modulation length calculated for ensuring

WAVELYNX EX. 1003, Pg. 997
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

detectability of the inserted watermarking signal in less than or equal to the cardinal number of said region.

[0042] According to a preferred embodiment of the invention, the method comprises the following steps:

- generation of a centred pseudo-random sequence equal in size to the cardinal number of a set of coefficients representative of at least a part of the image, formed from centred pseudo-random sub-sequences;
- modulation of the said set of coefficients by the said centred pseudo-random sequence in order to insert the same information bit on the said set of coefficients; and
- checking, over each region, of a criterion of detectability of the information bit inserted by modulation.

[0043] It is thus possible to achieve a partition of a set of coefficients into distinct regions, by carrying out an adaptive partitioning on the basis of a criterion of detectability of an information bit inserted on each region.

[0044] Such an adaptive partitioning exhibits the advantage of adapting to the content of the image signal and of guaranteeing the detectability of the watermark inserted on the different regions determined by this partition, in contrast to the choice of a random partitioning.

[0045] In practice, for each region of the partition, a criterion of detectability of an information bit inserted by modulation of the coefficients of the said region is checked. This criterion may consist in the comparison of a result of a standardised statistical test with a threshold value corresponding to a probability of detection fixed in advance.

[0046] By virtue of the method in accordance with the invention, it is possible to generate a centred pseudo-random sequence on the basis of the merging of centred pseudo-random sequences of smaller sizes, and to modulate all the available coefficients in order to achieve the insertion of a watermark.

[0047] By modulating all the coefficients with the same information bit and a centred pseudo-random sequence which is broken down into pseudo-random sub-sequences which are also centred on each region of the partition produced over the set of coefficients, the steps of generating a pseudo-random sequence and of modulation do not have to be reiterated at each new region tested.

[0048] According to one preferred characteristic of the invention, the method of inserting a watermark comprises a single step of applying a distortion to the said set of modulated coefficients, before the step of checking of a detectability criterion.

[0049] It is known to apply a predetermined distortion to a set of modulated coefficients and to carry out the check on the detectability criterion after this pre-distortion, in such a way that it is possible to guarantee the detection of the watermark inserted on a partition of the coefficients for a predetermined distortion.

[0050] By virtue of the invention, a pre-distortion can be applied to the set of modulated coefficients, in a unique way, and does not need to be reiterated at each new region tested in the partition.

[0051] In one particularly practical embodiment of the invention, the set of coefficients is a set of spectral coefficients originating from a spectral transformation of a digital image, and the step of applying a distortion includes the following sub-steps:

- inverse spectral transformation of the said set of modulated coefficients in order to obtain a watermarked image;
- application of a distortion to the said watermarked image; and
- spectral transformation of the watermarked image in order to obtain a set of modulated coefficients after distortion.

[0052] The saving obtained in terms of complexity of calculation is all greater in this case whenever the application of a distortion requires several steps of processing of the set of coefficients, and particularly the application of an inverse spectral transformation in order to obtain the watermarked image and to apply a distortion, such as compression/de-compression to it, and then the application of a forward spectral transformation of the image again so as to check the criterion of detectability in the spectral domain.

[0053] According to another particularly practical characteristic of the invention, the centred pseudo-random sequence is formed from pseudo-random sub-sequences of identical size.

[0054] Such a pseudo-random sequence is particularly well adapted to the application of a bottom-up or top-down iterative partitioning of the quadtree type which makes it possible iteratively to combine regions of identical sizes or iteratively to divide regions into sub-regions of identical sizes.

[0055] For preference, the pseudo-random sub-sequences have a size greater than or equal to a minimum number of coefficients forming a region of the said partition of a size which is statistically significant for validating the said criterion of detectability over the said region.

[0056] It is thus possible theoretically to form a maximum partition of the set of coefficients with the same unique centred pseudo-random sequence, each pseudo-random sub-sequence being centred on the regions with the smallest size which is statistically admissible for inserting a watermark by modulation into the set of coefficients.

[0057] According to one practical embodiment, which is inexpensive in terms of calculations, at the generation step, each centred pseudo-random sub-sequence is created by generating half of the pseudo-random samples of the said

WAVELYNX EX. 1003, Pg. 998
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

sub-sequence via a pseudo-random number generator and by symmetrising the said pseudo-random samples generated.

[0058] For preference, in this embodiment, at the generation step, each centred pseudo-random sub-sequence is created by moreover permutating the said pseudo-random samples using a secret key.

[0059] This permutation operation makes it possible better to preserve the intrinsic random-sequence nature of a sub-sequence created by symmetrising pseudo-random samples, and not to diminish the imperceptibility of the inserted watermark.

[0060] According to another practical embodiment of the invention, at the generation step, each centred pseudo-random sub-sequence is created by generating pseudo-random random samples via a pseudo-random number generator and by redistributing over each sample the sum of the said pseudo-random samples generated.

[0061] According to a preferred characteristic of the invention, a partitioning by iterative division of the digital image is performed and, for each region at a rank of said partitioning, a partitioning of a directly higher rank of said region is validated if and only if there exist at least two subregions of said region for which said detectability criterion is validated.

[0062] Thus, when it is attempted to divide a region into subregions, this partitioning of a higher rank is validated only if the number of regions in which a watermarking signal can actually be inserted whilst complying with the detectability criterion is actually increased.

[0063] Otherwise, it is preferable to keep the region before division, of greater size, in order to increase the detectability of the watermarking signal.

[0064] According to a preferred embodiment of the invention, for each region at a rank of said partitioning, the value of a capacity of the digital image is incremented when the partitioning of directly higher rank is not validated, the said capacity being equal to the cardinal number of the distinct regions obtained by the said partitioning on which the detectability criterion is validated.

[0065] It is thus possible to calculate the capacity of the digital image which thus corresponds to the number of information bits which can be inserted in the digital image.

[0066] By virtue of the adaptive partitioning performed by the invention, by reiterating the partitioning of each region as long as the detectability criterion is complied with, there is obtained the maximum capacity of the digital image which corresponds to the watermarking capacity of this image by the technique of insertion by modulation. This watermarking capacity can be defined as the maximum number of information bits which can be inserted imperceptibly in the image with a guarantee of detectability on decoding.

[0067] According to another embodiment of the invention, for each region at a rank of said partitioning, the value of a capacity is incremented when the partitioning of directly higher rank is not validated, said value of the capacity is compared with a fixed capacity value and the partitioning is reiterated for a region having a detectability amplitude which is the highest amongst all the other regions to be processed when said capacity value is less than said fixed capacity value.

[0068] This partitioning method makes it possible, in this embodiment, to find the best possible partitioning in terms of detectability when a predetermined number of information bits have to be inserted, equal to said fixed capacity value.

[0069] By selecting, during the partitioning, the regions for which the detection amplitude is the highest, the present invention makes it possible to determine the partitioning which, a priori, guarantees the best detectability on decoding of the watermarking signals making it possible to insert a predetermined number of information bits.

[0070] According to another embodiment of the invention, a partitioning is effected by iterative merging of the digital image and, for each region of said partitioning for which said detectability criterion is not validated, said region is merged with another region of said partitioning.

[0071] Preferably, in this embodiment, said other region of the partitioning is if possible a region for which said detectability criterion is not validated.

[0072] It is thus possible to increase the capacity of the digital image by joining the regions in which the detectability criterion is not satisfied.

[0073] The present invention also concerns a method of decoding a watermarking signal in a digital image, inserted by modulation of coefficients representing said image in distinct regions forming a partitioning of said digital image.

[0074] In accordance with the invention, this decoding method includes a step of determining a partitioning into distinct regions of the digital image to be decoded by effecting an adaptive partitioning as a function of a criterion of statistical detectability of an information bit obtained by demodulation of the coefficients on each region.

[0075] Thus this decoding method makes it possible to find, at the decoder, the adaptive partitioning performed for inserting a watermarking signal.

[0076] This is because, when the partitioning has been performed in an adaptive fashion as described above by a method of determining a partitioning in accordance with the first aspect of the invention, this partitioning, which depends on the content of the image, is not known to the decoder.

[0077] The decoding method according to the invention then consists of testing all the acceptable partitionings and verifying the detection of a watermarking signal on each of the regions associated with this partitioning.

[0078] According to a preferred characteristic of the invention, the decoding method includes a prior step of comparing the size of each region of the partitioning with a minimum size corresponding to the minimum size of a statistically

WAVELYNX EX. 1003, Pg. 999
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

significant sample for the detection of a watermarking signal inserted in said region.

[0079] According to a practical embodiment of the decoding method according to the invention, for each region of the partitioning, a detection amplitude is calculated from said detectability criterion and said detectability criterion is validated by comparing said detection amplitude with a threshold value predetermined for decoding.

[0080] The decoding method thus makes it possible to find the adaptive partitioning effected when the watermarking signal is inserted.

[0081] According to advantageous characteristic of this embodiment in the invention, the threshold value predetermined for decoding is less than said predetermined threshold value used during the method of determining a partitioning.

[0082] This is because, at decoding, the detection test is performed on coefficients which have a priori been modulated and possibly made noisy. These coefficients are different from the original coefficients, and the result of the detectability test at decoding will be different from that performed in order to determine the partitioning. By choosing different thresholds on decoding and coding, it is possible to take into account the tendency for variation in detection amplitude due to an increased variance in the coefficients which have been modulated and possibly made noisy.

[0083] Correlatively, the present invention also concerns a device for inserting a watermarking signal in a digital image by modulating coefficients of distinct regions, comprising means for partitioning into distinct regions the digital image wherein partitioning means are adapted to effect an adaptative partitioning as a function of a criterion of statistical detectability of an information bit inserted on each region.

[0084] According to a preferred embodiment, this device includes:

- means for generating a centred pseudo-random sequence equal in size to the cardinal number of the said set of coefficients, formed by centred pseudo-random sub-sequences;
- means for modulation of a set of coefficients by the said centred pseudo-random sequence in order to insert the same information bit on the said set of coefficients; and
- means for checking, over each region, a criterion of detectability of the information bit inserted by modulation.

[0085] Correlatively, the present invention also concerns a decoding device adapted to implement the decoding method according to the invention.

[0086] The present invention also concerns a computer adapted to implement the method of inserting a watermark and the decoding method in accordance with the invention.

[0087] This computer has characteristics and advantages similar to those described with reference to the methods which it implements.

[0088] The present invention also relates to an information storage means which can be read by a microprocessor, possibly removable, which stores a program implementing the method of inserting a watermark and/or decoding in accordance with the invention.

[0089] Other particularities and advantages of the invention will also emerge from the following description of the invention.

[0090] In the accompanying drawings, given by way of non-limitative examples:

- Figure 1 is an overall diagram illustrating a device for inserting a watermark into a digital image;
- Figure 2 schematically illustrates a step of spectral decomposition employed when inserting a watermark;
- Figure 3 is an algorithm of the step of determining a partitioning in accordance with a first embodiment of the invention;
- Figure 4 is an example of partitioning of a region by division;
- Figure 5 is an algorithm of the step of determining a partitioning in accordance with a second embodiment of the invention;
- Figure 6 is an algorithm of the decoding method according to a first embodiment of the invention;
- Figure 7 is an algorithm illustrating the application of the method of inserting a watermark of Figure 1 to a digital image;
- Figure 8 is an algorithm illustrating the application of the decoding method of Figure 4 to a digital image;
- Figure 9 is a block diagram illustrating a variant embodiment of the step of determining a partitioning in accordance with a third embodiment of the invention;
- Figure 10 illustrates the application of the step of determining a partition to a digital image according to a preferred embodiment of the invention;
- Figure 11 is an algorithm of the step of determining a partition in accordance with a first way of the preferred embodiment of the invention;
- Figure 12 is an algorithm of the step of determining a partition in accordance with a second way of the preferred embodiment of the invention ;
- Figure 13 is an algorithm of the insertion method according to one embodiment of the invention;
- Figure 14 illustrates, by means of a graph, the insertion method of the figure 13; and
- Figure 15 is a block diagram illustrating a device adapted to implement the methods in accordance with the invention.

WAVELYNX EX. 1003, Pg. 1000
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0091] A description will first of all be given, by reference to Figure 1, of the insertion of a watermark into a set of coefficients representative of a digital image I.

[0092] This digital image I can be represented by a set of coefficients, either in the spatial domain or in a transformed domain, the coefficients in this latter case being hybrid coefficients, that is to say coefficients located both in the spatial domain and in the frequency domain. Such a representation of the image is obtained, for example, by using a sub-band originating from a space-frequency decomposition of the image, for example a discrete wavelet decomposition.

[0093] Here, the insertion of the watermark is achieved via a spread-spectrum insertion technique, by modulation of coefficients of a space-frequency representation of the image, obtained by the space-frequency transformation of the digital image I.

[0094] By way of example, a discrete wavelet decomposition S can be used, represented diagrammatically in Figure 2. This space-frequency decomposition is well known in the image-processing field, and only the principle thereof is reiterated below. It makes it possible to segment the image into sub-bands of frequencies and to obtain hybrid coefficients, that is to say spectral coefficients which are also located in space, here in the plane of the image.

[0095] The image I consists of a series of digital samples. The image I is represented, for example, by a series of bytes, each byte value representing one pixel of the image I, which may be a black-and-white image with 256 grey levels.

[0096] The multi-resolution spectral decomposition means consist of a sub-band decomposition circuit, or analysis circuit, formed by a set of analysis filters, associated respectively with dividers-by-two. This decomposition circuit filters the image signal I in two directions, into sub bands of high spatial frequencies and of low frequencies. The circuit includes several successive analysis blocks for breaking down the image I into sub-bands according to several levels of resolution.

[0097] By way of example, the image I is broken down here into sub-bands with a level of decomposition d equal to 3.

[0098] A first analysis block receives the image signal I and filters it through two respectively low-pass and high-pass digital filters, in a first direction, for example horizontal. After passing through dividers-by-two, the resultant filtered signals are in their turn filtered by two respectively low-pass and high-pass filters, in a second direction, for example vertical. Each signal is again passed through a divider-by-two. Hence four sub-bands LL_1, LH_1, HL_1 and HH_1 are obtained at the output of this first analysis block, with the highest resolution in the decomposition.

[0099] The sub-band LL_1 includes the low-frequency components in the two directions of the image signal I. The sub-band LH_1 includes the low-frequency components along a first direction and high-frequency components along a second direction of the image signal I. The sub-band HL_1 includes the high-frequency components along the first direction and the low-frequency components along the second direction. Finally, the sub-band HH_1 includes the high-frequency components along the two directions.

[0100] A second analysis block in its turn filters the sub-band of low frequencies LL_1 so as, in the same way, to supply four sub-bands LL_2, LH_2, HL_2 and HH_2 with intermediate level of resolution in the decomposition. A third analysis block then filters the sub-band of low frequencies LL_2 so as to supply four sub-bands LL_3, LH_3, HL_3 and HH_3. Finally in this example, the sub-band LL_3 is in its turn analysed by a fourth analysis unit in order to supply four sub-bands LL_4, LH_4, HL_4 and HH_4 with the lowest resolution in this decomposition.

[0101] Hence thirteen sub-bands and four levels of resolution are obtained. Obviously, the number of levels of resolution, and consequently of sub-bands, may be chosen differently.

[0102] Obviously, other types of spectral transformation could be used, such as the discrete Fourier transform, the discrete cosine transform or the Fourier-Mellin transform.

[0103] In a general way, frequency sub-bands are obtained forming a set of spectral coefficients into which a watermark can be inserted.

[0104] The high-frequency sub-band of highest resolution HH_1 can be considered here in order to insert a watermark. This sub-band HH_1 thus supplies a set of coefficients X, equal to N in size, for example.

[0105] Let $X = \{X_i, 1 \leq i \leq N\}$ be the set of coefficients representative of the digital image I.

[0106] Obviously, it would be possible to consider a subset of coefficients of this set X, representative only of a part of the digital image I.

[0107] In order to insert a watermark into this set of coefficients X, one technique consists in inserting a pseudo-random signal, by spreading its spectrum, so as to render this signal undetectable by spectral or statistical analysis.

[0108] Let $w = \{w_j, 1 \leq j \leq P\}$ be a watermark of size $P \leq N$, a pseudo-random signal with known distribution and average of zero. The most widespread distributions are the binary distribution {-1, 1}, the uniform distribution over [-1, 1] and a centred normalised Gaussian distribution N (0, 1).

[0109] The linear insertion formula is :

$$X'_j = X_j + b\,\alpha_j\,w_j, \text{ with } 1 \leq j \leq P,$$

in which $\{X_j, 1 \leq j \leq P\}$ is a subset of the set of coefficients X, b is an information bit, and α_j is a weighting coefficient,

WAVELYNX EX. 1003, Pg. 1001
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

also called modulation amplitude.

[0110] The set {j, $1 \leq j \leq P$} is also called information-bit insertion carrier.

[0111] In order to insert a signal which may be formed from several information bits, it is worth partitioning the set of coefficients so as to determine the number of regions or the number of insertion carriers available in this set.

[0112] To do that, the insertion device 10 in accordance with the invention comprises a device for determining a partition 11 and insertion means 12.

[0113] The device for determining a partition 11 is suitable for carrying out adaptive partitioning of the set of coefficients as a function of the detectability of an inserted watermark.

[0114] This method of adaptive partitioning consists in varying the number of coefficients modulated in order to insert an information bit of the watermark, so as simultaneously to satisfy the criteria which are set of invisibility and of correct detection probability.

[0115] A description will first of all be given, with reference to Figure 3, of a method of determining a partitioning into distinct regions of a digital image which makes it possible to maximise the number of regions obtained in order to maximise the number of information bits inserted in the image.

[0116] Consideration is given to a representation of the digital image by a set of coefficients, either in the spatial domain, or in a transformed domain, the coefficients being in the latter case hybrid, that is to say located both in the spatial domain and in the frequency domain. Such a representation of the image is for example obtained by using a sub-band issuing from a spatio-frequency decomposition of the image, as a discrete wavelet decomposition previously described.

[0117] The partitioning of the image is effected in order to insert a watermarking signal by modulation of the coefficients of each region.

[0118] According to the invention, this partitioning into regions is performed by an adaptive partitioning as a function of a criterion of detectability of an information bit inserted on this region.

[0119] The number of regions obtained under constraint of the detectability criterion makes it possible to define a maximum capacity of the digital image. This maximum capacity corresponds to the number of information bits which it is possible to insert in the digital image whilst complying with the detectability criterion.

[0120] Initially, at a step E100, this capacity Q is initialised to 0 and the starting point is an initial partitioning which is limited here to a single region R of size P.

[0121] Naturally, the initial partitioning could be different and notably include already several distinct regions with sizes which might be different.

[0122] It is assumed that the size P of this initial region R is greater than a minimum size denoted P_{stat} which corresponds to the minimum size of a statistically significant sample of coefficients for detecting a watermarking signal inserted in these coefficients. Typically, this minimum size can be fixed at 100.

[0123] This initial region R can consist of the set of coefficients of the representation under consideration or a subset of this representation.

[0124] A test step E101 then tests the detectability of the insertion of a watermarking signal in the initial region R.

[0125] This detectability test can be effected by actual modulation and detection operations on the coefficients of the initial region R.

[0126] In practice, all the coefficients of the initial region R are copied into a working memory so as not to directly watermark the image.

[0127] Next all the coefficients of the initial region R are modulated by inserting the watermarking signal.

[0128] Conventionally, the following procedure is followed in order to effect this modulation:

The initial region R consists of a set of coefficients:

$$X : \{X_i, i = 1, \ldots P\}$$

Normally a linear modulation is used of the type:

$$X_i^* = X_i \pm \alpha_i W_i, \text{ with } i = 1, \ldots, P$$

where $W : \{W_i, i = 1, \ldots, P\}$ is the watermarking signal generally chosen as a pseudo-random sequence with a known distribution and a nil mean.

[0129] The value of the sign $\pm$ of the modulation depends on the binary value to be inserted: for example the sign -

WAVELYNX EX. 1003, Pg. 1002
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

corresponds to the value 0 and the sign + corresponds to the value 1.

[0130] It is possible to choose, by way of example, a pseudo-random sequence W which follows a uniform law on the interval [-1, 1].

[0131] Naturally, any pseudo-random watermarking with known distribution and nil mean can be suitable. The most usual distributions for the watermarking signal W are, apart from the aforementioned uniform distribution [-1, 1], the binary distribution {-1,1} and the centred standardised Gaussian distribution N(0, 1).

[0132] The modulation can optionally be protected by means of a secret key characterising for example the kernel for reproducing the pseudo-random sequence W.

[0133] The term α_i is the modulation amplitude, or weighting coefficient, applied to the coefficient X_i.

[0134] A constant weighting coefficient can be used for all the coefficients of the region R, such that $\alpha_i = \alpha_v$ for any i, the value of the weighting coefficients α_v being equal to a maximum value ensuring imperceptibility of the watermarking signal for the modulation of the set of coefficients representing said digital image.

[0135] This maximum value α_v (referred to as Just Noticeable Difference or JND amplitude) decreases in fact with the length of the sequence of the watermarking signal W, and consequently with the number of modulatable coefficients.

[0136] Given that the capacity Q will be maximised when all the coefficients of the representation of the digital image are used for the modulation, it is judicious to determine a modulation JND amplitude for a number of modulatable coefficients equal to the cardinal number of the set of coefficients representing the image.

[0137] This maximum value α_v or JND amplitude corresponds to the maximum modulation amplitude which can be used in the aforementioned linear insertion mode! beyond which an observer is capable of visually detecting a change in the reconstructed watermarked image.

[0138] In order to determine this JND amplitude, it is possible to use a visibility model which makes it possible to predict the visibility of a watermarking operation according to different parameters, namely the representation of the signal through a spatio-frequency transformation S used, the sub-band considered for the insertion, the type of distribution of the sequence of the watermarking signal W and the length P of the sequence W.

[0139] A simple model, developed by WATSON and described in the article entitled "Visibility of wavelet quantization noise", A.B. WATSON et al, IEEE Trans. on Image Process, 6(8), 1164-1175, 1997, makes it possible to predict the visibility of a set of modulated coefficients from the measurement of visibility of a single modulated coefficient. Reference can advantageously be made to this document for the detailed description of this model.

[0140] Thus use is made of a function dependent on the length P of the watermarking signal W, the type of transformation S used and the (base) sub-band considered for the insertion, but independent of all the coefficients to be watermarked X.

[0141] This calculation function used can be written:

$$\alpha_v(P, S, w) = \frac{\alpha_{base}(S)}{P^{1/\beta}\left(E[|w|^{\beta}]\right)^{1/\beta}}$$

where $\alpha_{base}(S)$ is a base value, dependent on the transformation used S and on the (base) sub-band considered for the insertion, of the maximum weighting coefficient ensuring imperceptibility during modulation of a single coefficient of this sub-band,

β is strictly greater than 2, and

$E[|w|^{\beta}]$ is the mathematical expectation of the function $|w|^{\beta}$.

[0142] The base values $\alpha_{base}(S)$ can be measured once and for all, for each sub-band of coefficients in the wavelet decomposition, from a single psychovisual measurement, and be stored in a table of visual amplitudes.

[0143] β is the exponent of a Minkowsky sum and can be chosen equal to 5, for example.

[0144] The mathematical expectation $E[|w|^{\beta}]$ corresponds to an estimation of the mean of the function $|w|^{\beta}$.

[0145] This visibility model does not take into account the image I to be watermarked itself and is independent thereof. This is equivalent to considering that the image I is uniform. It is a question of a "worst case" model since the presence of the image signal makes it possible to visually mask the modulation itself.

[0146] The JND amplitude can thus be calculated for a length P of the watermarking signal W equal to the cardinal number of all the modulatable coefficients of the sub-band under consideration.

[0147] However, it is judicious to exploit the fact that the image signal itself makes it possible to mask the modulation.

[0148] Thus, in this example, use is made, for each coefficient X_i to be modulated, of a weighting coefficient in accordance with a law of the form $\alpha_i = k_i.\alpha_v$, where k_i is a modulation factor dependent on the coefficients situated close to the coefficient considered on the region R and α_v is equal to the maximum JND value of the weighting coefficient.

[0149] Thus each coefficient will be modulated according to the local content, which makes it possible to locally increase the amplitude of the modulation to the benefit of detectability.

WAVELYNX EX. 1003, Pg. 1003
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0150] In order to test detectability in the test step E101, a detectability amplitude is next calculated from the detectability criterion and this detectability criterion is validated by comparing the detectability amplitude with a predetermined threshold value denoted Tc.

[0151] A calculation of correlation C(X*, W) between all the modulated coefficients X* and the marking signal W is generally made and it is decided whether there has actually been watermarking of the image when the result of the correlation calculation C(X*, W) is greater than the predetermined threshold value Tc.

[0152] A standardised statistical test can also be used for the detection, such as the one described in the article entitled "A method for signature casting on digital images" by I. PITAS, in Proc. ICIP, pages 215-218, September 1996. The detection is then characterised in terms of probability. It is thus possible to choose a threshold value Tc corresponding to a fixed detection probability level, for example 99.95%.

[0153] Thus, for a given region R defining a set of coefficients X of size P and with a fixed weighting coefficient α, it is possible to calculate a detectability amplitude and compare it with a threshold value Tc so as to validate or not the detectability criterion on this region R.

[0154] The detectability criterion is in fact in theory a function depending on the size P of the region R, the detection threshold Tc related to the required detection probability, the watermarking signal W, the variance σ^2_x of the coefficient X to be modulated on the region R and the weighting coefficient used α for modulating the coefficients X according to the linear model described above.

[0155] Thus, for example, for a detection by standardised hypothesis test and a value of the weighting coefficient α which is constant and equal to α_v for all the coefficients X_i of the region R, a minimum length $P_{min}(X)$ is defined by the function:

$$P\min(X) = \left(\frac{2Tc}{a\alpha}\right)^2 \left[b\sigma_X^2 + c\alpha^2 + d\right]$$

where a, b, c and d can be assimilated to constants. The signal being non-stationary, that is to say the variance σ^2_x being a function of space, it is indeed necessary to adapt the modulation length P generated by the watermarking signal to the image signal itself.

[0156] On decoding, the set of coefficients X being modulated, this function also depends on the variance σ^2_w of the inserted watermarking signal W.

[0157] In addition, it is necessary to provide for any distortions which the image may undergo after modulation, due for example to a compression of the image.

[0158] When this noise can be considered to be additive and decorrelated from the coefficients, it is possible to use a model dependent on the variance σ^2_q of this additive noise modelling any distortions applied to said coefficients after modulation.

[0159] Thus, to a given weighting coefficient α, making it possible to ensure invisibility of the inserted watermarking signal, a detection threshold Td fixed as a function of the detection probability required at decoding and a set of selected coefficients X, there also corresponds a minimum modulation length $P_{min}(X)$ which makes it possible to ensure detectability of the inserted watermarking signal.

[0160] On decoding, for a detection by standardised hypothesis test, this minimum length $P_{min}(X)$ is then defined by the function:

$$P\min(X) = \left(\frac{2Td}{a\alpha}\right)^2 \left[b(\sigma_X^2 + \alpha^2\sigma_W^2 + \sigma_q^2) + c\alpha^2 + d\right]$$

where a, b, c and d can be assimilated to constants.

[0161] It is therefore necessary, if the same detectability test is used during coding and decoding, to choose a threshold value Tc on coding greater than that Td used at the time of decoding if it is wished to be able to find the same partitioning on decoding of the image.

[0162] In practice, the threshold value Td on decoding which it is wished to use is fixed, that is to say for example the required detection probability level when the detection is made by a standardised hypothesis test, and a higher threshold Tc on coding is chosen, in order to take account of the variance in the watermarking signal W and the variance of an additive noise fixed a priori so as to anticipate the influence of the subsequent processing undergone by the image.

[0163] This condition thus makes it possible to find the same detectability criterion which constrains the partitioning of the digital image without having to transmit to the decoder the partitioning effected at the time of insertion of the

WAVELYNX EX. 1003, Pg. 1004
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

watermarking signal W.

[0164] In this example embodiment, a partitioning by iterative division of the digital image is effected. It is consequently considered, at step E101, that the detectability criterion is satisfied when the calculated detection amplitude is greater than or equal to the predetermined threshold Tc.

[0165] If the detectability criterion is not satisfied, then it is probable that the detectability criterion is also not satisfied in subregions of the initial region R of smaller size because the detection probability generally decreases with the size of the regions. A step E102 of stopping the method of determining a partitioning makes it possible to stop the process of iterative division of the image.

[0166] Insertion not being judged possible in the initial region R, the capacity Q of the image is therefore nil.

[0167] If on the other hand the detectability criterion is satisfied, that is to say here that the detection amplitude is greater than or equal to the threshold value Tc, it is possible that it is also satisfied for subregions of the initial region R.

[0168] It is therefore judicious to attempt to divide the region R as long as the detectability criterion is satisfied in order to increase the capacity Q.

[0169] There are of course several possible means for effecting the spatial division of the region R into subregions R_j, of sizes P_j, with j = 1, ..., K.

[0170] In this example a division into a quadtree is chosen, as illustrated in Figure 4.

[0171] This division consists of dividing each region into four subregions of identical size.

[0172] Thus, by way of example, in Figure 2, a digital image of initial size N is being partitioned into two sub-regions R5 and R6 of sizes N/4, seven subregions R1, R2, R3, R4, R7, R8, R9 of sizes N/16 and four subregions R10, R11,R12,R13ofsizesN/64.

[0173] Thus, at the division step E103, the region R is divided into subregions R_j, j = 1,..., K of sizes P_j. In a case of a division into a quadtree, K = 4 and P_j = P/4.

[0174] At step E104 a first subregion of index j (for example j = 1) is considered and a value of potential gain in capacity denoted G_Q is initialised to -1.

[0175] The partitioning determination method then includes a prior step E105 of comparing the size P_j of the region R_j with the minimum size P_{stat} corresponding to the minimum size of a statistically significant sample for the detection of a watermarking signal inserted in said region as described above.

[0176] If the size P_j of the region R_j is less than this minimum size P_{stat}, at step E108 the index J = J+1 is incremented in order to process the following sub-region R_{j+1}.

[0177] Otherwise, the detectability criterion is checked on the subregion R_j in the same way as previously described with reference to step E101.

[0178] In practice, the watermarking signal is inserted on the coefficients of the said region R_j, a detection amplitude is calculated and this detectability amplitude is compared with the threshold value Tc.

[0179] The detection amplitude can be a correlation value between the modulation signal X* and the carrier of the watermarking signal W or the result of a standardised hypothesis test.

[0180] If the detectability criterion is verified, the value of potential gain in capacity G_Q is increased by one unit at step E107.

[0181] Then at step E108 the index j of the subregions is incremented and it is checked at the test step E109 that this index j is less than or equal to the number of K.

[0182] In the affirmative, steps E105 to E109 are reiterated on the following subregion.

[0183] Otherwise, when the index j = K+1, it is checked in a test step E110, whether the potential gain in capacity value G_Q is strictly positive, that is to say whether there exist at least two subregions R_j of the initial region R for which the detectability criterion is validated.

[0184] In the negative, the partitioning of higher rank carried out on the initial region R is not validated and this region R is preserved. Such is the case when the detectability criterion has not been validated for any of the subregions R_j or only for a single subregion R_j.

[0185] In the latter case, it is preferable to keep the region R for inserting the watermarking signal since it is of size P greater than the size of the single validated subregion R_j.

[0186] At step E112, the value of the capacity Q is then increased by one unit and the region R of size P in the partitioning is kept.

[0187] An actual insertion step E113 by modulation of the coefficients of the region R can then be implemented in a normal fashion using the linear insertion model described above.

[0188] An elimination step E114 then makes it possible to eliminate the region R from a stack of regions to be processed.

[0189] On the other hand, if at step E110 the value of the potential gain capacity Gc is strictly positive, in an addition step E111 all the subregions R_j for which the detectability criterion is validated in the stack of regions R to be processed are added.

[0190] A return step E 115 makes it possible to reiterate all the steps E103 to E113 in order to process the regions of the stack in a recursive fashion.

WAVELYNX EX. 1003, Pg. 1005
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0191] At the end of the recursive partitioning method just described, a capacity value Qm corresponding to the maximum capacity of the image for insertion of a watermarking signal is obtained, guaranteeing a correct detection of this signal. This maximum capacity Qm is equal to the cardinal number of the distinct regions obtained by the said partitioning on which the detectability criterion is validated.

[0192] In addition, the insertion step proper E113 can be omitted during a first "pass" which then makes it possible only to determine the maximum capacity Qm of the image and the validated regions.

[0193] Once the maximum capacity Qm has been calculated and the corresponding partitioning is stored in memory, it is then possible for a user to determine the message which he wishes to insert, corresponding to a number of information bits equal to the maximum capacity Qm, and then to insert this message in a normal manner by modulating the coefficients of the different regions obtained by the previously determined partition.

[0194] A description will now be given, with reference to Figure 5, of a second embodiment of the invention in which it is wished to insert a message of fixed capacity Qs in an image I. Naturally, this fixed capacity Qs must have a value less than the maximum capacity Qm of the digital image to be watermarked.

[0195] As illustrated in Figure 5, the method of determining a partitioning in this embodiment includes steps E100 to E113 identical to those of the method of determining a partitioning of the embodiment of Figure 3 and which it is not necessary to describe again here.

[0196] As before, at step E112, the value of the capacity Q is incremented when the partitioning of rank directly higher is not validated.

[0197] Then the method includes a comparison step E116 in which this value of the capacity Q is compared with the fixed capacity value Qs.

[0198] In practice, it is tested at step E116 whether the capacity value Q is equal to the fixed capacity value Qs.

[0199] In the affirmative, a stop step E117 makes it possible to stop the iterative partitioning of the image since there are a number of regions equal to the number of information bits Qs which it is wished to insert.

[0200] Otherwise, in an elimination step E114, the processed region is eliminated from the stack of regions R to be processed formed at step E111.

[0201] The method of determining a partitioning also includes, in this embodiment, a sorting step E118 which sorts the regions R to be processed in the stack by detectability amplitude value calculated on these regions R.

[0202] Thus a return step E115 reiterates the partitioning from the division step E103 for a region R in the stack having the highest detectability amplitude amongst all the other regions to be processed.

[0203] A sorting variant can consist of sorting the regions to be processed in decreasing order of size so as to process, as a priority, the largest regions which a priori provide better detectability.

[0204] Naturally, a partitioning by iterative merging of the digital image could be carried out in the same way, for example also using a quadtree partitioning structure.

[0205] The initial partitioning then consists of regions with smaller acceptable sizes, greater than or equal to the previously defined minimum size P_{stat}.

[0206] For each region of the partitioning for which the delectability criterion is not validated, this region is merged with another region of the partitioning.

[0207] This other region of the partitioning is if possible a region for which the detectability criterion is not validated so as to increase the capacity.

[0208] Alternatively, another region can be a region satisfying the detectability criterion so as to make detection reliable.

[0209] There are many possibilities for the choice of the region to be merged. It is possible to take as the merger criterion the detection amplitude calculated on each of the regions and merge for example the regions associated with the lowest detection amplitudes.

[0210] In this particular case of a merging in a quadtree partitioning structure, the merging is structurally constrained and consists of deciding whether or not four adjacent blocks, for example R1, R2, R3 and R4 in Figure 4, must be merged.

[0211] A description will now be given, with reference to Figure 6, of the associated decoding method which makes it possible to find the partitioning when the watermarking signal inserted in a digital image is extracted.

[0212] Indeed, because of the adaptation of the partitioning to the digital image, this partitioning will not be known a priori at the decoder.

[0213] The decoding method then consists, in general terms, of testing all the acceptable partitionings. The same iterative implementation technique is used as the one used when the partitioning is determined for inserting the watermarking signal.

[0214] Thus a description will be given of an example embodiment in the case of a segmentation by dividing by blocks in a quadtree, symmetrical to that using the partitioning determination method of the embodiment described with reference to Figure 3.

[0215] At an initialisation step E200, there is an initial partitioning limited to a single region R of size P. This region consists of all the coefficients of the same representation of the digital image as the one used at the time of insertion of the watermarking signal.

WAVELYNX EX. 1003, Pg. 1006
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0216] A test step E201 makes it possible to verify that the size P of the initial region R is indeed greater than the minimum size P_{stat} as described previously.

[0217] In the affirmative, at step E203 a criterion of detectability of the information bit inserted on the region R, obtained by demodulation of the coefficients on this region R, is verified.

[0218] In practice, a detection amplitude is calculated for all the coefficients of the region R and the detectability criterion is validated by comparing this detection amplitude with a predetermined threshold value Td for decoding.

[0219] It is possible to proceed by means of a standardised statistical test, and the result compared with the predetermined threshold value Td.

[0220] As explained before, it is necessary, if the same detectability test is used during coding and decoding, to choose a threshold value Tc on coding greater than that Td used at decoding if it is wished to be able to find the same partitioning on decoding of the image even when the latter has been made noisy by post-processing.

[0221] This condition thus makes it possible to find the same detectability criterion which constrains the partitioning of the digital image without having to transmit, to the decoder, the partitioning effected when the watermarking signal W was inserted.

[0222] If the detectability criterion is not verified at step E203, a division is carried out, at step E204, of the region R into subregions R_j and sizes P_j with j = 1, ..., K. Then the same partitioning structure is used as the one used on coding, that is to say, in this example, a division of the region R into four subregions R_j of identical sizes.

[0223] Then, in an addition step E205, the subregions R_j are added in a stack of regions R to be processed and, at a return step E202, the decoding method is reiterated recursively as from the test step E201 on each region R of the stack.

[0224] When at the step of calculating the detectability criterion E203, the latter is verified for a region R, there is extracted at the extraction step E206 the information bit inserted in this region R as an element of the method inserted in the digital image I. This extraction is effected in a conventional fashion by calculating a detection amplitude. The result of the test gives, in absolute value, a detection amplitude to be compared with the threshold value Td of the decoding, the sign giving the value 0 or 1 of the information bit inserted.

[0225] It should be noted that this extraction is already partly effected during the detection step E203 so that the detection E203 and extraction E206 steps are structurally coupled.

[0226] An elimination step E207 is implemented in order to eliminate the region R from the stack of regions to be processed, which was formed at the addition step E205, and the return step E202 then makes it possible to implement the decoding method recursively on each region R of the stack to be processed.

[0227] A description will now be given, with reference to Figures 7 and 8, of a practical application of the method of determining a partitioning of a digital image in a particular embodiment of the invention.

[0228] In this application, the watermarking signal is inserted by means of a technique of insertion by spectrum spreading, by modulation of coefficients of a space-frequency representation of the image, obtained by a spatio-frequency transformation S of the digital image I as previously described with reference to figure 2.

[0229] In general terms S_j sub-bands are obtained, with J = 1, ..., M and M equal here to 13 at a transformation step E300.

[0230] Next, for each sub-band S_j of index j considered at step E301, a partitioning is effected at step E302 by implementing the method of determining a partitioning described previously to with reference to Figure 3.

[0231] In this way a capacity Q_j is derived for each sub-band S_j.

[0232] A step E303 of insertion by modulation of the coefficients next makes it possible to insert Q_j information bits in the Q_j regions validated.

[0233] In steps E304 and 305, the following sub-bands are next considered as long as all the sub-bands S_j have not been processed, and the steps E302 and E303 of partitioning and inserting a watermarking signal of capacity Q_j are reiterated on each sub-band S_j.

[0234] Next, an inverse transformation S^{-1} is applied to the image in order to obtain the watermarked image, of total capacity Q equal to the sum of the capacities Q_j calculated for each of the sub-bands S_j.

[0235] Thus, each sub-band of the representation is considered independently for the adaptive partitioning which is carried out both at coding and at decoding.

[0236] As illustrated in Figure 8, the decoding method in this embodiment is implemented in a similar fashion using the decoding method described with reference to Figure 6, the initial region R here corresponding each time to a sub-band of the decomposition of the image.

[0237] A step E400, identical to step E300, divides the image I into S_j sub-bands with j = 1, ... M.

[0238] A first sub-band S_j is considered at step E401. The order of processing of the sub-bands is identical to that used during coding in order to extract the inserted message in order.

[0239] The adaptive partitioning is implemented at the partitioning step E402 in order to calculate the capacity Q_j of the sub-band S_j. Next, at the extraction step E403, the Q_j information bits are extracted by demodulating the coefficients of the Q_j regions of the partitioning.

[0240] At the test steps E404 and E405, it is checked in the usual fashion that all the sub-bands have been processed and, in the negative, the decoding steps E402 and E403 (partitioning and extraction) are reiterated on the remaining

WAVELYNX EX. 1003, Pg. 1007
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

sub-bands.

[0241] In this way, at the output of the decoder, a message of Q bits is obtained, Q being equal to the sum of the capacities Q_j of each sub-band S_j.

[0242] In a variant of this method illustrated in Figure 9, it is possible to effect a partitioning on a post-processed image signal in order to obtain an a priori robustness of the watermarking signal to any post-processing undergone by the image.

[0243] The principle of this variant consists of performing a detectability test in a test step E309 which is no longer coupled to the steps of partitioning E302 and insertion E303 described previously.

[0244] After the insertion of the watermarking signal in a region, a reverse transformation S^{-1} is first of all performed at step E306 in order to find the watermarked image. Then, in a step E307, post-processing is applied, such as a compression of the digital image.

[0245] Next, in a step E308, the transformation S is reiterated in order to find the watermarked coefficients, possibly made noisy by the post-processing carried out on the image at step E307, and the detectability criterion is calculated as previously described.

[0246] Steps E300 to E309 are reiterated on another acceptable partitioning of the image, here for example by dividing the relevant region R into four, and the detectability test is performed at step E309 on the four sub-regions.

[0247] This partitioning is adopted only if it represents a gain in capacity, that is to say, in this example of quadtree division, if the detectability criterion is validated on at least two sub-regions.

[0248] This variant embodiment makes it possible to directly take into account the post-processings which will be applied to the digital image.

[0249] A method of determining a partition according to a preferred embodiment of the invention will now be described, by reference to Figure 10.

[0250] The method of inserting a watermark is employed on a digital image I.

[0251] This insertion method first of all includes a method of determining a partition of a set of coefficients representative of the digital image I.

[0252] This partition is applied as a function of a criterion of detectability of an information bit inserted on each region of the partition.

[0253] It should be noted that, in practice, a partition of a digital image into a maximum number of regions satisfying a detectability criterion can be sought so as to ascertain the practical capacity of this image with regard to the insertion of a watermark. This maximum capacity of the digital image corresponds to the

[0254] number of information bits which it is possible to insert into the digital image while complying with the detectability criterion.

[0255] It is also possible, for a given watermark, comprising a given number of information bits of less than the maximum capacity of the image I, to seek the best possible partition of the image I which makes it possible to insert this watermark of given length, for a given detection probability, and in regions of the largest possible sizes so as best to ensure invisibility of the inserted watermark.

[0256] The method of determining a partition first of all includes a step of spectral decomposition E500 of the wavelet-decomposition type described previously (Discrete Wavelet Transform or DWT).

[0257] Thus a set of spectral coefficients X is obtained, representative of the digital image I. These spectral coefficients are distributed into frequency sub-bands as illustrated diagrammatically in Figure 2, on completion of the decomposition step E500. The size of the set of coefficients X is equal to $N = M \times M$ for a square image. Obviously, the same method could be applied to a rectangular image.

[0258] In this embodiment of the invention, the method includes a step E501 of generating a centred pseudo-random sequence of size N equal to the cardinal number N of the set of coefficients X representative of the image I.

[0259] Let $w = \{w_{mn}, 0 \leq m, n \leq M\}$ be this pseudo-random sequence.

[0260] This pseudo-random sequence w is formed from centred pseudo-random sub-sequences w^k.

[0261] The pseudo-random sequence can be seen as the merging of the pseudo-random sub-sequences w^k.

[0262] Here, the centred pseudo-random sequence w is formed from pseudo-random sub-sequences w^k of identical size which correspond to a block, called unit block, of the set of coefficients X.

[0263] Obviously, the pseudo-random sub-sequences w^k could differ in size from one another.

[0264] Here, the size of these unit blocks corresponds to the minimum number of coefficients suitable for forming a region of a size which is statistically significant for satisfying the detectability criterion over this region.

[0265] As described later, when a standardised statistical detection test is applied to a set of coefficients, a minimum number of coefficients is necessary for this test to be significant.

[0266] The pseudo-random sub-sequences w^k are of a size $A = L \times L$ which is greater than or equal to this minimum number of coefficients.

[0267] For preference, pseudo-random sub-sequences w^k are chosen to be equal in size to this minimum size. This characteristic is particularly advantageous when partition is achieved by iterative combination by combining blocks from an initial segmentation of the image into unit blocks of size L x L. The initial segmentation then corresponds to the

WAVELYNX EX. 1003, Pg. 1008
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

maximum partition of the image which can be applied, beyond which the blocks of coefficients generated are no longer statistically significant for the insertion and detection of an information bit.

[0268] For example, L = 8 is chosen.

[0269] The pseudo-random sequence w is then the merging of N/64 pseudo-random sub-sequences w^k forming unit blocks.

[0270] On each unit block, in accordance with the invention, a centred pseudo-random signal of predefined distribution (Gaussian, uniform, etc.) has to be generated on the basis of a function depending on a secret key K and on the index k of each unit block. This key can be denoted f(K, k). It is then necessary to ensure that, in practice, the average of the signal w^k is exactly equal to zero over each unit block.

[0271] A first method for generating such a centred pseudo-random sequence consists in centring the sequence in a deterministic way, by symmetrisation. This method is suitable for generating a pseudo-random sub-sequence of even size A.

[0272] In this case, each centred pseudo-random sub-sequence w^k is created by generating one half, A/2, of the pseudo-random samples of the sub-sequence via a pseudo-random number generator of known centred distribution, and by symmetrising the pseudo-random samples thus generated in order to obtain the other half A/2 of the samples of the sub-sequence w^k.

[0273] For a single-dimensional sequence, a set of samples of size A/2 $\{w_j, 1 \leq j \leq A/2\}$ is therefore generated, and this set is made symmetric in order to obtain the other half of the samples $\{w_j = -w_{A-j}, A/2 < j \leq A\}$.

[0274] In order to reinforce the random character of the sequence thus obtained, permutation can be carried out on the set of samples obtained $\{w_j, 1 \leq j \leq A\}$ by using a secret key.

[0275] A second method of generating a centred pseudo-random sequence consists in creating each centred pseudo-random sub-sequence w^k by generating pseudo-random samples via a pseudo-random number generator and by re-distributing the sum of these pseudo-random samples generated over each sample.

[0276] Thus, first of all, by using the secret key f(K, k), a sequence of pseudo-random samples of the same size A as the unit block, i.e. $\{w_i, 1 \leq i \leq A\}$, is generated.

[0277] Next the exact sum of these samples is calculated:

$$S_k = \sum_{i=1}^{A} w_i$$

[0278] Then this sum S_k is redistributed over the samples so as to obtain a centred pseudo-random sequence, that is to say one with a sum exactly equal to zero.

[0279] Thus $w^k = \{w_i - S_k/A, 1 \leq i \leq A\}$ is obtained.

[0280] The pseudo-random sequence w is thus composed of the merging of the centred sub-sequences w^k in such a way that the partitioning of a set of coefficients modulated by the centred pseudo-random sequence w gives rise to subsets of coefficients also modulated by centred pseudo-random sub-sequences.

[0281] Obviously, other techniques could be used to generate centred pseudo-random sequences.

[0282] As illustrated in Figure 10, a step E502 of modulation of the set of coefficients by the centred pseudo-random sequence w is then implemented so as to insert an information bit onto the set of coefficients originating from the spectral decomposition.

[0283] In practice, the set of coefficients is copied into a working memory, for example a random-access memory in a computer, so as not to mark the image I directly.

[0284] The same information bit is modulated onto the set of coefficients, for example b = 1 here, according to the modulation formula:

$$X'_i = X_i + \alpha_i w_i, \text{ with } 0 \leq i \leq N.$$

[0285] The weighting amplitude α_i is chosen in the usual way so as to guarantee invisibility of the inserted information bit.

[0286] A constant weighting coefficient can be used for all the coefficients, such that $\alpha_i = \alpha_v$ for all i, the value of the weighting coefficient α_v being equal to a maximum value ensuring imperceptibility of the watermark for modulation of the set of coefficients representative of the digital image.

[0287] It may be worthwhile exploiting the fact that the image signal itself makes it possible to mask the modulation.

[0288] To this end, it is possible, for each coefficient X_i to be modulated, to use a weighting coefficient according to a rule of the form $\alpha_i = k_i.\alpha_v$, where k_i is a modulation factor depending on the coefficients situated in the vicinity of the

WAVELYNX EX. 1003, Pg. 1009
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

coefficient in question and α_v is equal to the maximum value of the weighting coefficient ensuring imperceptibility of the watermark for the modulation of the set of coefficients.

[0289] Thus, each coefficient will be modulated as a function of the local content of the image, which makes it possible locally to augment the amplitude of the modulation to the benefit of the detectability.

[0290] For preference, in this embodiment of the invention, it is wished to apply a partitioning to a post-processed image signal so as to obtain robustness, a priori of the inserted watermark, against any post-processing undergone by the image I.

[0291] To do that, a distortion is applied, in a distortion step E503, to the set of modulated coefficients.

[0292] By virtue of the modulation of the coefficients in a single operation, on the basis of a centred pseudo-random sequence, the distortion step E503 can be implemented once only upon determination of a partition, in contrast to the prior techniques in which each sub-region of coefficients was modulated independently of the other and required distortion to be applied to each level of the partition.

[0293] This is all the more advantageous since, here, the step E503 of applying a distortion includes the following sub-steps as illustrated in Figure 10:

- inverse spectral transformation E503a of the set of coefficients X'_i modulated in order to obtain a watermarked image;
- application proper, E503b, of distortion to the watermarked image; and
- spectral transformation E503c of the watermarked image in order to obtain a set of modulated coefficients after distortion.

[0294] The distortions applied are distortions which alter the value of the pixels without altering the geometry of the image, such as the addition of noise, alteration of the contrast, compression, low-pass or high-pass filtering, for example.

[0295] Compression of the image is considered here, according to the JPEG standard (for Joint Photographic Expert Group) with specified quality factor, with q = 75 typically by default for JPEG compression.

[0296] In practice, an inverse wavelet transformation DWT^{-1} is applied here, then compression followed by decompression of the image, and finally forward wavelet transformation again in order to be able to estimate the detectability of the information bit inserted in the spectral domain.

[0297] Next an iterative partitioning of the set of coefficients is applied, so as to search for a partition of the set of coefficients in which each inserted information bit can be detected correctly according to a fixed detection probability. The number of regions thus determined during the partition corresponds to the practical insertion capacity of the image I.

[0298] The means for displaying to the users Q bit determined by calculating the capacity should exist.

[0299] Various techniques for iterative segmentation by division/combination can be used as previously described.

[0300] A first way of performing the preferred embodiment of the invention will firstly be described, by reference to Figure 11, in which the partitioning is achieved by iterative division on the basis of an initial segmentation of the set of coefficients into regions of a statistically significant size for validating a detectability criterion over these regions.

[0301] Following on from the steps of transformation E500, generation E501, modulation E502 and distortion E503 as described above, a first frequency sub-band will be considered, in a step E504, as a set of coefficients to be partitioned.

[0302] The initial segmentation of this set of coefficients corresponds to a spatial segmentation of the image I into blocks of unit size as defined above.

[0303] By its very construction, the pseudo-random modulation sequence is centred on each of these unit blocks.

[0304] In a quadtree-mode combination, it is always four blocks of equal size which are grouped together, called "child blocks" in order to form a "parent block", and this combination is recommenced iteratively, giving the notion of recursiveness.

[0305] Obviously, partition takes place frequency sub-band by frequency sub-band of the signal arising from the spectral decomposition.

[0306] Each unit block is considered here, in a step E505, in an order of scanning of the sub-band, for example from left to right and from bottom to top.

[0307] A validity criterion is applied over a first unit block which has not yet been processed.

[0308] In a calculation step E506, a statistical detection test is applied to this unit block of modulated coefficients X'_i.

[0309] An example of a standardised statistical test is given below.

[0310] Let X'_i, $1 \leq i \leq P$ be the set of coefficients to be tested after insertion of the pseudo-random sequence w and application of pre-distortion.

[0311] The test consists in calculating, for this set of size P:

$$T = \frac{M}{\sqrt{V}} \sqrt{P}$$

WAVELYNX EX. 1003, Pg. 1010
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

in which M represents an average value of correlation between the values of each coefficient X'_i and of modulation w_i, and V the variance of these values.

[0312] Hence in practice:

$$M = \frac{1}{P}\sum_{i=1}^{P} w_i\left(X'_i - M_x\right), \text{ with } M_X = \frac{\sum X'_i}{P}$$

and

$$V = \frac{1}{P-1}\sum_{i=1}^{P}\left[w_i\left(X'_i - M_X\right) - M\right]^2 .$$

[0313] The calculation of this test value T requires knowledge of the pseudo-random modulation sequence w which is generated once and for all at the above-described generation step E501.

[0314] The detectability is given by the comparison of this test value T with a certain threshold Pp, which corresponds theoretically to a probability of correct detection of p% if the test T follows a Gaussian law with variance equal to 1 for the two hypotheses tested (presence or absence of watermark).

[0315] A comparison step E507 makes it possible to compare this test value T with the threshold value P_p or correct detection rate.

[0316] On completion of this comparison, if the calculated value T is higher than the correct detection rate, the block tested is held in memory, in a memory-storage step E509, as being a region available for inserting an information bit.

[0317] In practice, a capacity-calculating step E510 can be implemented in such a way that, for every block of coefficients tested which is suitable for having an information bit inserted, the value of the capacity is increased by one unit.

[0318] In contrast, if the calculated value T is less than the correct detection rate Pp, a block of higher level is selected, in a combining step E508, that is to say, here, a parent block corresponding to the combination of four unit blocks, and the steps E506 of calculating the test value T and of comparison E507 with the correct detection rate P_p are reiterated over this new block.

[0319] During this combining of child blocks in order to form a parent block, those child blocks are preferably chosen for which the detectability criterion is not satisfied.

[0320] For application of this detectability criterion, any standardised statistical test can be used for the detection, such as that described in the article entitled "A method for signature casting on digital images" by I. PITAS, in Proc. ICIP, pages 215-218, September 1996, which makes it possible to characterise the detection in terms of probability.

[0321] A threshold value P_p can be chosen, corresponding to a fixed level of detection probability, 99.95% for example.

[0322] Hence, for a given region defining a set of coefficients X of size P and with a fixed weighting coefficient α, it is possible to calculate a detectability amplitude and to compare the latter with a threshold value P_p so as to validate or not validate the detectability criterion over this region.

[0323] In a general way, the detection probability decreases with the size of the regions tested, such that, by combining regions in order to increase the size of the block of coefficients used for inserting a watermark, the value of the test T is increased over this new block.

[0324] Hence, on completion of these steps of adaptive partitioning E504 to E508, an image insertion capacity can be determined, equal to Q bits, as can an appropriate partition of the image corresponding to this capacity Q.

[0325] A watermark can then be formed, with length equal to Q bits, and can then be inserted, bit by bit, into the various regions of the partition.

[0326] Obviously, the step E520 of insertion proper of the watermark can be coupled with the determination of the partition, in such a way that each region available on conclusion of the detectability test E506, E507, can actually be watermarked by the insertion of an information bit by modulation of the coefficients of this region.

[0327] The insertion step E520 makes it possible actually to insert an information bit of the watermark, by choosing a coefficient value b = 1 or = -1 in the above-described modulation formula, the alternating of the +/-1 bits conveying the content of the message inserted.

[0328] A centred pseudo-random sequence of known distribution can be used, different for each region of the partition, and initialised by a secret key K', as illustrated in Figure 1.

[0329] It should be noted that this secret key K' may, if appropriate, be identical to the secret key K used during the

WAVELYNX EX. 1003, Pg. 1011
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

generation of the pseudo-random sequence w for determining the partition.

[0330] Moreover, a centred pseudo-random sequence w identical to that generated at the generation step E501 could be generated.

[0331] A partition of an image I is shown diagrammatically by way of example in Figure 10, on conclusion of steps E504 to E508, in which, for example, 25 separate regions are obtained making it possible to insert a 25-bit watermark.

[0332] Obviously, any other partitioning technique could be used.

[0333] A second way of performing the preferred embodiment of the invention will now be described, by reference to Figure 12, in which the partitioning is achieved by iterative division of the set of coefficients.

[0334] On conclusion of the steps of transformation E500, generation E501, modulation E502 and distortion E503 as described above, a first frequency sub-band will be considered, in a step E511, as set of coefficients to be partitioned.

[0335] A quadtree-mode division will be considered here, in which one block, called "parent block" is always divided into four blocks of equal size, called "child blocks".

[0336] Obviously, partition takes place frequency sub-band by frequency sub-band of signal originating from the spectral decomposition.

[0337] Hence, in a step E512, an initial block corresponding to a first frequency sub-band is considered.

[0338] This initial block is stored in memory in a list L of blocks to be processed.

[0339] Next, in a step E513, a first block B to be processed, coming from the list of blocks to be processed L, is considered.

[0340] A detectability criterion is applied on this block B in a checking step E514.

[0341] In practice, as previously described, the value T of a statistical detection test on this block of modulated coefficients is calculated in a calculation step E514a. This step is analogous to the calculation step E506 described by reference to Figure 11.

[0342] The detectability is then given by the comparison of this test value T with a certain threshold P_p, which theoretically corresponds to a correct detection probability of p% if the test T follows a Gaussian law with variance equal to 1 for the two hypotheses tested (presence or absence of watermark).

[0343] A comparison step E514b makes it possible to compare this test value T with the threshold value P_p or correct detection rate. This comparison step E514b is analogous to the comparison step E507 described by reference to Figure 11.

[0344] On completion of this comparison, if the calculated value T is less than the correct detection rate P_p, a check is made, in a test step E515, as to whether there are blocks remaining to be processed in the list L.

[0345] If not, the recursive partitioning algorithm is terminated.

[0346] Otherwise the following block B of the list L is considered at step E513, and the checking step E514 is reiterated.

[0347] If, on completion of the comparison step E514b, the calculated value of the test T is higher than the correct detection rate Pp, detectability is tested over each child block of this parent block B in a checking step E516.

[0348] In practice, the parent block B is divided into four child blocks and the detectability criterion is checked on each of these blocks according to a step analogous to the previously described checking step E514.

[0349] A test E517 makes it possible to verify whether the detectability criterion is valid over at least one child block.

[0350] if yes, a division step E518 is implemented in order to actually divide the block B into four child blocks, and an addition step E519 allows these child blocks to be added to the list of blocks to be processed L.

[0351] The test and checking steps E513 to E519 are then reiterated over each of the blocks of the list L until the latter is empty.

[0352] In contrast, if, on conclusion of test E517, the detectability criterion is not satisfied on any of the child blocks of the parent block B, the tested block B is held in memory in a memory-storage step E509 as a region available for inserting an information bit.

[0353] In practice, a step of updating the capacity E510 can be implemented as described previously, in such a way that, for each block of coefficients tested which is suitable for insertion of an information bit, the value of the capacity is increased by one unit.

[0354] Hence, on conclusion of these adaptive partitioning steps E511 to E519, an image insertion capacity can be determined, equal to Q bits, as can an appropriate partition of the image corresponding to this capacity Q.

[0355] A watermark can then be formed, with length equal to Q bits, and can then be inserted, bit by bit, into the various regions of the partition.

[0356] Obviously, as before, the step E520 of insertion proper of the watermark can be coupled with the determination of the partition, in such a way that each block B available on conclusion of the detectability test E507, can actually be watermarked by the insertion of an information bit by modulation of the coefficients of this block B.

[0357] The insertion step E520 is carried out in the same way as when partition is achieved by iterative combination.

[0358] Moreover, in one enhanced embodiment of this technique of partition by iterative division, a division of a parent block B into child blocks can be adopted on completion of the detectability test E507 only if it represents a gain in capacity, that is to say into a quadtree-mode division only if the detectability criterion is satisfied over at least two child blocks. Otherwise, it may be preferable to keep the parent block of larger size so as to guarantee better invisibility of the inserted

WAVELYNX EX. 1003, Pg. 1012
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

watermark.

[0359] Obviously, the partitioning techniques described previously are not in any way limiting.

[0360] Notably, it is possible to use various iterative segmentation techniques by division/merging, to which there belong the quadtree block partitioning described previously, but also graph partitioning. In general terms, there are the so-called bottom-up methods and the top-down methods depending on whether the iterative partitioning means is merging or division.

[0361] Hence it is possible, if appropriate, to combine two techniques of partitioning by division and combination. This is the case when an initial partition is chosen, for example, intermediate between the two extremes which are, on the one hand, a single region and, on the other hand, a partition into regions of the smallest admissible size, allowing both the operations of division and of combination.

[0362] It is also possible to implement the method of determining a partition in order to maximise the capacity of the digital image by using several different segmentation techniques and then choosing the partition which confers the greatest capacity Q for the digital image.

[0363] It is also possible to determine the best partition possible, that is to say the one yielding a set of blocks of coefficients of largest possible size, for inserting a fixed-length message, less than the maximum capacity of the digital image to be watermarked.

[0364] In all cases, the present invention makes it possible to generate and to insert a pseudo-random sequence once only over a set of coefficients which are available for carrying out the insertion, and, as a corollary, to apply only one single pre-distortion to the set of coefficients.

[0365] It is thus possible rapidly to obtain a partition of the set of coefficients which makes it possible to insert a watermark with a fixed correct detection probability for an entire range of distortion lying between "no distortion" and "predetermined distortion" applied during the determination of the partition. Moreover, the simulation of maximum distortion before insertion is a quasi-deterministic operation which confers an advantage with respect to a theoretical statistical calculation.

[0366] A description will be given now of the insertion method according to the invention in a preferred embodiment.

[0367] The watermarking signal is inserted after a transformation step E600, in a set of coefficients of the domain transformed into sub-bands.

[0368] As illustrated in Figure 13, in a choosing step E601, there is for example chosen the high-frequency sub-band HH_1, with the first resolution level, corresponding to a high-pass filtering in the horizontal and vertical directions.

[0369] There is thus a set of spatio-frequency coefficients, with a cardinal number equal to N, denoted for example $X = \{X_i, 1 \leq i \leq N\}$.

[0370] For an image I of size 512x512, the sub-band HH_1 is of size N = 256x256.

[0371] Since the watermarking has to be imperceptible and indelible, and therefore difficult to locate and remove by pirating, it is chosen to insert a pseudo-random watermarking signal, spreading its spectrum in order to make this signal undetectable by spectral or statistical analysis.

[0372] For example, a pseudo-random sequence w is considered, which follows a uniform law on the interval [-1,1] with $w = \{w_i, 1 \leq i \leq P\}$, the length P of the sequence being less than or equal to N.

[0373] Naturally, any pseudo-random watermarking signal, with a known distribution and a nil mean, may be suitable. The most usual distributions for the watermarking signal w are, apart from the uniform distribution on [-1, 1] mentioned above, the binary distribution {-1,1} and the centred standardised Gaussian distribution N(0, 1).

[0374] The modulation which it is wished to apply to the coefficients in order to insert the watermarking signal uses a linear model of the type:

$$X'_j = X_{j(i)} + \alpha w_j, \text{ with } 1 \leq j \leq P$$

where

$X_{j(i)}$ is a subset of spectral coefficients chosen from the set of coefficients X, and α is a weighting coefficient.

[0375] Here, the weighting coefficient α is constant for any j.

[0376] In this example embodiment, it is sought to determine whether the insertion of the watermarking signal w is actually possible in the set of coefficients X whilst meeting predetermined criteria of imperceptibility and detectability.

[0377] According to the invention, the insertion method first of all includes a step E602 of calculating a maximum value α_v of the weighting coefficient α as a function of the length P of the watermarking signal w ensuring imperceptibility of the watermarking signal w.

[0378] This maximum value or visual amplitude α_v corresponds to the maximum modulation amplitude which can be used in the aforementioned linear insertion model beyond which an observer is capable of visually detecting a change at the level of the reconstructed watermarked image.

WAVELYNX EX. 1003, Pg. 1013
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0379] In this embodiment, a visibility model is used which makes it possible to predict the visibility of a watermarking operation as a function of the different parameters, which are the representation of the signal through the spatio-frequency transformation T used, the sub-band HH_1 considered for the insertion, the type of distribution of the sequence of the watermarking signal w and the length P of the sequence w.

[0380] A simple model, developed by WATSON and described in the article entitled "Visibility of wavelet quantization noise", A.B. WATSON et al, IEEE Trans. on Image Process, 6(8), 1164-1175, 1997, makes it possible to predict the visibility of a set of coefficients modulated from the measurement of visibility of a single modulated coefficient. Reference can advantageously be made to this document for a detailed description of this model.

[0381] During the step E602 of calculating the maximum value α_v, use is thus made of a function dependent on the length P of the watermarking signal w and on the type of spectral transformation T used, but independent of the set of coefficients to be watermarked X.

[0382] This calculation function used can be written:

$$\alpha_v(P,S,w) = \frac{\alpha_{base}(S)}{P^{1/\beta}(E[|w|^{\beta}])^{1/\beta}}$$

where $\alpha_{base}(S)$ is a base value, dependent on the transformation used S and the (base) sub-band considered for the insertion, of the maximum weighting coefficient ensuring imperceptibility when a single coefficient of this sub-band is modulated,

β is strictly greater than 2, and

$E[|w|^{\beta}]$ is the mathematical expectation of the function $|w|^{\beta}$.

[0383] The base values $\alpha_{base}(S)$ can be measured once and for all, for each sub-band of coefficients in the wavelet decomposition, from a single psychovisual measurement, and be stored in a table of visual amplitudes.

[0384] β is the exponent of a Minkowsky sum and can be chosen equal to 5, for example.

[0385] The mathematical expectation $E[|w|^{\beta}]$ corresponds to an estimation of the mean of the function $|w|^{\beta}$.

[0386] This visibility model does not take into account the image I to be watermarked itself and is independent thereof. This is equivalent to considering that the image I is uniform. It is a question of a "worst case" model since the presence of the image signal makes it possible to visually mask the modulation itself.

[0387] In this example, this calculation step E602 is implemented in order to calculate the maximum value α_v of the weighting coefficient α for a length P of the watermarking signal w equal to the cardinal number N of the set of modulatable coefficients X. Thus a maximum value denoted $\alpha_v(N)$ is calculated, which ensures imperceptibility of the watermarking signal w at the limit of perceptibility.

[0388] In the example embodiment described here, for a value of $\beta = 5$, the visual amplitude for the set of coefficients of the sub-band HH_1 is given by:

$$\alpha_V(N) = \frac{6^{0,2}\alpha_{HH1}(T)}{N^{0,2}}$$

[0389] Next, in a calculation step E603, the length P of the watermarking signal w is calculated for a minimum value α_D of the weighting coefficient α equal to said maximum value $\alpha_v(N)$ calculated and for a predetermined detection probability level.

[0390] This is because, in order to meet a predetermined detectability criterion, the weighting coefficient α must be greater than a minimum value α_D referred to as the detection amplitude.

[0391] At the decoder, the received image I*, which corresponds to the watermarked initial image, possibly made noisy because of certain distortions applied to the image, is first of all transformed by a transformation identical to that used during the insertion of the watermarking signal in order to find once again the set of coefficients which are modulated.

[0392] Thus a set $X^* = \{X_i^*, 1 \leq i \leq N\}$ is obtained, which represents the set of coefficients liable to have been modulated. By hypothesis, it is assumed that any distortion suffered by these coefficients can be modelled by an additive noise, decorrelated from the image signal itself $n = \{n_i, 1 \leq i \leq N\}$.

[0393] Each coefficient can thus be written:

WAVELYNX EX. 1003, Pg. 1014
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$X_i^* = X_i + \alpha w_i + n_i, \text{ with } 1 \leq i \leq N.$$

[0394] The detection of the inserted watermarking signal w consists of constructing a hypothesis test for replying to the question "has the signal w been inserted in X*?".

[0395] The advantage of constructing a hypothesis test is that its result makes it possible to give a theoretical confidence level to the decision since a hypothesis test is standardised with respect to known distributions.

[0396] For a class of statistical tests based on correlation, it can be shown that this detection amplitude can be calculated from a calculation function of the type:

$$\alpha_D(P) = \frac{a(\sqrt{\sigma_X^2 + \sigma_n^2})}{\sqrt{bP - c}}$$

where σ_X^2 is equal to the variance of the coefficients to be modulated, σ_n^2 is equal to the variance of the additive noise and a, b and c are constants which depend on the distribution of the watermarking signal w and on the required detection probability level p.

[0397] Thus this minimum value α_D is determined according notably to the length P of the watermarking signal w, a detection probability level p, the variance of the coefficients to be modulated, the distribution of the watermarking signal and possibly the variance of an additive noise decorrelated from the coefficients modelling any distortions applied to the coefficients.

[0398] Conversely, it is also possible to express the minimum detection length, denoted P°, as a function of the weighting coefficient α, for a fixed detection probability level:

$$P^\circ(\alpha) = \frac{a^2\left(\sigma_X^2 + \sigma_n^2\right) + c\alpha^2}{b\alpha^2}$$

[0399] It would be possible to use this result to check the parameters which make it possible to insert a watermarking signal w which will be robust to any additive noise with an energy less than or equal to σ_n^2.

[0400] As illustrated on the curves in Figure 14, from the visual amplitude α_V calculated as a function of the length P of the watermarking signal to be inserted, the insertion method includes, in general terms, a step of determining compatible values of the length P of the watermarking signal w, of the weighting coefficient α and of the probability level p so that the value of the weighting coefficient determined α is less than or equal to the maximum value or visual amplitude α_V and greater than or equal to the minimum value or detection amplitude α_D for these determined values of the length P of the watermarking signal w and the detection probability level p.

[0401] The weighting coefficient α, the length P of the watermarking signal w and the detection probability level p must thus be determined so that the following inequality is satisfied:

$$\alpha_D \leq \alpha \leq \alpha_V$$

[0402] As illustrated in Figure 14, in order to calculate the minimum value P° of the watermarking signal w for which the aforementioned inequality will be satisfied, the formula linking the length P of the watermarking signal w to the amplitude of the weighting coefficient α is used, with $\alpha = \alpha_V(N)$ and with a detection probability level of p%.

[0403] In this example a standardised statistical test is taken, based on the correlation between the watermarked signal X* and the inserted watermarking signal w, as proposed for example in the document entitled "On Resolving Rightful Ownerships of Digital Images by Invisible Watermarks" by W. ZENG and B. LIU, in Proc. ICIP 97, pages 552-555, October 1997.

[0404] It can be shown that, for this test:

WAVELYNX EX. 1003, Pg. 1015
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$\alpha_D = \frac{t_0 \sqrt{E(w^2)}\left(\sqrt{\sigma_X^2 + \sigma_n^2}\right)}{\sqrt{E^2(w^2)P - t_0^2 \sigma_{w^2}^2}}$$

[0405] A calculation step E604 thus makes it possible to calculate the three aforementioned constants a, b and c so that

$$a = t_0 \sqrt{E(w^2)},$$

$$b = E^2(w^2),$$

and

$$c = t_0^2 \sigma_{w^2}^2 .$$

[0406] The values $E(w^2)$ and $\sigma_{w^2}^2$ can be calculated theoretically as a function of the distribution of w. For the uniform distribution considered here, the theoretical values are $E(w^2) = 1/3$ and $\sigma_{w^2}^2 = 4/45$.

[0407] The value t_0 is a threshold value, dependent on the probability of correct detection p : $t_0 = 2 \times t_p$. The values of tp are percentile of a centred Gaussian law and have a variance equal to 1. These values are tabulated in the state of the art, for example in the book entitled "Probability and Statistics" by A. PAPOULIS, Prentice-Hall, 1990.

[0408] For example, tp = 3,291 corresponds to p = 0,9995, that is to say to a detection probability level equal to 99,95%.

[0409] In this numerical example it is considered that any additive noise is not taken into account so that $\sigma_n = 0$.

[0410] In an estimation step E605, the variance of the set of coefficients X is also estimated. The variance is estimated according to the following formula:

$$\sigma_X^2 = \frac{1}{N-1} \sum_{i=1}^{N} (X_i - M_X)^2$$

with

$$M_X = \frac{1}{N} \sum_{i=1}^{N} X_i$$

[0411] Then, for a detection probability fixed at 99.95%, the function linking the length P of the watermarking signal w to be inserted and the weighting coefficient α is then derived therefrom:

$$P = \frac{14{,}44 \times \sigma_X^2 + 3{,}84\alpha^2}{0{,}11\alpha^2}$$

[0412] At the calculation step E603, the minimum length P° is determined from the above formula for a weighting coefficient equal to the maximum value $\alpha_v(N)$ calculated at the calculation step E602.

[0413] The insertion method includes, in this example embodiment, a step E606 of comparing this calculated length P° with the cardinal number N of the set of modulatable coefficients X.

WAVELYNX EX. 1003, Pg. 1016
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0414] If, at this comparison step E606, the calculated length P° is less than or equal to the cardinal number N of the set of modulatable coefficients X, it is deduced therefrom that the insertion of a watermarking signal w of length P° is possible and meets the required imperceptibility and detection criteria.

[0415] In reality, it is possible to effect an insertion of a watermarking signal w which meets these criteria since the length P of this watermarking signal lies between the calculated value P° and the cardinal number N of the set of modulatable coefficients X.

[0416] Then the insertion proper of a watermarking signal of length P is carried out by modulating a subset of coefficients with a cardinal number P according to the linear modulation level, with a weighting coefficient α equal to the calculated maximum value $\alpha_v(N)$.

[0417] The insertion method includes, in the usual fashion, a reverse spatio-frequency transformation step which makes it possible to obtain, at the output of the coder, the watermarked image I*.

[0418] Where insertion is possible, it is also possible to calculate the number of theoretical bits which can be inserted. This is because, at the decoder, the decoding operation consists of detecting whether a pseudo-random sequence w has been inserted. The response being binary (yes/no), it can be considered that a pseudo-random sequence of length P makes it possible to insert and extract an information bit in the image. By repeating the insertion operation on several subsets of spectral coefficients, it is thus possible to insert and extract several information bits.

[0419] Consequently, since in this example there are a set of coefficients of cardinal number N and since only a number P° of coefficients are necessary to insert and detect an information bit, it is possible to derive therefrom the total number Q of information bits which can be inserted, referred to as the capacity of the image: $Q = N/P°$.

[0420] Moreover, if at the comparison step E606 the calculated length P° is greater than the cardinal number N of the set of modulatable coefficients X, it is a priori deduced therefrom that the insertion of a watermarking signal meeting the criteria of imperceptibility and detectability is not possible.

[0421] In this case, the insertion method can if necessary include an additional step of calculating the detection probability level p' obtained for a minimum value α_D of the weighting coefficient equal to the maximum value $\alpha_v(N)$ calculated for a length P of the watermarking signal w equal to the cardinal number N of the set of modulatable coefficients X.

[0422] If this detection probability level, which will be less than that fixed initially at 99.95%, is judged satisfactory, the insertion of a watermarking signal of length equal to N can be effected, that is to say all the coefficients of the sub-band of frequency HH_1 are modulated.

[0423] In a second embodiment of the invention, the insertion method can include a step of calculating a threshold value P* of the length of the watermarking signal w, as illustrated in Figure 14.

[0424] This threshold value P* is determined so that the minimum value α_D of the weighting coefficient is equal to the maximum value α_v of the weighting coefficient for a length P of the watermarking signal w equal to this threshold value P* and a predetermined detection probability level p.

[0425] This calculation step makes it possible to determine, from formulae expressing the detection amplitude α_D and the visual amplitude α_v notably as a function of the length P of the watermarking signal w, the minimum value P* of the insertion signal from which the weighting coefficient α can satisfy the inequality $\alpha_D \leq \alpha \leq \alpha_v$.

[0426] In Figure 14, this minimum value P* is given by the intersection of the two curves representing the variation in the visual amplitude α_v and the variation in the detection amplitude as a function of the length P of the inserted watermarking signal w, for a predetermined detection probability level.

[0427] Thus, in general terms, the insertion method according to the invention has the advantage of being able to control a priori and theoretically the detection probability and imperceptibility of the watermarking signal which it is sought to insert in an image.

[0428] Naturally, many modifications could be made to the example embodiments described above without departing from the scope of the invention.

[0429] Thus the insertion technique used could be applied to the raw digital image, without undergoing any spatio-frequency transformation prior to the modulation of the coefficients.

[0430] In this case, the modulated coefficients are coefficients representing the digital image solely in the spatial domain.

[0431] Moreover, the spatio-frequency transformation applied to the image can use analysis and synthesis filters other than those described above, or even be a transformation other than discrete Fourier transformation, discrete cosine transformation or Fourier-Mellin transformation. These transformations are used currently in conventional processings of digital images.

[0432] In addition, the invention is not limited to the example embodiments described but also concerns any embodiment where the values of the weighting coefficient α, of the length P of the watermarking signal and of the detection probability level p are determined in a correlated fashion so as to satisfy the inequality $\alpha_D \leq \alpha \leq \alpha_v$.

[0433] The present invention also concerns a device for determining a partitioning and a decoding device which are adapted to implement the partitioning and decoding methods described previously.

[0434] These devices for determining a partitioning and decoding can be used in a computer 50 as illustrated in Figure

WAVELYNX EX. 1003, Pg. 1017
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

15, independently or in the same computer 50.

[0435] The partitioning determination device comprises partitioning means 500, 502, 503 adapted to perform an adaptive partitioning according to a criterion of detectability of an information bit inserted on each region.

[0436] These partitioning means use on coding a maximum value α_v of the weighting coefficient ensuring imperceptibility of the watermarking signal for modulating all the coefficients representing said digital image, possibly with a modulation factor k_i dependent on each coefficient, as described previously.

[0437] This device for determining a partitioning also has means 500, 502, 503 of comparing the size P of each region of the partitioning with a minimum size P_{stat} corresponding to minimum size of a statistically significant sample for the detection of a watermarking signal inserted in said region.

[0438] The device also has means 500, 502, 503 for applying a pre-distortion before calculating a detectability criterion.

[0439] The partitioning means comprise means 500, 502, 503 of modulating all the coefficients of each region by inserting the watermarking signal, means 500, 502, 503 of calculating a detectability amplitude from the detectability criterion and means 500, 502, 503 of validating the detectability criterion, adapted to compare the detectability amplitude with a predetermined threshold value Tc.

[0440] The partitioning means 500, 502, 503 are adapted to effect a partitioning by iterative division of the numerical image and, for each region at a rank in the said partitioning, the validation means 500, 502, 503 are adapted to validate a partitioning of a rank higher in the region if and only if there exist at least two subregions of the region for which the detectability criterion is validated.

[0441] This device also comprises means 500, 502, 503 of incrementing the value of a capacity Q of the digital image, adapted, for each region at a rank in the partitioning, to increment the capacity value Q when the partitioning of rank directly higher is not validated, the capacity Q being equal to the cardinal number of the distinct regions obtained by the partitioning on which the detectability criterion is validated.

[0442] In another embodiment, this device for determining a partitioning comprises incrementation means 500, 502, 503 adapted, for each region R at a rank in the partitioning, to increment the value of a capacity Q when the partitioning of rank directly higher is not validated, comparison means 500, 502, 503 adapted to compare the value of the capacity Q with a fixed capacity value Qs and reiteration means 500, 502, 503 adapted to reiterate the partitioning for a region having the highest detectability amongst all the other regions to be processed when the capacity value Q is less than the fixed capacity value Qs.

[0443] In a third embodiment of the invention, the partitioning means 500, 502, 503 are adapted to effect a partitioning by iterative merging of the digital image and there are adapted, for each region of the partitioning for which the detectability criterion is not validated, to merge the region with another region of the partitioning, and preferably with another region of the partitioning for which the detectability criterion is not validated.

[0444] In an entirely similar fashion, the device for decoding a watermarking signal in a digital image comprises means 500, 502, 503 of partitioning the digital image to be decoded into distinct regions, adapted to perform an adaptive partitioning as a function of a criterion of detectability of an information bit obtained by demodulating the coefficients on each region.

[0445] It also has means 500, 502, 503 of comparing the size P of each region R of the partitioning with a minimum size P_{stat} corresponding to the minimum size of a statistically significant sample for the detection of a watermarking signal inserted in the region.

[0446] It comprises means 500, 502, 503 of calculating a detection amplitude from the detectability criterion and means 500, 502, 503 of validating the detectability criterion, adapted to compare the detection amplitude with a predetermined threshold value Td for decoding.

[0447] This predetermined threshold value Td for decoding is less than the predetermined threshold value Tc used during the partitioning determination method described previously.

[0448] In a preferred embodiment, the device for determining a partition includes means 500, 502, 503 for checking a criterion of detectability, over each region, of an information bit inserted by means of a pseudo-random sequence with average of zero by modulation of the coefficients of the region.

[0449] It also includes means 500, 502, 503 for generating a centred pseudo-random sequence equal in size to the cardinal number of the set of coefficients representative of an image, here equal to N.

[0450] Means 500, 502, 503 of modulating the set of coefficients X by the centred pseudo-random sequence in order to insert the same information bit onto this set of coefficients are also incorporated into the device for determining a partition 11 as shown on figure 1.

[0451] The latter may also includes means 500, 502, 503 for applying a distortion D which makes it possible to provide for and guarantee the robustness of the inserted watermark in the case of certain types of distortion, typically a compression of the digital image in order to store it.

[0452] These means of applying a distortion make it possible actually to simulate a predetermined distortion over the set of modulated coefficients. Here they comprise, whenever the coefficients of the set X are spectral coefficients, means 500, 502, 503 for inverse spectral transformation of the set of coefficients modulated in order to obtain a watermarked

WAVELYNX EX. 1003, Pg. 1018
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

image, means 500, 502, 503 for applying a distortion to this watermarked image, and means 500, 502, 503 for spectral transformation of the watermarked image in order to recover the set of modulated coefficients after distortion.

[0453] In this example, the inverse-spectral-transformation means are suitable for implementing multi-resolution spectral wavelet recomposition and the forward spectral transformation means are suitable for again reiterating the breakdown of the digital image I into wavelets.

[0454] The device for determining a partition 11, in a first way, also includes means for partitioning by iterative combination, on the basis of an initial segmentation of the set of coefficients X.

[0455] For preference, this initial segmentation makes it possible to segment the set of coefficients X into a set of regions of a size which is statistically significant for validating the detectability criterion over these regions.

[0456] The means of partitioning 500, 502, 503 by iterative combination are suitable, for each region of the partition for which the detectability criterion is not satisfied, for combining the region with another region of the partition.

[0457] Obviously, the partitioning means 500, 502, 503 could also be suitable for forming this partition of the image by iterative division of the digital image according to a second way of performing the preferred embodiment of the invention.

[0458] This partition-determining device 11 makes it possible, as output, to obtain a partition into regions of the set of coefficients X, with it being possible to insert an information bit onto each of these regions with a reliable detection probability and robustness to a given distortion. The maximum number of regions which can be obtained by this adaptive partitioning of the set X corresponds to the practical insertion capacity of this set X.

[0459] As illustrated in Figure 1, an insertion device 10, incorporating the device for determining a partition 11 described above, moreover comprises means 13 for reading a watermark to be inserted, containing several information bits. By way of an example which is not at all limiting, a binary watermark may be 1000111, representing, for example, the coding of the name of the author of the image to be watermarked.

[0460] The insertion means 12 proper may be conventional and make it possible, by modulation, to insert the various information bits of the watermark onto the various insertion carriers determined by the device for determining a partition 11.

[0461] According to the invention, the device for inserting a watermarking signal w comprises means 500, 502, 503 of spatio-frequency transformation of an image I, and for example analysis filters associated with decimators by two adapted to effect a wavelet decomposition of an image I. It also has reverse spatio-frequency recomposition means 500, 502, 503 for recomposing the image I after the insertion of the watermarking signal in the domain transformed into subbands.

[0462] It also comprises means 500, 502, 503 of inserting a watermarking signal w of length P adapted to modulate a subset of coefficients of cardinal number P according to the linear model described previously using a weighting coefficient α.

[0463] This insertion device also comprises means 500, 502, 503 of calculating the maximum value α_v of the weighting coefficient as a function of the length P of the watermarking signal w ensuring imperceptibility of the watermarking signal. These calculation means use the function $\alpha_v(P, T)$ described above and dependent on the length P of the watermarking signal w and the spectral transformation T used for decomposing the image signal I.

[0464] In general terms, this insertion device also has means 500, 502, 503 of determining compatible values of the length P of the watermarking signal w, the weighting coefficient α and the probability level p so that the value of the weighting coefficient determined is less than or equal to the maximum value α_v and greater than or equal to the minimum value α_D for the determined values of the length P of the watermarking signal w and the detection probability level p.

[0465] The calculation means 500, 502, 503 are also adapted to determine a minimum value or detection amplitude α_D using the calculation functioning described above of the type:

$$\alpha_D(P) = \frac{a(\sqrt{\sigma_X^2 + \sigma_n^2})}{\sqrt{bP - c}}$$

[0466] In one embodiment of the invention, the insertion device also has means of calculating 500, 502, 503 the length P° of the watermarking signal w for a minimum value α_D of the weighting coefficient equal to a maximum value $\alpha_v(N)$ calculated for a length P of the watermarking signals w equal to the cardinal number N of the set of modulatable coefficients ensuring imperceptibility of the watermarking signal w at the limit of perceptibility and for a predetermined detection probability level p; and means 500, 502, 503 of comparing this length P° calculated with the cardinal number N of the set of modulatable coefficients X.

[0467] It also comprises means 500, 502, 503 of calculating a detection probability level p' obtained for a minimum value α_D of the weighting coefficient equal to the maximum value α_v calculated for a length P of the watermarking signal equal to the cardinal number N of the set of modulatable coefficients X.

[0468] In another embodiment, the insertion device comprises means 500, 502, 503 of calculating a threshold value P* of the length of the watermarking signal w determined so that the minimum value α_D of the weighting coefficient is

WAVELYNX EX. 1003, Pg. 1019
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

equal to the maximum value α_v of the weighting coefficient of the length P of the watermarking signal w equal to this threshold value P* and a predetermined detection probability level p.

[0469] All the previously described devices are incorporated in a microprocessor 500 of the computer 50, a read-only memory 502 being adapted to store a program for determining a partitioning and/or inserting a watermarking signal and/or decoding the watermarking signal and a random access memory 503 comprising registers adapted to store variables modified during the running of the programs.

[0470] The microprocessor 500 is integrated into the computer 50, which can be connected to different peripherals, for example a digital camera 507 or a microphone 511, by means of an input/output card 506 in order to receive and store documents.

[0471] The digital camera 507 makes it possible notably to supply images to be authenticated by inserting a watermarking signal.

[0472] This computer 50 has a communication interface 512 connected to a communication network 513 in order to receive, if necessary, images to be watermarked.

[0473] The computer 50 also has document storage means, such as a hard disk 508, or is adapted to cooperate, by means of a disk drive 509, with removable document storage means such as diskettes 510.

[0474] These fixed or removable storage means can also contain the code of the different methods according to the invention which, once read by the microprocessor 500, will be stored on the hard disk 508.

[0475] By way of variant, the program enabling the devices to implement the invention can be stored in the read only memory 502.

[0476] As a second variant, the program can be received in order to be stored as described above by means of the communication network 513.

[0477] The computer 50 also has a screen 504 for serving, for example, as an interface with an operator by means of the keyboard 514 or any other means.

[0478] The central unit 500 (CPU) will execute the instructions relating to the implementation of the invention. On powering up, the programs and methods relating to the invention stored with a non-volatile memory, for example the read only memory 502, are transferred into the random access memory 503 (RAM) which will then contain the executable code of the invention and the variables necessary for implementing the invention.

[0479] This random access memory 503 contains different registers for storing the variables necessary for the running of the program, and notably a register for storing the coefficients of the regions R which are temporarily modulated or demodulated in order to verify the detectability criterion, the minimum value P_{stat}, and the threshold value Tc and Td respectively on coding and decoding.

[0480] This random-access memory 503 also includes an X_i, X_j register for storing the coefficients of the regions which are modulated or demodulated temporarily so as to check the detectability criterion and a register w for storing the centred pseudo-random sequence generated in order to determine the partition of the set X.

[0481] Finally, the random access memory 503 contains a register for storing the table of visual amplitudes of α_{base} (T), a register for storing the spectral coefficients X, a register for calculating the visual amplitude $\alpha_v(N)$ at the limit of imperceptibility, a register for storing the values of the constants a, b, c and of the variance σ_x^2 necessary for determining the detection amplitude α_D as a function of the length P of the watermarking signal w and a register for storing the minimum value P° calculated.

[0482] A communication bus 501 affords communication between the different sub-elements of the computer 50 or linked to it. The representation of the bus 501 is not limitative and notably the microprocessor 500 is able to indicate instructions to any sub-element directly or by means of another sub-element.

Claims

1. Method of inserting a watermarking signal W into a digital image I by modulating coefficients X of distinct regions R representing said digital image I, comprising a step of determining a partitioning into distinct regions of the digital image **characterised in that** the partitioning into regions is effected by an adaptive partitioning as a function of a criterion of statistical detectability of an information bit inserted on each region R.

2. Method according to Claim 1, wherein the modulating of coefficients X is function of a weighting coefficient, **characterised in that** the detectability criterion is calculated by using a maximum value αv of the weighting coefficient ensuring imperceptibility of the watermarking signal for modulating all the coefficients representing said digital image.

3. Method of determining a partitioning according to claim 2, **characterised in that** a maximum value (αv) can be calculated as a function of the length P of the watermarking signal w by:

WAVELYNX EX. 1003, Pg. 1020
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$\alpha_v(P,S,w) = \frac{\alpha_{base}(S)}{P^{1/\beta}(E[|w|^{\beta}])^{1/\beta}}$$

where $\alpha_{base}(S)$ is a base value, dependent on the transformation used S and on the (base) sub-band considered for the insertion, of the maximum weighting coefficient ensuring imperceptibility when a single coefficient of said sub-band is modulated,
β is strictly greater than 2, and
$E[|w|^{\beta}]$ is the mathematical expectation of the function $|w|^{\beta}$.

4. Method according to one of Claims 2 or 3, **characterised in that** the detectability criterion is calculated by using, for each coefficient (X_i) to be modulated, a weighting coefficient in accordance with a law of the form $\alpha_i = k_i.\alpha_v$, where k_i is a modulation factor dependent on the coefficients situated close to the relevant coefficient (X_i) on said region and α_v is equal to said maximum value of the weighting coefficient.

5. Method according to one of claims 1 to 4, **characterised in that** it comprises a step (E307) of applying a distortion before calculating the detectability criterion.

6. Method according to one of Claims 1 to 5, **characterised in that** it includes a prior step (E105) of comparing the size P of each region R of the partitioning with a minimum size P_{stat} corresponding to the minimum size with a statistically significant sample for the detection of a watermarking signal inserted in said region.

7. Method according to one of Claims 1 to 6, **characterised in that**, for each region R of the partitioning, all the coefficients of said region are modulated by inserting the watermarking signal W, a detectability amplitude T is calculated from said detectability criterion and said detectability criterion is validated by comparing said detectability amplitude T with a predetermined threshold value Tc.

8. Method according to claim 7, **characterised in that** said detectability criterion is validated if a minimum modulation length $P_{min}(x)$ calculated for ensuring detectability of the inserted watermarking signal W is less than or equal to the cardinal number of said region R.

9. Method according to claim 1, **characterised in that** it comprises the following steps:

- generation (E501) of a centred pseudo-random sequence w equal in size to the cardinal number N of a set of coefficients representative of at least a part of an image I, formed from centred pseudo-random sub-sequences w^k;
- modulation (E502) of the said set of coefficients by the said centred pseudo-random sequence w in order to insert the same information bit on the said set of coefficients; and
- checking (E506, E507, E514, E516), over each region, of a criterion of detectability of the information bit inserted by modulation.

10. Method according to Claim 9, **characterised in that** it comprises a single step of applying a distortion (E503) to the said set of modulated coefficients, before the step of checking (E506, E507, E514, E516) of a detectability criterion.

11. Method according to Claim 10, **characterised in that** the said set of coefficients is a set of spectral coefficients X originating from a spectral transformation of a digital image, and **in that** the said step (E503) of applying a distortion includes the following sub-steps:

- inverse spectral transformation (E503a) of the said set of modulated coefficients in order to obtain a watermarked image;
- application (E503b) of a distortion to the said watermarked image; and
- spectral transformation (E503c) of the watermarked image in order to obtain a set of modulated coefficients after distortion.

12. Method according to one of Claims 9 to 11, **characterised in that** the centred pseudo-random sequence w is formed from pseudo-random sub-sequences w^k of identical size.

WAVELYNX EX. 1003, Pg. 1021
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

13. Method according to one of Claims 9 to 12, **characterised in that** the pseudo-random sub-sequences w^k have a size greater than or equal to a minimum number of coefficients forming a region of the said partition of a size which is statistically significant for validating the said criterion of detectability over the said region.

14. Method according to one of Claims 9 to 13, **characterised in that**, at the generation step (E501), each centred pseudo-random sub-sequence w^k is created by generating half of the pseudo-random samples of the said sub-sequence via a pseudo-random number generator and by symmetrising the said pseudo-random samples generated.

15. Method according to Claim 14, **characterised in that**, at the generation step (E501), each centred pseudo-random sub-sequence w^k is created by moreover permutating the said pseudo-random samples using a secret key.

16. Method according to one of Claims 9 to 13, **characterised in that**, at the generation step (E501), each centred pseudo-random sub-sequence w^k is created by generating pseudo-random random samples via a pseudo-random number generator and by redistributing over each sample the sum of the said pseudo-random samples generated.

17. Method according to one of Claims 7 to 16, **characterised in that** a partitioning by iterative division (E103) of the digital image is effected and **in that**, for each region at a rank of said partitioning, a partitioning of a directly higher rank of said region is validated if and only if there exist at least two sub-regions of said region for which said detectability criterion is validated.

18. Method according to Claim 17, **characterised in that**, for each region at a rank of said partitioning, the value of a capacity Q of the digital image is incremented (E112) when the partitioning of directly higher rank is not validated, said capacity Q being equal to the cardinal number of the distinct regions obtained by said partitioning on which the detectability criterion is validated.

19. Method according to Claim 18, **characterised in that**, for each region at a rank of said partitioning, the value of a capacity Q is incremented (E112) when the partitioning of immediately high rank is not validated, said value of the capacity Q is compared (E115) with a fixed capacity value Qs and the partitioning is reiterated for a region having the highest detectability amplitude amongst all the other regions to be processed when said capacity value is lower than said fixed capacity value.

20. Method according to one of Claims 7 to 16, **characterised in that** a partitioning by iterative merging of the digital image is effected and **in that**, for each region of said partitioning for which said detectability criterion is not validated, said region is merged with another region of said partitioning.

21. Method according to Claim 20, **characterised in that** said other region of the partitioning is if possible a region for which said detectability criterion is not validated.

22. Method of decoding a watermarking signal in a digital image, inserted by modulating coefficients X representing said image in distinct regions forming a partitioning of said digital image, **characterised in that** a partitioning into distinct regions R of the digital image to be decoded is determined by effecting an adaptive partitioning as a function of a criterion of statistical detectability of an information bit obtained by demodulating coefficients on each region R.

23. Decoding method according to Claim 22, **characterised in that** it includes a prior step (E201) of comparing the size P of each region of the partitioning with a minimum size P_{stat} corresponding to the minimum size of a statistically significant sample for the detection of a watermarking signal inserted in said region.

24. Decoding method according to one of Claims 22 or 23, **characterised in that**, for each region R of the partitioning, a detection amplitude T is calculated (E203) from said detectability criterion and said detectability criterion is validated (E203) by comparing said detection amplitude T with a predetermined threshold value Td for decoding.

25. Decoding method according to Claim 24, **characterised in that** the predetermined threshold value Td for decoding is less than said predetermined threshold value Tc used during the inserting method according to Claim 7.

26. Device for inserting a watermarking signal into a digital image by modulating coefficients of regions representing said digital image, comprising means for partitioning into distinct regions the digital image **characterised in that** partitioning means (500, 502, 503) are adapted to effect an adaptive partitioning as a function of a criterion of statistical detectability of an information bit inserted on each region.

WAVELYNX EX. 1003, Pg. 1022
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

27. Device according to claim 26, **characterised in that** it also includes means (500, 502, 503) for applying a distortion before calculating the detectability criterion.

28. Device according to one of claims 26 to 27, **characterised in that** it also has means (500, 502, 503) of comparing the size of each region of the partitioning with a minimum size corresponding to the minimum size of a statistically significant sample for the detection of a watermarking signal inserted in the said region.

29. Device according to one of Claims 26 to 28, **characterised in that** the partitioning means (500, 502, 503) comprise means (500, 502, 503) of modulating all the coefficients of each region by inserting the watermarking signal, means (500, 502, 503) of calculating a detectability amplitude from said detectability criterion and means (500, 502, 503) of validating said detectability criterion, adapted to compare said detectability amplitude with a predetermined threshold value.

30. Device according to claim 26, **characterised in that** it includes:

- means (500, 502, 503) for generating a centred pseudo-random sequence w equal in size to the cardinal number N of a set of coefficients representative of at least a part of an image I, formed by centred pseudo-random sub-sequences w^k;
- means (500, 502, 503) for modulation of the said set of coefficients by the said centred pseudo-random sequence w in order to insert the same information bit on the said set of coefficients; and
- means (500, 502, 503) for checking, over each region, a criterion of detectability of the information bit inserted by modulation.

31. Device according to Claim 30, **characterised in that** it comprises means (500, 502, 503) for applying a distortion to the said set of modulated coefficients.

32. Device according to Claim 31, **characterised in that** the said set of coefficients is a set of spectral coefficients Xi originating from a spectral transformation of a digital image, and **in that** the said means for applying a distortion comprise:

- means (500, 502, 503) for inverse spectral transformation of the said set of modulated coefficients in order to obtain a watermarked image;
- means (500, 502, 503) for application of a distortion to the said watermarked image; and
- means (500, 502, 503) for spectral transformation of the watermarked image in order to obtain a set of modulated coefficients after distortion.

33. Device according to one of Claims 29 to 32, **characterised in that** the partitioning means (500, 502, 503) are adapted to effect a partitioning by iterative division of the digital image and **in that**, for each region at a rank of said partitioning, the validation means are adapted to validate a partitioning of a directly higher rank of said region if and only if there exist at least two sub-regions of said regions for which said detectability criterion is validated.

34. Device according to Claim 33, **characterised in that** it also comprises means (500, 502, 503) of incrementing the value of a capacity of the digital image adapted, for each region at a rank of said partitioning, to increment the said capacity value when the partitioning of directly higher rank is not validated, said capacity being equal to the cardinal number of the distinct regions obtained by said partitioning on which the detectability criterion is validated.

35. Device according to Claim 33, **characterised in that** it also comprises incrementation means (500, 502, 503) adapted, for each region at a rank of said partitioning, to increment the value of a capacity when the partitioning of directly higher rank is not validated, comparison means (500, 502, 503) adapted to compare said value of the capacity with a fixed capacity value and reiteration means (500, 502, 503) adapted to reiterate the partitioning for a region having the highest detectability amplitude amongst all the other regions to be processed when said capacity value is lower than said fixed capacity value.

36. Device according to one of Claims 29 to 32, **characterised in that** the partitioning means (500, 502, 503) are adapted to effect a partitioning by iterative merging of the digital image and are adapted, for each region of said partitioning for which said detectability criterion is not validated, to merge said region with another region of said partitioning.

WAVELYNX EX. 1003, Pg. 1023
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

37. Device according to Claim 36, **characterised in that** said other region of the partitioning is if possible a region for which said detectability criterion is not validated.

38. Device according to one of Claims 26 to 37, **characterised in that** it is incorporated in a microprocessor (500), a read only memory (502) being adapted to store a program for determining a partitioning and a random access memory (503) comprising registers adapted to store variables modified during the running of said program.

39. Device for decoding a watermarking signal in a digital image, inserted by modulation of coefficients representing said image in distinct regions forming a partitioning of said digital image, **characterised in that** it comprises means (500, 502, 503) of partitioning of the digital image to be decoded into distinct regions, adapted to effect an adaptive partitioning as a function of a criterion of statistical detectability of an information bit obtained by demodulation of the coefficients on each region.

40. Decoding device according to Claim 39, **characterised in that** it also has means (500, 502, 503) of comparing the size of each region of the partitioning with a minimum size corresponding to the minimum size of a statistical significant sample for the detection of a watermarking signal inserted in said region.

41. Decoding device according to one of Claims 39 or 40, **characterised in that** it comprises means (500, 502, 503) of calculating a detection amplitude from said detectability criterion and means (500, 502, 503) of validating said detectability criterion adapted to compare said detection amplitude with a threshold value predetermined for the decoding.

42. Decoding device according to Claim 41, **characterised in that** the predetermined threshold value for the decoding is less than said predetermined threshold value used during the inserting method according to Claim 7.

43. Decoding device according to one of Claims 39 to 42, **characterised in that** it is incorporated in a microprocessor (500), a read only memory (502) being adapted to store a program for decoding a watermarking signal and a random access memory (503) comprising registers adapted to store variables modified during the running of said program.

44. Computer, **characterised in that** it comprises means adapted to implement an inserting method according to one of Claims 1 to 21.

45. Computer, **characterised in that** it comprises means adapted to implement the decoding method according to one of Claims 22 to 25.

46. Information storage means readable by a microprocessor, **characterised in that** it stores a program implementing an inserting method according to one of Claims 1 to 21.

47. Information storage means readable by a microprocessor, **characterised in that** it stores a program implementing a decoding method according to one of Claims 22 to 25.

Patentansprüche

1. Verfahren zum Einfügen eines Wasserzeichensignals W in ein digitales Bild I durch Modulieren von Koeffizienten X von verschiedenen Bereichen R, die das digitale Bild I darstellen, mit einem Schritt zum Bestimmen einer Partitionierung des digitalen Bildes in verschiedene Bereiche, **dadurch gekennzeichnet, dass** die Partitionierung in Bereiche durch eine adaptive Partitionierung als Funktion eines Kriteriums einer statistischen Erfassbarkeit eines in jedem Bereich R eingefügten Informationsbits ausgeführt wird.

2. Verfahren gemäß Anspruch 1, bei dem das Modulieren von Koeffizienten X eine Funktion eines Gewichtungskoeffizienten ist, **dadurch gekennzeichnet, dass** das Erfassbarkeitskriterium durch Verwendung eines Höchstwerts αv des Gewichtungskoeffizienten berechnet wird, der eine Nichtwahrnehmbarkeit des Wasserzeichensignals für eine Modulation aller Koeffizienten sicherstellt, die das digitale Bild darstellen.

3. Verfahren zum Bestimmen einer Partitionierung gemäß Anspruch 2, **dadurch gekennzeichnet, dass** ein Höchstwert (αv) als Funktion der Länge P des Wasserzeichensignals w berechnet werden kann durch:

WAVELYNX EX. 1003, Pg. 1024
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$\alpha_v(P,S,w) = \frac{\alpha_{Basis}(S)}{p^{1/\beta}\left(E\left[|w|^{\beta}\right]\right)^{1/\beta}},$$

wobei $\alpha_{Basis}(S)$ ein Basiswert, der von der verwendeten Transformation S und von dem für die Einfügung in Betracht gezogenen (Basis-)Teilband abhängig ist, von dem maximalen Gewichtungskoeffizienten ist, der eine Nichtwahrnehmbarkeit sicherstellt, wenn ein einziger Koeffizient des Teilbands moduliert wird,
β größer ist als 2, und
$E[|w|^{\beta}]$ der mathematische Erwartungswert der Funktion $|w|^{\beta}$ ist.

4. Verfahren gemäß einem der Ansprüche 2 oder 3, **dadurch gekennzeichnet, dass** das Erfassbarkeitskriterium berechnet wird, indem für jeden zu modulierenden Koeffizienten (X_i) ein Gewichtungskoeffizient gemäß einem Gesetz in der Form $\alpha_i = k_i \cdot \alpha_v$ verwendet wird, wobei k_i ein Modulationsfaktor ist, der von den Koeffizienten abhängig ist, die sich nahe an dem maßgeblichen Koeffizienten (X_i) in dem Bereich befinden, und α_v gleich dem Höchstwert des Gewichtungskoeffizienten ist.

5. Verfahren gemäß einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** es einen Schritt (E307) zum Anwenden einer Verzerrung vor einer Berechnung des Erfassbarkeitskriteriums aufweist.

6. Verfahren gemäß einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** es einen vorherigen Schritt (E105) zum Vergleichen der Größe P von jedem Bereich R der Partitionierung mit einer Mindestgröße P_{stat} aufweist, die der Mindestgröße eines statistisch signifikanten Abtastwerts für die Erfassung eines in dem Bereich eingefügten Wasserzeichensignals entspricht.

7. Verfahren gemäß einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** für jeden Bereich R der Partitionierung alle Koeffizienten des Bereichs moduliert werden, indem das Wasserzeichensignal W eingefügt wird, eine Erfassbarkeitsamplitude T aus dem Erfassbarkeitskriterium berechnet wird und das Erfassbarkeitskriterium durch Vergleich der Erfassbarkeitsamplitude T mit einem vorbestimmten Schwellenwert Tc validiert wird.

8. Verfahren gemäß Anspruch 7, **dadurch gekennzeichnet, dass** das Erfassbarkeitskriterium validiert wird, wenn eine minimale Modulationslänge $P_{min}(x)$, die zum Sicherstellen einer Erfassbarkeit des eingefügten Wasserzeichensignals W berechnet wird, kleiner oder gleich der Kardinalzahl des Bereichs R ist.

9. Verfahren gemäß Anspruch 1, **dadurch gekennzeichnet, dass** es die folgenden Schritte aufweist:

   - Erzeugung (E501) einer zentrierten Pseudozufallssequenz w, die größenmäßig gleich der Kardinalzahl N einer Menge von Koeffizienten ist, die für zumindest einen Teil eines Bildes I repräsentativ sind, wobei sie aus zentrierten Pseudozufallsuntersequenzen w^k gebildet wird;
   - Modulation (E502) der Menge von Koeffizienten durch die zentrierte Pseudozufallssequenz w, um das gleiche Informationsbit in die Menge von Koeffizienten einzufügen; und
   - Überprüfung (E506, E507, E514, E516) eines Kriteriums einer Erfassbarkeit des durch Modulation eingefügten Informationsbits über jeden Bereich.

10. Verfahren gemäß Anspruch 9, **dadurch gekennzeichnet, dass** es einen einzigen Schritt zum Anwenden einer Verzerrung (E503) auf die Menge von modulierten Koeffizienten vor dem Schritt der Überprüfung (E506, E507, E514, E516) eines Erfassbarkeitskriteriums aufweist.

11. Verfahren gemäß Anspruch 10, **dadurch gekennzeichnet, dass** die Menge von Koeffizienten eine Menge von Spektralkoeffizienten X ist, die aus einer Spektraltransformation eines digitalen Bildes stammen, und dass der Schritt (E503) zum Anwenden einer Verzerrung die folgenden Unterschritte aufweist:

   - inverse Spektraltransformation (E503a) der Menge von modulierten Koeffizienten, um ein mit Wasserzeichen versehenes Bild zu erhalten;
   - Anwendung (E503b) einer Verzerrung auf das mit Wasserzeichen versehene Bild; und
   - Spektraltransformation (E503c) des mit Wasserzeichen versehenen Bildes, um eine Menge von modulierten

WAVELYNX EX. 1003, Pg. 1025
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Koeffizienten nach einer Verzerrung zu erhalten.

12. Verfahren gemäß einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet, dass** die zentrierte Pseudozufallssequenz w aus Pseudozufallsuntersequenzen w^k identischer Größe gebildet wird.

13. Verfahren gemäß einem der Ansprüche 9 bis 12, **dadurch gekennzeichnet, dass** die Pseudozufallsuntersequenzen w^k eine Größe aufweisen, die größer oder gleich einer minimalen Anzahl von Koeffizienten ist, die einen Bereich der Partitionierung mit einer Größe bilden, die für eine Validierung des Erfassbarkeitskriteriums über den Bereich statistisch signifikant ist.

14. Verfahren gemäß einem der Ansprüche 9 bis 13, **dadurch gekennzeichnet, dass** im Erzeugungsschritt (E501) jede zentrierte Pseudozufallsuntersequenz w^k erstellt wird, indem die Hälfte der Pseudozufallsabtastwerte der Untersequenz über einen Pseudozufallszahlengenerator erzeugt wird, und indem die erzeugten Pseudozufallsabtastwerte symmetrisch gemacht werden.

15. Verfahren gemäß Anspruch 14, **dadurch gekennzeichnet, dass** im Erzeugungsschritt (E501) jede zentrierte Pseudozufallsuntersequenz w^k erstellt wird, indem außerdem die Pseudozufallsabtastwerte unter Verwendung eines geheimen Schlüssels permutiert werden.

16. Verfahren gemäß einem der Ansprüche 9 bis 13, **dadurch gekennzeichnet, dass** im Erzeugungsschritt (E501) jede zentrierte Pseudozufallsuntersequenz w^k erstellt wird, indem Pseudozufallsabtastwerte über einen Pseudozufallszahlengenerator erzeugt werden, und indem die Summe der erzeugten Pseudozufallsabtastwerte über jeden Abtastwert umverteilt wird.

17. Verfahren gemäß einem der Ansprüche 7 bis 16, **dadurch gekennzeichnet, dass** eine Partitionierung durch iterative Aufteilung (E103) des digitalen Bildes ausgeführt wird, und dass für jeden Bereich auf einer Ebene der Partitionierung eine Partitionierung einer direkt höheren Ebene des Bereichs validiert wird, wenn und nur wenn zumindest zwei Unterbereiche des Bereichs existieren, für die das Erfassbarkeitskriterium validiert wird.

18. Verfahren gemäß Anspruch 17, **dadurch gekennzeichnet, dass** für jeden Bereich auf einer Ebene der Partitionierung der Wert einer Kapazität Q des digitalen Bildes inkrementiert wird (E112), wenn die Partitionierung einer direkt höheren Ebene nicht validiert wird, wobei die Kapazität Q gleich der Kardinalzahl der verschiedenen durch die Partitionierung erhaltenen Bereiche ist, in denen das Erfassbarkeitskriterium validiert wird.

19. Verfahren gemäß Anspruch 18, **dadurch gekennzeichnet, dass** für jeden Bereich auf einer Ebene der Partitionierung der Wert einer Kapazität Q inkrementiert wird (E112), wenn die Partitionierung einer unmittelbar höheren Ebene nicht validiert wird, wobei der Wert der Kapazität Q mit einem festen Kapazitätswert Qs verglichen wird (E115) und die Partitionierung für einen Bereich wiederholt wird, der unter all den anderen zu verarbeitenden Bereichen die höchste Erfassbarkeitsamplitude aufweist, wenn der Kapazitätswert kleiner ist als der feste Kapazitätswert.

20. Verfahren gemäß einem der Ansprüche 7 bis 16, **dadurch gekennzeichnet, dass** eine Partitionierung durch iteratives Vereinigen des digitalen Bildes ausgeführt wird, und dass für jeden Bereich der Partitionierung, für den das Erfassbarkeitskriterium nicht validiert wird, dieser Bereich mit einem anderen Bereich der Partitionierung vereinigt wird.

21. Verfahren gemäß Anspruch 20, **dadurch gekennzeichnet, dass** der andere Bereich der Partitionierung, wenn möglich, ein Bereich ist, für den das Erfassbarkeitskriterium nicht validiert wird.

22. Verfahren zum Decodieren eines Wasserzeichensignals in einem digitalen Bild, das durch Modulieren von Koeffizienten X, die das Bild darstellen, in verschiedenen Bereichen, die eine Partitionierung des digitalen Bildes bilden, eingefügt ist, **dadurch gekennzeichnet, dass** eine Partitionierung in verschiedene Bereiche R des zu decodierenden digitalen Bildes bestimmt wird, indem eine adaptive Partitionierung als Funktion eines Kriteriums einer statistischen Erfassbarkeit eines Informationsbits ausgeführt wird, das durch Demodulieren von Koeffizienten in jedem Bereich R erhalten wird.

23. Decodierverfahren gemäß Anspruch 22, **dadurch gekennzeichnet, dass** es einen vorherigen Schritt (E201) zum Vergleichen der Größe P von jedem Bereich der Partitionierung mit einer Mindestgröße P_{stat} aufweist, die der

WAVELYNX EX. 1003, Pg. 1026
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Mindestgröße eines statistisch signifikanten Abtastwerts für die Erfassung eines in dem Bereich eingefügten Wasserzeichensignals entspricht.

24. Decodierverfahren gemäß einem der Ansprüche 22 oder 23, **dadurch gekennzeichnet, dass** für jeden Bereich R der Partitionierung eine Erfassungsamplitude T aus dem Erfassbarkeitskriterium berechnet wird (E203) und das Erfassbarkeitskriterium validiert wird (E203), indem die Erfassungsamplitude T mit einem vorbestimmten Schwellenwert Td für eine Decodierung verglichen wird.

25. Decodierverfahren gemäß Anspruch 24, **dadurch gekennzeichnet, dass** der vorbestimmten Schwellenwert Td für eine Decodierung kleiner ist als der vorbestimmte Schwellenwert Tc, der während des Einfügungsverfahrens gemäß Anspruch 7 verwendet wird.

26. Vorrichtung zum Einfügen eines Wasserzeichensignals in ein digitales Bild durch Modulieren von Koeffizienten von Bereichen, die das digitale Bild darstellen, mit einer Einrichtung zum Partitionieren des digitalen Bildes in verschiedene Bereiche, **dadurch gekennzeichnet, dass** eine Partitioniereinrichtung (500, 502, 503) angepasst ist zum Ausführen einer adaptiven Partitionierung als Funktion eines Kriteriums einer statistischen Erfassbarkeit eines in jedem Bereich eingefügten Informationsbits.

27. Vorrichtung gemäß Anspruch 26, **dadurch gekennzeichnet, dass** sie auch eine Einrichtung (500, 502, 503) zum Anwenden einer Verzerrung vor einer Berechnung des Erfassbarkeitskriteriums umfasst.

28. Vorrichtung gemäß einem der Ansprüche 26 bis 27, **dadurch gekennzeichnet, dass** sie auch eine Einrichtung (500, 502, 503) zum Vergleichen der Größe von jedem Bereich der Partitionierung mit einer Mindestgröße umfasst, die der Mindestgröße eines statistisch signifikanten Abtastwerts für die Erfassung eines in dem Bereich eingefügten Wasserzeichensignals entspricht.

29. Vorrichtung gemäß einem der Ansprüche 26 bis 28, **dadurch gekennzeichnet, dass** die Partitioniereinrichtung (500, 502, 503) eine Einrichtung (500, 502, 503) zum Modulieren aller Koeffizienten von jedem Bereich durch Einfügen des Wasserzeichensignals, eine Einrichtung (500, 502, 503) zum Berechnen einer Erfassbarkeitsamplitude aus dem Erfassbarkeitskriterium und eine Einrichtung (500, 502, 503) zum Validieren des Erfassbarkeitskriteriums aufweist, die angepasst ist zum Vergleichen der Erfassbarkeitsamplitude mit einem vorbestimmten Schwellenwert.

30. Vorrichtung gemäß Anspruch 26, **dadurch gekennzeichnet, dass** sie umfasst:

- eine Einrichtung (500, 502, 503) zum Erzeugen einer zentrierten Pseudozufallssequenz w, die größenmäßig gleich der Kardinalzahl N einer Menge von Koeffizienten ist, die für zumindest einen Teil eines Bildes I repräsentativ sind, wobei sie durch zentrierte Pseudozufallsuntersequenzen w^k gebildet wird;
- eine Einrichtung (500, 502, 503) für eine Modulation der Menge von Koeffizienten durch die zentrierte Pseudozufallssequenz w, um das gleiche Informationsbit in die Menge von Koeffizienten einzufügen; und
- eine Einrichtung (500, 502, 503) zum Überprüfen eines Kriteriums einer Erfassbarkeit des durch Modulation eingefügten Informationsbits über jeden Bereich.

31. Vorrichtung gemäß Anspruch 30, **dadurch gekennzeichnet, dass** sie eine Einrichtung (500, 502, 503) zum Anwenden einer Verzerrung auf die Menge von modulierten Koeffizienten aufweist.

32. Vorrichtung gemäß Anspruch 31, **dadurch gekennzeichnet, dass** die Menge von Koeffizienten ein Menge von Spektralkoeffizienten Xi ist, die aus einer Spektraltransformation eines digitalen Bildes stammen, und dass die Einrichtung zum Anwenden einer Verzerrung aufweist:

- eine Einrichtung (500, 502, 503) für eine inverse Spektraltransformation der Menge von modulierten Koeffizienten, um ein mit Wasserzeichen versehenes Bild zu erhalten;
- eine Einrichtung (500, 502, 503) zur Anwendung einer Verzerrung auf das mit Wasserzeichen versehene Bild; und
- eine Einrichtung (500, 502, 503) für eine Spektraltransformation des mit Wasserzeichen versehenen Bildes, um eine Menge von modulierten Koeffizienten nach einer Verzerrung zu erhalten.

33. Vorrichtung gemäß einem der Ansprüche 29 bis 32, **dadurch gekennzeichnet, dass** die Partitioniereinrichtung (500, 502, 503) angepasst ist zum Ausführen einer Partitionierung durch iterative Aufteilung des digitalen Bildes,

WAVELYNX EX. 1003, Pg. 1027
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

und dass die Validierungseinrichtung für jeden Bereich auf einer Ebene der Partitionierung angepasst ist, eine Partitionierung einer direkt höheren Ebene des Bereichs zu validieren, wenn und nur wenn zumindest zwei Unterbereiche des Bereichs existieren, für die das Erfassbarkeitskriterium validiert wird.

34. Vorrichtung gemäß Anspruch 33, **dadurch gekennzeichnet, dass** sie auch eine Einrichtung (500, 502, 503) zum Inkrementieren des Werts einer Kapazität des digitalen Bildes aufweist, die für jeden Bereich auf einer Ebene der Partitionierung angepasst ist zum Inkrementieren des Kapazitätswerts, wenn die Partitionierung einer direkt höheren Ebene nicht validiert wird, wobei die Kapazität gleich der Kardinalzahl der verschiedenen durch die Partitionierung erhaltenen Bereiche ist, in denen das Erfassbarkeitskriterium validiert wird.

35. Vorrichtung gemäß Anspruch 33, **dadurch gekennzeichnet, dass** sie auch aufweist: eine Inkrementierungseinrichtung (500, 502, 503), die für jeden Bereich auf einer Ebene der Partitionierung angepasst ist zum Inkrementieren des Werts einer Kapazität, wenn die Partitionierung einer direkt höheren Ebene nicht validiert wird, eine Vergleichseinrichtung (500, 502, 503), die angepasst ist zum Vergleichen des Werts der Kapazität mit einem festen Kapazitätswert, und eine Wiederholungseinrichtung (500, 502, 503), die angepasst ist zum Wiederholen der Partitionierung für einen Bereich, der unter all den anderen zu verarbeitenden Bereichen die höchste Erfassbarkeitsamplitude aufweist, wenn der Kapazitätswert kleiner ist als der feste Kapazitätswert.

36. Vorrichtung gemäß einem der Ansprüche 29 bis 32, **dadurch gekennzeichnet, dass** die Partitioniereinrichtung (500, 502, 503) angepasst ist zum Ausführen einer Partitionierung durch iteratives Vereinigen des digitalen Bildes und für jeden Bereich der Partitionierung, für den das Erfassbarkeitskriterium nicht validiert wird, angepasst ist zum Vereinigen des Bereichs mit einem anderen Bereich der Partitionierung.

37. Vorrichtung gemäß Anspruch 36, **dadurch gekennzeichnet, dass** der andere Bereich der Partitionierung, wenn möglich, ein Bereich ist, für den das Erfassbarkeitskriterium nicht validiert wird.

38. Vorrichtung gemäß einem der Ansprüche 26 bis 37, **dadurch gekennzeichnet, dass** sie in einem Mikroprozessor (500) eingebunden ist, wobei ein Festwertspeicher (502) angepasst ist zum Speichern eines Programms zum Bestimmen einer Partitionierung und ein Direktzugriffsspeicher (503) Register aufweist, die angepasst sind zum Speichern von Variablen, die während des Ablaufs des Programms modifiziert werden.

39. Vorrichtung zum Decodieren eines Wasserzeichensignals in einem digitalen Bild, das durch Modulieren von Koeffizienten, die das Bild darstellen, in verschiedenen Bereichen, die eine Partitionierung des digitalen Bildes bilden, eingefügt ist, **dadurch gekennzeichnet, dass** sie eine Einrichtung (500, 502, 503) zum Partitionieren des zu decodierenden digitalen Bildes in verschiedene Bereiche aufweist, die angepasst ist zum Ausführen einer adaptiven Partitionierung als Funktion eines Kriteriums einer statistischen Erfassbarkeit eines Informationsbits, das durch Demodulieren der Koeffizienten in jedem Bereich erhalten wird.

40. Decodiervorrichtung gemäß Anspruch 39, **dadurch gekennzeichnet, dass** sie auch eine Einrichtung (500, 502, 503) zum Vergleichen der Größe von jedem Bereich der Partitionierung mit einer Mindestgröße aufweist, die der Mindestgröße eines statistisch signifikanten Abtastwerts für die Erfassung eines in dem Bereich eingefügten Wasserzeichensignals entspricht.

41. Decodiervorrichtung gemäß einem der Ansprüche 39 oder 40, **dadurch gekennzeichnet, dass** sie eine Einrichtung (500, 502, 503) zum Berechnen einer Erfassungsamplitude aus dem Erfassbarkeitskriterium und eine Einrichtung (500, 502, 503) zum Validieren des Erfassbarkeitskriteriums aufweist, die angepasst ist zum Vergleichen der Erfassungsamplitude mit einem für die Decodierung vorbestimmten Schwellenwert.

42. Decodiervorrichtung gemäß Anspruch 41, **dadurch gekennzeichnet, dass** der vorbestimmte Schwellenwert für die Decodierung kleiner ist als der vorbestimmte Schwellenwert, der während des Einfügungsverfahrens gemäß Anspruch 7 verwendet wird.

43. Decodiervorrichtung gemäß einem der Ansprüche 39 bis 42, **dadurch gekennzeichnet, dass** sie in einem Mikroprozessor (500) eingebunden ist, wobei ein Festwertspeicher (502) angepasst ist zum Speichern eines Programms zum Decodieren eines Wasserzeichensignals und ein Direktzugriffsspeicher (503) Register aufweist, die angepasst sind zum Speichern von Variablen, die während des Ablaufs des Programms modifiziert werden.

44. Computer, **dadurch gekennzeichnet, dass** dieser eine Einrichtung aufweist, die angepasst ist zum Implementieren

WAVELYNX EX. 1003, Pg. 1028
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

eines Einfügungsverfahrens gemäß einem der Ansprüche 1 bis 21.

45. Computer, **dadurch gekennzeichnet, dass** dieser eine Einrichtung aufweist, die angepasst ist zum Implementieren des Decodierverfahrens gemäß einem der Ansprüche 22 bis 25.

46. Informationsspeichereinrichtung, die von einem Mikroprozessor lesbar ist, **dadurch gekennzeichnet, dass** sie ein Programm speichert, das ein Einfügungsverfahren gemäß einem der Ansprüche 1 bis 21 implementiert.

47. Informationsspeichereinrichtung, die von einem Mikroprozessor lesbar ist, **dadurch gekennzeichnet, dass** sie ein Programm speichert, das ein Decodierverfahren gemäß einem der Ansprüche 22 bis 25 implementiert.

Revendications

1. Procédé d'insertion d'un signal de marquage W dans une image numérique I en modulant des coefficients X de régions distinctes R représentant ladite image numérique I, comportant une étape consistant à déterminer un partitionnement en régions distinctes de l'image numérique **caractérisé en ce que** le partitionnement en régions est effectué par l'intermédiaire d'un partitionnement adaptatif en fonction d'un critère de détectabilité statistique d'un bit d'informations inséré sur chaque région R.

2. Procédé selon la revendication 1, dans lequel la modulation de coefficients X est fonction d'un coefficient pondérateur, **caractérisé en ce que** le critère de détectabilité est calculé en utilisant une valeur maximum αv du coefficient pondérateur assurant l'imperceptibilité du signal de marquage pour moduler tous les coefficients représentant ladite image numérique.

3. Procédé de détermination d'un partitionnement selon la revendication 2, **caractérisé en ce qu'**une valeur maximum (αv) peut être calculée en fonction de la longueur P du signal de marquage w par :

$$\alpha_v(P,S,w) = \frac{\alpha_{base}(S)}{P^{1/\beta}\left(E[|w|^{\beta}]\right)^{1/\beta}}$$

où $\alpha_{base}(S)$ est une valeur de base, dépendante de la transformation utilisée S et de la sous-bande (base) considérée pour l'insertion, du coefficient pondérateur maximum assurant l'imperceptibilité lorsqu'un coefficient unique de ladite sous-bande est modulé,
β est strictement supérieur à 2, et
$E[|w|^{\beta}]$ est l'espérance mathématique de la fonction $|w|^{\beta}$.

4. Procédé selon l'une des revendications 2 et 3, **caractérisé en ce que** le critère de détectabilité est calculé en utilisant, pour chaque coefficient (X_i) à moduler, un coefficient pondérateur conformément à une loi de la forme $\alpha_i = k_i.\alpha_v$, où k_i est un facteur de modulation dépendant des coefficients situés à proximité du coefficient approprié (X_i) sur ladite région et α_v est égal à ladite valeur maximum du coefficient pondérateur.

5. Procédé selon l'une des revendications 1 à 4, **caractérisé en ce qu'**il comporte une étape (E307) consistant à appliquer une distorsion avant de calculer le critère de détectabilité.

6. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce qu'**il inclut une étape préalable (E105) consistant à comparer la taille P de chaque région R du partitionnement à une taille minimum P_{stat} correspondant à la taille minimum avec un échantillon statistiquement significatif pour la détection d'un signal de marquage inséré dans ladite région.

7. Procédé selon l'une des revendications 1 à 6, **caractérisé en ce que**, pour chaque région R du partitionnement, tous les coefficients de ladite région sont modulés en insérant le signal de marquage W, une amplitude de détectabilité T est calculée à partir dudit critère de détectabilité et ledit critère de détectabilité est validé en comparant ladite amplitude de détectabilité T à une valeur de seuil prédéterminée Tc.

WAVELYNX EX. 1003, Pg. 1029
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

8. Procédé selon la revendication 7, **caractérisé en ce que** ledit critère de détectabilité est validé si une longueur de modulation minimum $P_{min(}x)$ calculée pour assurer la détectabilité du signal de marquage inséré W est inférieure ou égale au nombre cardinal de ladite région R.

9. Procédé selon la revendication 1, **caractérisé en ce qu'**il comporte les étapes suivantes :

- la génération (E501) d'une séquence pseudo-aléatoire centrée w égale en taille au nombre cardinal N d'un ensemble de coefficients représentatifs d'au moins une partie d'une image I, formée à partir de sous-séquences pseudo-aléatoires centrées w^k,
- la modulation (E502) dudit ensemble de coefficients par ladite séquence pseudo-aléatoire centrée w afin d'insérer le même bit d'informations sur ledit ensemble de coefficients, et
- le contrôle (E506, E507, E514, E516), sur chaque région, d'un critère de détectabilité du bit d'informations inséré par modulation.

10. Procédé selon la revendication 9, **caractérisé en ce qu'**il comporte une étape unique d'application d'une distorsion (E503) audit ensemble de coefficients modulés, avant l'étape de contrôle (E506, E507, E514, E516) d'un critère de détectabilité.

11. Procédé selon la revendication 10, **caractérisé en ce que** ledit ensemble de coefficients est un ensemble de coefficients spectraux X provenant d'une transformation spectrale d'une image numérique, et **en ce que** ladite étape (E503) consistant à appliquer une distorsion inclut les sous-étapes suivantes :

- la transformation spectrale inverse (E503a) dudit ensemble de coefficients modulés afin d'obtenir une image marquée,
- l'application (E503b) d'une distorsion à ladite image marquée, et
- la transformation spectrale (E503c) de l'image marquée afin d'obtenir un ensemble de coefficients modulés après distorsion.

12. Procédé selon l'une des revendications 9 à 11, **caractérisé en ce que** la séquence pseudo-aléatoire centrée w est formée à partir de sous-séquences pseudo-aléatoires w^k de taille identique.

13. Procédé selon l'une des revendications 9 à 12, **caractérisé en ce que** les sous-séquences pseudo-aléatoires w^k ont une taille supérieure ou égale à un nombre minimum de coefficients formant une région de ladite partition d'une taille qui est statistiquement significative pour valider ledit critère de détectabilité sur ladite région.

14. Procédé selon l'une des revendications 9 à 13, **caractérisé en ce que**, à l'étape de génération (E501), chaque sous-séquence pseudo-aléatoire centrée w^k est créée en générant la moitié des échantillons pseudo-aléatoires de ladite sous-séquence via un générateur de nombres pseudo-aléatoires et en symétrisant lesdits échantillons pseudo-aléatoires générés.

15. Procédé selon la revendication 14, **caractérisé en ce que**, à l'étape de génération (E501), chaque sous-séquence pseudo-aléatoire centrée w^k est créée en permutant en outre lesdits échantillons pseudo-aléatoires en utilisant une clé secrète.

16. Procédé selon l'une des revendications 9 à 13, **caractérisé en ce que**, à l'étape de génération (E501), chaque sous-séquence pseudo-aléatoire centrée w^k est créée en générant des échantillons aléatoires pseudo-aléatoires via un générateur de nombres pseudo-aléatoires et en redistribuant sur chaque échantillon la somme desdits échantillons pseudo-aléatoires générés.

17. Procédé selon l'une des revendications. 7 à 16, **caractérisé en ce qu'**un partitionnement par division itérative (E103) de l'image numérique est effectué et **en ce que**, pour chaque région au niveau d'un rang dudit partitionnement, un partitionnement d'un rang directement supérieur de ladite région est validé si et seulement s'il existe au moins deux sous-régions de ladite région pour lesquelles ledit critère de détectabilité est validé.

18. Procédé selon la revendication 17, **caractérisé en ce que**, pour chaque région au niveau d'un rang dudit partitionnement, la valeur d'une capacité Q de l'image numérique est incrémentée (E112) lorsque le partitionnement de rang directement supérieur n'est pas validé, ladite capacité Q étant égale au nombre cardinal des régions distinctes obtenues par ledit partitionnement sur lesquelles le critère de détectabilité est validé.

WAVELYNX EX. 1003, Pg. 1030
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

19. Procédé selon la revendication 18, **caractérisé en ce que**, pour chaque région au niveau d'un rang dudit partitionnement, la valeur d'une capacité Q est incrémentée (E112) lorsque le partitionnement du rang immédiatement supérieur n'est pas validé, ladite valeur de la capacité Q est comparée (E115) à une valeur de capacité fixe Qs et le partitionnement est répété pour une région ayant l'amplitude de détectabilité la plus élevée parmi toutes les autres régions à traiter lorsque ladite valeur de capacité est inférieure à ladite valeur de capacité fixe.

20. Procédé selon l'une des revendications 7 à 16, **caractérisé en ce qu'**un partitionnement par fusion itérative de l'image numérique est effectué et **en ce que**, pour chaque région dudit partitionnement pour laquelle ledit critère de détectabilité n'est pas validé, ladite région est fusionnée avec une autre région dudit partitionnement.

21. Procédé selon la revendication 20, **caractérisé en ce que** ladite autre région du partitionnement est si possible une région pour laquelle ledit critère de détectabilité n'est pas validé.

22. Procédé de décodage d'un signal de marquage dans une image numérique, inséré en modulant des coefficients X représentant ladite image dans des régions distinctes formant un partitionnement de ladite image numérique, **caractérisé en ce qu'**un partitionnement en régions distinctes R de l'image numérique à décoder est déterminé en effectuant un partitionnement adaptatif en fonction d'un critère de détectabilité statistique d'un bit d'informations obtenu en démodulant des coefficients sur chaque région R.

23. Procédé de décodage selon la revendication 22, **caractérisé en ce qu'**il inclut une étape préalable (E201) consistant à comparer la taille P de chaque région du partitionnement à une taille minimum P_{stat} correspondant à la taille minimum d'un échantillon statistiquement significatif pour la détection d'un signal de marquage inséré dans ladite région.

24. Procédé de décodage conformément à l'une des revendications 22 et 23, **caractérisé en ce que**, pour chaque région R du partitionnement, une amplitude de détection T est calculée (E203) à partir dudit critère de détectabilité et ledit critère de détectabilité est validé (E203) en comparant ladite amplitude de détection T à une valeur de seuil prédéterminée Td en vue d'un décodage.

25. Procédé de décodage selon la revendication 24, **caractérisé en ce que** la valeur de seuil prédéterminée Td pour effectuer un décodage est inférieure à ladite valeur de seuil prédéterminée Tc utilisée pendant le procédé d'insertion conformément à la revendication 7.

26. Dispositif d'insertion d'un signal de marquage dans une image numérique en modulant des coefficients de régions représentant ladite image numérique, comportant des moyens pour partitionner en régions distinctes l'image numérique **caractérisé en ce que** des moyens de partitionnement (500, 502, 503) sont adaptés pour effectuer un partitionnement adaptatif en fonction d'un critère de détectabilité statistique d'un bit d'informations inséré sur chaque région.

27. Dispositif selon la revendication 26, **caractérisé en ce qu'**il inclut également des moyens (500, 502, 503) pour appliquer une distorsion avant de calculer le critère de détectabilité.

28. Dispositif selon l'une des revendications 26 et 27, **caractérisé en ce qu'**il dispose également de moyens (500, 502, 503) de comparaison de la taille de chaque région du partitionnement à une taille minimum correspondant à la taille minimum d'un échantillon statistiquement significatif pour la détection d'un signal de marquage inséré dans ladite région.

29. Dispositif selon l'une des revendications 26 à 28, **caractérisé en ce que** les moyens de partitionnement (500, 502, 503) comportent des moyens (500, 502, 503) de modulation de tous les coefficients de chaque région en insérant le signal de marquage, des moyens (500, 502, 503) de calcul d'une amplitude de détectabilité à partir dudit critère de détectabilité et des moyens (500, 502, 503) de validation dudit critère de détectabilité, adaptés pour comparer ladite amplitude de détectabilité à une valeur de seuil prédéterminée.

30. Dispositif selon la revendication 26, **caractérisé en ce qu'**il inclut :

- des moyens (500, 502, 503) pour générer une séquence pseudo-aléatoire centrée w égale en taille au nombre cardinal N d'un ensemble de coefficients représentatifs d'au moins une partie d'une image I, formée par des sous-séquences pseudo-aléatoires centrées w^k,

WAVELYNX EX. 1003, Pg. 1031
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- des moyens (500, 502, 503) pour moduler ledit ensemble de coefficients par ladite séquence pseudo-aléatoire centrée w afin d'insérer le même bit d'informations sur ledit ensemble de coefficients, et
- des moyens (500, 502, 503) pour contrôler, sur chaque région, un critère de détectabilité du bit d'informations inséré par modulation.

31. Dispositif selon la revendication 30, **caractérisé en ce qu'**il comporte des moyens (500, 502, 503) pour appliquer une distorsion audit ensemble de coefficients modulés.

32. Dispositif selon la revendication 31, **caractérisé en ce que** ledit ensemble de coefficients est un ensemble de coefficients spectraux Xi provenant d'une transformation spectrale d'une image numérique, et **en ce que** lesdits moyens destinés à appliquer une distorsion comportent :

- des moyens (500, 502, 503) pour une transformation spectrale inverse dudit ensemble de coefficients modulés afin d'obtenir une image marquée,
- des moyens (500, 502, 503) pour l'application d'une distorsion à ladite image marquée, et
- des moyens (500, 502, 503) pour une transformation spectrale de l'image marquée afin d'obtenir un ensemble de coefficients modulés après la distorsion.

33. Dispositif selon l'une des revendications 29 à 32, **caractérisé en ce que** les moyens de partitionnement (500, 502, 503) sont adaptés pour effectuer un partitionnement par division itérative de l'image numérique et **en ce que**, pour chaque région au niveau d'un rang dudit partitionnement, les moyens de validation sont adaptés pour valider un partitionnement d'un rang directement supérieur de ladite région si et seulement s'il existe au moins deux sous-régions desdites régions pour lesquelles ledit critère de détectabilité est validé.

34. Dispositif selon la revendication 33, **caractérisé en ce qu'**il comporte également des moyens (500, 502, 503) d'incrémentation de la valeur d'une capacité de l'image numérique adaptée, pour chaque région au niveau d'un rang dudit partitionnement, pour incrémenter ladite valeur de capacité lorsque le partitionnement du rang directement supérieur n'est pas validé, ladite capacité étant égale au nombre cardinal des régions distinctes obtenues par ledit partitionnement sur lequel le critère de détectabilité est validé.

35. Dispositif selon la revendication 33, **caractérisé en ce qu'**il comporte également des moyens d'incrémentation (500, 502, 503) adaptés, pour chaque région au niveau d'un rang dudit partitionnement, pour incrémenter la valeur d'une capacité lorsque le partitionnement de rang directement supérieur n'est pas validé, des moyens de comparaison (500, 502, 503) adaptés pour comparer ladite valeur de la capacité à une valeur de capacité fixe et des moyens de répétition (500, 502, 503) adaptés pour répéter le partitionnement pour une région ayant l'amplitude de détectabilité la plus élevée parmi toutes les autres régions à traiter lorsque ladite valeur de capacité est inférieure à ladite valeur de capacité fixe.

36. Dispositif selon l'une des revendications 29 à 32, **caractérisé en ce que** les moyens de partitionnement (500, 502, 503) sont adaptés pour effectuer un partitionnement par fusion itérative de l'image numérique et sont adaptés, pour chaque région dudit partitionnement pour laquelle ledit critère de détectabilité n'est pas validé, pour fusionner ladite région avec une autre région dudit partitionnement.

37. Dispositif selon la revendication 36, **caractérisé en ce que** ladite autre région du partitionnement est si possible une région pour laquelle ledit critère de détectabilité n'est pas validé.

38. Dispositif selon l'une des revendications 26 à 37, **caractérisé en ce qu'**il est incorporé dans un microprocesseur (500), une mémoire à lecture seule (502) étant adaptée pour mémoriser un programme afin de déterminer un partitionnement et une mémoire à accès direct (503) comportant des registres adaptés pour mémoriser des variables modifiées pendant l'exécution dudit programme.

39. Dispositif de décodage d'un signal de marquage dans une image numérique, inséré par modulation de coefficients représentant ladite image dans des régions distinctes formant un partitionnement de ladite image numérique, **caractérisé en ce qu'**il comporte des moyens (500, 502, 503) de partitionnement de l'image numérique à décoder en régions distinctes, adaptés pour effectuer un partitionnement adaptatif en fonction d'un critère de détectabilité statistique d'un bit d'informations obtenu par démodulation des coefficients sur chaque région.

40. Dispositif de décodage selon la revendication 39, **caractérisé en ce qu'**il dispose également de moyens (500, 502,

WAVELYNX EX. 1003, Pg. 1032
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

503) de comparaison de la taille de chaque région du partitionnement à une taille minimum correspondant à la taille minimum d'un échantillon statistique significatif pour la détection d'un signal de marquage inséré dans ladite région.

41. Dispositif de décodage selon l'une des revendications 39 et 40, **caractérisé en ce qu'**il comporte des moyens (500, 502, 503) de calcul d'une amplitude de détection à partir dudit critère de détectabilité et des moyens (500, 502, 503) de validation dudit critère de détectabilité adaptés pour comparer ladite amplitude de détection à une valeur de seuil prédéterminée pour le décodage.

42. Dispositif de décodage selon la revendication 41, **caractérisé en ce que** la valeur de seuil prédéterminée pour le décodage est inférieure à ladite valeur de seuil prédéterminée utilisée pendant le procédé d'insertion selon la revendication 7.

43. Dispositif de décodage selon l'une des revendications 39 à 42, **caractérisé en ce qu'**il est incorporé dans un microprocesseur (500), une mémoire à lecture seule (502) étant adaptée pour mémoriser un programme pour décoder un signal de marquage et une mémoire à accès direct (503) comportant des registres adaptés pour mémoriser des variables modifiées pendant l'exécution dudit programme.

44. Ordinateur, **caractérisé en ce qu'**il comporte des moyens adaptés pour mettre en oeuvre un procédé d'insertion conformément à l'une des revendications 1 à 21.

45. Ordinateur, **caractérisé en ce qu'**il comporte des moyens adaptés pour mettre en oeuvre le procédé de décodage selon l'une des revendications 22 à 25.

46. Moyens de mémorisation d'informations lisibles par un microprocesseur, **caractérisés en ce qu'**ils mémorisent un programme mettant en oeuvre un procédé d'insertion conformément à l'une des revendications 1 à 21.

47. Moyens de mémorisation d'informations lisibles par un microprocesseur, **caractérisés en ce qu'**ils mémorisent un programme mettant en oeuvre un procédé de décodage conformément à l'une des revendications 22 à 25.

WAVELYNX EX. 1003, Pg. 1033
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

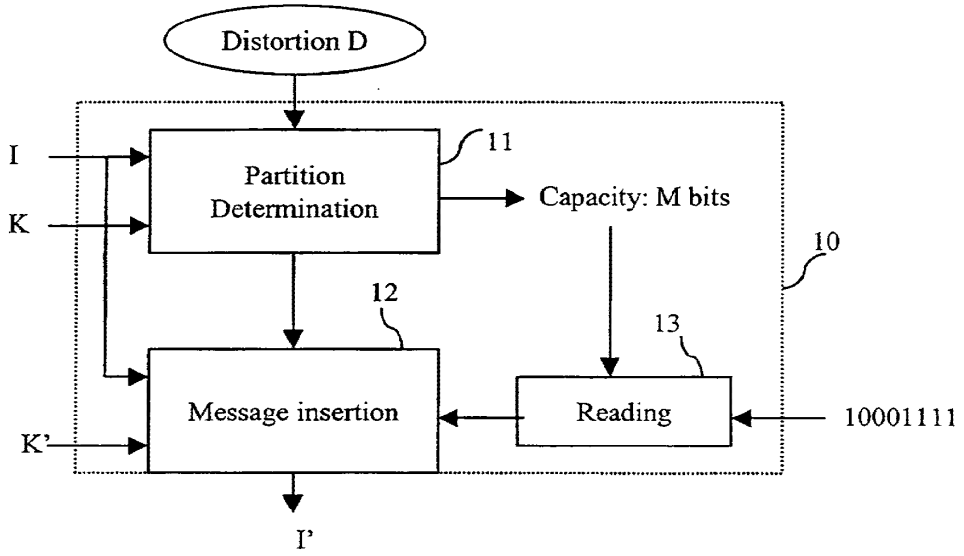


Figure 1

WAVELYNX EX. 1003, Pg. 1034
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

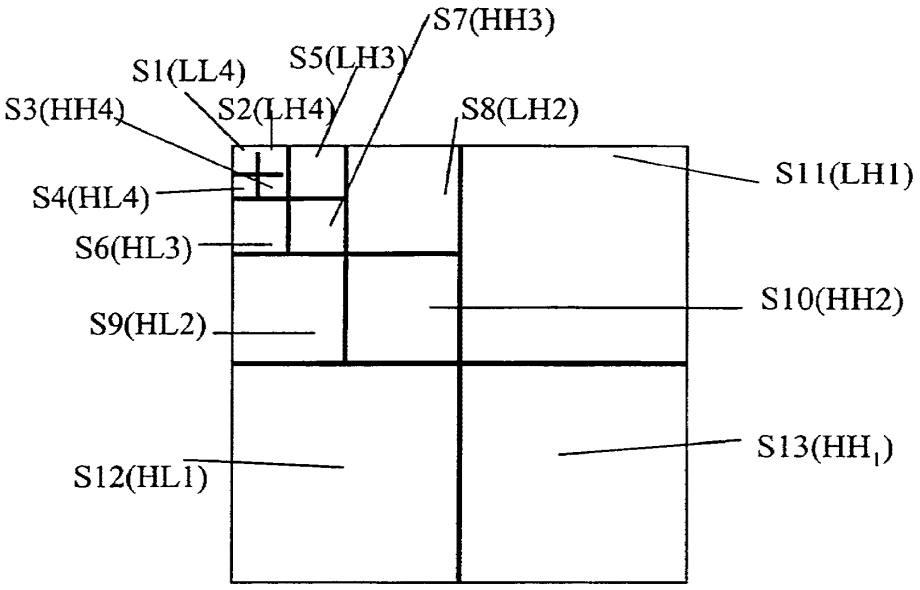
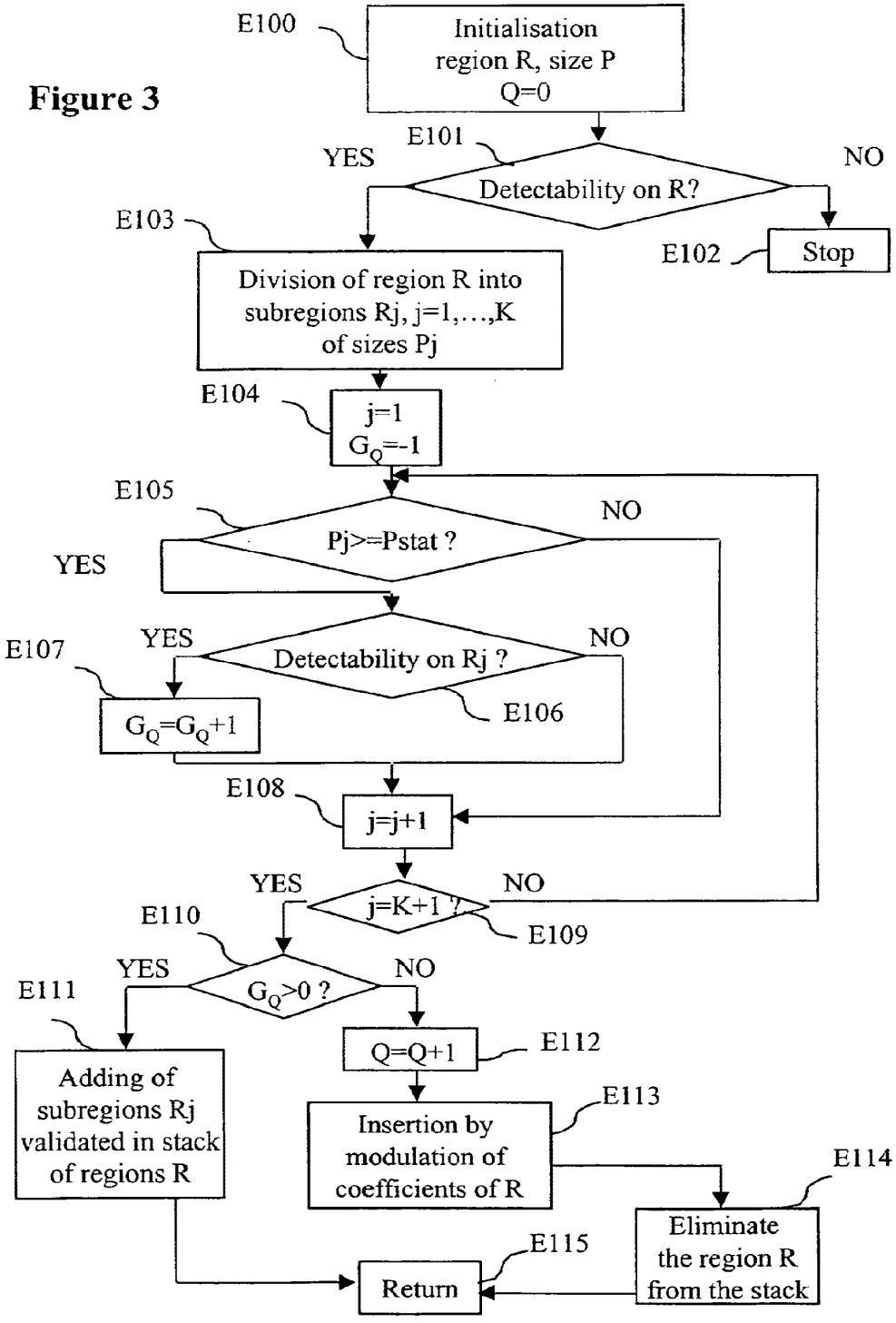


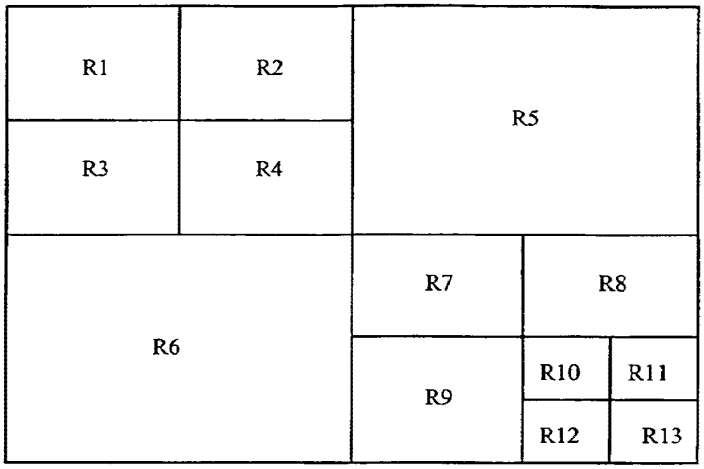
Figure 2

WAVELYNX EX. 1003, Pg. 1035
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Figure 3



WAVELYNX EX. 1003, Pg. 1036
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



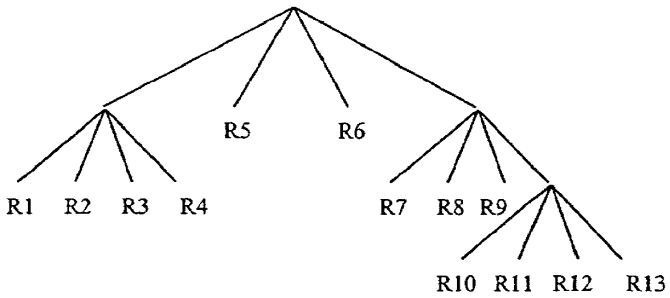


Figure 4

WAVELYNX EX. 1003, Pg. 1037
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

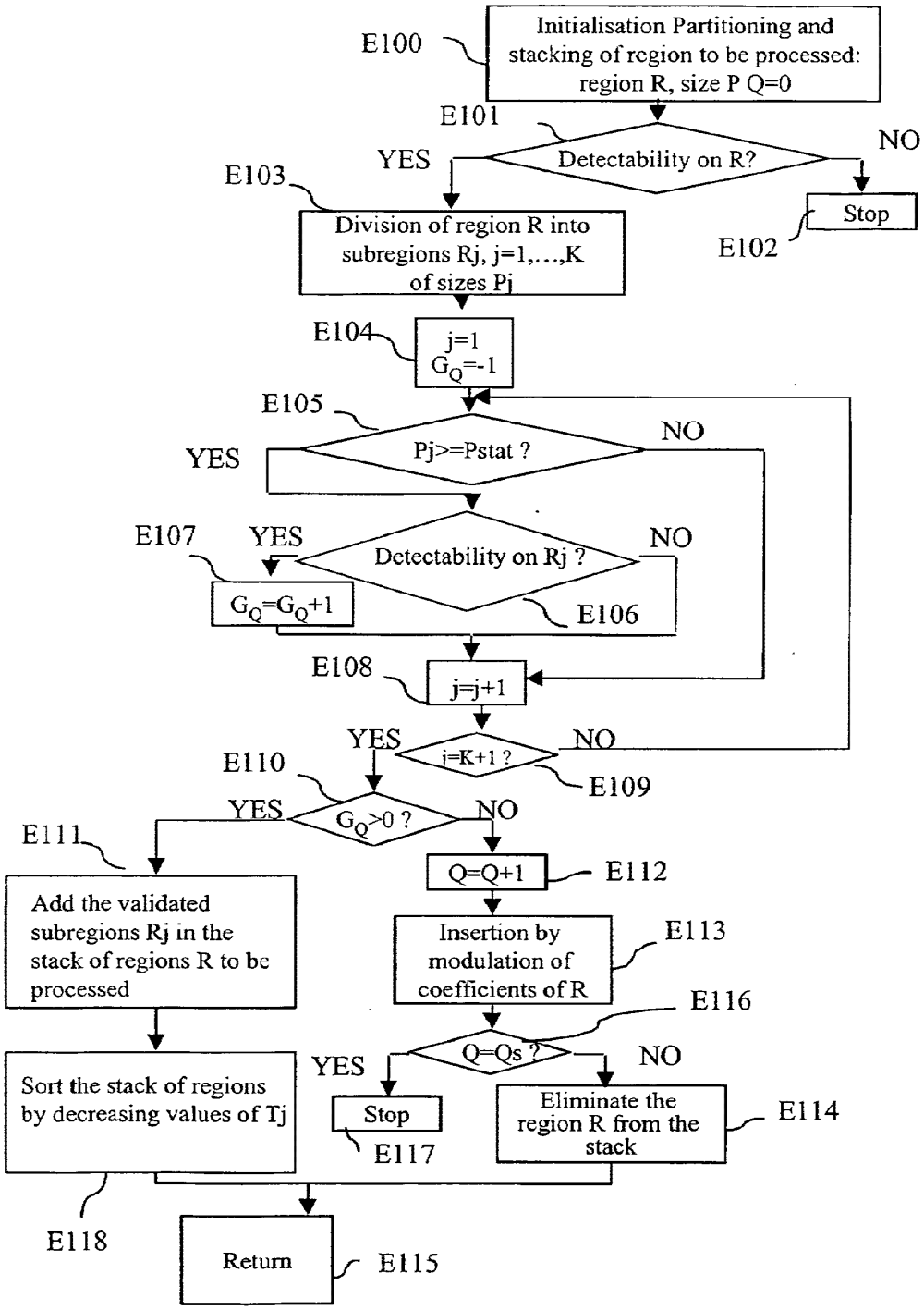


Figure 5

WAVELYNX EX. 1003, Pg. 1038
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

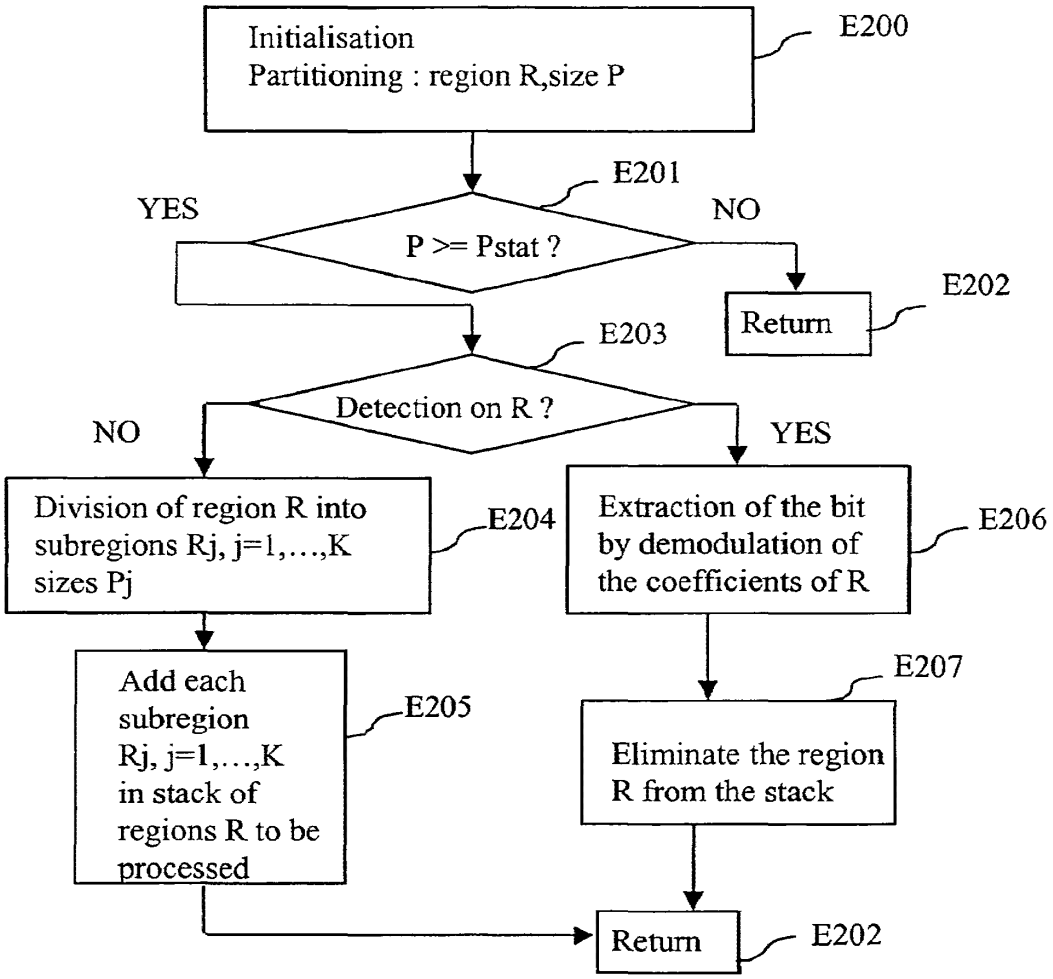


Figure 6

WAVELYNX EX. 1003, Pg. 1039
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

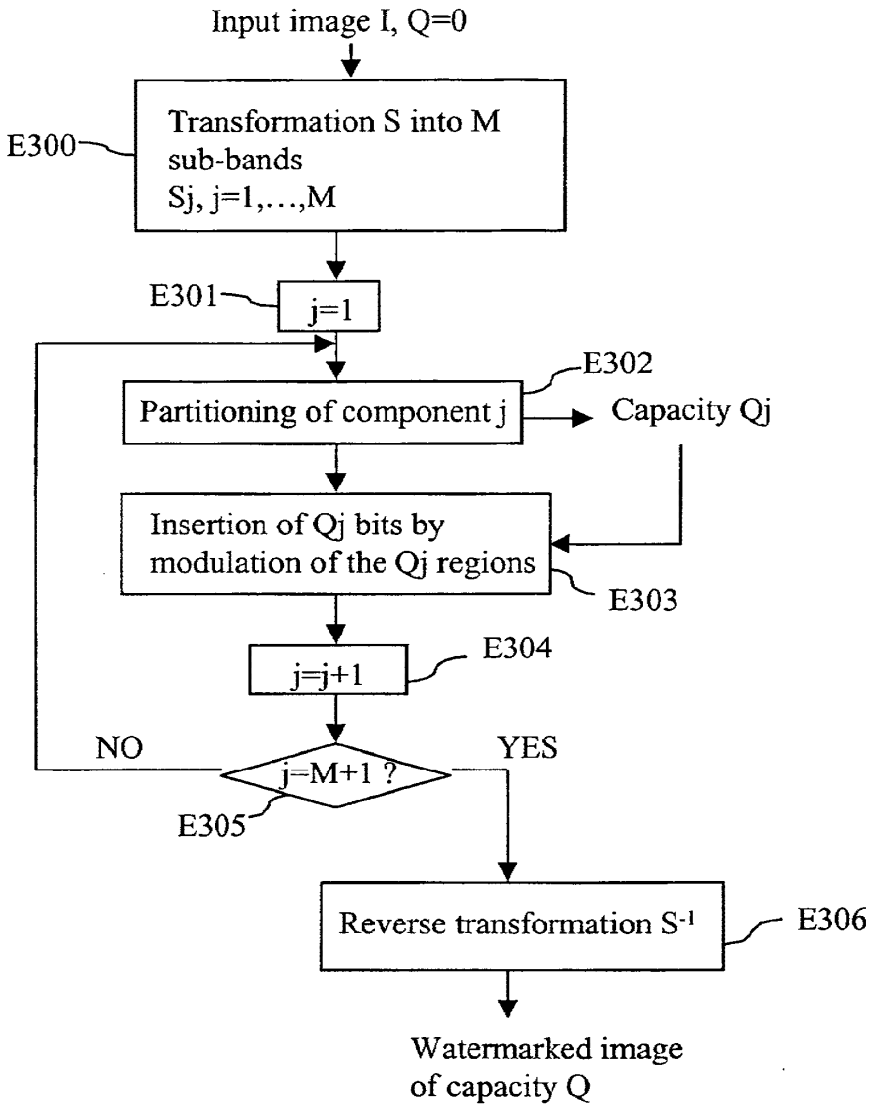


Figure 7

WAVELYNX EX. 1003, Pg. 1040
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

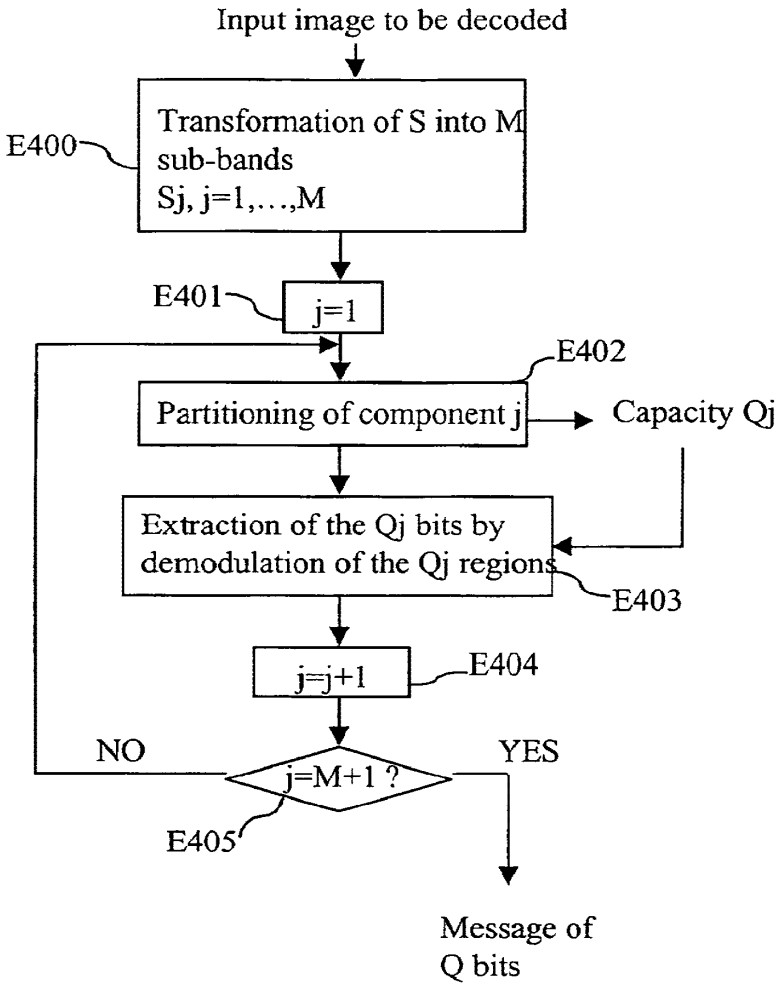


Figure 8

WAVELYNX EX. 1003, Pg. 1041
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

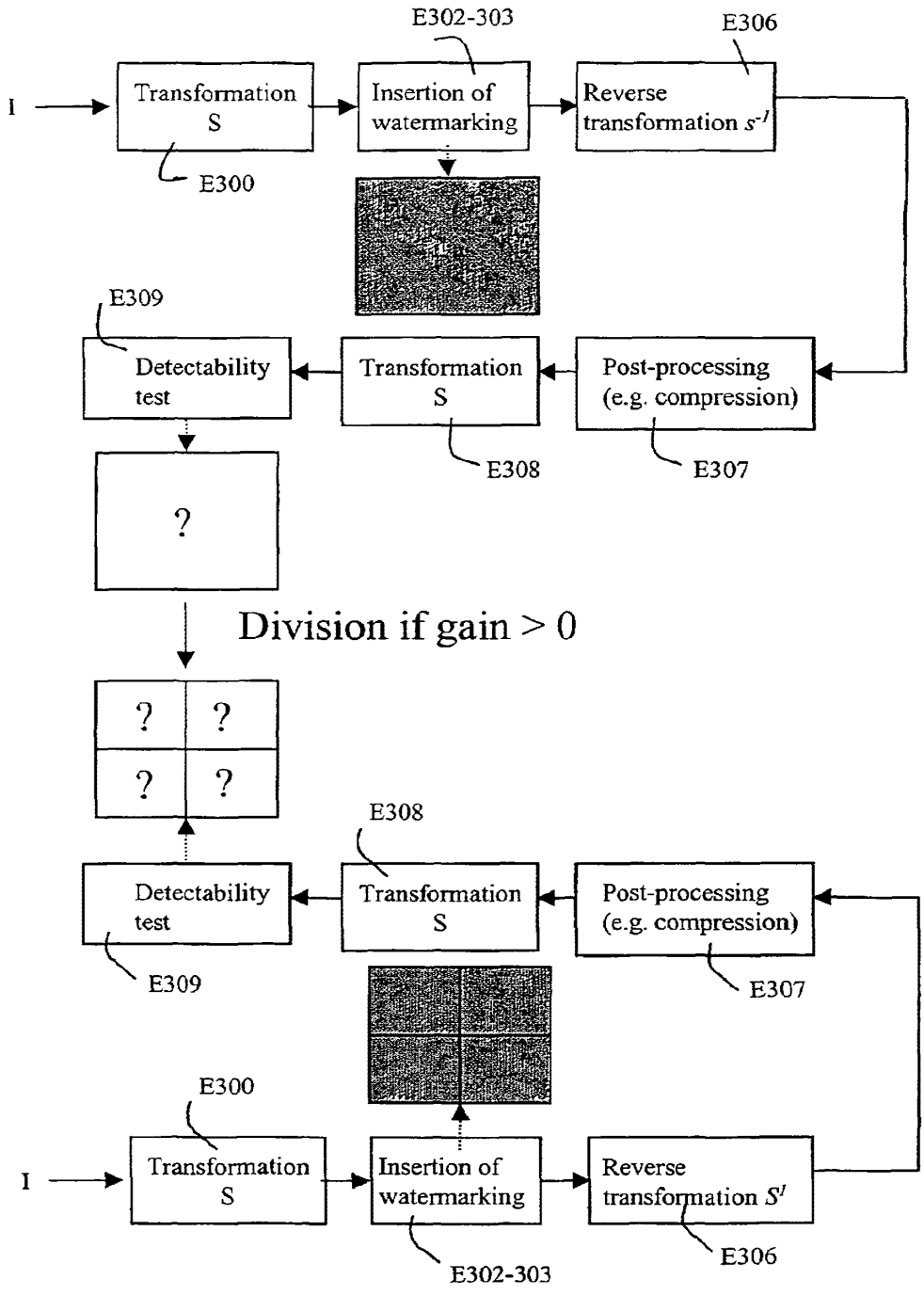


Figure 9

WAVELYNX EX. 1003, Pg. 1042
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

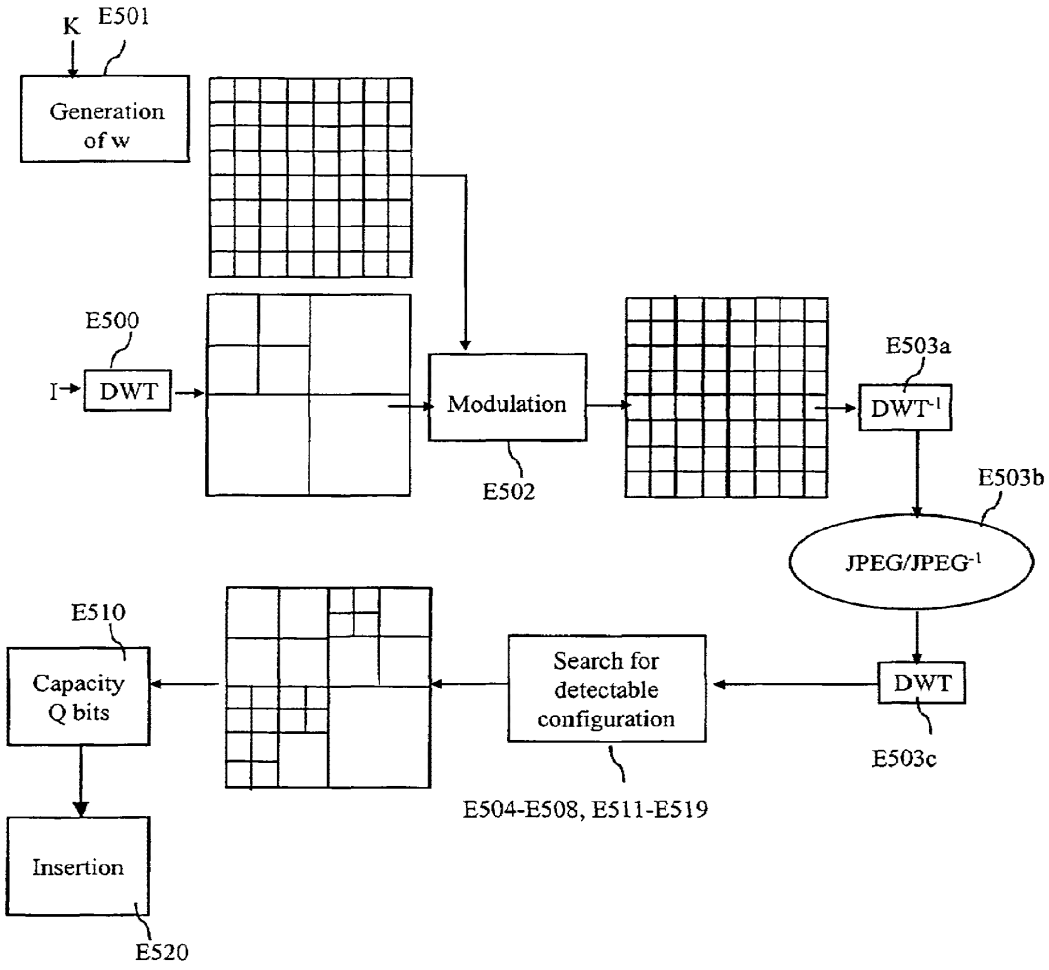


Figure 10

WAVELYNX EX. 1003, Pg. 1043
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

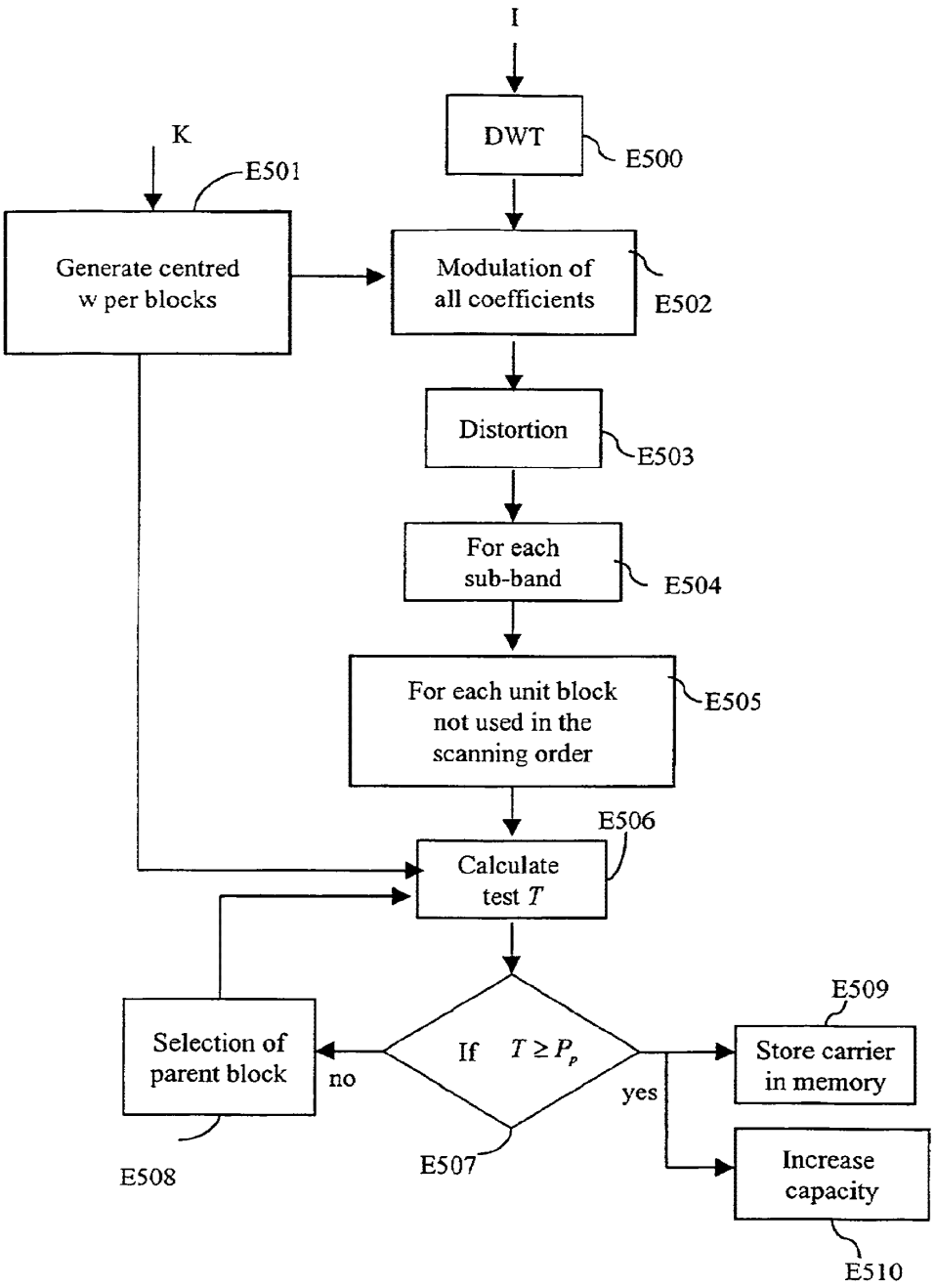


Figure 11

WAVELYNX EX. 1003, Pg. 1044
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

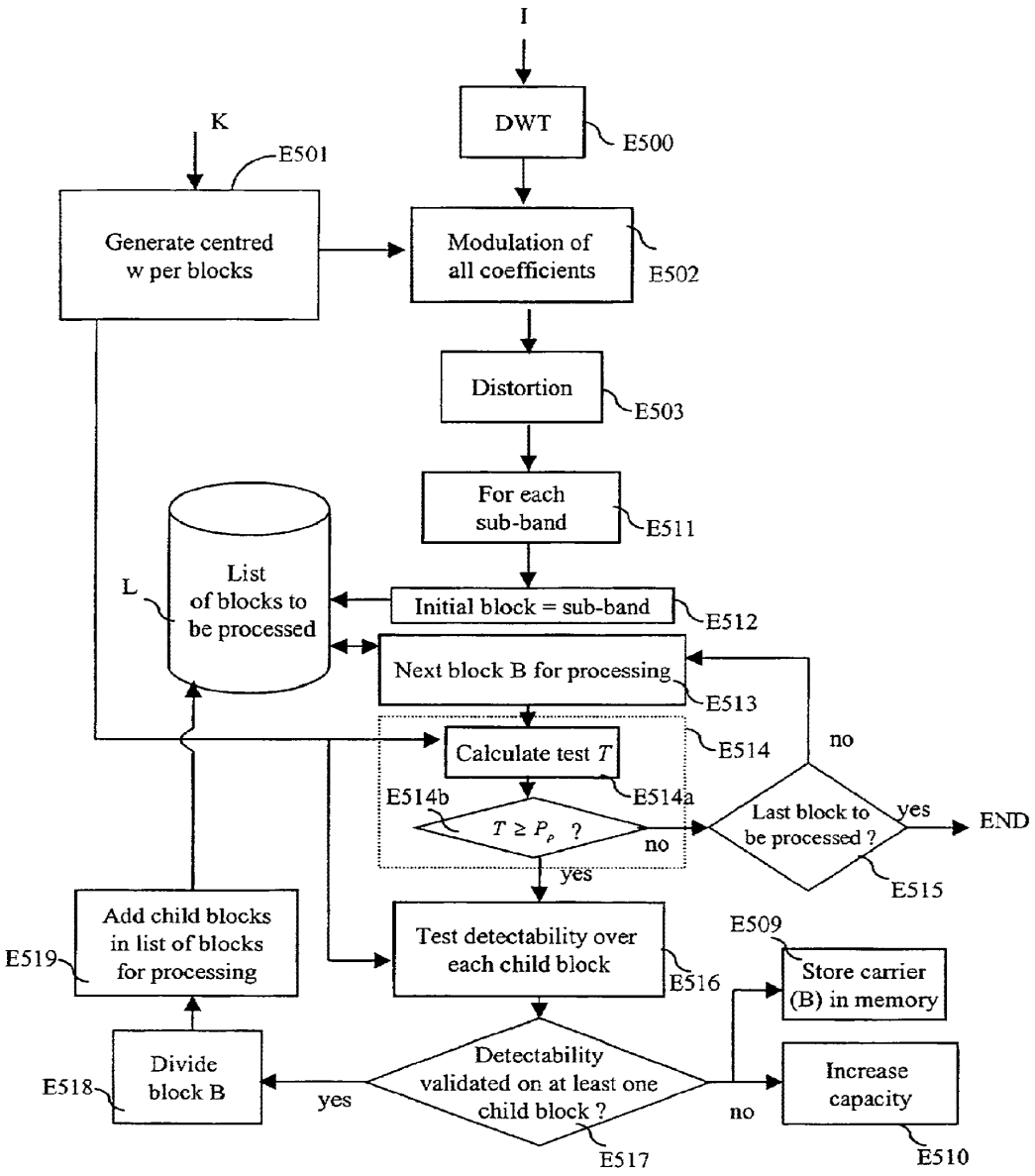


Figure 12

WAVELYNX EX. 1003, Pg. 1045
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

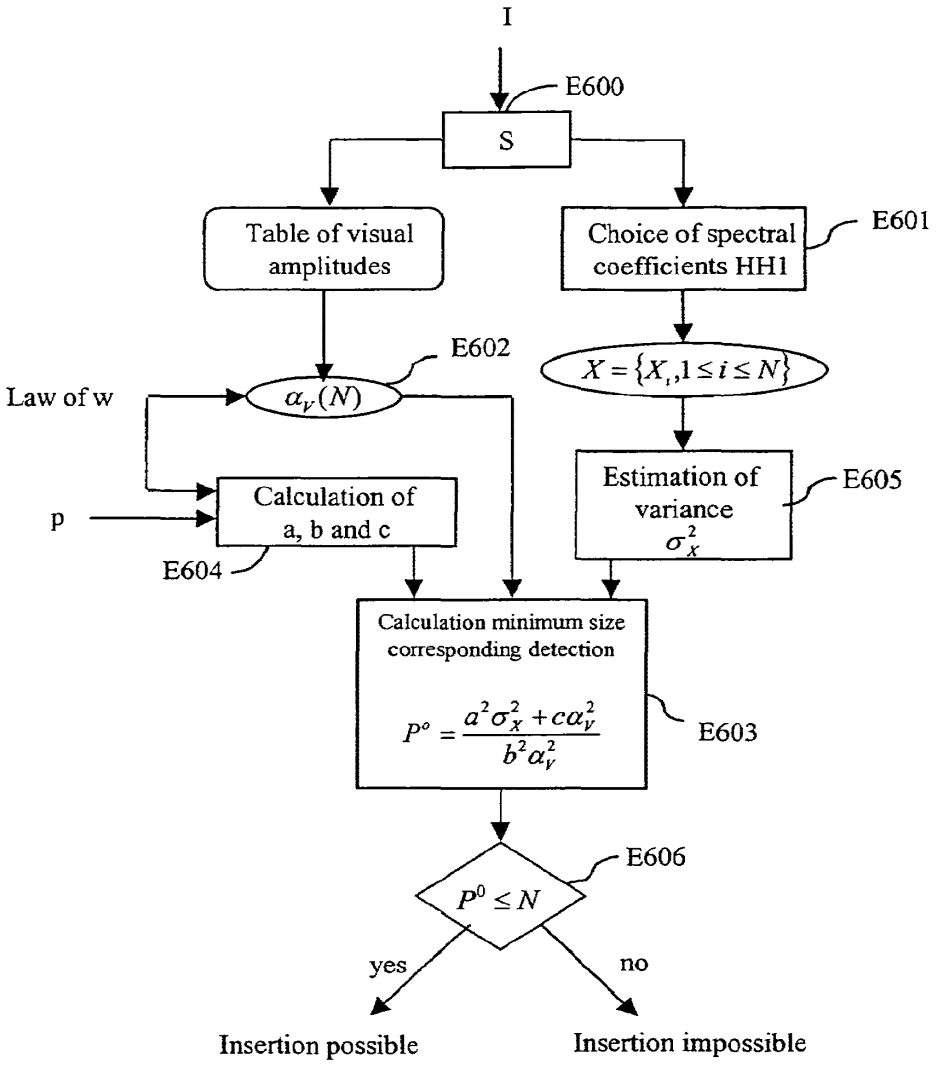


Figure 13

WAVELYNX EX. 1003, Pg. 1046
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

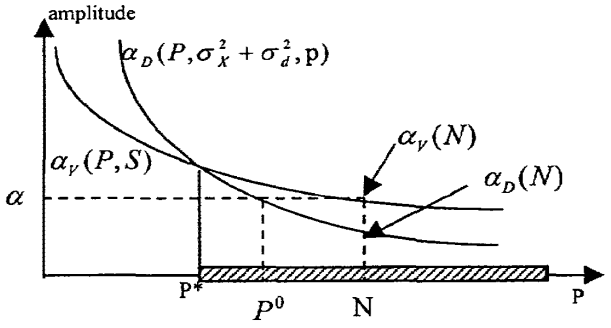


Figure 14

WAVELYNX EX. 1003, Pg. 1047
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

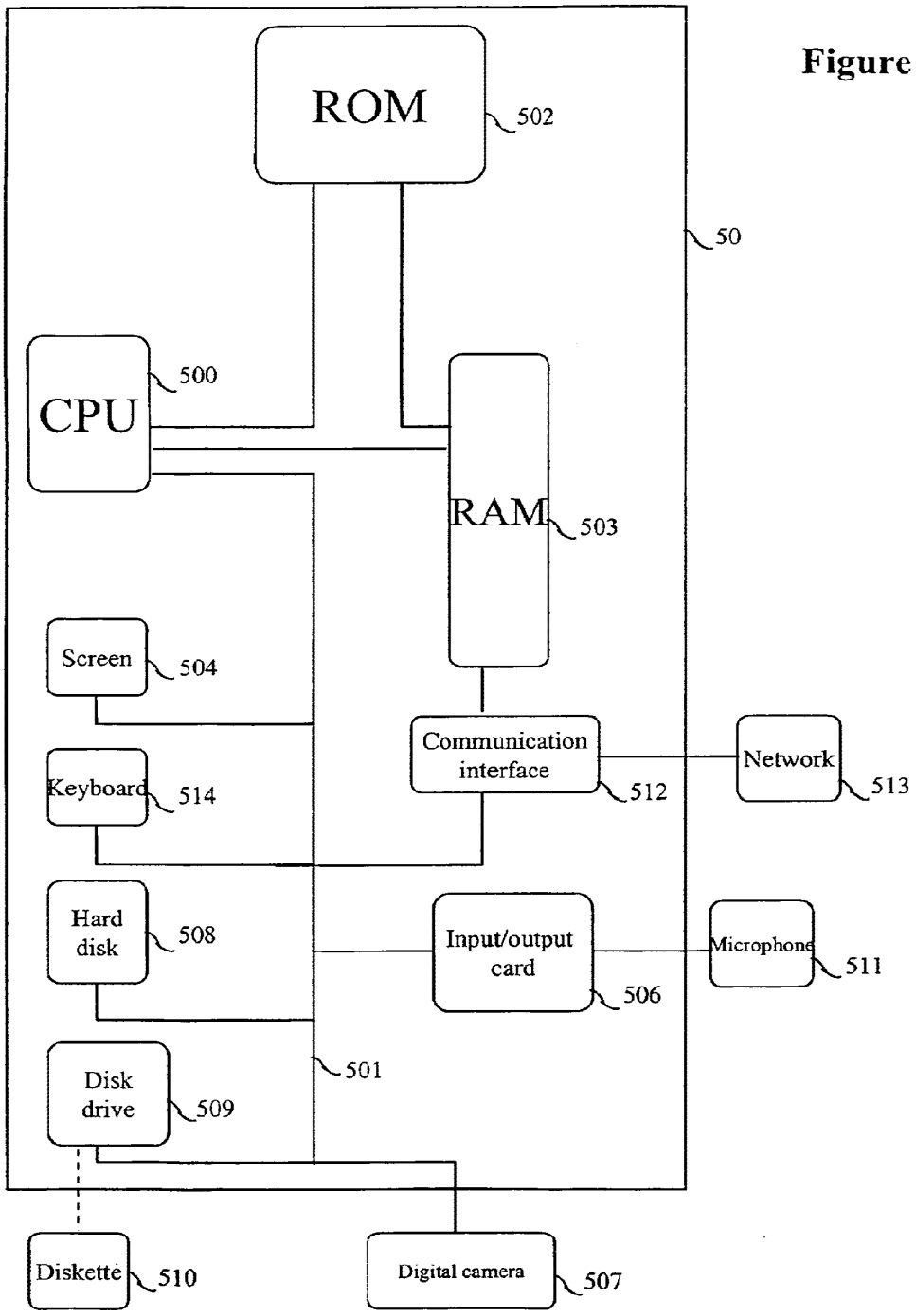


Figure 15

WAVELYNX EX. 1003, Pg. 1048
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 148 644 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
12.10.2005 Bulletin 2005/41

(43) Date of publication A2:
24.10.2001 Bulletin 2001/43

(21) Application number: **01303032.5**

(22) Date of filing: **30.03.2001**

(51) Int Cl.[7]: **H03K 3/84**, H04B 1/69, H03H 17/06, H04J 13/00

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **07.04.2000 JP 2000107047**

(71) Applicant: **National Institute of Information and Communications Technology, Independent Administrative Institution**
Tokyo 184-0015 (JP)

(72) Inventor: **Umeno, Ken, Comm.Res.Lab., Ministry of Public Mang**
Konagei, Tokyo 184-8795 (JP)

(74) Representative: **Smith, Norman Ian et al**
fJ CLEVELAND
40-43 Chancery Lane
London WC2A 1JQ (GB)

(54) **Pseudo-random number sequence output unit, transmitter, receiver, communication system and filter unit, pseudo-random number sequence output method, transmission method, receiving method and filtering method, and data recording medium**

(57) A pseudo-random number sequence output unit responsive to **s** ($1 \le s$) number of prescribed positive integers $q_1, q_2, ..., q_s$, a prescribed real impulse constant **r** ($-1 < r < 1$), and a prescribed non-zero real constant C for outputting a pseudo-random number sequence of length N ($1 \le N$), which output unit includes:

an input acceptance section that accepts input of **s** ($1 \le s$) number of real number sequence initial values $Y_1, Y_2, ..., Y_s$ ($-1 < Y_1 < 1, -1 < Y_2 < 1, ..., -1\ Y_s < 1$), and **s** number of integer parameters $p_1, p_2, ..., p_s$ ($2 \le p_1, 2 \le p_2, ... 2 \le p_s$) for which $q_1 \bmod p_1 \neq 0$, $q_2 \bmod p_2 \neq 0$ ..., $q_s \bmod p_s \neq 0$ respectively hold with respect to the prescribed positive integers $q_1, q_2 ... q_s$;
a calculation section that uses the prescribed real impulse constant **r**, the prescribed non-zero real constant C, the sequence initial values $Y_1, Y_2, ..., Y_s$, the integer parameters $p_1, p_2, ..., p_s$, the prescribed positive integers $q_1, q_2, ..., q_s$ and integers **j** ($1 \le j \le s$), m ($1 \le m \le 2N-2$) and **n** ($1 \le n \le 2N-1$) to calculate from the recurrence formula

$$T_p(\cos\theta) = T(p, \cos\theta) = \cos(p\theta)$$

$$y_j[1] = Y_j$$

$$y_j[m+1] = T(p_j, y_j[m])$$

$$z[n] = \prod_{j=1}^{s} T(q_j, y_j[n])$$

a pseudo-random number sequence z'[1], z'[2], .., z'[N] of length N that satisfies

$$z'[1] = C\sum_{j=1}^{N}(-r)^j z[j],$$

$$z'[2] = C\sum_{j=1}^{N}(-r)^j z[j+1],$$

.
.
.

$$z'[N] = C\sum_{j=1}^{N}(-r)^j z[j+N-1];$$

Printed by Jouve, 75001 PARIS (FR)

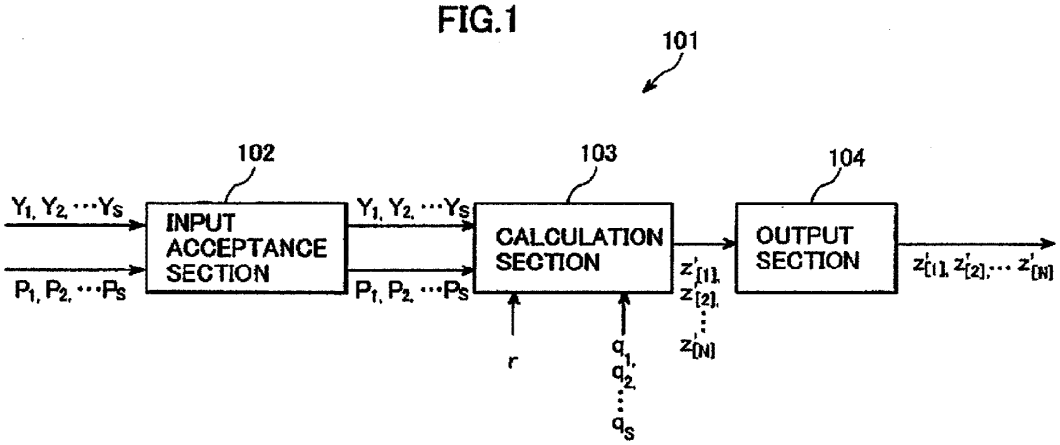
(Cont. next page)

EP 1 148 644 A3

WAVELYNX EX. 1003, Pg. 1049
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

and an output section that outputs the pseudo-random number sequence z'[1], z'[2], ..., z'[N]. A transmitter, receiver and communication system that utilize the output unit, a filter unit, a pseudo-random number sequence output method, transmission method, receiving method and filtering method are provided. A computer-readable data recording medium recorded with a program for operating the transmitter, receiver, communication system and implementing the output, transmission and receiving methods is also provided.

FIG.1



WAVELYNX EX. 1003, Pg. 1050
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 3032

DOCUMENTS CONSIDERED TO BE RELEVANT

	Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
2	X	KOHDA, TSUNEDA: "Pseudonoise sequences by chaotic nonlinear maps and their correlation properties" IEICE TRANSACTIONS ON COMMUNICATIONS, vol. E76-B, no. 8, August 1993 (1993-08), pages 855-862, XP000396888 TOKYO, JP * section 2 *	1-12, 15-24, 26-35,37	H03K3/84 H04B1/69 H03H17/06 H04J13/00
2	X,P	CHI-CHUNG CHEN ET AL.: "Optimal chaotic spread spectrum sequences for uplink CDMA systems" IEEE SYMPOSIUM ON ADAPTIVE SYSTEMS FOR SIGNAL PROCESSING, COMMUNICATIONS, AND CONTROL, 1 October 2000 (2000-10-01), pages 135-140, XP010521626 PISCATAWAY, US * section 1 * * section 5 *	1-37	
13	X,P	IN-SOON PARK ET AL.: "Design of powers-of-two coefficient FIR filters with minimum arithmetic complexity" ASIA-PACIFIC CONFERENCE ON CIRCUITS AND SYSTEMS, vol. 1, 28 October 2002 (2002-10-28), pages 517-520, XP010620756 Piscataway, US * abstract *	13,14, 25,36	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04J H03H
13	X	GENTILI ET AL.: "Evolutionary design of FIR digital filters with power-of-two coefficients" IEEE WORLD CONGRESS ON COMPUTATIONAL INTELLIGENCE, 27 June 1994 (1994-06-27), pages 110-114, XP010122864 New York, US * abstract *	13,14, 25,36	

-/--

3 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	3 August 2005	Scriven, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1051
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 3032

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
2 E	EP 1 401 100 A (JAPAN SCIENCE AND TECHNOLOGY CORPORATION; UMENO; YAMAGUCHI) 24 March 2004 (2004-03-24) * the whole document *	1-37	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

3 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	3 August 2005	Scriven, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1052
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

Application Number
EP 01 30 3032

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

WAVELYNX EX. 1003, Pg. 1053
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 01 30 3032

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-12 15-24 26-35 37

Derivation of spreading codes from Chebyshev polynomials.

---

2. claim: 13 14 25 36

Transversal filter.

WAVELYNX EX. 1003, Pg. 1054
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 30 3032

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

03-08-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1401100 A	24-03-2004	JP 2002290274 A	04-10-2002
		JP 3556190 B2	18-08-2004
		JP 2003115819 A	18-04-2003
		JP 3531869 B2	31-05-2004
		JP 2003249873 A	05-09-2003
		EP 1401100 A1	24-03-2004
		US 2004146095 A1	29-07-2004
		CN 1620756 A	25-05-2005
		WO 02078183 A1	03-10-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

WAVELYNX EX. 1003, Pg. 1055
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 292 882 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.07.2006 Bulletin 2006/30

(21) Application number: **01938930.3**

(22) Date of filing: **07.06.2001**

(51) Int Cl.:
G06F 7/58 *(2006.01)*

(86) International application number:
PCT/SE2001/001296

(87) International publication number:
WO 2001/095091 (13.12.2001 Gazette 2001/50)

(54) **METHOD AND DEVICE FOR ENCRYPTING A MESSAGE**

VERFAHREN UND EINRICHTUNG ZUM VERSCHL SSELN EINER NACHRICHT

PROCEDE ET DISPOSITIF POUR LE CODAGE D'UN MESSAGE

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **07.06.2000 SE 0002158**

(43) Date of publication of application:
19.03.2003 Bulletin 2003/12

(73) Proprietor: **Anoto AB**
223 69 Lund (SE)

(72) Inventors:
- **THUVESHOLMEN, Mikael**
  S-214 38 Malmö (SE)
- **EDSÖ, Tomas**
  S-222 41 Lund (SE)
- **DORÉ HANSEN, Mads**
  DK-9560 Hadsund (DK)
- **SKANTZE, Kristofer**
  S-222 29 Lund (SE)

(56) References cited:
EP-A2- 0 984 390
DE-A1- 19 907 600
US-A- 4 776 013
US-A- 5 852 434
US-A- 5 930 377

- **PATENT ABSTRACTS OF JAPAN & JP 09 083 512 A (OLYMPUS OPTICAL CO LTD) 28 March 1997**
- **TORU SASAKI ET AL: 'Stream cipher based on pseudorandom number generation with optical affine transformation' APPLIED OPTICS vol. 39, no. 14, 10 May 2000, pages 2340 - 2346**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 1 292 882 B1

Description

Field of invention

[0001] The present invention generally relates to the field of transmitting information from a sender to a receiver. More specifically, the present invention relates to a method and a device for encrypting a message for secure transmission of such a message from a sending device to a receiver. The invention further relates to a computer readable medium comprising instructions for bringing a computer to perform such a method, and a sending device and a system, respectively, comprising such a device.

Background of the invention

[0002] During transmission of information from a sender to a receiver, for example in a system including hand-held devices, there are basically four aspects that need to be fulfilled for obtaining a secure transmission with regards to authenticity, integrity, confidentiality and non-repudiation. However, confidentiality, i.e. that the information is kept secret during the transmission, is crucial in the field of digital communication, for example in financial transactions or in e-commerce. This aspect, as well as the other aspects, can be met by using cryptography.

[0003] When using cryptography or a network security algorithm based on cryptography, random number data is used for different reasons and play an essential role. For example, random numbers are frequently used as encryption keys or for generation of encryption keys. Furthermore, random data is by definition difficult to determine or guess.

[0004] Common methods of cryptography include symmetric encryption and asymmetric encryption. When using symmetric encryption, the same key is used for both encryption and decryption. The encryption key is used in conjunction with an encryption algorithm, and different keys will result in different outputs from the algorithm. The degree of security of the encrypted message depends on the secrecy of the key and therefore on the random number used as the key or for generating the key, not on the secrecy of the algorithm. This makes it possible to use powerful standard algorithms, such as AES (Advanced Encryption Standard), DES (Data Encryption Standard) or IDEA (International Data Encryption Standard). The degree of security also depends on the length or bit size of the key. The longer the encryption key, the more difficult it is to break the cipher.

[0005] When using asymmetric encryption, the sender and the receiver each has a private encryption key and a public encryption key. Thereby, confidentiality, authentication and non-repudiation is achieved. Commonly used asymmetric encryption algorithms include, for example, RSA (Rhivest-Shamir-Adleman) and DH (Diffie-Hellman).

[0006] It is a well-known problem that sources for true random numbers are difficult to find. Physical noise generators, such as pulse detectors of ionizing radiation events, gas discharge tubes, and leaky capacitors, are one potential source. However, such devices are of limited utility in network security applications. For example, incorporating one of these devices into a hand-held device will require a complex and possibly bulky design of the hand-held device. Furthermore, there are problems both with the degree of randomness and the precision of numbers generated by such devices.

[0007] Another approach for obtaining random numbers for cryptographic applications is to use algorithmic techniques. However, these algorithms are deterministic and therefore produce sequences of numbers that are not statistically random. Such numbers are often referred to as pseudo random numbers.

[0008] A widely used technique for pseudo random number generation is the linear congruential method. A sequence of numbers is obtained via the following equation

$$X_{n+1} = (aX_n + b) \bmod c,$$

where X_0 is an initial number, i.e. the random seed. Usually, in a handheld device or a computer, the microseconds of the internal clock are used as random seed to initiate the algorithm.

[0009] One problem with the above-mentioned method is that once a value, the random seed, has been chosen, the subsequent numbers in the sequence follow deterministically. This means that someone having knowledge of a part of the sequence could theoretically determine subsequent elements of the sequence.

[0010] It is possible to implement more advanced random number generators that use the internal clock as random seed, for example such as the algorithm used in Blue-tooth. This and similar algorithms are able to generate pseudo random numbers with improved statistical characteristics compared to the numbers generated by the linear congruential method. However, the pseudo random numbers are still of an insufficient quality in a statistical sense, i.e. when considering the degree of randomness.

[0011] The article "Stream cipher based on pseudorandom number generation with optical affine transformation", by Sasaki et al, published in Applied Optics, Vol. 39, No. 14, pp 2340-2346, on 10 May 2000, describes a technique for

WAVELYNX EX. 1003, Pg. 1057
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

generating an image with pseudorandom intensity distribution by optical processing. Specifically, optical feedback processing is used by displaying an initial image on a CRT (Cathode Ray Tube). The CRT image is then imaged onto a CCD camera, via optical components that split, rotate, reflect, translate and recombine the image, whereupon the processed image is displayed on the CRT. The same procedure is then repeated for a large number of iterations. The final output image is used to encrypt an image message by optical modulo-*n* addition of the final output image to the image message. Apart from its evident inability of being readily implemented in a hand-held device, the known optical technique appears to suffer from both limited precision and slow processing speed.

[0012] Thus, there remains a problem in finding a method, that can be implemented in a system comprising hand-held devices, that provide random numbers of good quality, according to the above-mentioned criterions, for generation of encryption keys for use in encryption algorithms in order to provide a secure transmission of information between a sender and a receiver.

[0013] An example of a hand-held device is shown in US-A-5 852 434, which relates to an absolute position determination device for indicating the instantaneous position and movement of a stylus on a surface formatted with a position-related code for indicating X-Y coordinates.

Summary of the invention

[0014] Thus, an object of the present invention is to provide an improved method and device for generating an encryption key and encrypting a message.

[0015] This and other objects are achieved according to the present invention by providing a method for encryption according to claim 1, a digital pen according to claim 20, and a method for authentication according to claim 36. Preferred embodiments are defined in the dependent claims.

[0016] Thus, the present invention is based on the advantageous insight of using optical data as random seed for generation of an encryption key, which in turn is used in an encryption algorithm for encrypting a message. The optical data obtained in accordance with the method of the present invention presents the requisite degree of randomness and unpredictability. In fact, the optical data can be considered as being "truly" random. Consequently, the degree of randomness is higher and the optical data used are more unpredictable as compared to the data used for random seed in the known methods described above. Thus, an improved degree of secrecy of the generated encryption key will be achieved.

[0017] Traditionally, two distinct and not necessarily compatible criteria are used to determine the quality of a sequence of random numbers, unpredictability and randomness. In a "true" random sequence, each number is statistically independent of any other number in the sequence and is therefore unpredictable. Two criteria are used to validate the randomness of a sequence of numbers. First, uniform distribution of random numbers, which means that the frequency of occurrence of each of the numbers should be approximately the same. Second, independence between random numbers, which means that no value in the sequence can be inferred from any of the others.

[0018] According to the preferred embodiment of the present invention, a surface, or a portion thereof, is scanned or read with an optical sensor, preferably a camera or a light-sensitive sensor, thereby obtaining optical data representative of characteristics the read surface. The light-sensitive sensor being, for example, a CCD sensor (Charge-Coupled Device) or a CMOS sensor (Complementary Metal-Oxide semiconductor). The obtained optical data are determined by and represent values of at least one optical parameter, which is representative of physical conditions on the portion of the surface.

[0019] Preferably, the optical data are obtained from a portion of a surface provided with a position code pattern, wherein the position code pattern includes optical readable markings. Each of said markings may be designed more or less arbitrarily. However, the design of each marking is preferably elementary, for example in the shape of round dots as shown in the detailed description below. The position code pattern is implemented using any parameter, which may be used to achieve symbols of the above-mentioned type that may be detected or sensed by an optical detector or optical sensor. The fact that the position code pattern is optically readable facilitates the appliance of the pattern onto the surface. Accordingly, the pattern should have the capability to reflect light, which not necessarily has to have a wavelength in the visible spectrum.

[0020] Preferably, the parameter sensed and used for the generation of the encryption key is brightness, which is a relative measure of the intensity of the energy output of a light source that is visible for an optical sensor. In the preferred embodiment of the present invention, the brightness of light that is reflected from a portion of an illuminated surface is registered. Of course, the sensed light does not necessarily have to constitute reflected light. Sensing of emitted light from luminous surfaces are also contemplated within the scope of the present invention, or any combinations of emitted and reflected light. The brightness in the sensed light may, for example, depend on variations in the surrounding illumination, the quality of the printing of the pattern, the blacking of the markings, and/or the quality of the surface, e.g. a paper surface. Biometric factors may also have an impact on the brightness, for example the inclination of the pen. These and other factors introduce a considerable degree of randomness in the optical data. Furthermore, the fact that

WAVELYNX EX. 1003, Pg. 1058
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the optical sensor in itself is a noise generator will even further enhance the degree of randomness in the optical data.

[0021] According to preferred embodiments of the invention, the optical data are processed according to a preprogrammed order or scheme and organized in data fields of a predetermined length. The data fields, in turn, are preferably organized in data records according to a predetermined scheme, e.g. in a predetermined order.

[0022] According to a specific preferred embodiment of the present invention, and in order to even further improve the stochasticity of the optical data organized in said data records, the order of the data fields within the data records are rearranged according to a cyclic reordering algorithm. According to the cyclic reordering algorithm, the order of the rearranged data fields in different data records may differ from one data record to another. Thus, a number of different reordering schemes may be used, including the case that for some data records, the order of the data fields is not altered at all. Preferably, the cyclic reordering is performed by shifting all data fields in each data record. The data fields may be shifted by a number of steps ranging from zero, i.e. no shift takes place, to a number corresponding to the number of data fields in the data record minus 1. Thus, the reordering algorithm contains information as to the number of steps each data field is shifted for a specific data record.

[0023] According to a specific embodiment of the present invention, the order of the data fields in each record included in a first set of data records are rearranged according to a first reordering algorithm. Thereby, a first set of rearranged data records is obtained. Then, the order of the data fields in each data record of a second set of data records are rearranged according to a second reordering algorithm, whereby a second set of rearranged data records is obtained. In the generation of the encryption key, the first set of rearranged data records forms key data and the second set of rearranged data records forms input data, or vice versa, of the encryption key used in the encryption algorithm. Alternatively, the key data and the input data form encryption data that can be used as material in an encryption process. For example, the material can be encrypted with the public key of the receiver, to be used as encryption key or key material, to be compressed to an encryption key, for a symmetric encryption algorithm. The advantage of the described rearranging process is that the statistical characteristics, i.e. the randomness and unpredictability, of the processed data are significantly improved.

[0024] According to a further preferred embodiment of the invention, it has surprisingly been found that a particular high degree of stochasticity have been achieved using the specific reordering algorithm explained in greater detail below. In fact, the output data of the encryption algorithm, when using the optical data as random seed and the described reordering algorithm, constitute uniformly distributed noise according to prevalent statistical testing methods.

[0025] According to an alternative preferred embodiment of the invention, the stochasticity of the obtained optical data organized in data records is improved using hash functions. According to this embodiment, a first hashing is performed on a set of a predetermined number of data records by a first algorithm, i.e. a first hash function. As understood by the person skilled in the art, hashing is an iterative process which will not be described in detail. Therefore, the term hashing output, as used hereinafter, refers to the result of all iterations included in the hashing. Thus, a first output, i.e. a first hashing output, is obtained from the first hashing. The first output is then used as an input to a second algorithm, which may be a second hash function. The output of the second algorithm, i.e. random numbers, is then, for example, used as the encryption key or for generating an encryption key in an encryption algorithm for encrypting a message. However, the second algorithm may alternatively be an iterative algorithm different from a hash function. For example, A3 or A5, which are stream ciphers and are used for symmetrical encryption, may be used.

[0026] The first hash function introduces distortion or noise in the obtained optical data used as input data. In other words, it shatter the regularities in the optical data and the correlation between data fields included in the data records. The use of a second hash function, or an alternative, preferably iterative, algorithm, on the first output further improves the statistical characteristics of the data and provides a further distortion on the first output. Thus, the statistical characteristics, i.e. the randomness and unpredictability, of the processed optical data are significantly improved using the method according to this embodiment. The improvement is such that the random numbers generated as a result of the method of this embodiment can be regarded as uniformly distributed white noise according to prevalent statistical testing methods. According to a preferred alternative of this embodiment, symmetrical encryption algorithms are used in the first and second algorithms. By using the same encryption algorithm for the algorithms, the advantages of a simplified implementation of the program code of the algorithms and a saving of memory capacity are achieved.

[0027] Furthermore, when using a symmetrical encryption algorithm, such as AES, for the actual encryption of the message, this encryption algorithm is preferably used in at least one of said algorithms as well, and preferably in both. However, it is conceivable within the scope of the present invention that other and different encryption algorithms may be used in each of said algorithms, as well as for the actual encryption of the message. Preferably, in order to even further improve the stochasticity of the encryption key, or of the random numbers used for generating the encryption key, statistical properties of the parameter are. This results in a higher degree of randomness and unpredictability. Examples of statistical properties preferably being used includes maximum, minimum and sum values of the sensed parameter. However, other statistical properties are conceivable, such as mean values, standard deviation values, etc. As realized by the person skilled in the art, the use of said calculation of statistical properties is by no means restricted to a specific embodiment of the present invention. Contrarily, the statistical properties of the optical data may be calculated

WAVELYNX EX. 1003, Pg. 1059
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

and the result thereof may be used to improve the stochasticity of the optical data, and the encryption key generated therewith, regardless of the chosen method for generating the encryption key.

[0028] Furthermore, the optical data used for generating an encryption key may constitute part of the message to be encrypted and transmitted. Alternatively, the optical data do not constitute part of the message. Furthermore, the step of obtaining optical data for encrypting the message may be obtained prior to, during, or following the procedure of obtaining the message to be encrypted. As an example, the encryption of the message may take place just prior to the actual transmission thereof. Then, the encryption key, including obtaining optical data, whether the optical data are extracted from the message or not, may be generated in connection with the encryption procedure. Alternatively, the generation of the encryption key may have been performed earlier, e.g. in connection with obtaining and storing the message, and a stored encryption key is used for the encryption.

[0029] Suitably, the optical data used for generating an encryption key are stored in a storage medium prior to processing thereof. In an alternative embodiment the optical data are stored after the processing thereof.

[0030] Preferably, a symmetrical encryption algorithm is used for the actual encryption of the message. There are a number of conceivable symmetrical encryption algorithms that are suitable, for example AES, DES, or IDEA. The use of an asymmetric encryption algorithm, such as the RSA, for the actual encryption of the message is also conceivable and lie within the scope of the present invention. However, the present invention is not limited to a specific encryption algorithm.

[0031] The method of the present invention is implemented in a digital pen. Such a digital pen comprises an optical sensor for obtaining a message to be transmitted, for instance from a surface provided with a position code pattern as described above. Preferably, the digital pen also comprises illumination means for illuminating a surface to be read by the optical sensor. The illumination means and the optical sensor may be restricted to a limited wavelength range, such that the optical sensor primarily detects reflected light that are provided by the illumination means. The optical sensor is also used for obtaining the optical data used for generating an encryption key. Thereby, no additional sensor or random number generator is required within the limited interior of the digital pen.

[0032] Furthermore, the digital pen comprises a processor or processing means for performing the steps of the present invention, as well as all the steps required for obtaining, encrypting and transmitting a message. Furthermore, the digital pen also comprises, inter alia, suitable storing means for storing data, power supply means, e.g. a battery, as well as transmission means for transmitting the message to a receiver.

[0033] According to a further embodiment of the invention, a pressure sensor is provided for obtaining pressure data. Since the pressure data relates to biometric factors, such as movements of the hand, the degree of randomness of the pressure data is high. The pressure data can then be used in combination with the optical data as random number data or random seed, in the generation of an encryption key, in order to enhance the degree of randomness in the random seed.

[0034] Also, according to yet another embodiment of the invention, time data are obtained and used in combination with the optical data as random seed in order to enhance the stochasticity of the random seed. Although time data is deterministic by nature, the degree of randomness of the combined data will not be decreased. The time data are preferably provided by the internal clock of the processing means. The thus obtained random seed may be subsequently used in the generation of the encryption key in the manner as described above.

[0035] As understood be the person skilled in the art, there are other related areas where the random numbers generated from optical data in accordance with the present invention may be utilized. One such area is authentication of a sent or received message.

[0036] Another area is key transport from a sender to a receiver. Then, the random numbers are encrypted with a public key of the receiver and are used as an encryption key or key data, to be subsequently compressed to an encryption key, for a symmetric encryption algorithm.

[0037] The random numbers can also be used to generate prime numbers for RSA or DH keys.

[0038] As realized by the person skilled in the art, the method and the device of the present invention, as well as the preferred embodiments thereof, are suitable to realize as a computer program or a computer readable medium, preferably within the contents of a digital pen.

[0039] Further objects and advantages of the present invention will be discussed below by means of exemplifying embodiments.

Brief description of the drawings

[0040] Preferred embodiments of the invention will now be described in greater detail with reference to the accompanying drawings, in which

Fig. 1 shows an embodiment of an information management system;
Fig. 2 schematically shows an embodiment of a product provided with a position-code pattern;
Fig. 3 schematically shows an embodiment of a sending device according to the present invention;

WAVELYNX EX. 1003, Pg. 1060
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Fig. 4 shows a flow diagram illustrating an embodiment of a method according to the present invention for encrypting a message using optical data;
Fig. 5 shows a flow diagram illustrating an algorithm of a first embodiment for increasing randomness in optical data used for generating an encryption key;
Fig. 6 schematically shows the order of data fields within a key data block and an input data block prior to a cyclic reordering procedure according to an embodiment of the present invention;
Figs 7A and 7B schematically show the order of data fields within the key data block and input data block, respectively, after said cyclic reordering procedure; and
Fig. 8 shows a flow diagram illustrating an algorithm of a second embodiment for increasing the randomness in the input data used for generating an encryption key.

Description of preferred embodiments

[0041] In the following, an information management system in which the present invention can be implemented is described with reference to Fig. 1. After this general presentation of the system structure, a product provided with a position code pattern will be described with reference to Fig. 2. Then, with reference to Fig. 3, a sending device, in which the present inventive method and device can be implemented, designed for reading and obtaining optical data from the position code of Fig. 2 is shown.

[0042] With reference first to Fig. 1, an information management system in which a position-code product and a sending device, such as a digital pen, can be integrated is shown. There are many inter-reliant actors involved in the system of Fig. 1: companies manufacturing the digital pens ("pen manufactures"), companies manufacturing the position-coded products ("paper manufactures"), companies providing different services by means of service handler units ("service handlers"), a company administrating the position-code based on the virtual space database ("pattern administrator"), operators providing the communication links between the digital pens and the different units ("network operators"), and a multitude of users of digital pens ("pen owners").

[0043] The system of Fig. 1 includes a multitude of sending devices or digital pens DP and position code products P (only one of which being shown in Fig. 1), a look-up unit ALS, and a plurality of service handler units SH (only one of which is shown in Fig. 1). It should be noted that the information can be transmitted in any suitable way from the digital pen DP to the look-up unit ALS and the service handler unit SH. In one embodiment, wireless transmission of information is effected from the digital pen DP to a network connection unit, which in turn transmits the information to the look-up unit ALS and service handler unit SH, respectively. The network connection unit can be an integral part of the digital pen DP. Alternatively, the network connection unit can be a mobile phone or a computer or any other suitable unit with an interface to a computer network such as the Internet or a LAN. The look-up unit ALS is connected to a virtual space database GSDB which includes data on the functionality of every position coded by the position code PC and the actor associated with each such position. The look-up unit ALS is also connected to a pen database PDB, which includes data on all digital pens in the system, such as the unique pen identifier of each pen and all settings or properties that are associated with each pen. The pen database PDB also includes data relating to the manufacturer of each pen. In addition thereto, the look-up unit ALS is connected to an event database GEDB, which includes data on the transactions taking place in the look-up unit ALS, i.e. the address requests made by the pens in the system and the address responses returned to the pens, as well as any errors occurring in the process. As an alternative to individual databases as shown in Fig. 1, the look-up unit ALS could be connected to one all-embracing database.

[0044] The system also includes one or more networks in which network operators handle the communication between the digital pens DP and the look-up unit ALS, and between the digital pens DP and the service handler unit SH. To this end, the owner of a pen has opened a subscription at one of the network operators. This network operator could also act as a service handler in the system, for example by means of a server unit SP providing communication services that allows the pen owner to send electronic messages, for example e-mail, SMS or fax, based on information written on the position-coded products P by means of the digital pen DP. The server unit SP of the network operator could also provide for network storage of information generated in the system, for example entries in an position-coded calendar or notebook. When acting as a service handler, the network operator maintains an application database ASDB which contains data on user-specific settings for different applications, for example a signature or electronic business card to be attached to e-mail messages, where and how to store sent messages, etc.

[0045] In the embodiment of Fig. 1, the system includes Internet portals hosted by one or more web servers which are interfaced with the databases of the system, one portal of which P1 being shown in Fig. 1. The portal P1 is a so-called Partner Portal, i.e. a portal which allows pen manufactures, paper manufactures, service handlers and network operators to access selected portions of the databases of the system, via an interface unit IF. An example of another portal is a so-called Pen Owner Portal, i.e. a portal which allows for the pen owners to access selected portions of the databases of the system. In an alternative embodiment, the functionalities of the two portals are merged into one common portal.

WAVELYNX EX. 1003, Pg. 1061
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0046] In the communication between the different participants illustrated in Fig. 1, it is desirable that the information is sent in a secure way, i.e. by using encryption and digital signatures. If the digital pen DP sends confidential information to the service handler unit SH, the digital pen DP encrypts the information and the service handler unit SH will, in order to decipher the information, decrypt it. The digital pen DP can use either symmetric encryption or asymmetric encryption.

[0047] In Fig. 2, a portion of a product, such as the position-coded product used in the system of Fig. 1, in the form of a paper 1, provided with, on its surface 2, an optical readable position code pattern 3 which enables a determination of the position. The position code pattern includes markings 4, which are methodically arranged over the surface 2. The Applicant proposes in the international patent application WO 01/16691, which is incorporated herein by reference, the use of a product having a writing surface which is provided with such a position code. The position code, which codes a plurality of positions on the surface, enables electronic recording of information that is being written on the writing surface, by means of a digital pen which detects the position code. The position code is capable of coding coordinates of a large number of positions, much larger than the number of required positions on the product. Thus, the position code can be seen as forming a virtual space which is defined by all positions that the position code is capable of coding, whereby different positions in the virtual space can be dedicated for different functions and/or actors. It should be noted that the position code pattern shown in Fig. 2 is, for the sake of clarity, greatly enlarged.

[0048] Fig. 3 shows a schematic representation of an embodiment of a sending device designed for reading, for example, a position code pattern of Fig. 2. The device is a digital pen. The pen DP comprises a housing 5, shaped in a pen-like form. An opening 6 is provided at one end portion of the housing 5. The opening is intended to rest against, or to be held at a short distance from, the surface S from which information is to be obtained.

[0049] Within the housing 5 an optical unit, an electronic unit, and a current supply unit are incorporated. According to further embodiments of the digital pen, a pressure sensor unit may also be comprised within the housing 5, which will be discussed below.

[0050] The optical unit comprises a diode 7, arranged to illuminate the surface provided with the position code, and a light-sensitive sensor 8, for example a CCD sensor (Charge-Coupled Device) or a CMOS sensor (Complementary Metal-Oxide semiconductor), arranged to register two-dimensional images. The current supply unit is in this embodiment a battery 9, arranged in a separate container.

[0051] The electronic unit 10 comprises a processor device including image-processing means, encryption means and a processor programmed to read images from the sensor 8 and to perform determination of the position and decoding of information on the basis of the images. Furthermore, the processor is programmed to perform computations in order to, for example from an image received from the sensor, calculate properties of the optical data obtained from the image. The data resulting from these computations can be used as input data for other computations or algorithms, such as encryption algorithms. In this embodiment, the AES and RSA algorithms are implemented in the processor device.

[0052] Also, the electronic unit 10 comprises a memory or data storage that is arranged, for example, to store data received from the processor or the sensor, as well as program instructions for the processor device.

[0053] Furthermore, the pen may comprise a keypad 11, which enables activation and controlling of the pen. A transceiver 12 for wireless communication, by means of IR-light or radio waves, with other participants of the system of Fig. 1 is also included. Additionally, a display 13 for showing, for example, registered information can be included. The keypad, the transceiver, and the display are in communication with and controlled by the electronic unit 10.

[0054] It should be noted that the illustration of Fig. 3 is schematical and that the actual configuration of the parts comprised within the pen may differ from the configuration shown without departing from the scope of the present invention.

[0055] In the above-mentioned embodiment, the position-code pattern is an optical readable pattern and, thus, the sensor is an optical sensor. The position code pattern can be based on another parameter than an optical parameter as mentioned above. In that case, the sensor must, of course, be of such a type that is capable of reading the parameter in question.

[0056] The combination of a digital pen and a position-coded product can be used as an input device to a computer, a PDA, a mobile phone, or the like.

[0057] For example, text and sketches written on a position-coded notepad can be transferred via the pen to a computer. Additionally, the combination of a pen and a position-coded product allows for global communication, directly from the product via the pen, by the position code on the product being dedicated for such communication. For example, the information registered by the pen can be transformed into a fax message, an e-mail or an SMS, and can then be sent from the pen to a recipient. Further, the combination of a pen and a position-coded product can be used in e-commerce. For example, the digital pen can be used to order an item from a position-coded advertisement in a magazine, by the position code in the advertisement being dedicated for such a service.

[0058] The above concept has been implemented in a system or infrastructure, which is shown in Fig. 1 and which is further disclosed in Applicant's international patent applications WO 0 148 678, WO 0 148 591 and WO 0 148 685.

[0059] There will now be presented in the form of a flow diagram, with reference to Fig. 4, the inventive method for encryption of a message based on information written on the position coded products of Fig. 2 by means of the sending

WAVELYNX EX. 1003, Pg. 1062
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

device of Fig. 3, and to thereby provide a secure transmission of said message from a sending device to a receiver, for example in the form of an e-mail, an SMS, or a fax. Furthermore, the position coded product and the sending device is preferably incorporated in a system as presented in Fig. 1.

[0060] Beginning at step 410, a patterned surface is read or scanned by the sensor 8, whereby an optical image OI is obtained. The image OI is then stored as a mapping of the pattern in an image storing medium. The optical image OI or the optical data representing the image includes a predetermined number of pixels. Each optical image OI is, in turn, divided into a predetermined number of subimages or image elements, wherein each image element includes a predetermined number of pixels. The size and number of these pixel representations, i.e. the resolution, is adjustable.

[0061] According to one exemplifying embodiment, each optical image includes 96x96 pixels. Furthermore, the 96x96 pixels are divided in a matrix constituent of 16x16 image elements, wherein each image element consequently consists of 6x6 pixels. Of course, there are any number of conceivable pixel configurations of an optical image that can be used without departing from the scope of the present invention.

[0062] At step 420, decoding of information comprised in the data of the optical image is performed. In the preferred embodiment, the resulting optical data OD comprise information of the brightness on the portion of the surface that has been read. Factors having an influence on the sensed brightness have already been discussed above. The brightness is represented by discrete values. In the preferred embodiment of the present invention, a white surface corresponds to a value of 255 and a black surface, e.g. a black marking, corresponds to a value of 0. To enhance the dynamics of the optical data, it is preferred that each image element, representing a portion of the surface, includes data of at least one marking and at least a portion of a surface surrounding the markings.

[0063] However, any of the input values from the digital pen's sensors, such as pen pressure, coordinates, time, or the like, can be used as parameters for key generation. These parameters are then used in combination with the optical data OD or in combination with computer random seeds.

[0064] At step 430, the optical data OD produced by the sensor are processed to calculate specific statistical properties of the optical data. According to the most preferred embodiments, a maximum value, a minimum value and a sum value of the intensity or brightness of a number of pixels are calculated and used in the continued process as optical data. The thus calculated statistical values are hereinafter referred to as processed optical data POD. This calculation is performed on each image element, i.e. on the optical data OD represented in each image element, respectively. There are, of course, other preferably statistical properties that may be calculated, such as a mean value, or a standard deviation value.

[0065] Thereafter, at step 440, the resulting sequence of processed optical data POD is organized in bit-groups or data fields. According to the most preferred embodiment of the present invention, each image element is represented by one data record DR and each data record DR consists of four data fields. The first two data fields contain the calculated sum value, the third contains the calculated minimum value, and the fourth contains the calculated maximum value. Thus, a sequence of data records DR is produced from one optical image, each data record corresponding to one image element of the image. When the data records DR are produced, they are optionally stored in a cyclic register, prior to the use as random number data, and are arranged in the processor device to be accessed by the processor when required, for example at the transmission of a message.

[0066] Then, at step 450, the sequence of data records DR is processed in an algorithm in order to increase the stochasticity of the processed optical data in the data records. This is due to the fact that the processed optical data POD are not one hundred percent random in a statistical sense. Thus, it is desirable to perform additional processing in order to improve the statistical characteristics of the optical data, i.e. increase the randomness or stochasticity of the processed optical data, before the processed optical data is used as a random seed. Figs 5 and 8 show two different algorithms of two alternative embodiments of the present invention for increasing the randomness of the processed optical data. These algorithms will be described in greater detail below.

[0067] Finally, at step 460, the processed optical data are used as an encryption key EK in an encryption algorithm and encryption of a message obtained from the position-coded surface using the digital pen is performed.

[0068] According to an alternative embodiment, the processed optical data is, at step 460, used for authentication of a sent message. Then, the processed optical data are used as random number data, which is encrypted by means of an encryption key, for example a private key of the digital pen, and the encrypted random number data is used for authentication of said sent message.

[0069] Encryption algorithms, such as the AES encryption algorithm, uses block encryption. A block cipher, i.e. an encryption algorithm using block encryption, is a method of encryption text (to produce ciphertext) in which an encryption key and algorithm are applied to a block of data at once as a group rather than to one bit at a time. The main alternative method, used much less frequently, is called the stream cipher.

[0070] There is a cryptologic difficulty when the text to be encrypted contains static data, that do not change from on text to the other. If different encryption keys are used to encrypt the text that contains static data, an attacker could draw conclusions regarding the key if the position of the static data is known by the attacker. In order to prevent this, it is common to apply the cipher text from the previous encrypted block to the next block in the sequence. This way of

WAVELYNX EX. 1003, Pg. 1063
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

encrypting in block ciphers are often referred to as CBC (Cipher Block Chaining) encryption. The encryption of the block including the static data is then dependent of all previous text blocks, which makes it more or less impossible to draw conclusions regarding the key from the encryption of the static data. To ensure this, an initiation vector derived from a random generator is combined with the text in the first block. Consequently, and according to preferred embodiments of the present invention, the processed optical data are used for forming both the encryption key, i.e. the key data block, and the initiation vector, i.e. the input data block.

[0071] With reference now to Fig. 5, there is shown a flow diagram of the method according to a first preferred algorithm in accordance with the present invention for increasing the randomness or stochasticity of the processed optical data and to produce random numbers. It should be noted that the following description with reference to Figs 5, 6, 7A, and 7B corresponds to step 450 of Fig. 4.

[0072] First, at step 510, the sequence of data records, obtained at step 440 of Fig. 4, is organized into data blocks, wherein each data block is determined or labeled as either a key data block KB or an input data block IB, in accordance with the description above. According to the most preferred embodiment of the present invention, four subsequent data records are organized in a single data block. Furthermore, every second data block is a key data block KB, and the intermediate data blocks are input data blocks IB.

[0073] Then, at step 520, the key data blocks KB are processed according to a first mathematical algorithm, and at step 530 the input data blocks IB are processed according to a second mathematical algorithm. The mathematical algorithms define a cyclic reordering or shifting procedure of the data fields included in the key data block KB and the input data block IB, respectively.

[0074] With particular reference to Fig. 6, the order of the data fields within a key data block KB or an input data block IB are shown prior to the shifting procedure. The records are shown schematically as boxes divided into four elements, each element representing a data field. In the most preferred embodiment, the fields indicated with 1 and 2 include the sum of brightness, the fields indicated with 3 the minimum, and the field indicated with 4 the maximum. The cyclic shifting scheme of the data fields included in the key data block KB is shown below in table 1.

Table 1

Data record	Steps
A	0
B	3
C	2
D	1

[0075] In Fig. 7A, the order of the data fields within the key data block after the cyclic shifting has been performed is shown. The data fields of the first data record, record A, retain their positions, the data fields within the second record, record B, are shifted three positions to the right, the fields within the third record, record C, are shifted two positions to the right, and the fields within the fourth record, record D, are shifted one position to the right. The data block output as a result of the reordering algorithm for a key data block is referred to as reordered key data block, RKB.

[0076] In table 2, the cyclic shifting scheme of the data fields included in the input data block IB is shown.

Table 2

Data record	Steps
A	1
B	2
C	3
D	0

[0077] In Fig. 7B, there is shown the order of the data fields within the input data block after the cyclic shifting, to the right, has been performed. The data fields within the first data record, record A, are shifted one position, the data fields within the second data record, record B, are shifted two positions, the data fields within the third data record, record C, are shifted three positions, and the data fields within the fourth data record, record D, retain their positions. The data block output as a result of the reordering algorithm for an input data block is referred to as reordered input data block, RIB.

[0078] It should be noted that a wide variety of shifting algorithms may be used within the scope of the present invention

WAVELYNX EX. 1003, Pg. 1064
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

to obtain reordered or rearranged key and input data blocks. However, it has surprisingly been found that the above described reordering of the data fields within the data records included in the key data block and the input data block provides a particular and considerable improvement of the desired statistical properties for the output data of an ensuing encryption, when using the result of the reordering procedure as key data and input data for the encryption. In other words, the randomness and stochasticity of the output data is increased and the predictability is decreased. In fact, according to statistical testing procedures recognized within the art, the output data of the encryption algorithm, i.e. the encrypted message, can be regarded as uniformly distributed white noise. This unexpected effect is due to the fact that the correlation between the processed optical data included in the data fields within a data record, which in turn is transmitted to the output data of the encryption algorithm, is shattered by the above-mentioned reordering procedure.

[0079] Then, at step 540, the data in the thus reordered key and input data blocks are used as the encryption key, key data KD, and the initiation vector, input data ID, respectively, for the encryption algorithm.

[0080] Finally, at step 550, the method is returned to the procedure shown in Fig. 4 at step 460, where the actual encryption of the message is performed using, in this preferred embodiment, the AES encryption algorithm. However, other encryption algorithms are of course contemplated within the scope of the present invention.

[0081] Below, a second alternative preferred embodiment of an algorithm for improving the statistical characteristics of the processed optical data will be described, with particular reference to Fig. 8.

[0082] The algorithm can be regarded as having two parts. In the first part, referred to as the seed update, a random seed is calculated based on the processed optical data. In the second part, referred to as the random number calculation, the thus calculated random seed is used as input data for calculation of the random numbers to be used in the encryption algorithm.

[0083] Data blocks that include a subset of the sequence of data records containing the processed optical data form the input data in the seed update part. The data records comprise data fields, preferably organized as is described above in relation to the first preferred embodiment. Thus, each data record includes four data fields, the first two including the sum value, the third the minimum value, and the fourth the maximum value, see Fig. 6.

[0084] At step 810, each data block is processed in a first hash function, which in this embodiment is an encryption algorithm, in order to increase the randomness of the data records containing the processed optical data. The first hash function is, in this embodiment, a symmetrical encryption algorithm. The data records containing the processed optical data are used as the encryption key, and an arbitrarily chosen vector is used as the initiation vector. However, it is preferred that the number of ones and zeros are substantially equal and appropriately distributed throughout the initiation vector. This can be achieved by using the previous seed as the initiation vector for the hashing algorithm, which will remove the risk of patterns that may be produced due to frequent seed updates with substantially similar input data, and will improve the quality of the random seed.

[0085] Then, at step 820, an iterative process concatenates each hashing output or hash value, HV, and thereby forms hashing output data blocks. This is due to the fact that a hashing process normally results in an output having a data size that is less, or much less, than the data size of the input data. The number of iterations is dependent on the desired size of the output data.

[0086] The output data blocks are then divided into key data blocks and seed data blocks at step 830. The key data blocks and seed data blocks are used as input data in the random number calculation part. This can mathematically be written as

Input data:	optical data	$= SU_{2^*m-1}..SU_1SU_0$
Calculation:	SI_x	$= Hash_n (SI_x, SU_x)$
Output data:	seed input	$= SI_{2^*m-1}..SI_1SI_0$
		$= SK_{m-1}..SK_1SK_0SD_{m-1}..SD_1SD_0$
	key data	$= SK_{m-1}..SK_1SK_0$
	seed data	$= SD_{m-1}..SD_1SD_0$

where = Y/n, Y is the bit-length of the random number to be generated in the second step, and n is the bit-length of the output data of the hashing algorithm, Hash. Furthermore, SU_x is input data block x, SI_x is output data block x, SK_x is key data block x and SD_x seed data block x. In this embodiment, the hashing algorithm is performed using a symmetric encryption algorithm, AES. As realized by the person skilled in the art, there are a significant number of conceivable algorithms that can be used to obtain an increased randomness and that can be implemented instead of the AES algorithm. The seed update can be performed with a full update of the seed, i.e. with all data blocks included in SI, or with one data block, SI_x. This is dependent on the requirements of the random number calculation algorithm in part two and the computer power at hand.

[0087] Then, at step 840, in the random number calculation part, the key data blocks and seed data blocks are used as input data in a second algorithm, which in this embodiment utilizes a symmetrical encryption algorithm, for example

WAVELYNX EX. 1003, Pg. 1065
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

AES. The algorithm performed at step 840 is an iterative algorithm. As mentioned above, there are a number of alternative encryption algorithms that can be used in said second algorithm instead of AES, for example IDEA or DES. Alternatively, A3 or A5, which are stream ciphers and are used for symmetrical encryption, may be used. A counter, seed count, is also included. It counts the number of times the random number calculation was used since the input data were updated in the seed update. Mathematically, the random number calculation can be written as

Input data:	key data	$= SK_{m-1}..SK_1SK_0$
	seed data	$= SD_{m-1}..SD_1SD_0$
	seed count	
Calculation	For x from 0 to (m-1)	
	1.1 PR_x	= Encrypt (key=SK_x, input=SD_x)
	1.2 $SK_{(x+2)\bmod m}$	= $SK_{(x+2)\bmod m}$ xor PR_x
	1.3 $SD_{(x+1)\bmod m}$	= $SD_{(x+1)\bmod m}$ xor PR_x
	seed count	= seed count + 1
Output data:	random number	$= PR_{m-1}..PR_1PR_0$
	key data	$= SK_{m-1}..SK_1SK_0$
	seed data	$= SD_{m-1}..SD_1SD_0$
	seed count	

where PR_x is a random number data block x, xor is an XOR operation, mod is a modulus operation, and encrypt is a symmetric encryption algorithm. Also, a block transformation is performed in the calculation step. This transformation further increases the randomness of the random numbers.

[0088] The transformation of steps 1.2 and 1.3 could be made in a number of other ways, but the described method ensures that all changes in a block is transformed through out most of the random seed, and thereby ensures a high quality random seed for the following calculation.

[0089] According to an alternative embodiment, the second algorithm is a hash function, preferably using the same symmetrical encryption algorithm as in the second algorithm described above.

[0090] Finally, at step 850, the method is returned to the procedure shown in Fig. 4 at step 460, where the actual encryption of the message is performed using, in this preferred embodiment, the AES encryption algorithm, where the random number data PR_x obtained through the above method are used as the encryption key at step 460 of Fig. 4.

[0091] Alternatively, an encryption of the random number data PR_x is performed, for example by the use of an asymmetric encryption algorithm. Then, the encrypted random number data is sent to the receiver of the encrypted message. The receiver performs a hashing on the encrypted random number data and uses the resulting hash value as a private encryption key, which then is used in an asymmetric encryption algorithm for decryption of the received message.

[0092] Although specific embodiments have been shown and described herein for purposes of illustration and exemplification, it is understood by those of ordinary skill in the art that the specific embodiments shown and described may be substituted for a wide variety of alternative and/or equivalent implementations without departing from the scope of the present invention. Those of ordinary skill in the art will readily appreciate that the present invention could be implemented in a wide variety of embodiments, including various hardware and software implementations, or combinations thereof. This application is intended to cover any adaptations or variations of the preferred embodiments discussed herein. Consequently, the present invention is defined by the wordings of the appended claims.

Claims

1. A method in a digital pen (DP) for encrypting a message for secure transmission of said message from the digital pen (DP) to a receiver (ALS, SH, SP), **characterized by** the steps of obtaining the message by registering images of a surface (2) provided with a position code pattern (3) using an optical sensor (8) in the digital pen (DP) and determining at least one position from the images;
obtaining (410-420) optical data for the generation of an encryption key using the optical sensor (8) in the digital pen (DP), said optical data electronically representing values of an optical parameter readable by said optical sensor (8);
generating (430-450), exclusively by electronic processing in a processor (10) of the digital pen, the encryption key using said optical data as random seed; and
encrypting (460) said message using said encryption key in an encryption algorithm.

WAVELYNX EX. 1003, Pg. 1066
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2. The method according to claim 1, wherein said optical parameter is brightness sensed by said optical sensor (8).

3. The method according to claim 1 or 2, wherein the step (410-420) of obtaining optical data comprises the step of obtaining said optical data from a portion of a surface (2) provided with a position code pattern (3), wherein said position code pattern (3) includes optical readable markings (4), and wherein said optical parameter is representative of said portion.

4. The method according to any one of claims 1-3, wherein the step (430-450) of generating an encryption key comprises the steps of
processing (430) said optical data according to a predetermined scheme,
organizing (440) said processed optical data in data fields, wherein each data field has a predetermined size, and
organizing (440) said data fields in a predetermined order in data records.

5. The method according to claim 4, wherein the step (430) of processing said optical data comprises the step of calculating statistical properties of sets of said optical parameter values represented by said optical data, whereby said statistical properties constitute said processed optical data.

6. The method according to claim 5, wherein said statistical properties comprise a maximum value, a minimum value and a sum value of said set of optical parameter values, and wherein the steps (440) of organizing comprises the steps of
organizing said maximum value in at least one maximum data field, said minimum value in at least one minimum data field, and said sum value in at least one sum data field, and
organizing said maximum, minimum, and sum data fields in a data record according to said predetermined order.

7. The method according to any one of claims 4-6, wherein the step (430-450) of generating an encryption key further comprises the steps of
rearranging (520) the order of said data fields within at least one data record of a first series of data records according to a first reordering algorithm, thereby obtaining a first series of rearranged data records, and
rearranging (530) the order of said data fields within at least one data record of a second series of data records according to a second reordering algorithm, thereby obtaining a second series of rearranged data records.

8. The method according to claim 7, wherein an encryption key comprises key data and input data, and wherein the step (430-450) of generating an encryption key comprises the steps of
using (540) said first series of rearranged data records as said key data, and
using (540) said second series of rearranged data records as said input data.

9. The method according to any one of claims 4-6, wherein the step (430-450) of generating an encryption key comprises the steps of
processing a set of a predetermined number of said data records in a first step (810-820) using a first hash function, thereby obtaining a first output,
processing said first output in a second step (830-840) using an iterative algorithm, thereby obtaining a second output, and
using (850) said second output as said encryption key or for generating said encryption key.

10. The method according to claim 9, wherein, in said second step (830-840), said first output is processed using a second hash function.

11. The method according to claim 9 or 10, wherein in said first and second steps (810-820, 830-840), a first and a second symmetrical encryption algorithm, respectively, is used.

12. The method according to claim 11, wherein one symmetrical encryption algorithm is used both as said first and as said second symmetrical encryption algorithms.

13. The method according to claim 12, wherein one symmetrical encryption algorithm is used both as said encryption algorithm for performing said step (460) of encrypting said message, and as said first and said second symmetrical encryption algorithms.

14. The method according to any one of the preceding claims, wherein the encryption key comprises key data and input

WAVELYNX EX. 1003, Pg. 1067
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

data, the method further comprising the steps of
using a first subset of said optical data for generating said key data, and
using a second subset of said optical data for generating said input data.

15. The method according to any one of the preceding claims, wherein said encryption algorithm for encrypting said message is a symmetric encryption algorithm.

16. The method according to claim 1, further comprising the steps of
obtaining pressure data using pressure sensing means, wherein the step (430-450) of generating an encryption key comprises the step of
generating the encryption key using said pressure data in combination with said optical data as random seed.

17. The method according to claim 1, further comprising the steps of
obtaining time data, wherein the step (430-450) of generating an encryption key comprises the step of
generating the encryption key using said time data in combination with said optical data as random seed.

18. The method according to any one of the preceding claims, wherein said steps are performed in a digital pen (DP) comprising said optical sensor (8) and transmission means (12).

19. Computer readable medium comprising instructions for bringing a computer to perform a method according to any one of the preceding claims.

20. A digital pen (DP) for encrypting a message for secure transmission of said message from the digital pen (DP) to a receiver (ALS, SH, SP), **characterized by** an optical sensor (8) for registering images of a surface (2) provided with a position code pattern (3);
receiving means (10) for receiving optical data from the optical sensor (8) for the generation of an encryption key, said optical data electronically representing values of an optical parameter readable by said optical sensor (8),
processing means (10) for generating, exclusively by electronic processing, the encryption key using said optical data as random seed, and for obtaining said message by determing at least one position from said recorded images;
encryption means (10) for encrypting the message to be transmitted using said encryption key.

21. The digital pen according to claim 20, wherein said optical data has been obtained from a portion of a surface (2) provided with a position code pattern (3) having optical readable markings (4).

22. The digital pen according to claim 21, wherein said processing means (10) is further arranged to
process said optical data according to a predetermined scheme,
organize said processed optical data in data fields, wherein each data field has a predetermined size, and
organize said data fields in a predetermined order in data records.

23. The digital pen according to claim 22, wherein said processing means (10) is further arranged to calculate statistical properties of sets of said optical parameter values represented by said optical data, whereby said statistical properties constitute said processed optical data.

24. The digital pen according to claim 23, wherein said properties comprise a maximum value, a minimum value and a sum value of said set of optical parameter values, and wherein said processing means (10) is further arranged to
organize said maximum value in at least one maximum data field, said minimum value in at least one minimum data field, and said sum value in at least one sum data field, and
organize said maximum, minimum, and sum data fields in a data record according to said predetermined order.

25. The digital pen according to any one of claims 22-24, wherein said processing means (10) is further arranged to
rearrange the order of said data fields within at least one data record of a first series of data records according to a first reordering algorithm, thereby obtaining a first series of rearranged data records, and
rearrange the order of said data fields within at least one data record of a second series of data records according to a second reordering algorithm, thereby obtaining a second series of rearranged data records.

26. The digital pen according to claim 25, wherein an encryption key comprises key data and input data, and wherein the processing means (10) is further arranged to
use said first series of rearranged data records as said key data, and

WAVELYNX EX. 1003, Pg. 1068
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

use said second series of rearranged data records as said input data.

27. The digital pen according to any one of claims 22-24, wherein the processing means (10) is further arranged to process a set of a predetermined number of said data records in a first step using a first hash function, thereby obtaining a first output,
process said first output in a second step using an iterative algorithm, thereby obtaining a second output, and
use said second output as said encryption key or for generating said encryption key.

28. The digital pen according to claim 27, wherein said processing means (10) is further arranged to use a second hash function for processing said first output in said second step.

29. The digital pin according to claim 27 or 28, wherein in said first and second steps, a first and a second symmetrical encryption algorithm, respectively, is used.

30. The digital pen according to claim 29, wherein the processing means is further arranged to use one symmetrical encryption algorithm both as said first and as said second symmetrical encryption algorithms.

31. The digital pen according to claim 29, wherein one and the same symmetrical encryption algorithm is used by said encryption means (10) for encrypting said message, and by said processing means (10) as said first and as said second symmetrical encryption algorithms.

32. The digital pen according to any one of claims 20-31, wherein said encryption means (10) is further arranged to encrypt said message using a symmetric encryption algorithm.

33. The digital pen according to any one of claims 20-32, wherein said encryption means (10) is further arranged to use a subset of said optical data as key data for said encryption algorithm, and
use a second subset of said optical data as input data for said encryption algorithm.

34. The digital pen according to claim 20, wherein said receiving means (10) is further arranged for receiving pressure data, and wherein said processing means (10) is arranged to generate said encryption key using said pressure data in combination with said optical data.

35. The digital pen according to claim 20, wherein said processing means (10) is further arranged to obtain time data, and to generate said encryption key using said time data in combination with said optical data.

36. A method for authentication of a sent message, wherein said message is sent from a digital pen (DP) to a receiver (ALS, SH, SP), **characterized by** the steps of obtaining the message by registering images of a surface (2) provided with a position code pattern (3) using an optical sensor (8) in the digital pen (DP) and determining at least one position from the images,
obtaining optical data for the generation of random number data using the optical sensor (8) in the digital pen (DP), said optical data electronically representing values of an optical parameter readable by said optical sensor (8),
using said optical data for generating the random number data, exclusively by electronic processing in a processor (10) of the digital pen (DP),
encrypting said random number data, and
using said encrypted random number data for authentication of said message.

Patentansprüche

1. Verfahren in einem digitalen Stift (DP) für die Verschlüsselung einer Nachricht für sichere Übertragung der Nachricht von dem digitalen Stift (DP) zu einem Empfänger (ALS, SH, SP), das durch die folgenden Schritte **gekennzeichnet** ist:

- Ermitteln der Nachricht durch Registrierung von Abbildern einer Oberfläche (2), die mit einem Positionscodemuster (3) versehen ist, unter Verwendung eines optischen Sensors (8) in dem digitalen Stift (DP) und Bestimmen mindestens einer Position aus den Abbildern;
- Ermitteln (410 - 420) von optischen Daten für die Erzeugung eines Verschlüsselungsschlüssels unter Verwendung des optischen Sensors (8) in dem digitalen Stift (DP), wobei die optischen Daten Werte eines optischen

WAVELYNX EX. 1003, Pg. 1069
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Parameters elektronisch repräsentieren, welcher durch den optischen Sensor (8) lesbar ist;
- Erzeugen (430 - 450) des Verschlüsselungsschlüssels ausschließlich durch elektronische Verarbeitung in einem Prozessor (10) des digitalen Stifts (8) unter Verwendung der optischen Daten als Zufallssaat; und
- Verschlüsseln (460) der Nachricht unter Verwendung des Verschlüsselungsschlüssels in einem Verschlüsselungsalgorithmus.

2. Verfahren nach Anspruch 1, wobei der optische Parameter die Helligkeit ist, die durch den optischen Sensor (8) erfasst wird.

3. Verfahren nach Anspruch 1 oder 2, wobei der Schritt (410 - 420) des Ermittelns von optischen Daten den Schritt umfasst des

- Ermittelns der optischen Daten von einem Abschnitt einer Oberfläche (2) die mit einem Positionscodemuster (3) versehen ist, wobei das Positionscodemuster (3) optisch lesbare Markierungen (4) umfasst und wobei der optische Parameter für den Abschnitt repräsentativ ist.

4. Verfahren nach irgendeinem der Ansprüche 1 - 3, wobei der Schritt (430 - 450) der Erzeugung eines Verschlüsselungsschlüssels die Schritte umfasst:

- Verarbeiten (430) der optischen Daten nach einem vorbestimmten Schema,
- Organisieren (440) der verarbeiteten optischen Daten in Datenfeldern, wobei jedes Datenfeld eine vorbestimmte Größe hat, und
- Organisieren (440) der Datenfelder in einer vorbestimmten Reihenfolge in Datensätzen.

5. Verfahren nach Anspruch 4, wobei der Schritt (430) der Verarbeitung optischer Daten den Schritt umfasst der

- Berechnung statistischer Eigenschaften von Sätzen der optischen Parameterwerte, welche durch die optischen Daten repräsentiert werden, wobei die statistischen Eigenschaften die verarbeiteten optischen Daten bilden.

6. Verfahren nach Anspruch 5, wobei die statistischen Eigenschaften einen Maximalwert, einen Minimalwert und einen Summenwert des Satzes optischer Parameter umfassen, und wobei die Schritte (440) des Organisierens die Schritte umfassen des

- Organisierens des Maximalwertes in mindestens einem Maximaldatenfeld, des Minimalwertes in mindestens einem Minimaldatenfeld und des Summenwertes in mindestens einem Summendatenfeld, und
- Organisierens des Maximaldatenfelds, des Minimaldatenfelds und des Summendatenfelds in einem Datensatz entsprechend der vorbestimmten Reihenfolge.

7. Verfahren nach irgendeinem der Ansprüche 4 bis 6, wobei der Schritt (430 - 450) des Erzeugens eines Verschlüsselungsschlüssels ferner umfasst den Schritt des

- Neuanordnens (520) der Reihenfolge der Datenfelder innerhalb mindestens einem Datensatz einer ersten Folge von Datensätzen entsprechend einem ersten Neuanordnungsalgorithmus, wodurch eine erste Folge von neu angeordneten Datensätzen erreicht wird, und
- Neuanordnens (530) der Reihenfolge der Datenfelder innerhalb mindestens einem Datensatz einer zweiten Folge von Datensätzen entsprechend einem zweiten Neuanordnungsalgorithmus, wodurch eine zweite Folge von neu angeordneten Datensätzen erreicht wird.

8. Verfahren nach Anspruch 7, wobei ein Verschlüsselungsschlüssel Schlüsseldaten und Eingabedaten umfasst, und wobei der Schritt (430 - 450) der Erzeugung eines Verschlüsselungsschlüssels die Schritte umfasst der

- Verwendung (540) der ersten Folge von neu angeordneten Datensätzen als die Schlüsseldaten, und
- Verwendung (540) der zweiten Folge von neu angeordneten Datensätzen als die Eingabedaten.

9. Verfahren nach irgendeinem der Ansprüche 4 bis 6, wobei der Schritt (430 - 450) des Erzeugens eines Verschlüsselungsschlüssels die Schritte umfasst des

- Verarbeitens eines Satzes einer vorbestimmten Anzahl der Datensätze in einem ersten Schritt (810 - 820)

WAVELYNX EX. 1003, Pg. 1070
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

unter Verwendung einer ersten Kontrollsummenfunktion, wodurch eine erste Ausgabe ermittelt wird,
- Verarbeitens der ersten Ausgabe in einem zweiten Schritt (830 - 840) unter Verwendung eines iterativen Algorithmus, wodurch eine zweite Ausgabe ermittelt wird, und
- Verwendens (850) der zweiten Ausgabe als Verschlüsselungsschlüssel oder für die Erzeugung des Verschlüsselungsschlüssels.

10. Verfahren nach Anspruch 9, wobei die erste Ausgabe in dem zweiten Schritt (830 - 840) unter Verwendung einer zweiten Kontrollsummenfunktion verarbeitet wird.

11. Verfahren nach Anspruch 9 oder 10, wobei in dem ersten Schritt (810 - 820) und in dem zweiten Schritt (830 - 840) ein erster symmetrischer Verschlüsselungsalgorithmus bzw. ein zweiter symmetrischer Verschlüsselungsalgorithmus verwendet wird.

12. Verfahren nach Anspruch 11, wobei genau ein symmetrischer Verschlüsselungsalgorithmus verwendet wird sowohl als der erste symmetrische Verschlüsselungsalgorithmus als auch als der zweite symmetrische Verschlüsselungsalgorithmus.

13. Verfahren nach Anspruch 12, wobei genau ein symmetrischer Verschlüsselungsalgorithmus verwendet wird sowohl als der Verschlüsselungsalgorithmus für die Durchführung des Schritts (460) der Verschlüsselung der Nachricht als auch als der erste symmetrische Verschlüsselungsalgorithmus und der zweite symmetrische Verschlüsselungsalgorithmus.

14. Verfahren nach irgendeinem der vorstehenden Ansprüche, wobei der Verschlüsselungsschlüssel Schlüsseldaten und Eingabedaten umfasst, und wobei das Verfahren ferner die Schritte umfasst des

- Verwendens einer ersten Untermenge der optischen Daten für die Erzeugung der Schlüsseldaten, und
- Verwendens einer zweiten Untermenge der optischen Daten für die Erzeugung der Eingabedaten.

15. Verfahren nach irgendeinem der vorstehenden Ansprüche, wobei der Verschlüsselungsalgorithmus für die Verschlüsselung der Nachricht ein symmetrischer Verschlüsselungsalgorithmus ist.

16. Verfahren nach Anspruch 1, das ferner die Schritte umfasst der

- Ermittlung von Druckdaten unter Verwendung einer Druckerfassungseinrichtung, wobei der Schritt (430 - 450) der Erzeugung eines Verschlüsselungsschlüssel den Schritt umfasst der
- Erzeugung des Verschlüsselungsschlüssels unter Verwendung der Druckdaten in Kombination mit den optischen Daten als Zufallssaat.

17. Verfahren nach Anspruch 1, das ferner die Schritte umfasst der

- Ermittlung von Zeitdaten, wobei der Schritt (430 - 450) der Erzeugung eines Verschlüsselungsschlüssel den Schritt umfasst der
- Erzeugung des Verschlüsselungsschlüssels unter Verwendung der Zeitdaten in Kombination mit den optischen Daten als Zufallssaat.

18. Verfahren nach irgendeinem der vorstehenden Ansprüche, wobei die Schritte in einem digitalen Stift (DP) ausgeführt werden, welcher den optischen Sensor (8) und eine Übertragungseinrichtung (12) umfasst.

19. Computer lesbares Medium, das Anweisungen umfasst für die Durchführung eines Verfahrens nach irgendeinem der vorstehenden Ansprüche auf einem Computer.

20. Digitaler Stift (DP) für die Verschlüsselung einer Nachricht für sichere Übertragung der Nachricht von dem digitalen Stift (DP) zu einem Empfänger (ALS, SH, SP), **gekennzeichnet durch**

- einen optischen Sensor (8) für die Registrierung von Abbildern auf einer Oberfläche (2), die mit einem Positionscodemuster (3) versehen ist;
- eine Empfangseinrichtung (10) für den Empfang optischer Daten von dem optischen Sensor (8) für die Erzeugung eines Verschlüsselungsschlüssels, wobei die optischen Daten Werte eines optischen Parameters

WAVELYNX EX. 1003, Pg. 1071
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

elektronisch repräsentieren, welcher **durch** den optischen Sensor (8) lesbar ist;
- Verarbeitungseinrichtung (10) für die Erzeugung des Verschlüsselungsschlüssels ausschließlich **durch** elektronische Verarbeitung unter Verwendung der optischen Daten als Zufallssaat, und für die Ermittlung der Nachricht **durch** Bestimmen mindestens einer Position aus den aufgezeichneten Abbildern; und
- Verschlüsselungseinrichtung (10) für die Verschlüsselung der zu übertragenden Nachricht unter Verwendung des Verschlüsselungsschlüssels.

21. Digitaler Stift nach Anspruch 20, wobei die optischen Daten von einem Abschnitt einer Oberfläche (2) ermittelt wurden, der mit einem Positionscodemuster (3) mit optisch lesbaren Markierungen (4) versehen ist.

22. Digitaler Stift nach Anspruch 21, wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um

- die optischen Daten nach einem vorbestimmten Schema zu verarbeiten,
- die verarbeiteten optischen Daten in Datenfeldern zu organisieren, wobei jedes Datenfeld eine vorbestimmte Größe hat, und
- die Datenfelder in einer vorbestimmten Reihenfolge in Datensätzen zu organisieren.

23. Digitaler Stift nach Anspruch 22, wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um statistische Eigenschaften von Sätzen von den durch die optischen Daten repräsentierten, optischen Parameterwerten zu berechnen, wobei die statistischen Eigenschaften die verarbeiteten optischen Daten bilden.

24. Digitaler Stift nach Anspruch 23, wobei die Eigenschaften einen Maximalwert, einen Minimalwert und einen Summenwert des Satzes optischer Parameterwerte umfassen, und wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um

- den Maximalwert in mindestens einem Maximaldatenfeld, den Minimalwert in mindestens einem Minimaldatenfeld und den Summenwert in mindestens einem Summendatenfeld zu organisieren, und
- das Maximaldatenfeld, das Minimaldatenfeld und das Summendatenfeld in einem Datensatz entsprechend der vorbestimmten Reihenfolge zu organisieren.

25. Digitaler Stift nach irgendeinem der Ansprüche 22 - 24, wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um

- die Reihenfolge der Datenfelder innerhalb mindestens einem Datensatz einer ersten Folge von Datensätzen entsprechend einem ersten Neuanordnungsalgorithmus neu anzuordnen, wodurch eine erste Folge von neu angeordneten Datensätzen erreicht wird, und
- die Reihenfolge der Datenfelder innerhalb mindestens einem Datensatz einer zweiten Folge von Datensätzen entsprechend einem zweiten Neuanordnungsalgorithmus neu anzuordnen, wodurch eine zweite Folge von neu angeordneten Datensätzen erreicht wird.

26. Digitaler Stift nach Anspruch 25, wobei ein Verschlüsselungsschlüssel Schlüsseldaten und Eingabedaten umfasst, und wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um

- die erste Folge von neu angeordneten Datensätzen als die Schlüsseldaten zu verwenden, und
- die zweite Folge von neu angeordneten Datensätzen als die Eingabedaten zu verwenden.

27. Digitaler Stift nach irgendeinem der Ansprüche 22 bis 24, wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um

- einen Satz einer vorbestimmten Anzahl der Datensätze in einem ersten Schritt unter Verwendung einer ersten Kontrollsummenfunktion zu verarbeiten, wodurch eine erste Ausgabe ermittelt wird,
- die erste Ausgabe in einem zweiten Schritt unter Verwendung eines iterativen Algorithmus zu verarbeiten, wodurch eine zweite Ausgabe ermittelt wird, und
- die zweite Ausgabe als einen Verschlüsselungsschlüssel oder für die Erzeugung des Verschlüsselungsschlüssels zu verwenden.

28. Digitaler Stift nach Anspruch 27, wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um eine zweite Kontrollsummenfunktion zu verwenden für die Verarbeitung der erste Ausgabe in dem zweiten Schritt.

WAVELYNX EX. 1003, Pg. 1072
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

29. Digitaler Stift nach Anspruch 27 oder 28, wobei in dem ersten Schritt und dem zweiten Schritt eine erster bzw. ein zweiter symmetrischer Verschlüsselungsalgorithmus verwendet wird.

30. Digitaler Stift nach Anspruch 29, wobei die Verarbeitungseinrichtung ferner angeordnet ist, einen symmetrischen Verschlüsselungsalgorithmus sowohl als den ersten symmetrischen Verschlüsselungsalgorithmus als auch als den zweiten symmetrischen Verschlüsselungsalgorithmus zu verwenden.

31. Digitaler Stift nach Anspruch 29, wobei ein und derselbe symmetrische Verschlüsselungsalgorithmus von der Verschlüsselungseinrichtung (10) verwendet wird für die Verschlüsselung der Nachricht, und von der Verarbeitungseinrichtung (10) verwendet wird als der erste symmetrische Verschlüsselungsalgorithmus und als der zweite symmetrische Verschlüsselungsalgorithmus.

32. Digitaler Stift nach irgendeinem der Ansprüche 20 - 31, wobei die Verschlüsselungseinrichtung (10) ferner angeordnet ist, um die Nachricht unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus zu verschlüsseln.

33. Digitaler Stift nach irgendeinem der Ansprüche 20 - 32, wobei die Verschlüsselungseinrichtung (10) ferner angeordnet ist, um

- eine erste Untermenge der optischen Daten als Schlüsseldaten für den Verschlüsselungsalgorithmus zu verwenden, und
- eine zweite Untermenge der optischen Daten als Eingabedaten für den Verschlüsselungsalgorithmus zu verwenden.

34. Digitaler Stift nach Anspruch 20, wobei die Empfangseinrichtung (10) ferner angeordnet ist, um Druckdaten zu empfangen und wobei die Verarbeitungseinrichtung (10) angeordnet ist, um den Verschlüsselungsschlüssel unter Verwendung der Druckdaten in Kombination mit den optischen Daten zu erzeugen.

35. Digitaler Stift nach Anspruch 20, wobei die Verarbeitungseinrichtung (10) ferner angeordnet ist, um Zeitdaten zu ermitteln und um den Verschlüsselungsschlüssel unter Verwendung der Zeitdaten in Kombination mit den optischen Daten zu erzeugen.

36. Verfahren für die Authentifizierung einer gesendeten Nachricht, wobei die Nachricht von einem digitalen Stift (DP) an einen Empfänger (ALS, SH; SP) gesendet wurde, **gekennzeichnet durch** die Schritte des

- Ermittelns der Nachricht **durch** Registrierung von Abbildern einer Oberfläche (2), die mit einem Positionscodemuster (3) versehen ist, unter Verwendung eines optischen Sensors (8) in dem digitalen Stift (DP) und Bestimmens mindestens einer Position aus den Abbildern,
- Ermittelns optischer Daten für die Erzeugung von Zufallszahldaten unter Verwendung des optischen Sensors (8) in dem digitalen Stift (DP), wobei die optischen Daten Werte eines optischen Parameters elektronisch repräsentieren, der **durch** den optischen Sensor (8) lesbar ist,
- Verwendens der optischen Daten für die Erzeugung der Zufallszahldaten ausschließlich **durch** elektronische Verarbeitung in einem Prozessor (10) des digitalen Stifts (DP),
- Verschlüsselns der Zufallszahldaten, und
- Verwendens der verschlüsselten Zufallszahldaten für die Authentifizierung der Nachricht.

Revendications

1. Procédé, dans un crayon numérique (DP), pour crypter un message pour une transmission sécurisée dudit message depuis le crayon numérique (DP) jusqu'à un récepteur (ALS, SH, SP), **caractérisé par** les étapes de :

obtention du message en enregistrant des images d'une surface (4) munie d'un motif de code de position (3) en utilisant un capteur optique (8) dans le crayon numérique (DP) et en déterminant au moins une position à partir des images ;
obtention (410-420) de données optiques pour la génération d'une clé de cryptage en utilisant le capteur optique (8) dans le crayon numérique (DP), lesdites données optiques représentant électroniquement des valeurs d'un paramètre optique lisible par ledit capteur optique (8) ;
génération (430-450), de manière exclusive par traitement électronique dans un processeur (10) du crayon

WAVELYNX EX. 1003, Pg. 1073
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

numérique, de la clé de cryptage en utilisant lesdites données optiques en tant que germe aléatoire ; et
cryptage (460) dudit message en utilisant ladite clé de cryptage dans un algorithme de cryptage.

2. Procédé selon la revendication 1, dans lequel ledit paramètre optique est une luminosité qui est détectée par ledit capteur optique (8).

3. Procédé selon la revendication 1 ou 2, dans lequel l'étape (410-420) d'obtention de données optiques comprend l'étape de :

obtention desdites données optiques à partir d'une partie d'une surface (2) qui est munie d'un motif de code de position (3), dans lequel ledit motif de code de position (3) inclut des marquages lisibles optiques (4) et dans lequel ledit paramètre optique est représentatif de ladite partie.

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel l'étape (430-450) de génération d'une clé de cryptage comprend les étapes de :

traitement (430) desdites données optiques conformément à un schéma prédéterminé ;
organisation (440) desdites données optiques traitées selon des zones de données, où chaque zone de données présente une dimension prédéterminée ; et
organisation (440) desdites zones de données selon un ordre prédéterminé dans des enregistrements de données.

5. Procédé selon la revendication 4, dans lequel l'étape (430) de traitement desdites données optiques comprend l'étape de :

calcul de propriétés statistiques de jeux desdites valeurs de paramètre optique représentées par lesdites données optiques et ainsi, lesdites propriétés statistiques constituent lesdites données optiques traitées.

6. Procédé selon la revendication 5, dans lequel lesdites propriétés statistiques comprennent une valeur maximum, une valeur minimum et une valeur de somme dudit jeu de valeurs de paramètre optique et dans lequel les étapes (440) d'organisation comprennent les étapes de :

organisation de ladite valeur maximum dans au moins une zone de données maximum, de ladite valeur minimum dans au moins une zone de données minimum et de ladite valeur de somme dans au moins une zone de données de somme ; et
organisation desdites zones de données maximum, de données minimum et de données de somme dans un enregistrement de données conformément audit ordre prédéterminé.

7. Procédé selon l'une quelconque des revendications 4 à 6, dans lequel l'étape (430-450) de génération d'une clé de cryptage comprend en outre les étapes de :

réagencement (520) de l'ordre desdites zones de données à l'intérieur d'au moins un enregistrement de données d'une première série d'enregistrements de données conformément à un premier algorithme de ré-ordonnancement, d'où ainsi l'obtention d'une première série d'enregistrements de données réagencés ; et
réagencement (530) de l'ordre desdites zones de données à l'intérieur d'au moins un enregistrement de données d'une seconde série d'enregistrements de données conformément à un second algorithme de ré-ordonnancement, d'où ainsi l'obtention d'une seconde série d'enregistrements de données réagencés.

8. Procédé selon la revendication 7, dans lequel une clé de cryptage comprend des données de clé et des données d'entrée et dans lequel l'étape (430-450) de génération d'une clé de cryptage comprend les étapes de :

utilisation (540) de ladite première série d'enregistrements de données réagencés en tant que dites données de clé ; et
utilisation (540) de ladite seconde série d'enregistrements de données réagencés en tant que dites données d'entrée.

9. Procédé selon l'une quelconque des revendications 4 à 6, dans lequel l'étape (430-450) de génération d'une clé de cryptage comprend les étapes de :

WAVELYNX EX. 1003, Pg. 1074
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

traitement d'un jeu constitué par un nombre prédéterminé desdits enregistrements de données au niveau d'une première étape (810-820) en utilisant une première fonction de hachage, d'où ainsi l'obtention d'une première sortie ;
traitement de ladite première sortie au niveau d'une seconde étape (830-840) en utilisant un algorithme itératif, d'où ainsi l'obtention d'une seconde sortie ; et
utilisation (850) de ladite seconde sortie en tant que dite clé de cryptage ou pour générer ladite clé de cryptage.

10. Procédé selon la revendication 9, dans lequel, au niveau de ladite seconde étape (830-840), ladite première sortie est traitée en utilisant une seconde fonction de hachage.

11. Procédé selon la revendication 9 ou 10, dans lequel, au niveau desdites première et seconde étapes (810-820, 830-840), des premier et second algorithmes de cryptage symétriques sont respectivement utilisés.

12. Procédé selon la revendication 11, dans lequel un algorithme de cryptage symétrique est utilisé à la fois en tant que dits premier et second algorithmes de cryptage symétriques.

13. Procédé selon la revendication 12, dans lequel un algorithme de cryptage symétrique est utilisé à la fois en tant que dit algorithme de cryptage pour réaliser ladite étape (460) de cryptage dudit message et en tant que dits premier et second algorithmes de cryptage symétriques.

14. Procédé selon l'une quelconque des revendications précédentes, dans lequel la clé de cryptage comprend des données de clé et des données d'entrée, le procédé comprenant en outre les étapes de :

utilisation d'un premier sous-jeu desdites données optiques pour générer lesdites données de clé ; et
utilisation d'un second sous-jeu desdites données optiques pour générer lesdites données d'entrée.

15. Procédé selon l'une quelconque des revendications précédentes, dans lequel ledit algorithme de cryptage pour crypter ledit message est un algorithme de cryptage symétrique.

16. Procédé selon la revendication 1, comprenant en outre les étapes de :

obtention de données de pression en utilisant un moyen de détection de pression, dans lequel l'étape (430-450) de génération d'une clé de cryptage comprend l'étape de :

génération de la clé de cryptage en utilisant lesdites données de pression en combinaison avec lesdites données optiques en tant que germe aléatoire.

17. Procédé selon la revendication 1, comprenant en outre les étapes de :

obtention de données temporelles, dans lequel l'étape (430-450) de génération d'une clé de cryptage comprend l'étape de :

génération de la clé de cryptage en utilisant lesdites données temporelles en combinaison avec lesdites données optiques en tant que germe aléatoire.

18. Procédé selon l'une quelconque des revendications précédentes, dans lequel lesdites étapes sont réalisées dans un crayon numérique (DP) comprenant ledit capteur optique (8) et un moyen d'émission (12).

19. Support lisible par ordinateur comprenant des instructions pour amener un ordinateur à réaliser un procédé selon l'une quelconque des revendications précédentes.

20. Crayon numérique (DP) pour crypter un message pour une transmission sécurisée dudit message depuis le crayon numérique (DP) jusqu'à un récepteur (ALS, SH, SP), **caractérisé par** :

un capteur optique (8) pour enregistrer des images d'une surface (2) munie d'un motif de code de position (3) ;
un moyen de réception (10) pour recevoir des données optiques depuis le capteur optique (8) pour la génération d'une clé de cryptage, lesdites données optiques représentant de façon électronique des valeurs d'un paramètre optique lisible par ledit capteur optique (8) ;

WAVELYNX EX. 1003, Pg. 1075
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

un moyen de traitement (10) pour générer, de façon exclusive par traitement électronique, la clé de cryptage en utilisant lesdites données optiques en tant que germe aléatoire et pour obtenir ledit message en déterminant au moins une position à partir desdites images enregistrées ; et
un moyen de cryptage (10) pour crypter le message destiné à être émis en utilisant ladite clé de cryptage.

21. Crayon numérique selon la revendication 20, dans lequel lesdites données optiques ont été obtenues à partir d'une partie d'une surface (2) munie d'un motif de code de position (3) comportant des marquages lisibles optiques (4).

22. Crayon numérique selon la revendication 21, dans lequel ledit moyen de traitement (10) est en outre agencé pour :

traiter lesdites données optiques conformément à un schéma prédéterminé ;
organiser lesdites données optiques traitées selon des zones de données où chaque zone de données présente une dimension prédéterminée ; et
organiser lesdites zones de données selon un ordre prédéterminé dans des enregistrements de données.

23. Crayon numérique selon la revendication 22, dans lequel ledit moyen de traitement (10) est en outre agencé pour calculer des propriétés statistiques de jeux desdites valeurs de paramètre optique représentées par lesdites données optiques et ainsi, lesdites propriétés statistiques constituent lesdites données optiques traitées.

24. Crayon numérique selon la revendication 23, dans lequel lesdites propriétés comprennent une valeur maximum, une valeur minimum et une valeur de somme dudit jeu de valeurs de paramètre optique et dans lequel ledit moyen de traitement (10) est en outre agencé pour :

organiser ladite valeur maximum selon au moins une zone de données maximum, ladite valeur minimum selon au moins une zone de données minimum et ladite valeur de somme selon au moins une zone de données de somme ; et
organiser lesdites zones de données maximum, minimum et de somme dans un enregistrement de données conformément audit ordre prédéterminé.

25. Crayon numérique selon l'une quelconque des revendications 22 à 24, dans lequel ledit moyen de traitement (10) est en outre agencé pour :

réagencer l'ordre desdites zones de données à l'intérieur d'au moins un enregistrement de données d'une première série d'enregistrements de données conformément à un premier algorithme de ré-ordonnancement, d'où ainsi l'obtention d'une première série d'enregistrements de données réagencés ; et
réagencer l'ordre desdites zones de données à l'intérieur d'au moins un enregistrement de données d'une seconde série d'enregistrements de données conformément à un second algorithme de ré-ordonnancement, d'où ainsi l'obtention d'une seconde série d'enregistrements de données réagencés.

26. Crayon numérique selon la revendication 25, dans lequel une clé de cryptage comprend des données de clé et des données d'entrée et dans lequel le moyen de traitement (10) est en outre agencé pour :

utiliser ladite première série d'enregistrements de données réagencés en tant que dites données de clé ; et
utiliser ladite seconde série d'enregistrements de données réagencés en tant que dites données d'entrée.

27. Crayon numérique selon l'une quelconque des revendications 22 à 24, dans lequel le moyen de traitement (10) est en outre agencé pour :

traiter un jeu constitué par un nombre prédéterminé desdits enregistrements de données au niveau d'une première étape en utilisant une première fonction de hachage, d'où ainsi l'obtention d'une première sortie ;
traiter ladite première sortie au niveau d'une seconde étape en utilisant un algorithme itératif, d'où ainsi l'obtention d'une seconde sortie ; et
utiliser ladite seconde sortie en tant que dite clé de cryptage ou pour générer ladite clé de cryptage.

28. Crayon numérique selon la revendication 27, dans lequel ledit moyen de traitement (10) est en outre agencé pour utiliser une seconde fonction de hachage pour traiter ladite première sortie au niveau de ladite seconde étape.

29. Crayon numérique selon la revendication 27 ou 28, dans lequel, au niveau desdites première et seconde étapes,

WAVELYNX EX. 1003, Pg. 1076
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

des premier et second algorithmes de cryptage symétriques sont respectivement utilisés.

30. Crayon numérique selon la revendication 29, dans lequel le moyen de traitement est en outre agencé pour utiliser un algorithme de cryptage symétrique à la fois en tant que dits premier et second algorithmes de cryptage symétriques.

31. Crayon numérique selon la revendication 29, dans lequel un seul et même algorithme de cryptage symétrique est utilisé par ledit moyen de cryptage (10) pour crypter ledit message et par ledit moyen de traitement (10) en tant que dits premier et second algorithmes de cryptage symétriques.

32. Crayon numérique selon l'une quelconque des revendications 20 à 31, dans lequel ledit moyen de cryptage (10) est en outre agencé pour crypter ledit message en utilisant un algorithme de cryptage symétrique.

33. Crayon numérique selon l'une quelconque des revendications 20 à 32, dans lequel ledit moyen de cryptage (10) est en outre agencé pour :

utiliser un sous-jeu desdites données optiques en tant que données de clé pour ledit algorithme de cryptage ; et utiliser un second sous-jeu desdites données optiques en tant que données d'entrée pour ledit algorithme de cryptage.

34. Crayon numérique selon la revendication 20, dans lequel ledit moyen de réception (10) est en outre agencé pour recevoir des données de pression et dans lequel ledit moyen de traitement (10) est agencé pour générer ladite clé de cryptage en utilisant lesdites données de pression en combinaison avec lesdites données optiques.

35. Crayon numérique selon la revendication 20, dans lequel ledit moyen de traitement (10) est en outre agencé pour obtenir des données temporelles et pour générer ladite clé de cryptage en utilisant lesdites données temporelles en combinaison avec lesdites données optiques.

36. Procédé pour l'authentification d'un message envoyé, dans lequel ledit message est envoyé depuis un crayon numérique (DP) jusqu'à un récepteur (ALS, SH, SP), **caractérisé par** les étapes de :

obtention du message en enregistrant des images d'une surface (2) qui est munie d'un motif de code de position (3) en utilisant un capteur optique (8) dans le crayon numérique (DP) et en déterminant au moins une position à partir des images ;
obtention de données optiques pour la génération de données de nombre aléatoire en utilisant le capteur optique (8) dans le crayon numérique (DP), lesdites données optiques représentant électroniquement des valeurs d'un paramètre optique lisible par ledit capteur optique (8) ;
utilisation desdites données optiques pour générer les données de nombre aléatoire, de manière exclusive au moyen d'un traitement électronique dans un processeur (10) du crayon numérique (DP) ;
cryptage desdites données de nombre aléatoire ; et
utilisation desdites données de nombre aléatoire cryptées pour l'authentification dudit message.

WAVELYNX EX. 1003, Pg. 1077
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

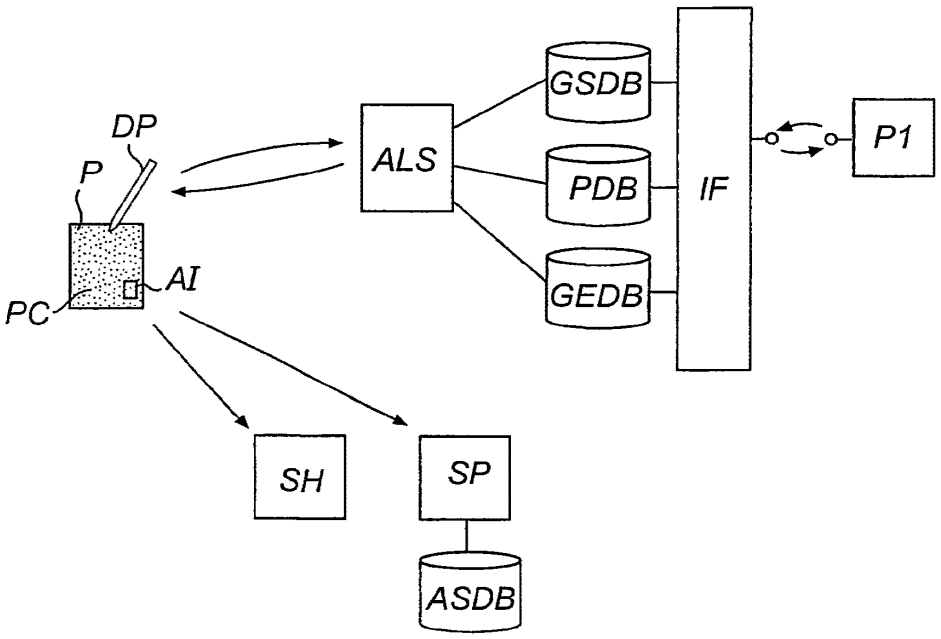


Fig. 1

WAVELYNX EX. 1003, Pg. 1078
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

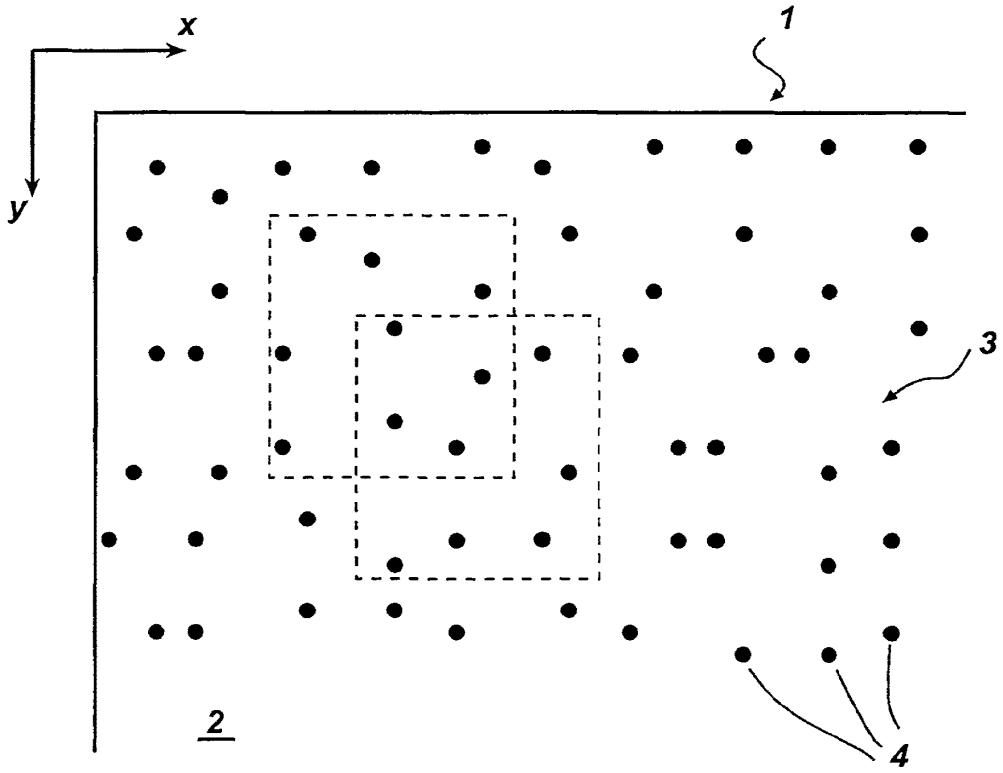


Fig. 2

WAVELYNX EX. 1003, Pg. 1079
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

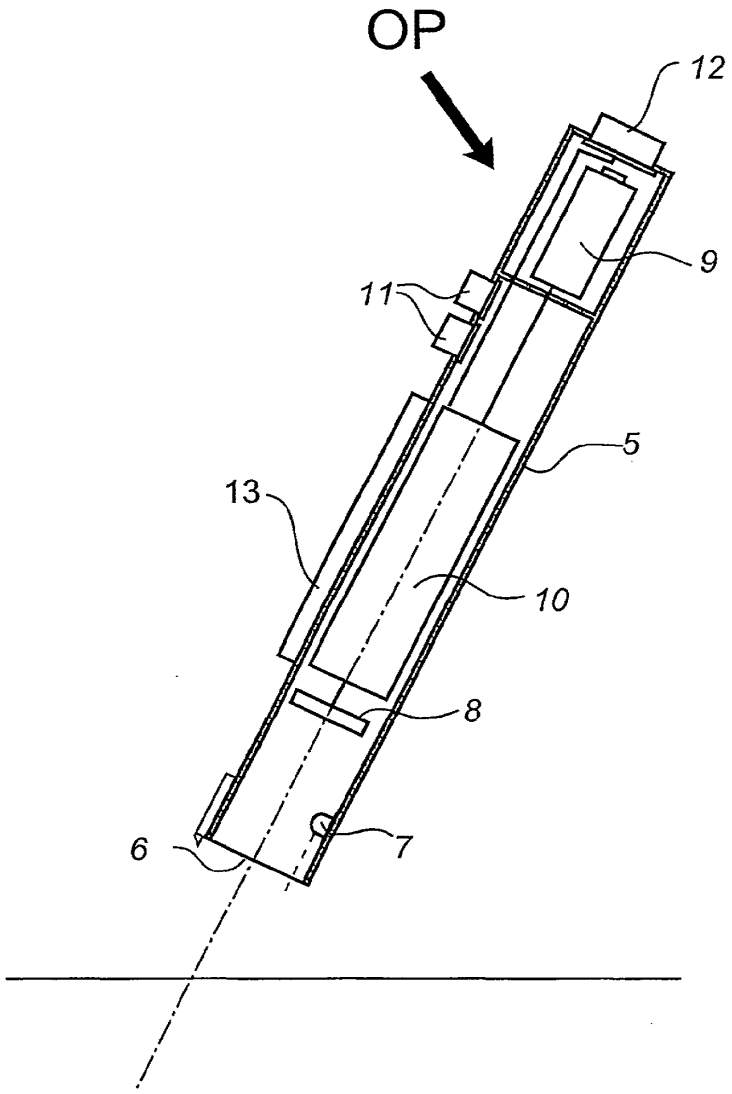


Fig. 3

WAVELYNX EX. 1003, Pg. 1080
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

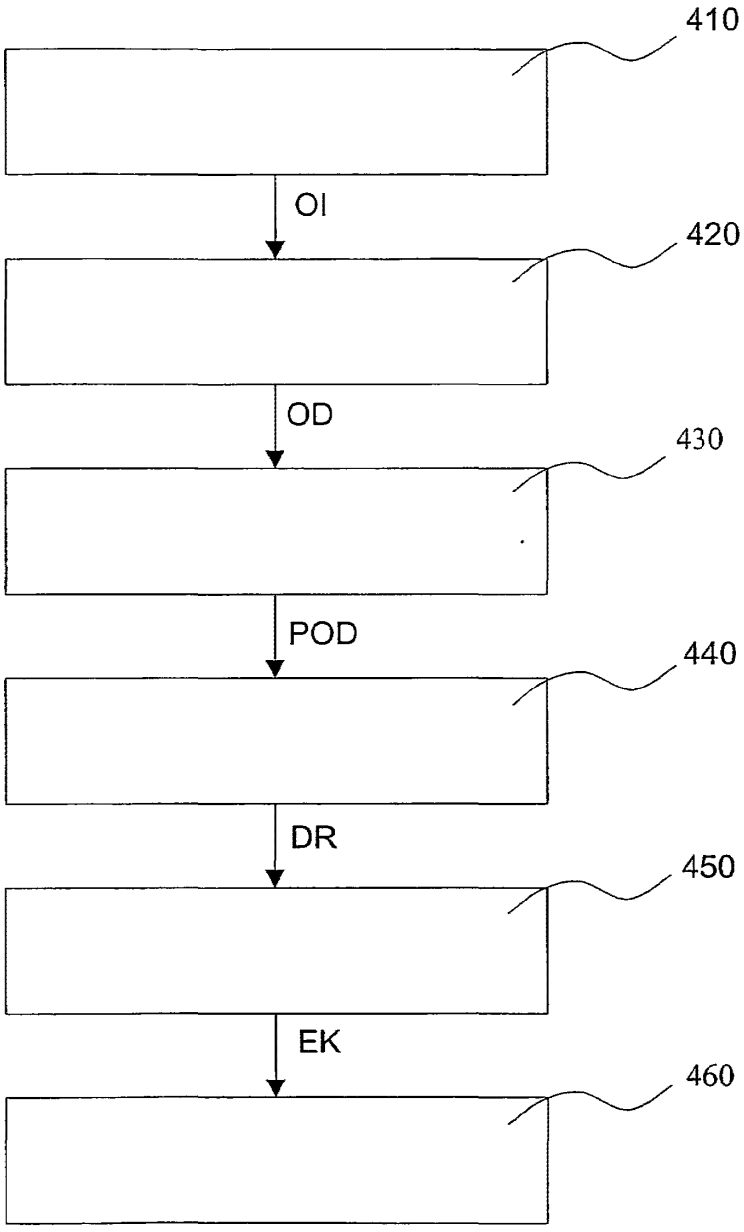


Fig. 4

WAVELYNX EX. 1003, Pg. 1081
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

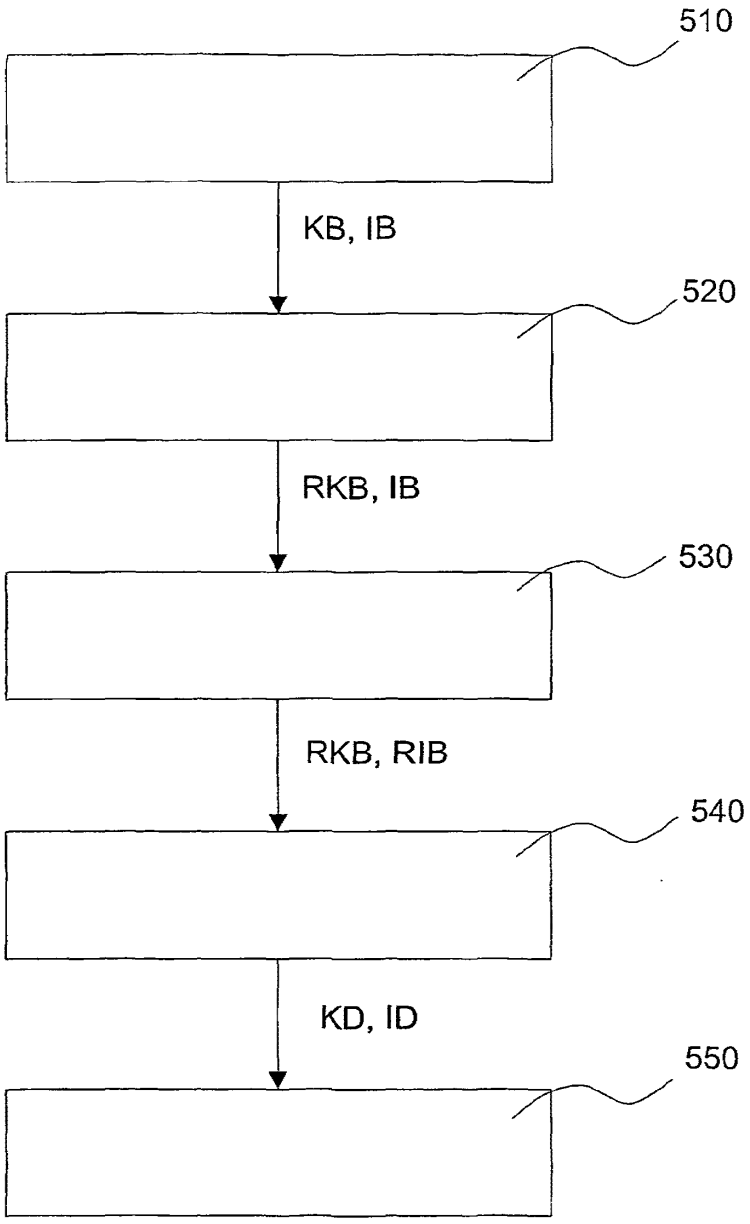


Fig. 5

WAVELYNX EX. 1003, Pg. 1082
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

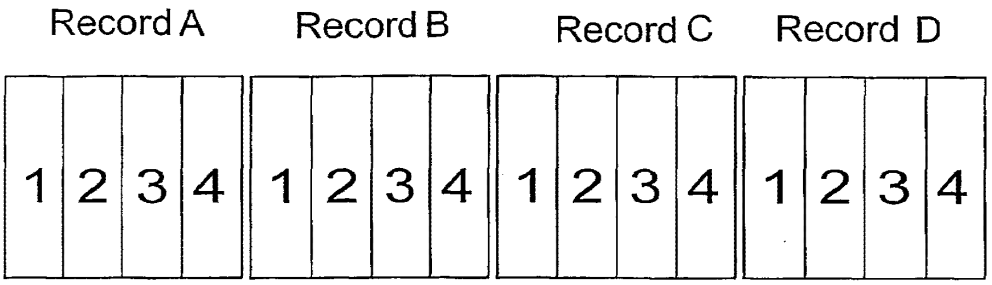


Fig. 6

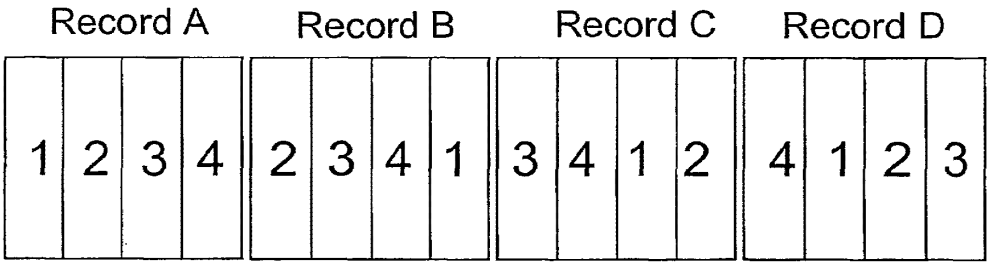


Fig. 7A

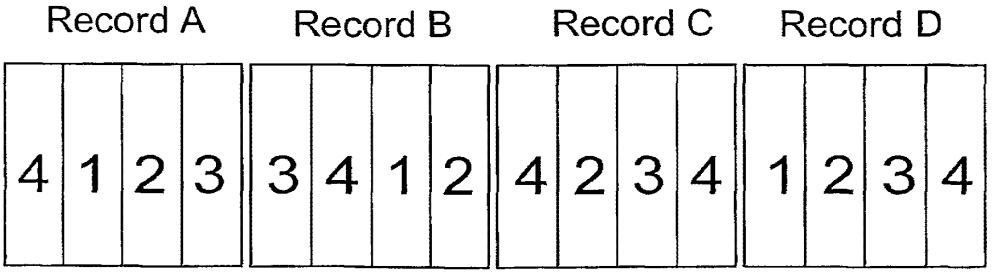


Fig. 7B

WAVELYNX EX. 1003, Pg. 1083
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

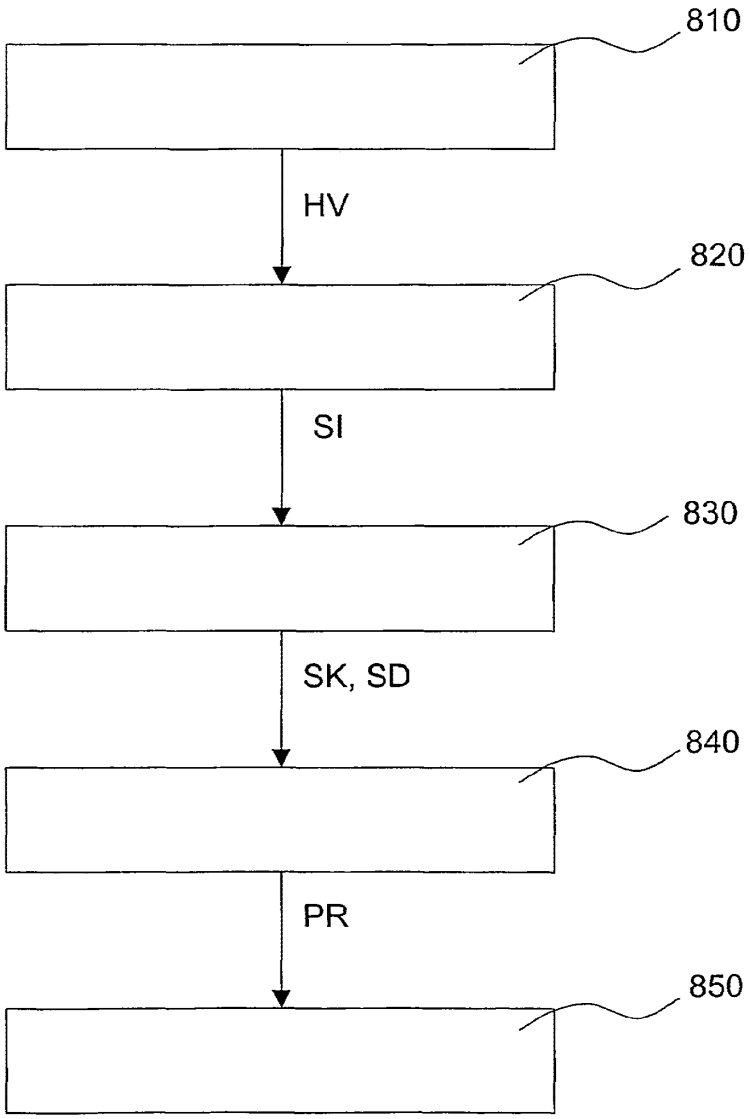


Fig. 8

WAVELYNX EX. 1003, Pg. 1084
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 398 691 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.03.2006 Bulletin 2006/09

(43) Date of publication A2:
17.03.2004 Bulletin 2004/12

(21) Application number: **03020450.7**

(22) Date of filing: **12.09.2003**

(51) Int Cl.:
G06F 7/58 *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **13.09.2002 JP 2002269129**

(71) Applicant: **KABUSHIKI KAISHA TOSHIBA**
Tokyo (JP)

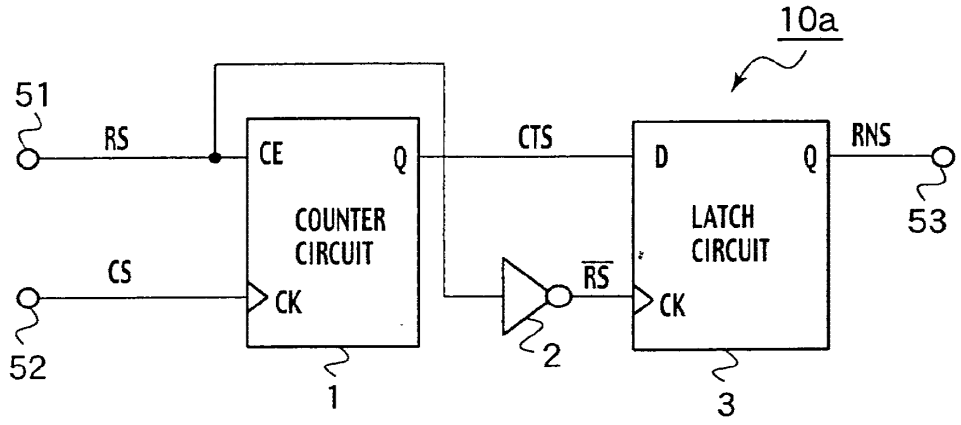
(72) Inventors:
- **Yasuda, Shinichi**
  1-1 Shibaura 1-chome
  Minato-ku
  Tokyo (JP)
- **Fujita, Shinobu**
  1-1 Shibaura 1-chome
  Minato-ku
  Tokyo (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Random number generator

(57) A random number generator comprising a counter circuit configured to be supplied with a clock signal and a random signal, and to provide a count value of the clock signal with respect to a transition of the random signal, and a first latch circuit configured to latch the count value with respect to the transition of the random signal, and to provide a first random number signal.

FIG. 1



EP 1 398 691 A3

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1085
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 02 0450

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	ASANO T ET AL: "PHYSICAL RANDOM-NUMBER GENERATOR USING SCHOTTKY MOSFET" EXTENDED ABSTRACTS OF THE INTERNATIONAL CONFERENCE ON SOLID STATE DEVICES AND MATERIALS, JAPAN SOCIETY OF APPLIED PHYSICS. TOKYO, JA, vol. 2001, 26 September 2001 (2001-09-26), pages 96-97, XP001074511 * figure 4 *	1-20	G06F7/58
A	EP 1 239 363 A (KABUSHIKI KAISHA TOSHIBA) 11 September 2002 (2002-09-11) * paragraphs [0055], [0058], [0073] - [0078]; figure 9 *	1-20	
A	US 3 866 029 A (CHEVALIER ET AL) 11 February 1975 (1975-02-11) * abstract * * column 2, line 28 - column 3, line 6 *	1-20	
A	US 3 716 796 A (HARNA H,US) 13 February 1973 (1973-02-13) * column 7, line 22 - line 33; figure 3 *	1-20	TECHNICAL FIELDS SEARCHED (IPC) G06F H03K
A	PETRIE C S ET AL: "A NOISE-BASED IC RANDOM NUMBER GENERATOR FOR APPLICATIONS IN CRYPTOGRAPHY" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I: FUNDAMENTAL THEORY AND APPLICATIONS, IEEE INC. NEW YORK, US, vol. 47, no. 5, May 2000 (2000-05), pages 615-621, XP001124059 ISSN: 1057-7122 * abstract; figures 2,10 *	1-20	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	6 January 2006	Cohen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1086
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 02 0450

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	JUN ET AL: "The Intel Random Number Generator" CRYPTOGRAPHIC RESEARCH, INC., [Online] 22 April 1999 (1999-04-22), pages 1-8, XP002361777 Retrieved from the Internet: URL:http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf> [retrieved on 2006-01-04] * paragraph [04.2]; figure 1 *	1-20	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	6 January 2006	Cohen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1087
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 02 0450

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06-01-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1239363 A	11-09-2002	JP 2002268874 A	20-09-2002
		US 2002126841 A1	12-09-2002
US 3866029 A	11-02-1975	NONE	
US 3716796 A	13-02-1973	CA 970839 A1	08-07-1975

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

WAVELYNX EX. 1003, Pg. 1088
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 420 542 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.05.2004 Bulletin 2004/21

(51) Int Cl.[7]: **H04L 9/00**, H04L 9/18

(21) Application number: **02425689.3**

(22) Date of filing: **12.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **STMicroelectronics S.r.l.**
20041 Agrate Brianza (Milano) (IT)

(72) Inventors:
- **Kocarev, Ljupco**
  San Diego CA 92122 (US)
- **Amato, Paolo**
  20051 Limbiate (IT)
- **Rizzotto, Gianguido**
  23862 Civate (IT)

(74) Representative: **Pellegri, Alberto et al**
c/o Società Italiana Brevetti S.p.A.
Piazza Repubblica, 5
21100 Varese (IT)

(54) Method and apparatus of generating a chaos-based pseudo-random sequence

(57) A method of generating cryptographically secure (or unpredictable) pseudo-random numbers uses simple functions whose inverse is not a well-defined function and has a large number of branches, although the inverse could be easily computed on each particular branch. In this way the sequence of numbers is practically unpredictable and at the same time may be generated using very simple functions.

A hardware generator of chaos-based pseudo random bit sequences implementing an embodiment of the method comprises:

— circuit means for storing bit strings representing integer numbers of the pseudo-random sequence;
— a shift register coupled to the circuit means;
— a command circuit generating shift commands for the shift register;
— second circuit means for storing the bits output by the shift register;
— an adder modulo 2 summing the bits stored in the second circuit means, generating a bit of the chaos-based pseudo-random bit sequence;
— a second adder summing up the bit strings currently stored in the shift register and in the first circuit means, generating a bit string representing a successive number of the pseudo-random sequence.

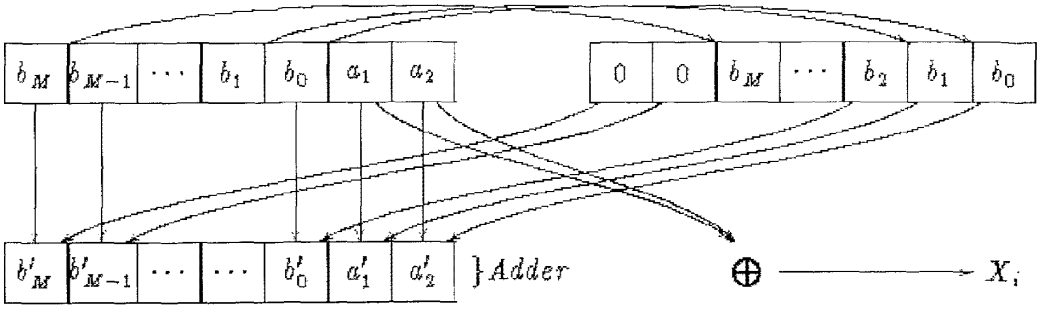


FIG. 1

EP 1 420 542 A1

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1089
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

FIELD OF THE INVENTION

[0001] The present invention relates to pseudo random numbers generations and in particular to a method for generating a sequence of chaos-based pseudo random numbers and a relative hardware implementation thereof.

BACKGROUND OF THE INVENTION

[0002] Pseudo-random number generators (PRNG) are useful in every applications that use Monte Carlo methods and also in cryptography [1]. PRNGs are algorithms implemented on finite-state machines for generating sequences of numbers which appear random-like under many aspects. These sequences are necessarily periodic but their periods are very long, they pass many statistical tests and they may be easily implemented with simple and fast software routines.

[0003] Chaotic systems may be used either in cryptography (see [2Xkjra2001]) and in generating pseudo-random numbers. For example, in a series of papers [3], a chaos derived pseudo-random number generator has been proposed. It has been numerically observed that the average cycle and transient lengths grow exponentially with the precision of implementation, and from this fact it has been deduced that using high-precision arithmetic it is possible to obtain PRNGs which are still of cryptographic interest. The usual statistical tests applied to PRNGs for use in Monte Carlo simulations are generally simple.

[0004] In cryptography, PRNG should not only have good statistical properties, but also be "cryptographically secure", i.e. given a sequence of pseudo random bits it should be impossible to predict the next number of the sequence with a probability much greater than 1/2. For this reason, PRNGs suitable for cryptographic applications must pass the next-bit test.

[0005] The actual cryptographically secure PRNG are not computationally efficient. Then they are used only for highly critical off-line operations, while for on-line tasks (like stream ciphers) fast but not secure PRNG are employed. The drawback of this fact is that stream ciphers can be attacked by exploiting the weakness of their PRNG.

[0006] Statistical properties of binary sequences generated by class of ergodic maps with some symmetrical properties are discussed in [4]. The authors derived a sufficient condition for this class of maps to produce a sequence of independent and identically distributed binary random variables. However, the implementation of these maps on finite-state machines and the consequence this implementation may have on the randomness of the generated sequences have not been discussed.

[0007] For a better comprehension of a possible field of application of the invention, a brief introduction to the basic concepts of pseudo-random bit generations is provided, according to the approach of [1] (see also [5]).

[0008] **Definition 1** *A (truly) random bit generator is a device which outputs a sequence of statistically independent and unbiased binary digits.*

[0009] A random bit generator can be used to generate random numbers. For a chaos-based generator of truly random bits see [6].

[0010] **Definition 2** *A* pseudo-random bit generator *(PRBG) is a deterministic algorithm which, given a truly random binary sequence of length k, outputs a binary sequence of length l >> k which "appears" to be random. The input of the PRBG is called the* **seed,** *while the output of the PRBG is called a* **pseudo-random bit sequence.**

[0011] **Definition 3** *A pseudo-random bit generator is said to pass all polynomial-time statistical tests if no polynomial-time algorithm can correctly distinguish between an output sequence of the generator and a truly random sequence of the same length with probability significantly greater that* 1/2.

[0012] **Definition 4** *A pseudo-random bit generator is said to pass the next-bit test if there is no polynonaial-time algorithm which, on input of the first l bits of an output sequence s, can predict the* $(l + 1)$*st bit of s with probability significantly greater than* 1/2.

[0013] In this case a PRBG is said unpredictable.

[0014] **Theorem 1** *A pseudo-random bit generator passes the next-bit test if and only if it passes all polynomial-time statistical tests.*

[0015] **Definition 5** *Let* $\mathbf{G} = \{G_n, n \geq 1$ *be an ensemble of generators, with* $G_n : \{0,1\}^n \rightarrow \{0,1\}^{p(n)}$*, where* $p(\cdot)$ *is a polynomial satisfying* $n + 1 \leq p(n) \leq n^c + c$ *for some fixed integer c. We say that* **G** *is a cryptographically secure pseudo-random bit generator if:*

- *There is a deterministic polynomial-time algorithm that on input of any n-bit string outputs a string of length p(n).*
- *For sufficiently large n, the generator* G_n *passes the next-bit test.*

[0016] All above definitions and the theorem are informal. For a formal definition of statistical test (definition 3), see

WAVELYNX EX. 1003, Pg. 1090
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Yao [7]. The notion of cryptographically secure pseudo-random bit generator was introduced by Blum and Micali [8]. The theorem 1 (universality of the next-bit test) is due to Yao [7].

[0017] The last three definitions above are given in complexity-theoretic terms and are asymptotic in nature because the notion of "polynomial-time" is meaningful for asymptotically large inputs only. Therefore, the security results for a particular family of PRBGs are only an indirect indication about the security of individual members.

[0018] Blum and Micali [8] presented the following construction of cryptographically secure PRBG. Let D be a finite set, and let $f: D \rightarrow D$ be a permutation that can be efficiently computed. Let $B: D \rightarrow \{0, 1\}$ be a Boolean predicate with the property that $B(x)$ is hard to compute given only $x \in D$, however, $B(x)$ can be efficiently computed given $y = f^{-1}(x)$. The output sequence $z_1, z_2, \ldots, z_l$ corresponding to the seed $x_0 \in D$ is obtained by computing $x_i = f(x_{i-1})$, $z_i = B(x_i)$, for $1 \leq i \leq l$.

[0019] Blum and Micali [8] proposed the first concrete instance of cryptographically secure PRBG. Let p be a large prime. Define $D = Z^* = \{1, 2, \ldots, p - 1\}$ and α a generator of Z_p^*. The function $f: D \rightarrow D$ is defined by $f(x) = \alpha^x \bmod p$. The function $B: D \rightarrow \{0, 1\}$ is defined by $B(x) = 1$ if $0 \leq \log_\alpha x \leq (p-1)/2$ and $B(x) = 0$ if $\log_\alpha x \geq (p-1)/2$. Assuming the intractability of the discrete logarithm problem in Z_p^*, the Blum-Micali generator was proven to satisfy the next-bit test. Other examples of cryptographically secure PRBGs are RSA generator [9] and Blum-Blum-Shub generator [10].

Linear congruential generators

[0020] A *linear congruential generator* produces a pseudo-random sequence of numbers $x_1, x_2, \ldots$ according to the linear recurrence

$$x_n = (ax_{n-1} + b) \bmod m, \quad n \geq 1$$

[0021] Integers a, b and m are parameters which characterize the generator, while x_0 is the seed. Generators of this form are widely used in Monte Carlo methods, taking x_i/m to simulate uniform draws on [0, 1].

[0022] For a study of linear congruential generators, see Knuth [11]. Plumstead [12] and Boyar [13] showed how to predict the output sequence of a linear congruential generator given only a few elements of the output sequence, and when the parameters a, b, and m of the generator are unknown. Boyar [13] extended her methods and showed that linear multivariate congruential generators,

$$x_n = (a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_l x_{n-l}) \bmod m$$

and quadratic congruential generators,

$$x_n = (ax_{n-1}^2 + bx_{n-1} + c) \bmod m$$

are cryptographically insecure. Krawczyk [14] showed how the output of any multivariate polynomial generator can be efficiently predicted. A truncated linear congruential generator is one where a fraction of the least significant bits of x_i are discarded. Frieze et al. [15] showed that these generators can be efficiently predicted if the parameters a, b, and m are known. Stern [16] extended this method to the case where only m is known. Boyar [17] presented an efficient algorithm for predicting linear congruential generators when O(log log m) bits are discarded, and the parameters are unknown.

[0023] No efficient prediction algorithms are known for truncated multivariate polynomial congruential generators.

OBJECT AND SUMMARY OF THE INVENTION

[0024] It has been found a method of generating a sequence of a chaos-based pseudo-random numbers and hardware pseudo-random bit generators easy to realize. The sequence of numbers is practically unpredictable and at the same time may be generated using very simple functions.

[0025] The known methods of generating cryptographically secure (or unpredictable) pseudo-random numbers are

WAVELYNX EX. 1003, Pg. 1091
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

based on the use of complicate functions whose inverse is well-defined but is hard to compute. According to the common knowledge this is necessary, because otherwise it would be easy to predict the numbers of a pseudo-random sequence.

[0026] As a consequence, known methods are relatively slow and hardware generators that implement them have a quite complex architecture.

[0027] On the contrary, the method of the invention consists in generating pseudo-random numbers by using simple functions, but their inverse is not a well-defined function and has a large number of branches, although the inverse could be easily computed on each particular branch.

[0028] More precisely, an object of the present invention is a method of generating a chaos-based pseudo-random sequence comprising the steps of:

- defining a chaotic map for generating a pseudo-random sequence of integer numbers comprised in a certain interval;
- defining a function on the first interval whose inverse has a plurality of branches;
- choosing a seed of the pseudo-random sequence of integer numbers comprised in the interval;
- generating numbers of the pseudo-random sequence;
- calculating numbers of a chaos-based pseudo-random sequence by applying the function to corresponding integer numbers of the pseudo-random sequence.

[0029] This method is preferably used for generating chaos-based pseudo-random bit sequences and may be implemented in a hardware generator of chaos-based pseudo random bit sequences, comprising:

- circuit means for storing bit strings representing integer numbers of the pseudo-random sequence;
- a shift register coupled to the circuit means;
- a command circuit generating shift commands for the shift register;
- second circuit means for storing the bits output by the shift register;
- an adder modulo 2 summing the bits stored in the second circuit means, generating a bit of the chaos-based pseudo-random bit sequence;
- a second adder summing up the bit strings currently stored in the shift register and in the first circuit means, generating a bit string representing a successive number of the pseudo-random sequence.

[0030] The invention is more precisely defined in the annexed claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] The different aspects and advantages of the invention will appear even more clearly through the following description referring to the attached drawings, wherein:

Figure 1 is a diagram describing in a basic manner a preferred embodiment of the method of the invention for generating chaos-based pseudo-random bit sequences;
Figure 2 is a hardware generator implementing an embodiment of the method of the invention;
Figure 3 is a particular embodiment of a hardware generator of the invention implementing the method described in Figure 1 for k=2.

DESCRIPTION OF SEVERAL EMBODIMENTS OF THE INVENTION

[0032] In order to illustrate in a easy manner the gist of the invention, let us refer to the following sample algorithm for generating a sequence of (real) numbers X_1, X_2, ...

[0033] First of all, a chaotic map is chosen:

$$x_{n+1} = f(x_n) = \left(\frac{p}{2^m} \cdot x_n\right) \bmod 2^M \qquad (1)$$

where n = 0, 1, ..., $x_0 \in [0, 2^m]$, $p > 2^m$, p is an odd integer. The generic term X_n of the sequence is given by

WAVELYNX EX. 1003, Pg. 1092
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$X_n = H(x_n) = sin^2(x_n) \qquad (2)$$

[0034] Is the sequence $X_1, X_2, \ldots$ predictable? In other words, knowing a finite number of elements of this sequence, say $X_j, X_{j+1}, \ldots, X_{j+k-1}$, is it possible to predict the previous and the next elements of the sequence: X_{j-1} and X_{j+k}?

[0035] Let us start our discussion from the simplest case: $p = 3$ and $m = 1$. Using the following well known relations

$$sin^2\left(\frac{3}{2}\alpha\right) = \frac{1}{2}[1 - \cos(3\alpha)]$$

$$\cos(3\alpha) = \pm\sqrt{1\text{-}sin^2(3\alpha)}$$

and

$$sin^2(3\alpha) = sin^2(\alpha)\cdot[3 - 4sin^2(\alpha)]^2$$

we find

$$(2X_{n+1} - 1)^2 + X_n(3 - 4X_n)^2 = 1$$

[0036] It is easy to show that for almost all X_n there are 2 equally likely values for X_{n+1}. In a similar way, for almost all X_{n+1} there are 3 equally likely values for X_n. Furthermore, the number of points X_i for which there are less than 2 values of X_{i+1} (or less than 3 values of X_{i-1}) is finite.

[0037] This result can be generalized for arbitrary p and m. After a simple algebra we find a functional relation between X_n and X_{n+1}:

$$\left[2\cdots 2\left((2X_{n+1} - 1)^2 - 1\right)^2 \cdots - 1\right]^2 + F_p(X_n) = 1 \qquad (3)$$

where the first term in the left-hand side of this equation is polynomial of order 2^m and F_p is the p-th order Chebyshev map. Thus, for arbitrary m and almost all x_0, equation (3) has 2^m solutions for X_{n+1} when X_n is known and p solutions for X_n when X_{n+1} is known. Therefore, for large m and almost all x_0 the sequence $\{X_i\}_1^\infty$ is one-step unpredictable: for any element X_k in the sequence $\{X_i\}_1^\infty$ one can only guess with probability $1/2^m$ (among 2^m equally distributed values of X_{k+1}) what is next element X_{k+1} and with probability $1/p$ (among p equally distributed values of X_{k-1}) what was the previous element X_{k-1}. The set of initial conditions x_0 for which the above statement does not hold is finite.

[0038] What are the properties of the sequence $X_1, X_2, \ldots$? The map $H(.)$ in (2) is not a distribution preserving map and thus the output sequence is not equally distributed. It is possible to avoid this problem using, for example, a periodic tent map instead of the sinus function.

[0039] There are much more serious problems related to the sequence $X_1, X_2, \ldots$: it has been proved that this sequence is 1-step unpredictable, from which does not follow that the sequence is k-step unpredictable. In fact, the sequence $X_1, X_2, \ldots$ is 3-step predictable as follows from the following analysis.

[0040] Let $b_m \ldots b_1 b_0 . a_1 a_2 \ldots$ be the binary presentation of $x \in [0, q]$, $q = 2^m$ and $x = (b_m, \ldots b_1, b_0; a_1, a_2, \ldots)$. Let us define the functions $c(x)$ and $d(x)$ as $c(x) = b_m \ldots b_1 b_0$, $d(x) = 0.a_1 a_2 \ldots$. Suppose to know the value of $d(r \times c \bmod q)$, where

WAVELYNX EX. 1003, Pg. 1093
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$c \in \{0, 1, ..., q\text{-}1\}$, $r = p/q$, $q = 2^m$, $gcd(p, q) = 1$, $p>q$

being *gcd(.,.)* is the greatest common divider function.

[0041] Is the value of c predictable? Let $0.r_{-1}...r_{-m}$ and $c_{m-1}...c_1c_0$ be the binary presentations of $d(r)$ and c, respectively, and let $0.a_1a_2...a_m$ be the binary presentation of $d(r \times c \bmod q)$. Given that $a_m = c_0 \cdot r_{-m}$ and $r_{-m} = 1$ (p must be an odd number), it holds that $c_0 = a_m$. Therefore, by knowing the value of a_m, c_0 can be easily determined. Furthermore, from the relation $a_{m-1} = r_{-m+1} \cdot c_0 \oplus r_{-m} \cdot c_1$ and the previously determined value of c_0 it is possible to determine the value of c_1. By repeating these arguments, the values of all bits c_0, c_1, ...c_m may be computed.

[0042] **Proposition 1** *Let $c \in \{0, 1, ..., q - 1\}$ and $r = p/q$, where $p > q$, $gcd(p, q) = 1$, and $q = 2^m$. If we know the value of $d((r \cdot c) \bmod q)$, then we can uniquely determine the value of c.*

[0043] We say that the sequence $X_1, X_2, X_3, ...$ is k-step predictable if there exist $X_n, X_{n+1}, ... X_{n+k-1}$ such that knowing them one can predict the values of X_{n-1} or X_{n+k}.

[0044] **Theorem 2** *The sequence $X_1, X_2, X_3, ...$ is 3-step predictable.*

[0045] **Proof.** It holds that $X_1 = H(x_1)$, $X_2 = H(x_2)$ and $X_3 = H(x_3)$. Let $c_1 = c(x_1)$, $d_1 = d(x_1)$, $c_2 = c(x_2)$ and $d_2 = d(x_2)$. According to the first relation the value of d_1 is either $d_{11} = arcsin(\sqrt{X_1}) \in [0,\pi/2]$ or $d_{12} = \pi - d_{11}$. Analogously, the value of d_2 is either $d_{21} = arcsin(\sqrt{X_2}) \in [0,\pi/2]$ or $d_{22} = \pi - d_{21}$. Furthermore, x_1 and x_2 are related as $x_2 = (r \cdot x_1) \bmod q$. Therefore we have

$$d_2 = d\left(\left(r \cdot \left(c_1 + d_1\right)\right) \bmod q\right) = d\left(d\left(\left(r \cdot c_1\right) \bmod q\right) + d\left(\left(r \cdot d_1\right) \bmod q\right)\right) \qquad (4)$$

[0046] Let $c_1(i, j)$ denotes the solution of the equation (4x1-6006r4) if such a solution exists. There are at most four possible values of x_1: $c_1(1, 1) + d_{11}$, $c_1(1, 2) + d_{11}$, $c_1(2, 1) + d_{12}$ and $c_1(2, 2) + d_{12}$. The actual value of x_1 can be determined by checking for which of these values, the third member of the sequence is X_3. Once the value of x_1 is determined, it is easy to compute all subsequent members X_4, X_5.

[0047] There are several ways to generalize equations (1) and (2). First, $f(.)$ in (1) can be an arbitrary chaotic map defined on $[0, q]$, where q is a large integer. Second, $H(.)$ in (2) can be an arbitrary non-periodic function $H : [0, q] \rightarrow [0, 1]$ such that its inverse $H^{-1}(.)$ has q branches. Third, the proof of the theorem 2 uses the fact that $H(.)$ is a periodic function from $[0, q]$ to $[0, 1]$, but, for example, $H(.)$ can be any periodic function $H : [0, q] \rightarrow C$, where C is a finite small set, for example $C = \{0,1\}$. Some of these possibilities are examined hereinafter.

Cryptographically Secure PRNGs

[0048] The construction of cryptographically secure PRBGs of Blum and Micali [8] is based on the assumption that the inverse of a function is a well-defined function but is hard to be computed.

[0049] On the contrary, according to the method of the present invention, it is possible to have cryptographically secure PRNGs (and thus cryptographically secure PRBGs) using simple functions $H(.)$ whose inverse is not a well-defined function and has large number of branches, although the inverse is ease to compute on a particular branch. In particular, if the inverse of the function $H : [0, q] \rightarrow C$ has q branches, even knowing a value X_n of the random number sequence $X_1, X_2, ...$, the effectively used value x_n such that $X_n = H(x_n)$ may be predicted only with a probability of $1/q$, that is x_n may be any of the integers of the interval $[0, q]$.

[0050] This approach is much more convenient than the approach of Blum and Micali [8] because the function $H(.)$ may be very simple, and thus it may be easily implemented for realizing effectively unpredictable sequences of pseudo-random numbers.

[0051] Because of the importance of PRBGs, in the ensuing description reference will be made to a preferred embodiment of the invention for generating a pseudo-random sequence of bits, but what will be stated could be easily repeated, *mutatis mutandis*, for generators of sequences of pseudo-random numbers.

[0052] An objective of the invention is to design a class of pseudo random bit generators that use only binary operations and may be implemented as a fast algorithm. To keep the connection with the previous description as close as possible, we slightly abuse of notation and write X_j for the output sequence of bits.

[0053] Let $b_M...b_1b_0.a_1a_2...$ be the binary representation of $x \in I = [0, 2^M]$ and $x = (b_M, ..., b_1, b_0; a_1, a_2, ...)$. Let us define a set

$$I^{(k)} = \left\{x \middle| x = \left(b_M, \ldots, b_0; a_1, a_2, \ldots, a_k\right)\right.$$

WAVELYNX EX. 1003, Pg. 1094
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

as a set of truncated real numbers in I. Let $trunc_k : I \to I^{(k)}$ and $H : I^{(k)} \to \{0, 1\}$ be two functions defined as follows:

$$trunc_k(x) = (b_M, \ldots, b_0; a_1, a_2, \ldots, a_k) \tag{5}$$

and

$$H(x) = a_1 \oplus a_2 \oplus \ldots \oplus a_k \tag{6}$$

[0054] The seed of the generator is the string of 0s and 1s of length $M + k + 1$, which is written in the form $x_0 = (b_M, \ldots, b_0; a_1, \ldots, a_k)$. The output of the generator is a sequence of bits $X_1, X_2, \ldots$ produced as described hereinbelow.

[0055] Two sample pseudo-random bit generators are presented. In the first case the next bit is generated as:

$$x_{i+1} = trunc_k\left(\frac{p}{2^m} \cdot x_i \bmod 2^M\right) \tag{7}$$

$$X_{i+1} = H(x_{i+1}) \tag{8}$$

[0056] In the second case, let the bit X_i has been produced. The next bit is generated as:

$$y_i = x_i \oplus X_i \tag{9}$$

$$x_{i+1} = trunc_k\left(\frac{p}{2^m} \cdot y_i \bmod 2^M\right) \tag{10}$$

$$X_{i+1} = H(x_{i+1}) \tag{11}$$

[0057] In the above equations $i = 0, 1, 2\ldots$, p, m, M, k are the parameters of the generator, $X_0 = 0$ and

$$x_i \oplus X_i = (\alpha_1, \alpha_2, \ldots) \oplus \beta = (\alpha_1 \oplus \beta, \alpha_2 \oplus \beta, \ldots)$$

[0058] Equations (7) and (10) are discrete version of (1). An additional parameter M has been introduced making in this way the algorithm more flexible: m can be arbitrary integer, while 2^M should always be a large number. The output of the generator is given by (8) or (11): instead of the sine function a periodic function H defined by (6) is used. Finally, with (9) the initial point (seed) of the generator is changed in each iteration. The parameters of the generator have the following constrains: p is an arbitrary odd integer such that $p > 2^m$, M is an integer such that $M \geq 64$, $M \gg m$, m and k are arbitrary integers.

[0059] Simple arguments (not a proof) for an elementary explanation of the unpredictability of the generator are given. The next bit X_{i+1} of the generator (or the previous bit X_{i-1}) may be determined only if all bits of x_i are known, which is however, not possible: x_i has the form $x_i = (c_M, \ldots, c_0; d_1, \ldots c_k)$ and one can only guess among 2^M equally distributed values what is x_i. Moreover, it has been numerically verified that the probability

WAVELYNX EX. 1003, Pg. 1095
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$p\left(X_j \middle| X_{j-1} X_{j-2} \ldots\right)$$

does not depend on the previous generated bits and is equal approximately to 0.5.

[0060] Let **G** = $\{G_n, n \geq 1$ be an ensemble of generators, with $G_n : \{0,1\}^n \rightarrow \{0,1\}^{p(n)}$, where $p(\cdot)$ is a polynomial satisfying $n + 1 \leq p(n) \leq n^c + c$ for some fixed integer c. It is well known that: if a cryptographically secure PRBG with $p(n) = n + 1$ exists, then there is a cryptographically secure PRNG with $p(n) = n^c + c$ for each $c \geq 2$. Therefore, using all above arguments it is possible to conclude that the presented bit generators are cryptographically secure.

[0061] By defining *p, m, M* and *k* a particular pseudo-random number generator can be realized. Two examples are presented.

[0062] **Example 1** *The generator is defined by equations* (7) *and* (8). *The parameters of the pseudo-random number generator are:* $p = 5$, $m = 2$, $M = 256$ *and* $k = 2$.

[0063] **Example 2** *The generator is defined with equations (9), (10) and (11). The parameters are:* $p = 419$, $m = 8$, $M = 64$ *and* $k = 64$.

[0064] Statistical tests cannot prove that a sequence is random, tests can only show that a sequence is not random. In other words, tests help only to detect certain kinds of weaknesses a generator may have. If a sequence passes a finite number of statistical tests, it is not guaranteed that the sequence was indeed generated by a (truly) random number generator.

[0065] Five standard tests, commonly used for determining whether a binary sequence has some properties that a truly random sequence would be likely to exhibit, are [1]: frequency test, serial test, poker test, runs test and autocorrelation test. Linear congruential generators pass standard tests. Additional package of tests was proposed in [18] for which standard random number generators (congruential, shift-register and lagged-Fibonacci generators) give poor results.

[0066] All these tests to the generators described in the previous section have been performed and the results are summarized in the following table.

Tab. 1

	PRNG1	PRNG2	PRNG3
Birthday Spacings	FAIL	pass	pass
Overlapping 5-permutation	FAIL	pass	pass
Binary rank for 31x31 matrices	FAIL	pass	pass
Binary rank for 32x32 matrices	FAIL	pass	pass
Binary rank for 6x8 matrices	FAIL	pass	pass
Bistream	FAIL	pass	pass
OPSO	FAIL	pass	pass
OQSO	FAIL	pass	pass
DNA	FAIL	pass	pass
Count-the-1's on a stream of bytes	FAIL	pass	pass
Count-the-1's for specific bytes	FAIL	pass	pass
Parking lot	FAIL	pass	pass
Minimum distance	FAIL	pass	pass
3DSpheres	FAIL	pass	pass
Squeeze	FAIL	pass	pass
Overlapping sums	pass	pass	pass
Runs	pass	pass	pass
Craps	FAIL	pass	pass

[0067] PRNG1 is a linear congruential generator with $a = 84589$, $b = 45989$, and $m = 217728$. The values of the parameters are taken from [19]; we obtain similar results with different values for *a, b* and *m*. PRNG2 and PRNG3 are generators from Examples 1 and 2.

Description of a hardware generator of the invention

[0068] Once fixed the parameters *p, m, k* and *M* of equations 7 and 8 (or of equations 9, 10 and 11), a hardware

WAVELYNX EX. 1003, Pg. 1096
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Pseudo Random Bit Generator may be easily and efficiently implemented.

[0069] Following Example 1 (PRNG2), we take $p = 5$, $m = 2$, $k = 2$ and $M = 256$. Now $x_i = b + a$, where (in base 2) $b = b_M \ldots b_1 b_0$ and $a = 0.a_1 a_2$, and $\frac{p}{2^m} = 1 + \frac{1}{2^2}$. Then

$$\left(\frac{p}{2^m} \cdot x_i\right) \bmod 2^M$$

can be rewritten as

$$\left(b + \frac{1}{2^2} b + a + \frac{1}{2^2} a\right) \bmod 2^M$$

[0070] The term $\frac{1}{2^2} b$ can be obtained by shifting b by 2 bits towards right (i.e., $\frac{1}{2^2} b = 00 b_M \ldots b_3 b_2 . b_1 b_0$). Moreover, since the term $\frac{1}{2^2} a$ is less than $\frac{1}{2^2}$, it is immaterial with respect to the truncation operation $trunc_2$ and we can omit it. At last, the mod 2^M operation is simply obtained by discarding the overflow of the M bit summation. Therefore, the quantity

$$trunc_k\left(\left(\frac{p}{2^m} \cdot x_i\right) \bmod 2^M\right)$$

is substantially the sum between the two bit strings $b_M \ldots b_3 b_2 b_1 b_0 . a_1 a_2 + 00 b_M \ldots b_3 b_2 . b_1 b_0$.

[0071] Summing up, the operations involved in the PRNG2 are bit shift, bit sum and XOR (while, for examples, Micali-Blum generator uses power operators and Blum-Blum-Shub generator uses product). Figure 1 depicts the application of the equations (7) and (8) at the generic i-th step.

[0072] In the above mentioned figure, the array of bit $b'_M \ldots b'_0 . a'_1 a'_2$ indicates the result of the sum between $b_M \ldots b_3 b_2 b_1 b_0 . a_1 a_2$ and $00 b_M \ldots b_3 b_2 . b_1 b_0$ and is stored in a temporary buffer for (the base 2 representation of) x_{i+1}. At the subsequent $(i + 1)$th step, the content of this buffer shall be overwritten on the bits $b_M \ldots b_3 b_2 b_1 b_0 . a_1 a_2$.

[0073] A basic realization of a hardware generator of a chaos-based pseudo-random bit sequence of the invention is depicted in Figure 2. It comprises a first memory buffer MEM in which storing bit strings representing integer numbers x_n of the PRN sequence, a shift register R1 driven by a command circuit, a second memory buffer storing the bits output by the shift register R1, a first adder ADD1 modulo 2 and a second adder ADD2.

[0074] Preliminarily, a seed x_0 is stored in the memory buffer MEM; then the desired bit sequence X_n is generated by repeating cyclically the following steps:

- the content of the first buffer is copied in the shift register R1;
- the command circuit provides a certain number k of shift commands to the shift register R1, which outputs the k least significant bits of the string representing the number x_n;
- the bits output by the shift register are stored in the second buffer R2 and are summed by the first adder modulo 2 ADD1, generating a bit X_n of the chaos-based pseudo-random bit sequence;
- the second adder ADD2 sums the bit strings currently stored in the shift register and in the memory MEM, generating a bit string representing a successive number x_{n+1} of the pseudo-random sequence which is stored in the first buffer MEM.

[0075] The hardware generator of Figure 2 may be used whichever the number k is.

[0076] A simpler embodiment of a hardware generator of the invention, especially designed for implementing the method of the invention for k=2, is depicted in Figure 3. Differently from the generator of Figure 2, the register R2 is not present and R1 can be a register of any kind.

[0077] Initially, the memory buffer MEM is loaded with a seed x_0, then according to the embodiment of the method of the invention described in Figure 1 the following operations are carried out:

WAVELYNX EX. 1003, Pg. 1097
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- copying in the register R1 a bit string stored in the memory buffer MEM representing a current number x_n of the pseudo-random sequence,
- generating a bit X_n of chaos-based pseudo-random bit sequence by summing modulo 2 (XORing) the two (k=2) least significant bits of the bit string stored in the register R1,
- generating a bit string representing a successive number x_{n+1} of the pseudo-random sequence by summing up the bit string representing the current number x_n and the bit string obtained eliminating the two least significant bits of the bit string stored in the register R1,
- storing in the memory buffer MEM the bit string representing the successive number x_{n+1}.

[0078] As it will be apparent to the skilled practitioner, once the generator of Figure 3 has been realized, it cannot be used for any value of $k \neq 2$, because it would be necessary to change the connections between the register R1 and the cascade of adding gates [+] that constitute the adder modulo 2 ADD2.

REFERENCES

[0079]

[1] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1997.

[2] L. Kocarev, G. Jakimoski, G. Rizzotto, and P. Amato, "Chaos-based data protection using time-discrete dynamical systems", European Patent Application n.01130846.7, 27 Dec 2001.

[3] R. A. J. Matthews, "On the Derivation of a 'Chaotic' Encryption Algorithm", *Cryptologia*, vol. 13, pp. 29-42 (1989); D. D. Wheeler, "Problems with Chaotic Cryptosystems", *Cryptologia*, vol. 13, pp. 243-250, (1989); D. D. Wheeler and R. A. J. Matthews, "Supercomputer Investigations of a Chaotic Encryption Algorithm", *Cryptologia*, vol. 15, no. 2, pp. 140-152 (1991).

[4] T. Kohda and A. Tsuneda, "Statistics of Chaotic Binary Sequences," *IEEE Trans. on Information Theory,* **43**, pp. 104 - 112 (1997).

[5] O. Goldreich, "Modern Cryptography, Probabilistic Proofs and Pseudorandomness," Springer-Verlag, Algorithms and Combinatorics, Vol 17, (1998).

[6] F. Italia, L. Kocarev, M. Porto, G. Rizzotto and T. Stojanovski, "Chaos Based Random Number Generators", European Patent Application n.01830764.5, 13 Dec 2001.

[7] A. Yao, "Theory and applications of trapdoor functions," *IEEE 23rd Symposium on Foundations of Computer Science,* pp. 80 - 91 (1982).

[8] M. Blum and S. Micali, "How to generate cryptographically storng sequences of pseudorandom bits," *IEEE 23rd Symposium on Foundations of Computer Science,* pp. 112 - 117 (1982).

[9] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, " RSA/Rabin bits are $\frac{1}{2} + \frac{1}{poly(\log n)}$ secure, "*IEEE 25th Symposium on Foundations of Computer Science,* pp. 449 - 457 (1987).

[10] L. Blum, M. Blum, and M. Shub, "A Simple Unpredictable Pseudo-Random Number Generator," *SIAM J. Comput.* , **15**, pp. 364 - 383 (1986).

[11] D.E. Knuth, *The Art of Computer Programming - Seminumerical Algorithms,* vol. 2, Reading, Mass. : Addison-Wesley Pub. Co., (1981).

[12] J. B. Plumstead, "Inferring a sequence generated by a linear congurence," *IEEE 23rd Symposium on Foundations of Computer Science,* pp. 153 - 159 (1982).

[13] J. Boyar, "Inferring sequences produces by pseudo-random number generators," *Journal of the Association of Computing Machinery,* **36**, pp. 129 - 142 (1989).

[14] H. Krawczyk, "How to predict congurential generators," *Journal of Algorithms,* **13**, pp. 527 - 545 (1992).

WAVELYNX EX. 1003, Pg. 1098
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[15] A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and S. Shamir, "Reconstructing truncated integer variables satisfying linear congruences," *SIAM Journal of Computing,* **17**, pp. 262 - 280 (1988).

[16] J. Stern, "Secret linear congruential generators are not cryptographically secure," *IEEE 28th Symposium on Foundations of Computer Science,* pp. 421 - 426 (1987).

[17] J. Boyar, "Inferring sequences produces by a linear congruential generator missing low-order bits," *Journal of Cryptology*, **1,** pp. 177 - 184 (1989).

[18] http://stat.fsu.edu/geo/diehard.html

[19] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, 2nd Ed. New York : John Wiley&Sons, 1996.

Claims

1. A method of generating a chaos-based pseudo-random sequence (X_n) comprising the steps of:

   defining a chaotic map for generating a pseudo-random sequence of integer numbers (x_n) comprised in a certain interval ([0, q]);
   defining a function ($H(x)$) on said first interval ($x \in [0, q]$) whose inverse has a plurality of branches;
   choosing a seed (x_0) of said pseudo-random sequence of integer numbers (x_n) comprised in said interval ([0, q]);
   generating numbers of said pseudo-random sequence (x_n);
   calculating numbers of a chaos-based pseudo-random sequence (X_n) by applying said function ($H(x)$) to corresponding integer numbers of said pseudo-random sequence (x_n).

2. The method of claim 1, wherein the inverse of said function ($H(x)$) has a number of branches equal to the largest bound (q) of said interval ([0, q]).

3. The method of claim 1, wherein said chaotic map is a linear congruential generator.

4. The method of claim 3, wherein said linear congruential generator is defined by:

   choosing a first integer number (m);
   choosing a second odd integer number (p) greater than the power of 2 raised to said first integer number (2^m);
   choosing a third integer number (M) much greater than said first integer number (m);
   said chaotic map being defined by the following equation:

$$x_{n+1} = \left(\frac{p}{2^m} \cdot x_n \right) \bmod 2^M .$$

5. A method of generating a chaos-based pseudo-random bit sequence (X_n) comprising the operations of:

   choosing a function ($H(x)$) that may assume only two values ({0,1});

   generating said chaos-based pseudo-random bit sequence (X_n) with the method of claim 1.

6. The method of claim 5, comprising the steps of:

   representing in binary form said integer numbers (x_n) of said pseudo-random sequence;
   defining a second integer number k;
   defining said function (H(x)) as the binary sum of the k least significant bit of the binary representation of its argument (x).

WAVELYNX EX. 1003, Pg. 1099
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

7. The method of claim 5, wherein said chaotic map is a truncated linear congruential generator.

8. The method of claim 7, wherein said truncated linear congruential generator is defined by:

choosing a first integer number (m);
choosing a second odd integer number (p) greater than the power of 2 raised to said first integer number (2^M);
choosing a third integer number (M) much greater than said first integer number (m);
said chaotic map being defined by the following equation:

$$x_{n+1} = trunc_k\left(\left(\frac{p}{2^m}\cdot x_n\right) \bmod 2^M\right).$$

9. The method of claim 7, wherein said linear congruential generator is defined by:

choosing a first integer number (m);
choosing a second odd integer number (p) greater than the power of 2 raised to said first integer number (2^m);
choosing a third integer number (M) much greater than said first integer number (m);
said chaotic map being defined by the following equations:

$$\begin{cases} y_n = x_n \oplus X_n \\ x_{n+1} = trunc_k\left(\left(\frac{p}{2^m}\cdot y_n\right) \bmod 2^M\right) \end{cases}$$

10. The method according to one of claims 4, 8 or 9, wherein said third integer number (M) is greater than or equal to 64.

11. The method of claims 6 and 8, comprising the steps of:

providing circuit means (MEM) for storing bit strings representing integer numbers (x_n) of said pseudo-random sequence;
providing a shift register (R1) coupled to said circuit means (MEM);
storing a seed (x_0) in said circuit means (MEM);
carrying out cyclically the following operations:

- copying in said shift register (R1) a bit string stored in the circuit means (MEM) representing a current number (x_n) of said pseudo-random sequence,
- providing k shift commands to said shift register (R1),
- generating a bit (X_n) of said chaos-based pseudo-random bit sequence by summing modulo 2 the k bits output by said shift register (R1),
- generating a bit string representing a successive number (x_{n+1}) of said pseudo-random sequence by summing up the bit string currently stored in said shift register (R1) and the bit string representing said current number (x_n),
- storing in the circuit means (MEM) the bit string representing said successive number (x_{n+1}).

12. The method of claims 6 and 8, comprising the steps of:

providing circuit means (MEM) for storing bit strings representing integer numbers (x_n) of said pseudo-random sequence;
providing a register (R1) coupled to said circuit means (MEM);
storing a seed (x_0) in said circuit means (MEM);
carrying out cyclically the following operations:

- copying in said register (R1) a bit string stored in the circuit means (MEM) representing a current number

WAVELYNX EX. 1003, Pg. 1100
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(x_n) of said pseudo-random sequence,

- generating a bit (X_n) of said chaos-based pseudo-random bit sequence by summing modulo 2 the k least significant bits of the bit string stored in said register (R1),
- generating a bit string representing a successive number (x_{n+1}) of said pseudo-random sequence by summing up the bit string representing said current number (x_n) and the bit string obtained eliminating the k least significant bits of the bit string stored in said register (R1),
- storing in the circuit means (MEM) the bit string representing said successive number (x_{n+1}).

13. A generator of chaos-based pseudo random bit sequences for implementing the method of claim 12, comprising:

circuit means (MEM) for storing bit strings representing integer numbers (x_n) of said pseudo-random sequence;
a register (R1) coupled to said circuit means (MEM);
an adder modulo 2 (XOR) summing the k least significant bits of the of the bit string stored in said register (R1), generating a bit (X_n) of said chaos-based pseudo-random bit sequence;
a second adder (ADD2) summing up the bit string representing said current number (x_n) and the bit string obtained eliminating the k least significant bits of the bit string stored in said register (R1).

14. A generator of chaos-based pseudo random bit sequences for implementing the method of claim 11, comprising:

circuit means (MEM) for storing bit strings representing integer numbers (x_n) of said pseudo-random sequence;
a shift register (R1) coupled to said circuit means (MEM);
a command circuit (CONTROL) generating shift commands for said shift register (R1);
second circuit means (R2) for storing the bits output by said shift register (R1);
an adder modulo 2 (ADD1) summing the bits stored in said second circuit means (R2), generating a bit (X_n) of said chaos-based pseudo-random bit sequence;
a second adder (ADD2) summing up the bit strings currently stored in said shift register (R1) and in said first circuit means (MEM), generating a bit string representing a successive number (x_{n+1}) of said pseudo-random sequence.

WAVELYNX EX. 1003, Pg. 1101
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

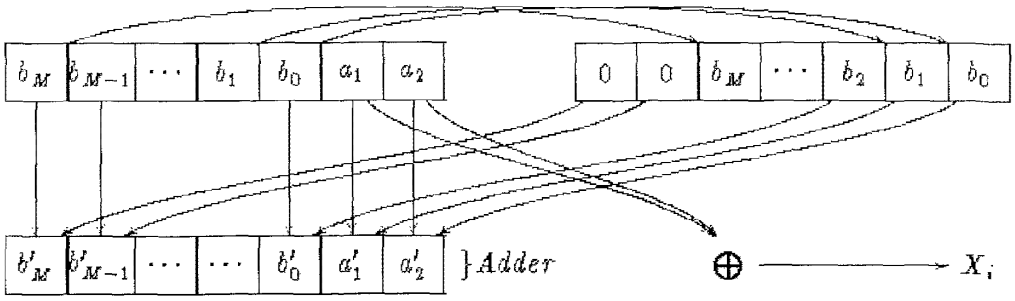


FIG. 1

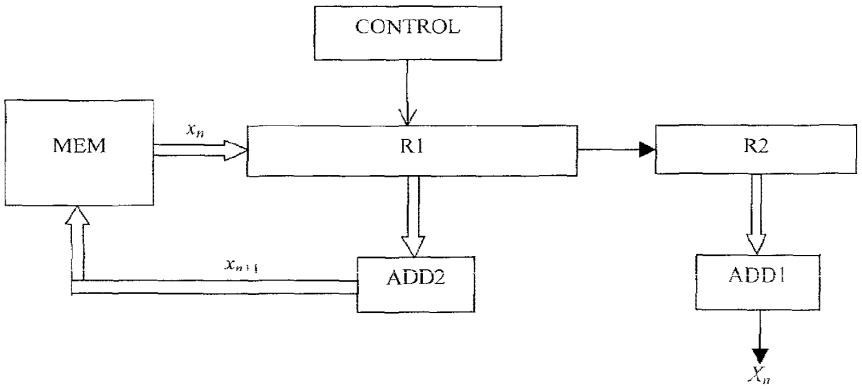


FIG. 2

WAVELYNX EX. 1003, Pg. 1102
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

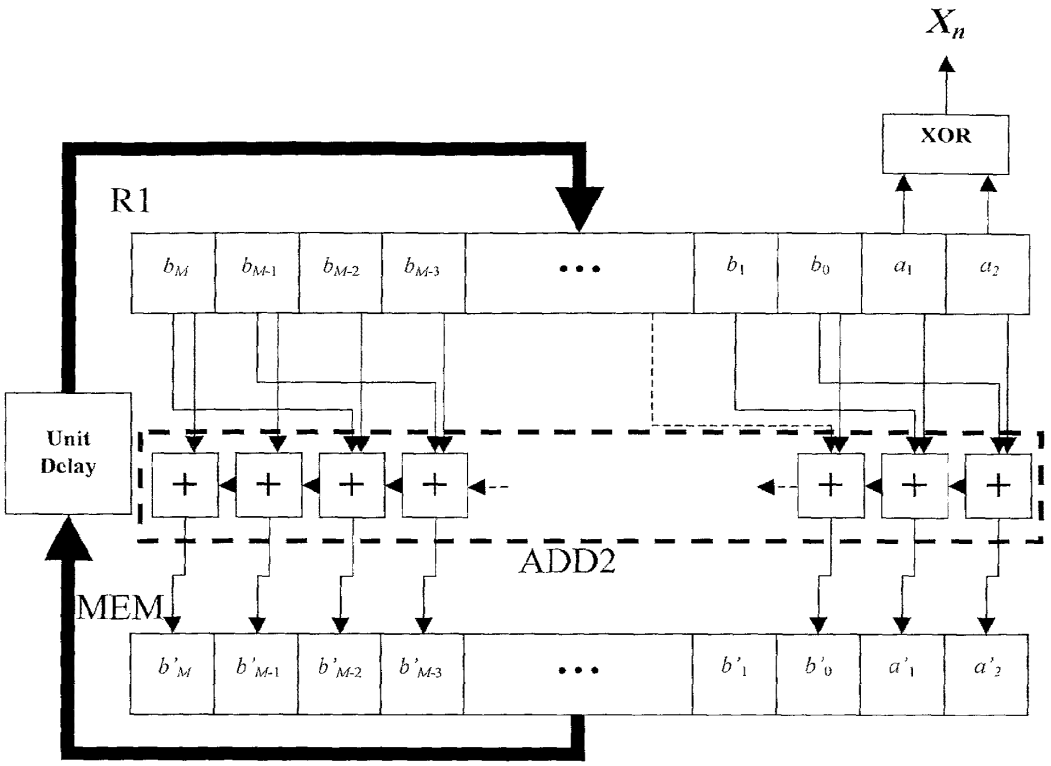


FIG. 3

WAVELYNX EX. 1003, Pg. 1103
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 42 5689

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 732 138 A (MENDE ROBERT G ET AL) 24 March 1998 (1998-03-24) * column 3, line 60 - column 4, line 27 * * column 4, line 28 - line 32 * * column 5, line 18 - column 6, line 20; figure 1 *	1	H04L9/00 H04L9/18
Y		6,11-14	

Y	MENEZES, OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, , 1997, pages 362-363, XP002264603 BOCA RATON, FL, US ISBN: 0-8493-8523-7 * page 362, paragraph 9.6.2 - page 363 *	6,11-14	

A	SILVA, YOUNG: "Introduction to chaos-based communications and signal processing" THE AEROSPACE CORPORATION, vol. 11, 1 February 2000 (2000-02-01), pages 279-299, XP010518483 * page 286, right-hand column - page 288, left-hand column *	1-14	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L

A	GARCIA P ET AL: "Communication through chaotic map systems" PHYSICS LETTERS A, NORTH-HOLLAND PUBLISHING CO., AMSTERDAM, NL, vol. 298, no. 1, 27 May 2002 (2002-05-27), pages 35-40, XP004358780 ISSN: 0375-9601 * page 36 - page 38 * * page 39, right-hand column, paragraph 3 *	1-14	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	10 December 2003	Carnerero Álvaro, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1104
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 42 5689

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

10-12-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5732138 A	24-03-1998	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

WAVELYNX EX. 1003, Pg. 1105
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 460 573 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.09.2004 Bulletin 2004/39

(51) Int Cl.[7]: **G06F 17/60**

(21) Application number: **04251365.5**

(22) Date of filing: **10.03.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(30) Priority: **21.03.2003 US 393894**

(71) Applicant: **Nokia Corporation**
02150 Espoo (FI)

(72) Inventors:
- **Wakim, Peter**
  00100 Helsinki (FI)
- **Engeström, Jyri**
  00530 Helsinki (FI)

(74) Representative: **Walaski, Jan Filip et al**
Venner Shipley LLP
20 Little Britain
London EC1A 7DH (GB)

(54) Apparatus and method for remote content delivery

(57) Merchant-media information is communicated to a selected user in response to a user identification (ID) being presented at a media location. According to one example embodiment, a user presents an ID tag to an ID tag reader at a merchant-media arrangement (*e.g.*, a billboard, display screen, audio speaker or advertisement) having a media content ID. The ID tag communicates a user ID to the ID tag reader, and an information request signal including data representing the user ID and the media content ID is sent to a remote server. The remote server uses the user ID and the media content ID to send media content information (*e.g.*, product data, a discount voucher, *etc.*) to a user address. With this approach, users can request and/or receive information at a point-of-use media display.

EP 1 460 573 A2

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

[0001] This invention relates in general to communications, and more particularly to a system, method and apparatus for initiating delivery of remote information, content, services and applications.

[0002] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the U.S. Patent & Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND OF THE INVENTION

[0003] Traditional approaches to data communication in public places, such as advertising or providing other information in public places, have relied upon relatively simple approaches, typically involving printed and/or displayed media. This displayed media approach is relatively devoid of interactive communications. Billboards, kiosks, vending machines, restaurant menus and other forms of public advertising do not provide a means to directly initiate interactive communication between merchants and consumers. For instance, when a consumer wishes to obtain data or learn more about a particular advertisement, he or she must typically either remember or write down information, and at a later time seek out any additional information he or she is interested in learning about. Similarly, merchants currently have to rely on indirect methods, such as polls and market research, to discover whether customers noticed their announcements.

[0004] In some instances, public data communications have involved wireless technologies that have improved the ability of consumers to communicate in public places. For example, wireless telephones enable users to make and receive calls when not at home. Wireless Internet appliances enable users to access the Internet and retrieve information from a public place where wireless communications are present. Other wireless devices, such as personal digital assistants (PDAs) are also growing in use. These approaches have been found useful in conveying information to users in public locations. However, even with wireless appliances, information retrieval has typically required users to actively seek data (*i.e.,* make a telephone call or browse the Internet). Moreover, many users do not have access to wireless appliances and, while access may be available, such access is often inconvenient.

[0005] In view of the above, there is a need for interactive information exchange that is convenient and inexpensive.

SUMMARY OF THE INVENTION

[0006] The present invention is directed to a system, apparatus, and method for requesting information and services/applications for merchant-type products and/or services, as well as facilitating receipt of information such as advertising information.

[0007] In accordance with one embodiment of the invention, a merchant-media arrangement communicates with a user-communications device within a local proximity of the merchant-media arrangement for obtaining identification (ID) data from the user-communications device. The user ID data is obtained by the merchant-media arrangement and used for selecting a communications-user receipt address. Stored data for the merchant-media arrangement is then communicated to the selected communications-user-receipt address.

[0008] In another example embodiment of the present invention, a radio frequency (RF) reader communicates with an RF tag within a local proximity of the RF reader. The RF tag includes at least one transponder having a user ID and adapted for responding to wireless activation signals from the RF reader by communicating an RF signal including the user ID to the RF reader. The RF reader then communicates the user ID and a unique RF reader ID to a remote processing arrangement. The remote processing arrangement uses the user ID to identify a particular type of communications medium and address that are to be used, and also uses the RF reader ID to identify a particular type of content to be communicated. The content is then communicated to the communications address via the particular type of communications medium (*e.g.*, email, voice mail, voice call, short-message service (SMS), Java application, multi-media message service (MMS) message, the initiation of an Internet browser session or paper).

[0009] In another example embodiment of the present invention, a merchant-media arrangement is adapted for conveying merchant-media information (*i.e.*, audio and/or visual advertisements) to a user and, in response to the user presenting an RFID tag, to send merchant-media information to an address specified by the user. The merchant-media arrangement includes a RFID reader, a microcontroller (*e.g.*, a microprocessor) and a transceiver for communicating with a remote processing arrangement, such as discussed above. The remote processing arrangement includes a memory having information stored therein, including address information corresponding to an ID of the RFID tag and merchant-media information corresponding to an ID of the RFID reader. In response to receiving communications including the RFID tag ID and the RFID reader ID, the remote processing arrangement accesses the memory and sends the merchant-media information using the address information.

[0010] In another example embodiment of the present invention, the merchant-media arrangement discussed above is further adapted for interactively communicating

WAVELYNX EX. 1003, Pg. 1107
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

with a local user presenting a RFID tag. In one instance, a user interface such as a keyboard, switch (*e.g.*, a push button), touch screen or other arrangement is used for inputting user selections, such as content selections and communications medium selections. In another instance, a wireless communications link at the merchant-media arrangement communicates with the local user, for example, for sending information or receiving requests.

[0011] The above summary of the present invention is not intended to describe each illustrated embodiment or implementation of the present invention. The figures and the associated discussion that follows describe further embodiments and implementations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Various aspects of the invention are described in connection with the example embodiments illustrated in the figures, in which:

FIG. 1 is a system for the communication of merchant-media data to a user via a user RFID tag, according to an example embodiment of the present invention;

FIG. 2 is another system for the communication of merchant-media data to a user, according to another example embodiment of the present invention;

FIG. 3 is a portable media communications arrangement for implementation in connection with merchant-media, according to another example embodiment of the present invention; and

FIG. 4 is an information block used for the communication of merchant media to a user, according to another example embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0013] In the following description, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration the example embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized, as structural and operational changes may be made without departing from the scope of the present invention.

[0014] Generally, the present invention is directed to approaches for retrieving information from a remote server using local communication technology, such as those short-range communications technologies involving electromagnetic/electrostatic-coupling technology. In one embodiment, electromagnetic and/or electrostatic coupling is implemented in the radio frequency (RF) portion of the electromagnetic spectrum, using for example radio frequency identification (RFID) technology. A merchant-media device is equipped with an RF reader adapted to emit RF activation waves, and transponders or "tags" brought within the range of the RF reader are activated by the RF activation. When activated, the tags transmit information possessed by the tags to the RF reader. For instance, when the RF reader is emitting the activation waves while the tag is within a range of the RF reader sufficient to allow two-way communications between the RF reader and the tag, identification information at the tag is transmitted to the RF reader.

[0015] In one embodiment of the invention, the tag provides user specific information, such as a particular user identification (ID) that corresponds to the user of the tag. When brought in proximity range of a transmitting RFID reader, the user ID of the tag is transmitted to the RFID reader, which in turn may transmit the received user ID and information relating to the RFID reader itself to a remote processor arrangement. In one instance, the RFID reader transmits a unique ID for the RFID reader to the remote processor arrangement, which associates the unique ID with a particular type of information. In another instance, the RFID reader transmits information relating to the RFID reader that includes an identification of a particular type of information being displayed near the RFID reader. The remote processor arrangement then uses the user ID and the information relating to the RFID reader for sending content to the user at a particular communications-user-receipt address, such as a mail address, email address or telephone number. For instance, by associating the user ID with stored user-receipt addresses in order to send the requested information to a right destination.

[0016] In one embodiment of the invention the tag is a user-communications device including a memory that may store information, such as a unique identification number, and means for delivering the stored information to a requesting source. The means for delivering the stored information including, but not limited to, a RFID tag (active or passive), a barcode, a chip card, a smartcard, a magstripe, a WLAN and a bluetooth device.

[0017] In one implementation, a merchant-media arrangement including the RFID reader discussed in the above paragraph provides the content to the user without necessarily using the remote processor arrangement. In one instance, the tag includes information regarding the communications medium and/or content, which is in turn communicated to and used by the merchant-media information for sending requested information to the particular communications-user-receipt address. In another instance, the remote processor arrangement is located in the merchant-media arrangement, and operates as discussed above. In still another instance, the merchant-media arrangement is adapted for receiving tag information from a plurality of RFID readers in an independent merchant-media system. For instance, several media displays at a particular location, such as at a public transportation location, at a sporting event or other venue, a local remote processor arrangement can be implemented for RFID readers at various displays and advertisements. The system could be dis-

WAVELYNX EX. 1003, Pg. 1108
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

tributed or even consisting of a plurality of independent systems.

[0018] In a more particular implementation, the remote processor arrangement is adapted to store content for merchant subscribers and to assign an RFID reader ID to particular content. When a tag is brought within range of the RFID reader such that the user ID is transmitted via the RFID reader to the remote processor arrangement, the particular content associated with the RFID reader ID is communicated to the user.

[0019] The remote processor arrangement discussed above is adapted to store communications data for registered users in connection with another example embodiment of the present invention. When a registered user presents a tag to a RFID reader field (*i.e.*, within range of an RFID reader), user ID information from the tag is transmitted to the RFID reader, which in turn may send the user ID information to the remote processor arrangement. The remote processor arrangement then uses the user ID information to identify a particular communication medium over which to send the content to the user. In one instance, a registered user provides the remote processor arrangement with user preferences including registered contact information (*i.e.*, email address or telephone number). The remote processor arrangement then uses the preferred contact information to send information to the user.

[0020] In one implementation, the user stores data including two or more addresses at the remote processor arrangement. The RFID reader transmits information related to a selection of one of the two addresses to the remote processor arrangement, and in response, the remote processor arrangement selects one of the two addresses for delivery of information to the user. In one example, two or more RFID readers are present at a merchant-media arrangement (*e.g.*, a billboard advertisement, an active video display, an audio broadcast or other media-conveying device with the RFID readers attached thereto). The RFID readers are spaced apart such that an RFID tag does not simultaneously transmit to both of the RFID readers, such that a user can select only one of the readers for interaction, if desired. Each of the RFID readers is programmed with a particular type of communications to be associated with it (*e.g.*, email address or telephone number). A user places his or her tag in proximity of one of the RFID readers, based upon the desired communications medium that the user wishes to use for receiving information relating to the merchant-media arrangement (*e.g.*, displayed product information).

[0021] In another example embodiment of the present invention, a RFID reader arrangement is adapted for receiving communications media selections from a particular user, such as from a push button at a merchant-media location or from a wireless device, in connection with a user ID from a tag. For instance, selections that can be made include the selection of a particular type of communications media through which content is to be sent or of a particular type of content (*e.g.*, content related to a specific one of several types of products/services available from a particular merchant). Users desiring information place a tag within a proximity range of an RFID reader arrangement and make corresponding selections. The RFID reader arrangement receives not only user ID data from the tag but also receives communications media selections from the user.

[0022] FIG. 1 is a block diagram illustrating another example embodiment of the present invention, in which a particular RFID tag 102 communicates with a merchant-media arrangement 112 using an RFID reader 110. The merchant-media arrangement 112 further includes a microcontroller 114 that communicates data representing the RFID tag and the merchant-media arrangement to a remote processing arrangement 140 using a communications link 142.

[0023] The embodiment of FIG. 1 is shown generally to permit for different types of applications and arrangements. For example, the merchant-media arrangement could be adapted to accommodate applications serving different types of providers such as advertisers, merchants or even government entities. Various alternative implementations of the merchant-media arrangement 112 could vary from a bus stop including a car advertisement delivering information using SMS or email, to a tax office including an information point delivering tax preparation information to the user's home address or email.

[0024] The communications link 142 includes one or more of a variety of links, such as wired and/or wireless link, a mobile telephone link or an Internet link. In addition, the communications link 142 is adapted for communicating one or more types of data, such as Internet protocol data, packet data and telephony data. The merchant-media arrangement 112 initiates programmed tasks, such as communicating applications, services or other specific actions, in response to detecting that the RFID tag 102 is within a certain range of the RFID reader 110, as discussed herein.

[0025] FIG. 1 depicts a number of such RFID tags, namely RFID tags 102, 104, 106, 108, with each RFID tag shown having a corresponding communications range. When a particular RFID tag is brought within its range of the RFID reader 110, a user ID at the RFID tag is transmitted to the RFID reader. The coverage area of any one of these RF (or RFID) tags is largely dependent on the RF tag antenna characteristics, interrogation signal power and the type of RF communication employed (*e.g.*, frequency spectrums and communication protocol). In various applications, any of a variety of RF communication types could be used, including but not limited to those described in the following: ISO/IEC 18001 Information Technology AIDC Techniques-RFID for Item Management - Application Requirements Profiles; and The Air Interface Standards of ISO/IEC JTC 1/SC 31 are contained in the various Parts of ISO/IEC 18000, Radio-frequency Identification Standard for Item Man-

WAVELYNX EX. 1003, Pg. 1109
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

agement -- Air Interface (see frequency ranges respectively listed in Parts 1-6). Other frequency spectrums are advantageous for applications benefiting from a passive antenna arrangement that can be energized wirelessly.

[0026] The communication between the RFID reader 110 and one or more RFID tags utilizes electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum. The RFID reader 110 includes at least an antenna 111 and a transceiver 113. An RF signal is transmitted from the RFID reader 110 that activates the tags 102, 104, 106, 108 when touched to, or within a predetermined range of, the reader. When a tag has been activated, it transmits information back to the RFID reader 110. More particularly, in the case of a passive tag, the tag is energized by a time-varying electromagnetic RF wave generated by the RFID reader 110. When the RF field passes through the antenna coil associated with the tag, a voltage is generated across the coil. This voltage powers the tag and makes possible the tag's return transmission of information to the reader, sometimes referred to as backscattering. For general information regarding RFID principles, and for specific information regarding RFID approaches that may be implemented in connection with one or more example embodiments discussed herein, reference may be made to "Radio Frequency Identification -RFID: A Basic Primer", published by the Automatic Identification Manufacturers (AIM), October 23, 2001 and fully incorporated herein by reference.

[0027] The transmission range of the reader/tag link is at least partially dictated by the frequency employed in the transmission. Referring again to FIG. 1, the required proximity of the RFID reader 110 to a tag can range from a very short range (touching or near touching) to many meters, depending on the frequency employed and the power output. Each of the RFID tags shown in FIG. 1 illustrates a range for that RFID tag, as related to the tag transmission (*i.e.*, antenna) arrangement. For example, when the RFID reader is within a range 120 of RFID tag 102, the tag 102 can receive the signal from the RFID reader 110 and respond with the desired information (*i.e.*, user ID). Other ranges 122,124,126 are illustrated for RFID tags 104,106, 108 respectively. As shown, the other RIFD tags 104,106 and 108 are outside of their corresponding ranges (122, 124 and 126) of the RFID reader 110.

[0028] In connection with one example embodiment, two or more RFID readers *(i.e.,* similar to RFID reader 110) are used, with each RFID reader spaced from other RFID readers at a distance that is greater than the RFID tag range. With this approach, the transmission of RFID tag data can be limited to one of the two or more RFID readers.

[0029] In one particular implementation, a tag having substantially no transmission range is used for communicating with a RFID reader. The tag includes contacts that physically (or nearly physically) couple to corresponding contacts on the RFID reader 110, with user ID information being communicated to the RFID reader 110 using the physical coupling. For example, the contacts may include contacts for transmitting power and/or signals to the tag from the RFID reader.

[0030] In another example implementation, the merchant-media arrangement 112 also transmits other information, such as audio-visual advertising information, in a range 130 from the RFID reader 110. RFID tag arrangements equipped to receive a signal from the RFID reader arrangement can then receive the information. For instance, when a RFID tag is implemented in connection with a mobile phone or laptop, wireless communications from the merchant-media arrangement 112 are transmitted thereto for soliciting the user. If a user holding an RFID tag is interested in receiving more information, he or she moves his or her RFID tag within a particular range of the RFID reader 110 to transmit a user ID from the RFID tag. In this instance, a user holding RFID tag 102 is within range for transmitting the user ID information to the RFID reader 110. A user holding RFID tag 104 is within range of receiving wireless communications from the merchant-media arrangement 112 and positions his/her RFID tag 104 within the range 122 of the RFID reader 110 to retrieve additional data. Users holding RFID tags 106 and 108 are out of the range 130 and do not receive the wireless information from the merchant-media arrangement 112.

[0031] In various implementations, a plurality of different types of RFID tags is used in connection with the present invention. For example, RFID tags can be either active or passive. Active tags often employ an internal battery or other power source and are often read/write tags (*e.g.*, they can read information from a merchant-media arrangement, as discussed above). Passive tags do not necessarily require a dedicated power source, and obtain operating power generated from the reader. Further, tags may come in a variety of shapes and sizes, such as those based on a custom designed silicon integrated circuit. Any transponder/tag may be used in connection with the present invention, and the tag type, size, *etc.* depends on the particular environment and purpose in which physical browsing in accordance with the invention will be employed. For instance, an RFID tag can be installed a simple card, such as a credit card, a travel card (for public transportation use), payment card, loyalty card or an identification card, or even an access key. In other instances, the RFID tag installed in a device such as a mobile phone, a personal digital assistant (PDA) or a laptop computer, and in some implementations, is implanted in a human.

[0032] Any number of RFID readers, such as those discussed above, can be positioned at various locations in which a user may physically encounter. For example, such RFID readers can be located at retail stores, hotels, restaurants, night clubs, bus stops, train stations and airports, offices, taxis, conference centers, *etc.* Any of a variety of locations may serve as a venue for a RFID reader in accordance with the present invention; partic-

WAVELYNX EX. 1003, Pg. 1110
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ular applications facilitate the communication between the merchant-media arrangement and the RFID users.

[0033] In one implementation, advertisements having RFID readers are located at a bus stop or other boarding/queuing area typically present in public transportation systems. The RFID readers communicate with RFID tags in travel cards used for travel in the public transportation system. In another example, a restaurant includes an RFID reader near its front door or other display area that provides the restaurant menu. Users wishing to hear more about a particular type of entrée or wine place their RFID tag near the RFID reader and corresponding information is sent to the user (*e.g.*, using a real-time email or phone call to a wireless device of the user). Alternatively, the RFID reader may use the user's RFID tag to send an address such as a Uniform Resource Locator (URL) of the restaurant's web site to the user, where the user can make a reservation, view a menu and/or view current seating wait times. In still another example, a night club may use such a RFID reader to provide taxi service information, such as taxi service contact information, or even to initiate a taxi request. Such a RFID reader can be attached or embedded into the night club door frame, tables, or a dedicated taxi station or kiosk located therein. Information such as one or more taxi service contact numbers of the best or closest taxi service can then be sent to the user. In still another example, a remote processor is further programmed to send information including user billing (*e.g.*, credit card) information to a particular merchant offering the RFID reader, such as for paying for a taxi ordered in connection with the previous example.

[0034] In another implementation, the merchant-media provider has instructions posted near an RFID reader telling a user with an RFID tag what action will occur, if a RFID tag is presented to the RFID reader. For instance, using the restaurant example above, a menu may have an RFID reader node indicating to the user, "Place your travel card (*i.e.*, RFID tag) here to have our web site address sent with SMS to your mobile phone." The RFID reader node is correspondingly adapted to send an interrogation signal and read the RFID tag information, and to send the information including the user ID from the RFID tag to a remote processor, which uses the user ID to determine where to send content (in this example, an SMS message including the web site address). Another RFID reader node may be used for receiving the user ID for requesting reservation availability information. For instance, a user can place his or her RFID tag near an RFID reader node to receive and email indicating available reservation times, to which the user can respond for making a reservation.

[0035] As can be seen from the foregoing examples, such physical tag (RFID tag) association with merchant-media can be implemented with a variety of types of advertising approaches. By utilizing physical tags in this manner, users can access information directly from a merchant-media source (*e.g.*, a billboard or menu). For example, because essentially all restaurants have menus and possible seating wait times, it is foreseeable that a person will want to know that information while physically near the restaurant. Rather than requiring a passer-by to search for information, the information can simply be provided to the user, either at the RFID reader site (*e.g.*, through a wireless device) or using other means, such as email or paper mail that the user obtains at a later time.

[0036] FIG. 2 is a system 201 for conveying merchant-media content from a merchant 270 to a user address location 250 using an RFID tag 200, according to another example embodiment of the present invention. User information *(i.e.,* a user ID) at the RFID tag 200 is associated with the user address location 250 and is communicated through a merchant-media arrangement 204, which processes data received from the RFID tag 200 for communicating a merchant-information request. The data is processed, for example, using a microprocessor located in the merchant-media arrangement 204. The system 201 is adapted for initiating a number of representative service types using the RFID tag 200 and one or more RFID readers including RFID readers 202, 203, 206 and 207. When RFID tag 200 is brought within a transmission range of the RFID reader 202, the user ID data is transmitted from the RFID tag 200 to the RFID reader 202. Each of the RFID readers is spaced sufficiently apart such that an RFID tag can be positioned to communicate exclusively with one of the RFID readers.

[0037] After the RFID tag information is processed at the merchant-media arrangement 204, a transceiver 210 (*e.g.*, a wired and/or wireless modem or mobile telephony appliance) sends the merchant-information request to a remote processing arrangement 212 using wireless or wireline connection. According to various embodiments of the present invention, the merchant-information request may be transferred using for example SMS, MMS, voice call, email, TCP/IP or even physical mail. The merchant-information request is representative of the user ID received from the RFID tag 200 and of a particular type of information content request associated with the merchant-media arrangement 204. For example, using a unique merchant-media ID stored at the merchant-media arrangement, the type of content displayed at the merchant-media arrangement can be identified.

[0038] In one particular implementation, the transceiver 210 is a mobile telephone transceiver adapted to send the merchant-information request via a mobile telephone network. The remote processing arrangement 212 receives the merchant-information request and, in response, processes the request by associating RFID tag information with a set of user address locations and sends content information such as, for example an image, a ringtone, a URL, a video clip , a V-Card, a calendar entry, terminal configuration settings, a picture message, an operator logo, a receipt, loyalty bonus points, a customer service call, a ticket, a discount voucher or

WAVELYNX EX. 1003, Pg. 1111
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

an advertising brochure) to a specific user address location 250 by way of a communications link 251. The user address location 250 may be defined with the received RFID reader ID or it can be a default address, if no specific address is identified. The communications link (*e.g.*, wired and/or wireless links, the Internet and conventional mail) is selected based upon a communications media type selected by the user. According to various non-limiting embodiments of the present invention, the user address may be a mobile- or fixed-line phone number, an IP or email address, or even a postal address.

[0039] The remote processing arrangement 212 includes a microcontroller programmed for conveying the content information to the proper user address location 250 using one or more of a variety of approaches. In one implementation, a merchant processing arrangement 270 communicates with the remote processing arrangement 212 for storing the content information in a memory 213 at the remote processing arrangement. In another implementation, the remote processing arrangement 212 is adapted for informing the merchant processing arrangement 270 of the merchant-information request, the user address location 250 and the particular communications medium. The merchant processing arrangement then uses this information to send content information directly to the user address location 250. In still another implementation, the remote processing arrangement 212 accesses information stored at the merchant processing arrangement 270 and conveys content information including the information stored at the merchant processing arrangement to the user address location 250.

[0040] In another implementation, a user sends user preference information to the remote processing arrangement 212 (*e.g.*, using a registration approach) including one or more of preferred communications medium, address and/or other information. The user registration may involve the user signing up, for example, at the merchant-media arrangement 204, when purchasing an RFID tag device, using SMS (*e.g.*, to a mobile phone) or at a recharge point (*e.g.*, a kiosk for recharging a RFID tag device). When registering at the merchant-media arrangement, one or more of types of user interfaces, such as a keypad, touch screen or other type of interface is used for inputting data for the registration. In some implementations, user registration is free, such that host providers can charge merchants for access to the user's registration information and/or for sending information to the user. In other implementations, user registration is fee-based, where users pay to have their information stored and to receive information upon request (*e.g.*, in response to placing his or her RFID tag in proximity of an advertisement).

[0041] According to various other implementations of the present invention, the registration process for subscribing to services may be performed by linking user ID with existing customer database. The database could be implemented, for example, as a database provided by a loyalty program or any other trusted entity. The registration may also be performed at the merchant-media arrangement site, for example, wherein the user could send an SMS message including some available service identification to a certain number that is identified by the merchant-media arrangement. The remote processing unit may then respond by sending back e.g. an SMS message or a voice call informing the user to put his/her RFID tag to the RFID reader field in order to register to the service. According to other implementations, the registration may be done, *e.g.*, over the Internet by the user.

[0042] The merchant-information request is associated with one or more of the merchant-media arrangement 204, the particular RFID reader 202 or a switch arrangement 209 at the merchant-media arrangement 204. The remote processing arrangement 212 includes stored information including address and communications medium preferences associated with the particular user ID, as well as content information (*e.g.*, product data, advertisement, electronic ticket or discount coupon or even a voucher) associated with the merchant-media arrangement 204. The remote processing arrangement 212 sends the content information to a particular user address location 250 based on one or more of: information stored at the remote processing arrangement and information stored at the merchant-media arrangement 204. In one instance, the merchant-media arrangement 204 sends content identification data, such as a RFID reader ID or a merchant ID stored at the merchant-media arrangement 204, to the remote processing arrangement 212. In response, the remote processing arrangement 212 matches the content-identification data with content information stored at the remote processing arrangement 212 and sends the stored content information to the user address location 250.

[0043] In another instance, the merchant-media arrangement 204 sends content information to the remote processing arrangement 212, which in turn sends the received content information to the user address location 250 using the user ID. With this approach, a merchant advertising with the merchant-media arrangement 204 has the option of storing product information at a merchant-media arrangement 204 and/or at the remote processing arrangement 212.

[0044] In another implementation, the merchant-media arrangement 204 includes all of the RFID readers 202, 203, 206 and 207, with each reader being associated with a particular type of merchant-information request. Users at the merchant-media arrangement position an RFID tag 200 within range of one of the plurality of RFID readers to request different types of communications. For instance, when the merchant-media arrangement is advertising a product (*e.g.*, an automobile type) having different options (*e.g.*, different automobile models), a local user places his or her RFID tag near an RFID reader corresponding to the particular option (*e.*

WAVELYNX EX. 1003, Pg. 1112
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

g., model) for which he or she is requesting information.

[0045] The user input device 209 is adapted for selecting a particular type of merchant-information request, in connection with another example embodiment. For instance, when the merchant-media arrangement 204 is advertising different types of products, the user input device 209 is used for requesting information for the particular type of product. A user brings his or her RFID tag 200 within range of one or more of the RFID readers 202, 203, 206 and 207 and makes a selection using the user input device 209. The transceiver 210 then sends a communication to the remote processing arrangement 212 including a user ID from the RFID tag and information regarding the particular type of information requested using the user input device 209. For this embodiment, FIG. 2 illustrates the merchant-information request (from the merchant media arrangement 204 to the remote processing arrangement 212) as including, in addition to the "USER ID" and the "RF READER ID," data representing "USER SELECTION."

[0046] In another example embodiment, the merchant-media arrangement 204 is adapted for offering selections to a local user bearing the RFID tag 200 including a type of communications medium through which the local user wishes to receive merchant information. In one implementation, the RFID readers 202, 203, 206 and 207 are each associated with a particular type of communications medium through which merchant-media content is to be sent to a user. In another implementation, the user input device 209 is used for selecting a particular type of communications medium. In response to either a particular RFID reader receiving communications from an RFID tag and/or the user input device 209, the transceiver 210 sends merchant-information request data to the remote processing arrangement 212. The merchant-information request data includes a request for the particular type of communications media through which the merchant-media content is to be delivered, which may, for example, include instructions for using a particular type of communications medium. Alternatively, or in addition, the merchant-information request data includes a code *(i.e.,* an RFID code), and the remote processing arrangement 212 has stored information including the particular type of communications medium that is associated with the code.

[0047] As discussed above, various types of communication medium requests can be initiated at the merchant-media arrangement 204. The example communication medium requests are respectively directed to requests including, but not necessarily limited to: a short-messaging-service (SMS) request, an MMS request, a URL request, a wireless download request, an email request, a telephone call request, a mobile gambling request and a physical mail *(i.e.,* paper) request. Using at least one RFID tag 200, the RFID readers 202, 203, 206 and 207 and the user input device 209, one or more such communications medium requests are selected.

[0048] Referring again to FIG. 2, in another example embodiment of the present invention, the merchant-media arrangement 204 further includes a communications link 260 for communicating with a user device. For instance, a communications link adapted for using Bluetooth-type communications approaches may be used. The user device may, for example, also include the user address location 250 and/or the RFID tag 200. For instance, when a user in possession of the RFID tag 200 also includes a wireless communications device, such as a mobile phone, he or she can communicate with the merchant-media arrangement directly through the communications link 260. Information such as merchant-information request data and communications medium request data is communicated from a user to the merchant-media arrangement 204 through the communications link 260. In one particular implementation, the remote processing arrangement 212 sends content information to the user address location 250 back through the merchant-media arrangement 204 *(i.e.,* wherein the communications link 251 includes the merchant-media arrangement and the communications link 260).

[0049] In another implementation, the communications link 260 is adapted for providing Wireless Application Protocol (WAP) browsing, or an analogous protocol facilitating mobile browsing, to a user having the RFID tag 200 at the merchant-media arrangement 204. WAP is a set of protocols that accounts for characteristics and functionality of both Internet standards and standards for wireless services, and integrates the Internet and other networks with wireless network platforms. WAP thus bridges the gap between the wired Internet paradigm and the wireless domain, to allow wireless device users to enjoy the benefits of the Internet across both platforms. In one implementation, the RFID tag 200 is used to enable a wireless connection between a user at the merchant-media arrangement 204 and the communications link 260. For instance, a mobile phone, PDA or laptop computer may include the RFID tag 200 and further include a user ID that can be wirelessly transmitted to the merchant-media arrangement 204 through the communications link 260 *(i.e.,* for verifying the user is enabled for using the wireless link).

[0050] An active display 214, such as a video display and/or a moving physical display (*e.g.*, a scrolling banner or rotating panel display), is included at the merchant-media arrangement 204 in connection with another example embodiment. The active display 214 is adapted to display media to a local user bearing the RFID tag 200. The displayed media is optionally changed, such as for displaying different products from the same or different merchants at different time intervals. In such an instance, the merchant-media arrangement 204 is adapted for sending data to the remote processing arrangement 212 that corresponds to a particular type of media being displayed when a signal from the RFID tag 200 is received. For instance, by storing merchant content information related to the particular type of products being displayed at the merchant-media

WAVELYNX EX. 1003, Pg. 1113
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

arrangement, data identifying the type of product being displayed is accessed and sent to the remote processing arrangement 212 when the RFID tag 200 is read.

[0051] In another example embodiment, merchants using the remote processing arrangement 212 for conveying advertising information register to a service provided by a host of the remote processing arrangement. The registration is a paid subscription provided by the host for advertising purposes, with the remote processing arrangement 212 storing a merchant registration status. Merchants having paid for their subscription are currently registered, and those failing in payment are non-currently registered. In this implementation, when a request is received for information from a particular merchant-media arrangement, the remote processing arrangement 212 verifies that the particular merchant for whom the merchant-media arrangement conveys information has a current registration. If the registration is not current, information is not sent to the user address location 250. In the instance where the merchant-media arrangement 204 includes the active display 214, the remote processing arrangement 212 is adapted for controlling the display in response to the subscription status of a merchant. For example, if a merchant registration lapses, the remote processing arrangement 212 communicates with the merchant-media arrangement for disabling the content for the particular merchant.

[0052] In another example embodiment of the present invention, feedback to a user at the merchant-media arrangement is provided to indicate that the user's user ID has been read. For instance, referring again to FIG. 2, the merchant-media arrangement 204 includes a feedback device, such as an LED (light-emitting diode) or a speaker emitting an audio signal, that alerts a user when his or her RFID tag has been read. In one implementation, the communications link 260 includes the feedback device. With this approach, a user receives confirmation that his or her ID has been read.

[0053] In another example embodiment of the present invention, the merchant-media arrangement 204 of FIG. 2 is further adapted for limiting the number of repetitive communications from a particular user-communications device. For instance, when a user presents his or her RFID tag to an RFID reader, it is typically desirable that only one request for information be made, such that a user does not inadvertently or intentionally request information more than once. In one implementation, the merchant-media arrangement 204 includes pre-set timer, and the pre-set time sets a time period during which communications from a particular RFID tag can not be processed. By starting the timer when RFID tag information is read from a certain RFID reader, the subsequent receipt of duplicate RFID tag information received through the same RFID reader can be ignored for a preset amount of time.

[0054] FIG. 3 shows a portable add-on media communications arrangement 300 adapted for implementation with fixed and mobile conventional advertising arrangements, such as a billboard or other advertisement arrangement on stationary display or in public transportation vehicles (*e.g.*, busses, subways and trains). The media communications arrangement 300 is adapted for coupling with one or more of a plurality of types of media, such as advertising billboards, display screens, vending machines, advertising kiosks, ticketing machines, point-of-sale terminals and others. Optionally, fasteners 302, 304, 306 and 308 (*e.g.*, screws and/or adhesive) are used to fasten the media communications arrangement 300 to advertising media. The media communications arrangement 300 includes an RFID reader 310 and an identification (ID) storage device 330 that are coupled to a transceiver 320. The RFID reader 310 is adapted to send activation signals for activating RFID tags brought within a particular range of the RFID reader arrangement 300 (*e.g.*, as discussed above in connection with FIG. 1). The ID storage device 330 stores a unique ID for the RFID reader arrangement 300.

[0055] In response to the RFID reader 310 receiving RFID tag information, the transceiver 320 sends a wireless signal to a remote wireless processor arrangement 350, the wireless signal including the unique ID for the media communications arrangement 300 and the RFID tag information. The remote wireless processor arrangement 350 is pre-programmed with media content information assigned to the unique ID for the media communications arrangement and with user preferences including user address information and one or more preferred types of communications associated with the RFID tag. In response to receiving the wireless signal from the transceiver 320, the remote wireless processor arrangement 350 uses the unique ID to retrieve media content information associated therewith and uses the RFID tag information to send the media content information to the user address using the preferred type of communications.

[0056] The media communications arrangement 300 is adaptable for use with existing advertising media and also can be moved or implemented with updated advertising media. For instance, when the media communications arrangement 300 is moved to a different type of advertising media, the remote wireless processor 350 is programmed to assign the unique ID to a new type of media content associated with the different advertising media.

[0057] Similarly, when the advertising media to which the media communications arrangement 300 is attached is changed, the remote wireless processor 350 is correspondingly reprogrammed to assign the unique ID to a new type of media content, consistent with the changed advertising media. For instance, when the content of a billboard is changed, the unique ID is assigned to the changed content. The content may also be audio information delivered through loudspeakers installed at the merchant media arrangement.

[0058] FIG. 4 shows an information block 400 used in the transmission of data in connection with a merchant-

WAVELYNX EX. 1003, Pg. 1114
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

media arrangement, according to another example embodiment of the present invention. The information block 400 may be implemented, for instance, in connection with the example embodiments described herein, such as those discussed in connection with the figures. The information block 400 includes a RFID reader identifier field 402 used to identify a particular RFID reader from which the information block is communicated. RFID tag information identifier field 404 is used to identify a tag read by the particular RFID reader. Field 406 is optional and may include a variety of other information, such as user-selected media content or communications medium type. Each of the fields shown in information block 400 are varied in length, depending upon the implementation; for instance, field 406 is eliminated or expanded depending upon the need for optional communications.

[0059] In one implementation, field 406 includes content type information for use in communicating information in addition to RFID tag and RFID reader information, such as information regarding user selections and other data. For instance, when implemented in connection with the communications link 260 and/or user input device 209 of FIG. 2, the optional field 406 is implemented for communicating data received from a local user to the remote processing arrangement 212. The content type of such data may include SMS, MMS, URL for use with WAP browsing, Java program download requests and/or Java programs (*e.g.*, MIDlets), UPC/EPC, smart message, and the like. Each of these and other content types can be identified using the optional field 406.

[0060] The information block 400 optionally includes a certificate field 407, shown as one octet but of any desired length. This field 407 may be used, for example, to provide an electronic signature to guarantee authenticity of the communications. A check sum field, such as Cyclic Redundancy Check (CRC) field 408, may also be provided with the information block 400. The CRC information may be used to determine whether errors occurred in connection with the reading of the tag information 400. Other and/or different information may also be provided, as the present invention contemplates any number of different tag content types, formats, fields, *etc.*

[0061] Using the description provided herein, the invention may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof.

[0062] Any resulting program(s), having computer-readable program code, may be embodied on one or more computer-usable media such as resident memory devices, smart cards or other removable memory devices, or transmitting devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program that exists permanently or temporarily on any computer-usable medium or in any transmitting medium which transmits such a program.

[0063] As indicated above, memory/storage devices include, but are not limited to, disks, optical disks, removable memory devices such as smart cards, SIMs, WIMs, semiconductor memories such as RAM, ROM, PROMS, *etc.* Transmitting mediums include, but are not limited to, transmissions using wireless/radio wave communication networks, the Internet, intranets, telephone/modem-based network communication, hard-wired/cabled communication network, satellite communication, and other stationary or mobile network systems/communication links.

[0064] From the description provided herein, those skilled in the art are readily able to combine software created as described with appropriate general purpose or special purpose computer hardware to create a mobile computer system and/or computer subcomponents embodying the invention, and to create a mobile computer system and/or computer subcomponents for carrying out the method of the invention.

[0065] The foregoing description of the exemplary embodiments of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, it will be apparent to those skilled in the art from the foregoing description that the invention is equally applicable to other current or future radio frequency identification technologies using, for example, electromagnetic/electrostatic coupling, and thus the present invention is not limited to "RFID" technology as this term is currently used. It is intended that the scope of the invention be limited not with this detailed description, but rather defined by the claims appended hereto.

Claims

1. An interactive communications system for use in conveying information to a selected user having a communications-user-receipt address stored with respective other communications-user-receipt addresses for other users, the interactive communications system comprising:

   a user-communications device including user identification (ID) data stored therein and being adapted to communicate the user ID data for the selected user;

   a merchant-media arrangement having at least one merchant-media ID code and being adapted to receive and process the user ID data by sending a merchant-information-request signal that includes data representative of the merchant-media ID code and the user ID data; and

WAVELYNX EX. 1003, Pg. 1115
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

a data processing arrangement adapted to access, in response to receiving the merchant-information-request signal, stored merchant information corresponding to the merchant-media ID code and a stored communications-user-receipt address corresponding to the user ID data, and to send the accessed merchant information to the accessed communications-user-receipt address of the selected user.

2. The interactive communications system of claim 1, wherein the user-communications device includes a radio frequency identification (RFID) tag including the user ID and adapted for transmitting the user ID via an RF signal and wherein the merchant-media arrangement includes an RFID reader adapted to read the RF signal.

3. The interactive communications system of claim 2, wherein the RFID tag is adapted for transmitting the user ID via the RF signal in response to an activation signal.

4. The interactive communications system of claim 3, wherein the merchant-media arrangement is adapted for transmitting the activation signal.

5. The interactive communications system of claim 1, wherein the user-communications device is a wireless-communications device and includes a transponder adapted to transmit the user ID data in response to a signal received thereby.

6. The interactive communications system of claim 5, wherein the wireless communications device includes a device selected from the group of: an identification card, travel card, payment card, loyalty card, an access key, a wireless telephone, a computer and a PDA.

7. The interactive communications system of claim 1, wherein the user-communications device is a passive wireless-communications device adapted to transmit the user ID data in response to an activation signal from the merchant-media arrangement while using the activation signal to power the transmission of the user ID data.

8. The interactive communications system of claim 1, wherein the user-communications device includes a power source used for communicating the user ID data.

9. The interactive communications system of claim 1, wherein the user-communications device is adapted to physically interface with the merchant-media arrangement and to communicate the user ID data to the merchant-media arrangement via the physical interface.

10. The interactive communications system of claim 1, wherein the merchant-media arrangement is adapted to convey media information to a user in possession of the user-communications device.

11. The interactive communications system of claim 1, wherein:

the user-communications device is a wireless-communications device;
the merchant-media arrangement includes at least two receivers spaced apart at a selected distance and adapted to receive user ID data from the wireless communications device; and
the wireless-communications device is adapted to transmit the user ID data for a selected range, the selected distance at which the at least two receivers are spaced being sufficient such that the wireless-communications device cannot simultaneously transmit the user ID data to both receivers.

12. The interactive communications system of claim 11, wherein:

each receiver has a unique merchant-media ID code;
the merchant-media arrangement is adapted to send a merchant-information-request signal that includes data representative of the at least one merchant-media ID code from one of the at least two receivers that receives user ID data;
the selected user has at least two types of stored communications-user-receipt addresses; and
the data-processing arrangement is adapted to access a first one of the two types of stored communications-user-receipt addresses in response to receiving a merchant-information-request signal including data representative of a first one of the merchant-media ID codes, and to access a second one of the two types of stored communications-user-receipt addresses in response to receiving a merchant-information-request signal including data representative of a second one of the merchant-media ID codes.

13. The interactive communications system of claim 1, wherein the merchant-media arrangement further includes a user interface adapted to receive user inputs including merchant-information-type request input data, the merchant-media arrangement being adapted to receive and process the user ID data and the user inputs by sending a merchant-informa-

WAVELYNX EX. 1003, Pg. 1116
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

tion-request signal that includes data representative of the merchant-media ID code, the user ID data and the merchant-information-type request input data.

14. The interactive communications system of claim 13, wherein the merchant-media arrangement is adapted to send merchant-information-type request input data that includes a communications medium type selection for selecting the a communications medium via which the stored merchant information is sent.

15. The interactive communications system of claim 13, wherein the merchant-information-type request input data includes a communications medium type selection for sending the stored merchant information.

16. The interactive communications system of claim 13, wherein the merchant-media arrangement includes a user interface adapted for receiving information from the data processing arrangement and for communicating the received information to a user at the merchant-media arrangement in response to the user-communications device communicating the user ID data.

17. The interactive communications system of claim 16, wherein the user interface is adapted for communicating at least two different types of advertising media to the user at exclusive time periods, wherein the merchant-media arrangement includes a unique merchant-media ID code for each of the at least two different types of advertising media and is adapted for sending a merchant-information-request signal including one of the unique merchant-media ID codes corresponding to the one of the at least two different types of advertising media being displayed when the user ID data is transmitted.

18. The interactive communications system of claim 1, wherein the merchant-media arrangement includes the data processing arrangement.

19. The interactive communications system of claim 1, further comprising a feedback device adapted to communicate a signal to a user at the merchant-media arrangement when the merchant-media arrangement receives the user ID data.

20. The interactive communications system of claim 1, wherein the merchant-media arrangement is further adapted to mitigate repetitive sending of a merchant-information-request signal in response to a user-communications device consecutively communicating the user ID data for the selected user.

21. An interactive communications system for use in conveying information to a selected user, the interactive communications system comprising:

a wireless-communications device including user identification (ID) data stored therein and being adapted to transmit the user identification (ID) data;
a merchant-media arrangement having at least one merchant-media ID code and being adapted to receive and process the user ID data by sending a merchant-information-request signal that includes data representative of the merchant-media ID code and the user ID data;
a first memory storing respective predetermined communications-user-receipt addresses for selected users;
a second memory storing merchant information for the merchant-media ID code; and
a data processing arrangement adapted to receive the merchant-information-request signal and to access the first and second memories, and in response to the merchant-information request signal including data representative of user ID data that corresponds to one of the selected users, adapted to send the stored merchant information to the predetermined communications-user-receipt address of the one of the selected users.

22. The interactive communications system of claim 21, wherein the second memory is located at a remote merchant processing arrangement that is remote from the data processing arrangement and corresponds to the merchant-media ID code and wherein the data processing arrangement is adapted to send the stored merchant information to the predetermined communications-user-receipt address by sending the predetermined communications-user-receipt address to the remote merchant processing arrangement, which responds by sending the stored merchant information to the communications-user-receipt address of the selected user.

23. The interactive communications system of claim 21, wherein the remote processing arrangement is adapted to send the stored merchant information directly to the wireless communications device via a wireless communications link.

24. For use with an interactive communications system having a data processing arrangement that stores respective communications-user-receipt addresses for selected user IDs and sends selectable merchant information to selectable communications-user-receipt addresses, a merchant-media arrangement comprising:

WAVELYNX EX. 1003, Pg. 1117
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

a display media for displaying information available from a merchant;
a receiver adapted to wirelessly receive user identification (ID) data from a user communications device;
a memory adapted to store at least one merchant-media ID code that identifies media displayed at the merchant-media arrangement; and
a wireless transmitter adapted to wirelessly send a merchant-information-request signal that includes data representative of the merchant-media ID code and user ID data received by the receiver, the merchant-information-request signal indicating to the interactive communications system a selected communications-user-receipt address as a function of the user ID data and indicating selected merchant information for sending to the selected communications-user-receipt address as a function of the stored merchant-media ID code.

25. The merchant-media arrangement of claim 24, further including a plurality of RFID readers, each RFID reader having a unique ID that identifies the merchant media arrangement.

26. The merchant-media arrangement of claim 24, wherein the receiver, the memory and the wireless transmitter are included in a portable add-on arrangement adapted for coupling to existing display media.

27. The merchant-media arrangement of claim 26, wherein the portable add-on arrangement has a reprogrammable merchant-media ID code programmed to correspond to a merchant offering the display media to which the portable add-on arrangement is coupled.

28. The merchant-media arrangement of claim 24, wherein the display media, receiver, memory and wireless transmitter are included in a mobile arrangement adapted for coupling to a moving display location.

29. For use with an interactive communications system that stores respective communications-user-receipt addresses for selected users, a method of conveying information to one of the selected users, the method comprising:

wirelessly communicating user identification (ID) data for the one selected user to a merchant-media arrangement having at least one merchant-media ID code;
sending a merchant-information-request signal that includes data representative of the merchant-media ID code and the user ID data from the merchant media arrangement; and
at a data processing arrangement, receiving the merchant-information-request signal and, in response thereto, accessing stored merchant information that corresponds to the merchant-media ID code and sending the stored merchant information to a communications-user-receipt address that corresponds to the user ID data.

30. The method of claim 29, wherein wirelessly communicating user ID data includes wirelessly activating a transponder and, in response thereto, wirelessly communicating the user ID data to the merchant-media arrangement.

31. The method of claim 29, further comprising registering a communications-user-receipt address that corresponds to the user ID data with the data processing arrangement and wherein sending the stored merchant information includes sending the stored merchant information to the registered communications-user-receipt address.

32. The method of claim 29, further comprising registering with the data processing arrangement a merchant registration status that corresponds to the merchant-media ID code, the merchant registration status being indicative of the currency of a particular merchant's registration, wherein accessing stored merchant information includes determining that the merchant-media ID code corresponds to a current merchant registration status and wherein sending the stored merchant information includes sending the stored merchant information in response to the merchant registration status being current.

33. The method of claim 29, further comprising communicating user-input data via a user interface at the merchant-media arrangement, wherein sending the merchant-information request signal includes sending data representative of the user-input data and wherein accessing stored merchant information and sending the stored merchant information includes accessing and sending the stored merchant information in response to the data representative of the user-input data.

34. The method of claim 29, further comprising communicating merchant-media data to the one selected user via the merchant-media arrangement.

35. The method of claim 34, wherein communicating merchant-media data to the one selected user includes communicating the accessed stored merchant information to the one selected user via the merchant-media arrangement.

WAVELYNX EX. 1003, Pg. 1118
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

36. An interactive communications system for communicating information to a selected user, the system comprising:

a user device (102);
transceiver means (112); and
data processing means (140); wherein
the user device (102) is arranged to communicate user identification data for the selected user to the transceiver means,
the transceiver means (112) is arranged to receive the user identification data and to send data identifying the user and data identifying the transceiver means to the data processing means, and
the data processing means (140) is arranged to retrieve a user address based on the received user identity data, to retrieve information associated with the received transceiver identity data and to send the retrieved information to the user address.

WAVELYNX EX. 1003, Pg. 1119
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

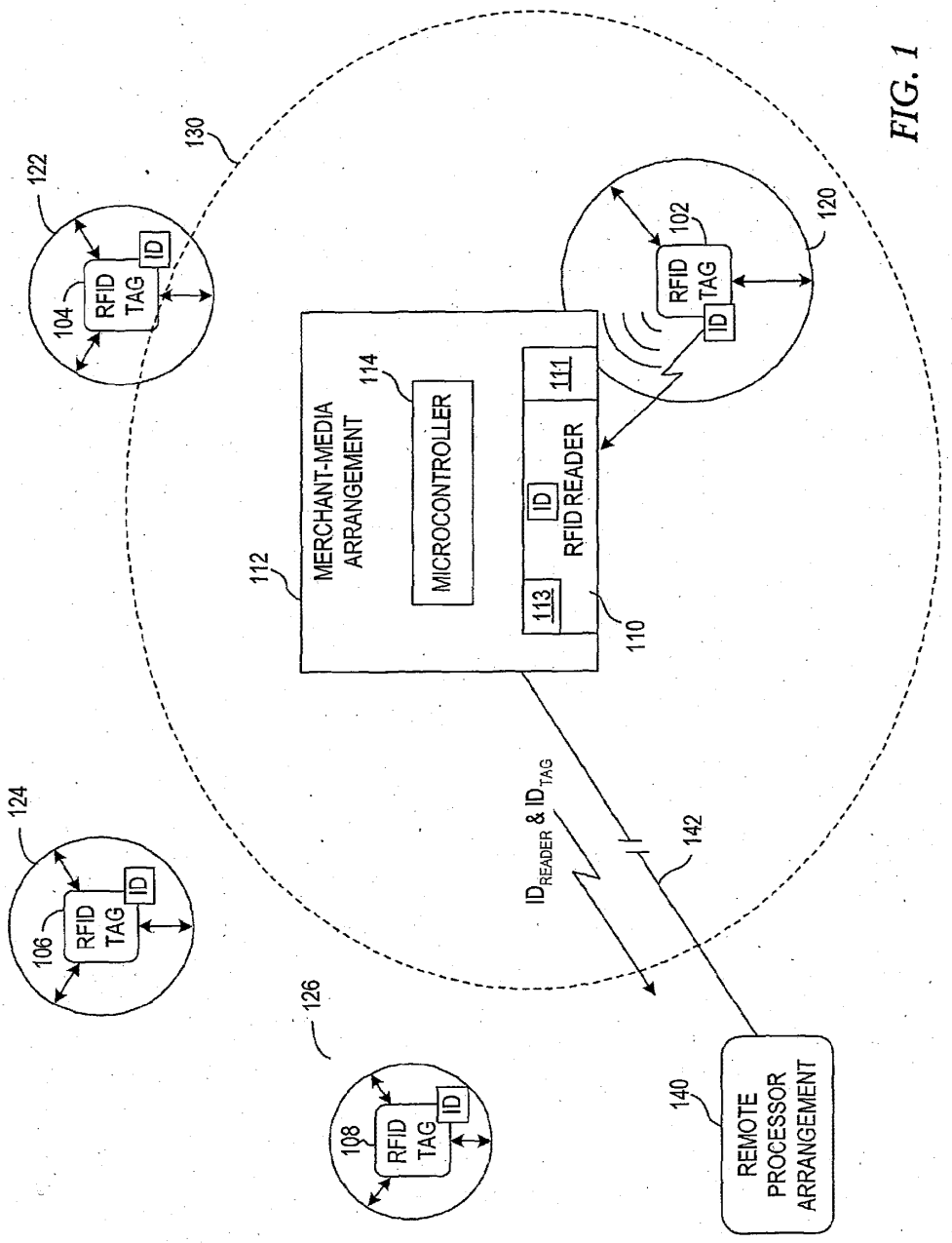


FIG. 1

WAVELYNX EX. 1003, Pg. 1120
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

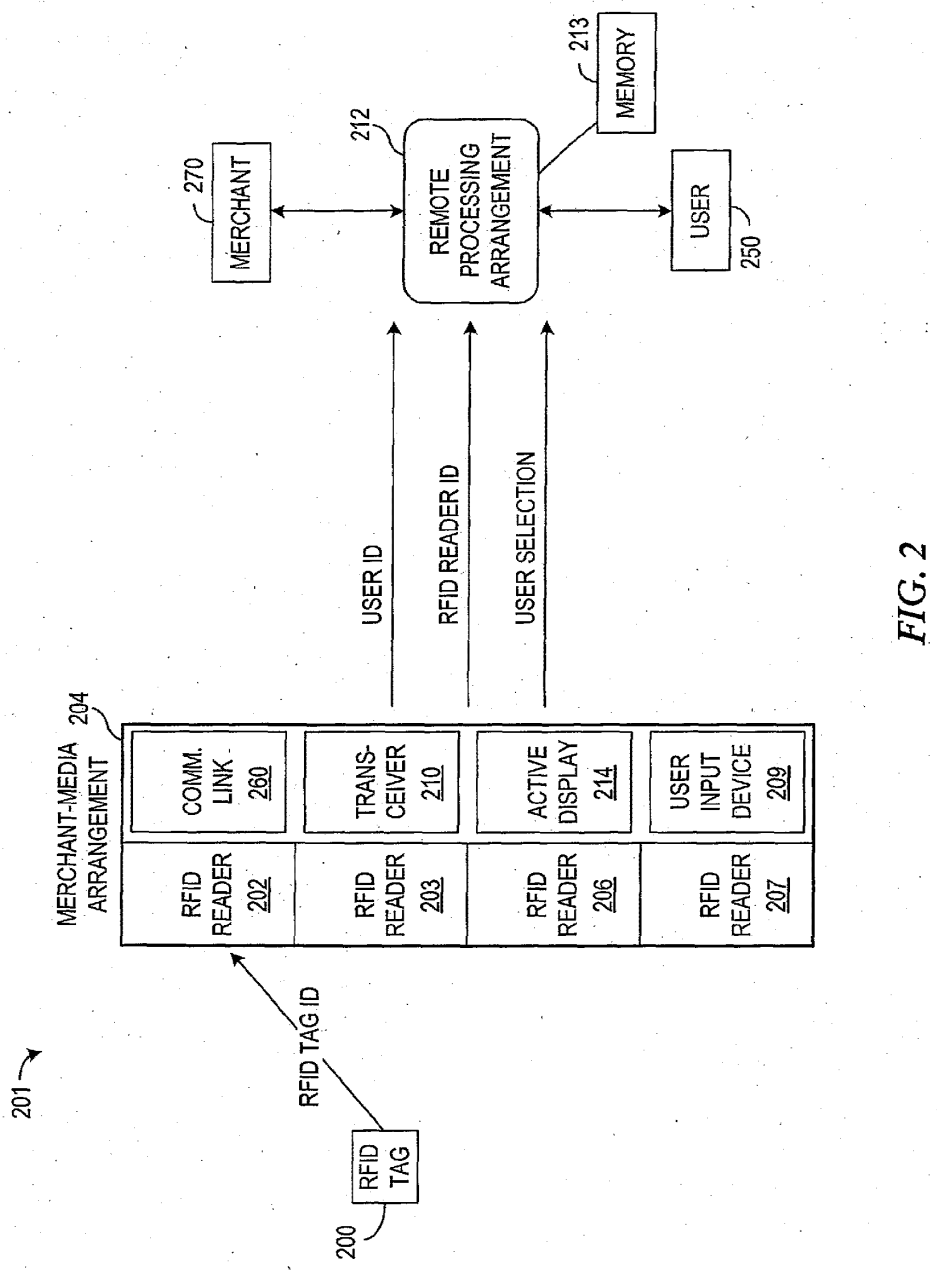


FIG. 2

WAVELYNX EX. 1003, Pg. 1121
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

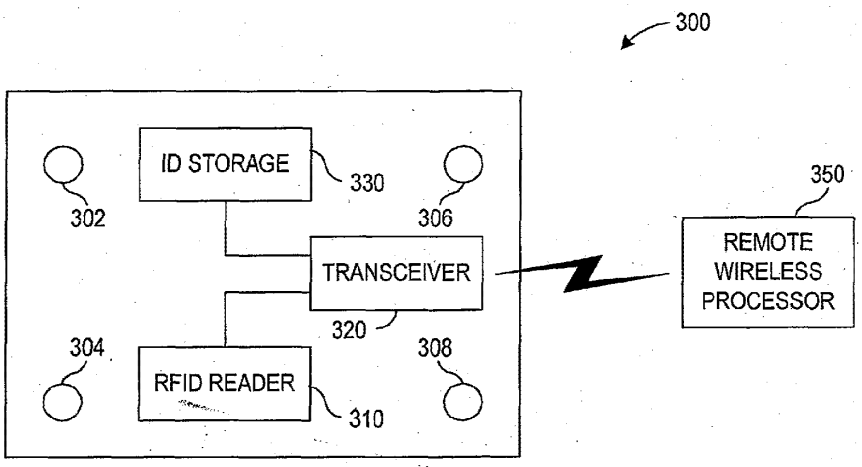


FIG. 3

	OCTET	DESCRIPTION
402	0	RFID READER ID
	1	RFID READER ID
	2	RFID READER ID
	⋮	RFID READER ID
	n	RFID READER ID
404	⋮	RFID TAG ID
	⋮	RFID TAG ID
	⋮	RFID TAG ID
406	⋮	OPTIONAL FIELDS
	⋮	OPTIONAL FIELDS (CONTENT, COMMUNICATIONS MEDIUM TYPE)
407	n+m-2	CERTIFICATE FIELD (OPTIONAL)
408	n+m-1	CYCLIC REDUNDANCY CHECK SUM
	n+m	CYCLIC REDUNDANCY CHECK SUM

FIG. 4

WAVELYNX EX. 1003, Pg. 1122
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Random number generator and method for random number generation

Publication number: EP1643643 (A1)
Publication date: 2006-04-05
Inventor(s): LAZICH DEJAN DR [DE]; ALRUTZ HERBERT DR [DE]; TEMERINAC MIODRAG DR [DE]; SCHOBER STEFFEN DIPL INFORM [DE] +
Applicant(s): MICRONAS GMBH [DE] +
Classification:
- international: ***H03K3/84; G06F7/58;*** **H03K3/00; G06F7/58**
- European: G06F7/58R; H03K3/84
Application number: EP20050020294 20050916
Priority number(s): DE200410047425 20040928

Also published as:
EP1643643 (B1)
US2006069706 (A1)
JP2006139756 (A)
DE102004047425 (A1)
DE102004047425 (B4)
more >>

Cited documents:
US5963104 (A)
WO03081417 (A2)
US5961577 (A)

Abstract of **EP 1643643 (A1)**

The method involves receiving digital oscillating signals of equal or unequal periodicity from the ring oscillators (41-43). An external parity signal (PS) is generated for feeding back to external parity inputs (45-47) of respective ring oscillators. The external parity signal is set to logical state "1", only when odd number of digital oscillating signals exhibit logical state "1". An independent claim is also included for random number generator.

Data supplied from the ***espacenet*** database — Worldwide

WAVELYNX EX. 1003, Pg. 1123
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Europäisches Patentamt
European Patent Office
Office européen des brevets

Description of EP1643643	Print	Copy	Contact Us	Close

Result Page

Notice: This translation is produced by an automated process; it is intended only to make the technical content of the original document sufficiently clear in the target language. This service is not a replacement for professional translation services. The esp@cenet® Terms and Conditions of use are also applicable to the use of the translation tool and the results derived therefrom.

[0001] The invention relates to a random number generator in accordance with the preamble of the claim 14 as well as a method to the generation of random numbers after the preamble of the claim 1.

[0002] Random number generators (English. Random NUMBER of generator - RNGs) serve the automatic generation of random binary or multi-valued numbers (random numbers). Random number generators become required in a multiplicity of scopes. To it belong for example:
Kryptografi applications,
Stochastic simulations,
Testing of software and hardware,
Computer games.

[0003] In the following exclusive kryptografische applications of random number generators become considered. To these applications belong for example:
For Authentifikation:
Challenge responseprotocols,
Zero Knowledge evidences.
For key exchange protocols:
top
Diffie Hellmann method,
To the key production,
Session key for symmetrical coding procedures,
Key production for asymmetric coding procedures (publication IC key methods),
Generation of binary noises (Ontetime PAD, Mc-Eleice publication IC key method),
Parameter production for publication IC key method (z. B. the generation random prime numbers).
For other kryptografische applications:
Password production,
Initial values (English. Seeds) for deterministic random number generators (pseudo-random number generators),
Addition of plain language blocks (English. Padding),
Safe deletion of storage mediums (by multiple overwriting with random bit patterns).

[0004] Generally two main kinds of generators distinguished become, the deterministic (English. Pseudo random NUMBER generator - PRNG) and the physical random number generators (English. True random NUMBER generator - TRNG). With deterministic generators it concerns algorithmic methods, which from a random selected initial value (English. Initially VALUE - IV) a much longer sequence of numbers produce, which appear random. Natural one cannot be this sequence, by the deterministic character of the production method, by SE genuine random.

[0005] In order to be able to produce actual random sequences of numbers, therefore a physical random number generator so mentioned must become used. This uses not-deterministic or chaotic physical processes to the generation of the random numbers either. By measurement and processing of certain process measured variables (z. B. Voltage of the thermal noise at a resistor), then the random numbers generated become.

[0006] Object of this invention is to realize a physical random number generator which in integrated circuits (Integrated Circuits = ICs) used (embedded) can become and which the subsequent kryptografischen and economical relevant control criteria satisfied:
Exclusive capable of being implemented using standardized devices of the conventional highly integrated circuits (z. B. logic gate),
Constructed bottom use of fewer a devices as possible (inexpensive, with small surface and small current consumption),
Embedded one as independent, independent unit on the IC, protected before the influence of other units
Switching independent on and off the remaining units on the IC
Rapid restore of the functionality after switching on on (short a heating time)
If possible high number of generated coincidence bits per time (high rate)
Robustness in relation to site conditions (temperature, electromagnetic interferences, changes of the supply voltage, etc.)

WAVELYNX EX. 1003, Pg. 1124
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Robustness in relation to invasive and not-invasive manipulation attempts (attacks)
Passive attacks
Active attacks
Fulfilment of statistical tests, which judge the quality of the coincidence of both generated bits
As little as possible deterministic rework of the generated random numbers
Possibility of a functionality and a quality inspection during the operation (on-line test).

[0007] In the following is assumed a kryptografischer random number generator is realized as source of bit. Depending upon application the single bits become blocks summarized (z. B. 56 bits for a key DATA of the Encryption standard -). Generally is to be assumed the bit sequences generated by a kryptografischen random number generator (z. B. a key) secret to remain must, in order not to compromise the safety of the Kryptosystems (in the applications listed in the previous portion this applies to all methods, up to Challenge responseprotocols and Zero Knowledge evidences). In these cases the generated random number generator the secret (English. Secret) of the respective Kryptoverfahrens. Assistance of this secret now z become. B. Plaintexts encrypted. Case the aggressor the secret unknown is, has he the choice all possible bit sequences to always try one after the other (complete search). In the above example this would mean that the aggressor, who a plaintext encrypted with the unknown key has observed in (statistical) the means 2< 55> possible keys to try one after the other must, until it can expect the actual generated key to have found. This attack is from view of the aggressor schlechtest possible case. In order to attack a system successful, the aggressor must be in the layer to meet a prediction over a certain number from bits to a generator to a particular time the generated. This can happen without knowledge of other bit sequences generated of the generator or bottom knowledge of bit sequences, which the generator before or after the unknown bit sequence generated has. The aggressor can try either the generated bit sequence complete or only to parts guess. In the latter case he can find the remaining bits by a complete search.

[0008] In order to meet such a prediction, all known technical and scientific means are to the aggressor at the disposal. It is reduced only regarding the costs which can be spent on the attack. One can assume these have to be appropriate for bottom one been fixed cost limit (an economic argument: The gain by the attack, which can be expected, should not exceed the costs for the attack).

[0009] Depending upon height of the cost limit the source of bit in various safety stages can become divided. If a source of bit for a given cost limit resists all attacks, then it, concerning this cost limit, is when practical safe source of bit referred become.

[0010] The fig 14 shows a model of a physical random number generator TRNG in form of a physical source of bit. Essential component of the sources is a physical dynamic, unvorhersagbares system, the source of coincidence in such a way specified 1. With this source of coincidence 1 an internal (more time-dependent) state associated can become. In temporal distances the value of the condition of the source of coincidence becomes 1 measured and processed (value determination 2) and from this or several coincidence bit a generated (coincidence bit generation 3). Sequences of these such generated coincidence bits become referred as internal coincidence bits. These can be submitted of a subsequent algorithmic rework 5. The mathematical rework 5 serves generally the purpose to improve the quality of the internal random numbers (a measure for the quality of random numbers must become here still defined. Details in the following for this portion). Generally one speaks of coincidence extraction 5. By this the elimination is to be understood about responses between the one on the other subsequent generated bits and the elimination of an often present bias (unequal distribution of the zeroes and ones). The here generated coincidence bits are deposited if necessary in an other step outputted and in an output buffer (coincidence bit output 5).

top

[0011] As in fig 14 shown, is not a physical random number generator TRNG isolated system, but embedded into a physical environment 6. It is to be assumed the measured state and concomitantly the generated coincidence bits of certain physical quantities of the environment are 6 dependent. To it sizes belong, like z. B. the supply voltage supplied to the apparatus, the ambient temperature or electromagnetic fields.

[0012] On the basis the type of the physical system several kinds of generators can become distinguished. Two substantial types of the used physical systems can be constituted:
Quantum-physical systems,
Classical physical systems.

[0013] A bottom quantum-physical system understands one a system, which becomes described by the laws of quantum mechanics. After the current general scientific view are the phenomena occurring here here, on which then the coincidence production pushes away, genuine random. Examples for this are decay processes of radioactive materials.

[0014] Classical physical systems however become described by the deterministic laws (classical) of physics. The fact that these systems can be nevertheless unvorhersagbar can have several reasons. For systems with many degrees of freedom the arising interactions are to be predicted within the system often too complex around it exact. In addition it comes that the initial state of the system cannot become often exact certain. This circumstance has other effects in case of chaotic systems so mentioned. In such systems smallest changes in the initial state, in courses of the time, to itself do not lead strong differentiating, predictable supervisor states.

[0015] In order to judge a kryptografische source of bit, it must become with the properties that managing presented practical safe kryptografischen source of bit compared. To it a statistical judgment of the generated bit sequences and an examination of the possibilities of the side channel attacks in such a way specified belong. With the use of random number

WAVELYNX EX. 1003, Pg. 1125
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

generators in embedded systems an actual large meaning comes to these attacks. A bottom side channel attack is to be understood an experiment to predict the numbers generated of the generator and/or. to affect their generation. This is done non-invasive via determination of measurement values from the environment of the generator (passive attacks), and/or. by a targeted interference of the environment (active attacks). The invasive side channel attacks represent an other aggravation of such an attack (for the example the IC could be drilled out to measure signals over there). Typical passive, non-invasive attacks are for the example the measurement of the electromagnetic radiation or the current consumption of the generator.

[0016] For the statistical judgment, by a generator generated bit sequences various statistical tests are to that at the disposal (z. B. Killmann, Wolfgang; Schindler, Werner: "A proposal too: Functionality classes and evaluation methodology for physical random number generators ", Federal Office for safety in the information technology, 2001; /Marsaglia, G. The hard: "A Battery OF test for Randomness", URL http://stat.fsu.edu/pub/diehard/. 1996; /Ruhkin, A.L. ; Sotot, J.; Nechvatal, J.; Smid, M.; Levenson, M.; Bank, D.; Vangle, M.; Leigh, S.; Vo, S.; Dray, J.: "A Statistical test Suite for the Validation OF Cryptography random NUMBER of generator", National Institute of Standards and Technology, Gaithersburg, MD, 2000; /Schindler, Werner: "Evaluation criteria for True (Physical) random NUMBER of generator Used in Cryptographic Applictions", in: Jr., Burton S.K. (Hrsg.); Kaya Koc, Cetin (Hrsg.); Pair, Christof (Hrsg.): "Cryptographic hardware and Embedded of system - CHES 2002", 4< th> International workshop, Redwood Shores, APPROX., the USA, Augusts 13-15, 2002, Revised PAPER. BD. 2523. Springer, 2003 (Lecture Notes in computer Science). - ISBN 3-540-00409-2, S. 1-2.).

[0017] In principle one stands with the judgment of these finite bit sequences before the problem of the definition of the term of a random finite sequence. After Kolmogorov (Kolmogorov, Andrei N.: "Three of approaches ton the quantitative definition OF information", in: "Problem in information transmission 1" (1965), No. 1) a finite sequence is random, if it cannot become compressed. This means that the length of their shortest algorithmic description, concerning a selected computer model, from which same order of magnitude is like the length of the sequence (this is the Kolmogorov complexity in such a way specified of a sequence, with the Turning machine as computer model). The principle here is that a sequence, which is more compressible must exhibit regularities, in order to make the compression possible. Random sequences do not exhibit thus in this sense any regularities. Unfortunately no direct tests for the eventuality can be derived from sequences from this concept, since the Kolmogorov complexity is not calculable in the sense of the predictability theory.

[0018] The statistical tests are to be examined only in the layer a bit sequence concerning certain properties, which one assigns random (finite) bit sequences. These properties are often derived from intuitive ideas, which one has after general view of the coincidence. Actual one could become by series test shown that they, by bit sequences random in the sense Kolmogorov, are existed (left, Ming; Vitannyi, Paul: "At Introduction ton of Kolmogorov Complexity and its Applications", Springer publishing house, 1993, - ISBN 0-387-94053-7).

top

[0019] From the state of the art now physical random number generators are in a multiplicity of modifications known. Starts of the random-number generator development predominantly external became, D. h. not in ICs embedded random number generators developed. For this a larger selection at used sources of coincidence is available. In present, external random number generators a multiplicity of sources of coincidence becomes used, for example radioactive sources, electronic, thermal noise in resistors or random events in the environment (z. B. Time intervals between palpation jerks on a keyboard).

[0020] Only in youngest time random number generators become embedded in commercial ICs. Here play now the type of the source of coincidence, their surface area on the IC, the technical implementation and miniaturization an important role. However noted hardly becomes to today the immunity of the random number generators against side channel attacks. Examples for realized embedded random number generators are in DE 101 17 362 A1; Cryptography Research, Inc. "Evaluation OF the VIA C3 Nehemiah random NUMBER generator", URL http://www.cryptography.com/resources/whitepapers/VIA_rng.pdf; Cryptography Research, Inc. "The Intel random NUMBER generator" URL http://www.cryptography.com/resources/whitepapers/ IntelRNG.pdf; US 2002/0186 086 A1; US 4,855,690; DE 101 03 071 A1; Fischer, Viktor; Drutarovsky, Milos: "True random NUMBER generator Embedded in Reconfigurable hardware", in: Jr., Burton S.K. (Hrsg.); Kaya Koc, Cetin (Hrsg.); Pair, Christof (Hrsg.): "Cryptographic hardware and Embedded of system - CHES 2002", 4< th> International workshop, Redwood Shores, APPROX., the USA, Augusts 13-15, 2002, Revised PAPER. BD. 2523. Springer, 2003 (Lecture Notes in computer Science). - ISBN 3-540-00409-2, S. 415-430, US 5,706,218; WHERE 03/081417, DE 102 13 269 A1; US 2003/0185392 A1; EP 1,343,073 a2; Tkacik, Thomas's E.: "A hardware random NUMBER generator", in: Jr., Burton S.K. (Hrsg.); Kaya Koc, Cetin (Hrsg.); Pair, Christof (Hrsg.): "Cryptographic hardware and Embedded of system - CHES 2002", 4< th> International workshop, Redwood Shores, APPROX., the USA, Augusts 13-15, 2002, Revised PAPER. BD. 2523. Springer, 2003 (Lecture Notes in computer Science), - ISBN 3-540-00409-2, S. 450-453.

[0021] The invention proceeds from a so called inverter chain random number generator, as it is described in accordance with the state of the art in most different embodiment. Exemplarily to the DE 102 13 269 A1 one refers.

[0022] Basic module of these random number generators is a ring oscillator so mentioned 8. It consists of the serial link of an odd number K von Invertern inv1, inv2,... invK (logical emergency gates), whereby the output of the last inverter is invK with the input of the first inverter inv1 connected (see Fig. 15a). By the delay times of the single inverters inv1, inv2, ... invK it comes only with an odd number of K von Gattern inv1, inv2,... invK to a periodic oscillation.

[0023] To start over this oscillation and/or. to stop, the first inverter can become inv1 by a Nand gate nand1 with control input start/stop replaced (see Fig. 15b). If this control input start/stop on logical one ("1") becomes set, the ring oscillator

WAVELYNX EX. 1003, Pg. 1126
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

9 begins to swing.

[0024] Fig. 16a shows a ring oscillator 10 for K=3 with two inverters inv2, inv3 and a Nand gate nand1. Fig. 16b shows an idealized signal process at the input 11 and output 12 of an inverter inv, its delay time amounts to. One accepts, that the gates nand1, inv2, inv3 in the ring oscillator 10 after Fig. 16a a so idealized behavior exhibit, then Fig shows. 16c the idealized signal process of the ring oscillator 10 in accordance with the fig 16a at the points S, B, C and A=A', after the input S for a run time T on "1" set became.

[0025] For a technical implementation of the ring oscillator 10 with K=3 with the CMOS device 74HCT04 (without entrance Nand gate, Fig. 17a), is a signal process 14 at the point A' received with an oscilloscope in Fig. 17b represents. Like itself from the cutout enlargement of the signal process 14 (in Fig. 17b) results in, from thermal movement of the electrons in the lines of the circuit 74HCT04 a thermal noise signal is added. Fig. 17c shows the envelope 15 of the noisy oscillation signal 14 observed over a longer time interval t. As is to be noticed, that leads noise in the edges of the signal 14 to an earlier or later excess of the decision level relative to the intoxication-free signal. This temporal random displacement of the edges becomes referred as jitters. The difference between the maximum possible flank shifts, observed concerning a fixed time T1 (Fig. 17c), is with the reference numeral referred. The amount of this difference increases, the further the edge of the point of reference time is T1 remote. This phenomenon is known as jitter accumulation.

[0026] In Fig. 18 is an oscillation signal 14 of the ring oscillator 10 from Fig. 17a, with a frequency f of approx. 25 MHZ, 512 times over the durations of 0,2 s averaged, shown. The envelope 13 of this averaged signal indicates the course to the autocorrelation for various temporal distances of the point of trigger. As one from Fig. to see the signal 14 can do, becomes 18 only after approximately. 0.28 s by accumulated jitter complete dekorreliert.
This means that the generated bits only with a scanning rate from 3 hzs (or small) dekorreliert would be and thus used for a source of coincidence bit will could. In order to increase the maximum possible rats of the max generated coincidence bits, one knows several ring oscillators with various periods (i.e. with various values for K) combine. Fig 19 shows two embodiments for circuit arrangements based on a number L von Ringoszillatoren 17, 18, 19, 20, 21, 22. Here in each case a parity cheque (so called XORing) of the outputs becomes performed. Concrete one means this that the outputs of the respective Ringoszilatoren 17, 18, 19, 20, 21, 22 with the inputs of a XOR gate become xor connected, so that at its output accurate then a "1" - signal generated becomes, if against the outputs of the Ringoszilatoren an odd number of logical "1" rests to 17, 18, 19, 20, 21, 22. An even number of logical "1" will produce 0" - signal at the output of the XOR gate xor ". Therefore the signal at the output of the XOR gate becomes xor subsequent as parity signal HP of referred.

[0027] The two circuits in accordance with the figs 19a and/or. 19b differ only in the procurement the start/stop inputs of the ring oscillators 17, 18, 19, 20, 21, 22. With the first execution variant in accordance with the Fig. 19a become those start/stop inputs of the single ring oscillators 17, 18, 19 common driven. Second in Fig. 19b represented possibility consists of heading for the inputs separate in order to shift with it the initial phases of the single oscillation signals against each other.

top

[0028] In Fig. 20a is a circuit with parity cheque of two ring oscillators 24, 25 with common start/stop signal shown. As in Fig. 20b and 20c to see is, remains the period P of the parity signal HP, 29 constant. By slow phase shifts of the single ring oscillator signals 27, 28 the signal process 29 of the parity signal HP, within a period P over larger time intervals, changes which in Fig. 21a significant to see is. The envelope 30 of the parity signal HP, 29 over a period of approx. 0,2.s in Fig. 21b shows a more variable autocorrelation, which is smaller, than the autocorrelation of the individual components (see Fig. 18). This parity cheque of ring oscillators becomes used in many implementations of random number generators. With this technology one cannot remove the correlations for complete and therefore becomes an additional, the rats disparaging, deterministic rework unavoidably.

[0029] The object of the invention consists now of it, a random number generator of the genericin accordance with-eaten type as well as a method to the generation of a Zufallszahlenfolge, like it of the state of the art known is to implement in such a manner and/or. to train further that a deterministic rework is necessary no longer.

[0030] This object becomes by a random number generator with the features of the claim 14 as well as 1 dissolved by a method with the features of the claim.

[0031] Favourable embodiments and developments of the invention are in the Unteransprüchen indicated.

[0032] The invention proceeds from a method to the generation with random numbers, with which of at least two ring oscillators oscillatory digital outputs same or different periodicity generated become and become with a logic state, i.e. logical "0" or a "1", illustrative external parity signal generated, which accurate takes then the logic state "1", if an odd number of the outputs has the logic state "1", and otherwise the logic state "takes 0". Provided is according to invention that the external parity signal is fed back on in each case an external parity entrance of the respective ring oscillators. As used from the state of the art known is can the external parity signal the generation of coincidence bits become, by becoming scanned. Due to the feedback of the parity signal to (external parity) the input of the respective ring oscillator the autocorrelation of the parity signal becomes significantly reduced opposite from the state of the art the prior art method without feedback. Therefore significant increased can become with the invention process the rats of the generated coincidence bits.

[0033] A random number generator according to the invention covers at least two preferably ring oscillators constructed from independent freerunning fed back inverter chains with an odd number at connected in series inverters, which those

WAVELYNX EX. 1003, Pg. 1127
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

produces oscillatory digital outputs managing specified same or different periodicity, as well as first, preferably by an exclusive OR gate formed, parity signal generation means, which produce the aforementioned external parity signal in corresponding manner. According to invention for example formed feeding back means are provided by exclusive OR gates, which back-couple this external parity signal in each case on that an external parity entrance of the respective (from inverter chains formed) ring oscillators.

[0034] Provided is according to invention in a prefered execution variant that to each ring oscillator in each case a predetermined logic state (e.g. "1") illustrative internal parity signal generated becomes, if either the output of the respective ring oscillator or the signal a predetermined logic state fed back on the external parity entrance of the respective ring oscillator (e.g. "1") takes. These internal parity signals can become again by other parity signal formation that managing described type into an other parity signal transfered, which in managing described manner the generation of coincidence bits used can become, by becoming scanned. As a result of this other parity formation arises a signal, whose autocorrelation is again significantly reduced in relation to the external parity signal. So that accompanying the possible sampling rate can become the generation of the coincidence bits again significant increased in this way.

[0035] The random number generator according to invention covers accordingly to the generation of the inner parity signals corresponding parity signal generation means. These preferably cover exclusive OR gates with in each case an external parity entrance and an output signal input. Because of the external parity entrance is a signal derived of the external parity signal, e.g. the parity signal or a signal, whose generation becomes subsequent described in the detail, on. Against the output signal input the respective output of the respective ring oscillator rests. To the generation of the other parity signal the random number generator according to invention covers other parity signal generation means, which produce a logic state "0" or "1" illustrative other parity signal, if an odd number of the internal parity signals a predetermined logic state (e.g. "1") takes. Also these means cover in corresponding way preferably an exclusive OR gate (XOR gate) against its inputs the internal parity signals rest.

[0036] How managing already mentioned became, a starting problem can occur in particular with ring oscillators formed from inverter chains. Around this problem to avoid according to the invention starting means provided with the random number generator, which, is according to invention a start signal (e.g. a logical "1") produce and to a start/a STOP input at least one of the ring oscillators supply, so that this becomes the oscillation excited. For this this exhibits a Nand gate with two inputs for example in place of a input inverter. Input and the output of this Nand gate are interconnected in place of the input and the output of the taken out inverter with the remaining inverter chain. The other input forms the aforementioned start/STOP input to supplies of the start signal.

[0037] All ring oscillators separate can become fundamental over corresponding start/stop inputs started. It proved however in many cases as favorable, if all ring oscillators, preferably simultaneous, with the help of the same start signal (e.g. logical "1") the oscillation excited become. For this purpose for example all ring oscillators are provided in place of a input inverter with a Nand gate in each case, their start/stop inputs to supplies of the start signal (e.g. a logical "1") connected with one another are.

top

[0038] Depending upon constellation still still another starting problem can occur. This starting problem can be eliminated by the fact that at least an external parity entrance an inverter is upstream, which becomes the external parity signal supplied. To the one a delay of the signal at this external parity entrance and on the other hand steps occurs a polarity reversal of the signal at this external parity entrance with upstream inverter by this inverter. The latter leads to a polarity reversal at the input of the corresponding ring oscillator and thus to a Ingangsetzen of the oscillation in this ring oscillator. In the sequence also the other connected ring oscillators become the oscillation excited.

[0039] In certain applications it turned out as favourable, if all external parity entrances inverter chains with a different number at inverters are upstream, which become the external parity signal supplied. An oscillation of the circuit arrangement comes off if the sum is some odd multiple one of a delay time of a gate (Inventer, Nand gate, XOR gate) amounting to periodicity one of the output generated of first of the ring oscillators and a multiple one of the delay time the amounting to deceleration time duration of the external parity signal at the external parity entrance first of the ring oscillators an odd multiple one of the delay time and if the sum is some odd multiple one of the delay time amounting to periodicity one of the output generated of second of the ring oscillators and a multiple one of the delay time the amounting to deceleration time duration of the external parity signal at the external parity entrance second of the ring oscillators an even multiple one of the delay time.

[0040] As managing already mentioned became to be able both the external parity signal and the other parity signal the generation of coincidence bits used become. The random number generator according to the invention can exhibit therefore scanning means, which the external parity signal to the generation of coincidence bits with predetermined rats to scan and/or scanning means, which scan the other parity signal to the generation of coincidence bits with predetermined rats.

[0041] The maximum sampling rate other increased can become, if several random number generators become managing that described type combined. On the basis of random number generators, which external, in particular scanned, parity signals can produce and/or be produced which other, in particular scanned, parity signals by repeated and/or. repeated parity formation from these parity signals (there is arbitrary variations of parity signal formations possible) random number generators form with those (super) the parity signal planned for random number production an almost arbitrary reduced autocorrelation exhibits.

WAVELYNX EX. 1003, Pg. 1128
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0042] The other random number generation requires a sample. Here it does not play roller whether the external parity signals or the other parity signals or other parity signals of low order to the generation of coincidence bits with predetermined rats a synchronous scanned become or (super) the parity signal of highest order becomes the generation of coincidence bits with the predetermined rats scanned.

[0043] The sample can take place in temporal constant distances, according to invention is however also provided, a sample in random to accomplish not uniform sampling intervals. For example a random sample can be reached, if the sample becomes a time performed, if a generated coincidence bit a pre-determined logic state random of one that managing described random number generators (e.g. "1") takes.

[0044] The sample can take place for example by means of a D-flip-flop, which becomes managing in a clock ring oscillators that fed back by a clock generator, in particular of an astable multivibrator (with temporal constant sampling intervals) or of described type (with temporal random sampling intervals), driven.

[0045] The invention becomes now more near described on the basis the designs. Show:
Fig 1 ring oscillators with fed back parity signal.
Fig 2 an example of the starting problem with fed back ring oscillators:
a) before the start;
b) after the start.
Fig 3 a solution of the starting problem from fig 2;
a) before the start;
b) after the start.
Fig 4 the signal process of the parity signal HP in the circuit from Fig. 3 in one time interval of:
a) 10ns;
b) 40ns;
c) 200ns;
d) 400ns;
e) 1000ns;
f) 2000ns.
Fig 5 an averaged parity signal of the circuit from Fig. 3.
Fig 6 a general diagram of fed back ring oscillators (RRO).
Fig 7 a circuit of RRO (4; 1, 3, 4, 5; 3, 2, 1, 0).
Fig of 8 internal parity signals of the RRO (4; 1, 3, 4, 5; 3, 2, 1, 0) after the fig 7 in the points P1, P2, P3 and P4.
Fig 9 a coincidence bit generator realized with RROs.
Fig 10 an example of a random number generator with RRO (4; 1, 3, 4, 5; 3, 2, 1, 0).
Fig 11 a random number generator with a number of N RROs and scanned superparity signal.
top
Fig 12 a random number generator with a number of N scanned RROs and scanned superparity signal.
Fig 13 a random number generator with a number of N synchronized, scanned RROs and scanned superparity signal.
Fig 14 a model of a physical random number generator (state of the art).
Fig 15 ring oscillators in accordance with the state of the art
a) Inverter chain ring oscillator;
b) Inverter chain ring oscillator with control input.
Fig 16 an example for the operation of a ring oscillator to the state of the art
a) a ring oscillator for K=3 (state of the art);
b) an idealized delay of an inverter;
c) a course of a Schwingsignals.
Fig 17 an example for the practical implementation of the ring oscillator after fig 16
a) Implementation ring oscillator for K=3 with the device 74HCT04,
b) Course of its oscillation signal with added thermal noise;
c) Envelope of the noisy oscillation signal.
Fig 18 an averaged oscillation signal of the ring oscillator from Fig. 17a.
Fig 19 an example for the execution of a so called parity cheque (state of the art)
a) a circuit for the parity cheque of L ring oscillators with common driven start/stop signal;
b) a circuit for the parity cheque of L ring oscillators with separate driven start/stop signal.
Fig 20 an example for the practice after the parity cheque the Fig. 19a
a) an example for a circuit for parity cheque of two ring oscillators with common driven start/stop signal
b) Signals of the individual components and course of the parity signal.
c) Signals of the individual components and course of the parity signal.
Fig 21 an example for the practice of the parity cheque after the fig 19a
a) Signals of the individual components and course of the parity signal;
b) an averaged parity signal of the circuit from Fig. 20a.
Fig 22 a RRO with neutralized remainder bias

[0046] The fundamental idea of the invention exists, like stated became managing, in the feedback of the parity signal on the inputs of the single ring oscillators.

[0047] The Fig. 1 shows a first embodiment of a random number generator according to invention based on a number L von Ringoszillatoren 32, 33, 34, their outputs respective inputs of a XOR gate xor supplied becomes, at which a parity signal becomes HP of formed.

[0048] Like Fig. 1 shows, becomes the supply of the fed back parity signal HP on the single inputs of the ring oscillators

WAVELYNX EX. 1003, Pg. 1129
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

32, 33, 34 XOR gates xor1, logical by a number, xor2,... xorL achieved. The respective input, against which the parity signal HP rests, is to become as external parity entrance 36, 37, 38 referred.

[0049] Important one is to be noticed that for all value combinations of the parameters L, c1,..., does not come KL an oscillation of this circuit, like the example in Fig. 2 for L=3, C1=3, K2=5 and K3=7 shows and like subsequent in the detail described becomes.

[0050] In Fig. 2a is the logic state of the switched off circuit shown. Fig. 2b shows the state of the circuit after switching on on (i.e. after setting start/stop signal to logical "1"). How is to be noticed, the circuit is still in a static (not swinging) state, there itself all outputs of the Nand gates nandi, 1 for i=1, 2, 3 not changed has. This starting problem can be repaired by inserting an other inverter inv3, -1 before the external parity entrance 47 of the XOR gate (see Fig. 3).

[0051] The parity signal HP of this circuit swinging now is in Fig. 4 for various time intervals shown. It is to be seen unique that the feedback for a suitable (swinging) parameter combination leads to one much irregular shape of the parity signal HP. The averaged parity signal HP shows a very small and constant autocorrelation (see Fig. 5). Compared with Fig. 21b is this a significant improvement, it the allowed, the rats to increase the generated coincidence bits significant.

[0052] In order to solve the starting problem of general to introduce and in order additional jitter accumulation i=1,..., becomes L, chains of inverters invi, - j, i=1... L, j=1,... Mi introduced before the XOR gates xori. The length of the single chains M1,... ML varied here. In order to place safer that that does not arise to start/stop problem, the parameters Mi and AI must become particular selected. It must apply that at least a pair i, j with i, j, {1,... L} x (1,...,} existed to L, so that one of the two sums Mi is + AI and Mj+ Kj odd and the other straight.

[0053] Fig. a general diagram with fed back parity signal HP shows 6. This circuit is to become in the following as fed back ring oscillators RRO referred. The signals at the outputs P1 to PL, the XOR gates xor1 to xorL, examine the parity of their input signals and become therefore as internal parity signals referred. The discrimination the parity signal is to become HP at the output of the XOR gate XOR as external parity signal referred.

[0054] Fig. an instance of the RRO with the parameters L=4, C1=1, K2=3, K3=4, K4=5 shows 7; M1=3, M2=2, M3=1, M4=0. As short way of writing RRO (4 becomes; 1,3,4,5; 3,2,1,0) used. The inner parity signals are very different by the construction of the RRO, like this the Fig. , the generation of coincidence bits used shows and can 8 become.

[0055] By an other parity cheque PP of the inner parity signals P1, P2,... PL, with which an other parity signal becomes PP generated, the quality is continued to improve and can become after sample as coincidence bit sequence E.G. used, like this in Fig. 9 shown is. The sample made by a D-flip-flop 85, which becomes driven by a periodic clock signal Cp. The clock signal Cp can become by an astable multivibrator 87 generated and become its period (uniform scanning interval) by a binary counter 86 certain. Around random, uniform sampling intervals to obtained, the astable multivibrator cannot become 87 by a RRO replaced. In Fig. 10 is a coincidence number generator with the RRO instance RRO (4; 1,3,4,5; 3,2,1,0) with uniform sample shown. Statistical tests of this random number generator have a small unequal distribution (bias) and a small correlation of the bits 7 shown.

top

[0056] In order to eliminate these, several RROs became by an other (super) parity cheque FR coupled. This coupling can become on many way performed. In Fig. 11 the made uniform sample after the parity cheque PP, whereas in Fig. 12 the single RROs before (Super) the parity cheque FR scanned becomes. Since this asynchronous happens, around coincidence bits 7 same durations obtained, the superparity signal FR again scanned must become. Around this to avoid the sample can become also synchronous performed, as in Fig. 13 shown becomes.

[0057] Often a small however still disturbing bias shows up in the practice. A coincidence bit sequence generated, which is not good enough, becomes corresponding. Also different electronic realized TRNGs possesses this lack, which is mostly conditional by the maladjusted operating points of the used active semiconductor components. In order to neutralize this remainder bias, various deterministic reworks become after the sample (on digital plane) performed, like e.g. in prior practice. the often used of new one method. All these algorithms decrease the rats of the generated coincidence bits substantial.

[0058] Nevertheless, with fed back ring oscillators RRO this remainder bias can become before the sample neutralized, if at the outputs P1, P2,...., PL of the ring oscillators RRO (see Fig. 9) binary counters 881, 882,... 88L of the length Z (here with a number of Z JK-flip-flop JK1, JK2... JKZ) connected become. The outputs of these counters 881, 882,... 88L become connected to the inputs of the XOR gate, which other parity signal PP supplies, (Fig. 22). By counting the signal transitions between both signal statuses (high ones and low ones with unequal durations) one receives new (longer) signal statuses. These new signal statuses are each other continuousmoderate similar, as signal statuses of the original signal. The per large number Z is, the better compensations that signal status lasting can one achieve and thus the remainder bias on arbitrary small values suppress. Already with Z=1 achieved one good results.

Reference symbol list/abbreviations

[0059]
1 : Source of coincidence

WAVELYNX EX. 1003, Pg. 1130
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2 : Valuation
3 : Coincidence bit generation
4 : algorithmic rework/coincidence extraction
5 : Coincidence bit output
6 : physical environment
8 : Ring oscillator
9 : Ring oscillator with control input
10 : Ring oscillator
11 : Input signal
12 : Output
13 : Signal envelope
14 : Signal process at point of line A'
15 : Envelope
17 : Ring oscillator
18 : Ring oscillator
19 : Ring oscillator
20 : Ring oscillator
21 : Ring oscillator
22 : Ring oscillator
24 : Ring oscillator
25 : Ring oscillator
27 : first input signal of the XOR gate
28 : second input signal of the XOR gate
29 : Parity signal
30 : Envelope of the averaged parity signal
32 : Ring oscillator
33 : Ring oscillator
34 : Ring oscillator
36 : external parity entrance
37 : external parity entrance
38 : external parity entrance
41 : Ring oscillator
42 : Ring oscillator
43 : Ring oscillator
45 : external parity entrance
46 : external parity entrance
47 : external parity entrance
47 deg. : external parity entrance
top
71 : Ring oscillator
72 : Ring oscillator
73 : Ring oscillator
81 : Ring oscillator
82 : Ring oscillator
83 : Ring oscillator
84 : Ring oscillator
85 : D-flip-flop
851 : D-flip-flop
... 86 : binary counter
861 : binary counter
... 87 : astable multivibrator
871 : astable multivibrator
... 881 : binary counter
... A: Point of line
B: Point of line
C: Point of line
A': Point of line
OF THE: DATA Encryption standard
f: Frequency
inv: Inverter
inv1: Inverter/emergency gate
inv2: Inverter/emergency gate...
invk: Inverter/emergency gate
JK1: JK-flip-flop
JK2: JK-flip-flop...
JKz: JK-flip-flop
K: Number of the gates
C1: Number of the gates
C1: Number of the gates
K2: Number of the gates
K3: Number of the gates...
KL: Number of the gates
L: Number of the ring oscillators
M: Number of the gates
M1: Number of the gates

WAVELYNX EX. 1003, Pg. 1131
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

M2: Number of the gates
M3: Number of the gates
M4: Number of the gates...
ML: Number of the gates
N: Number of the ring oscillators
nand1: Nand gate
nand2: ...
P: Period
P1: internal parity signal
P2: internal parity signal...
PL: internal parity signal
PRNG: deterministic random number generator
HP: external parity signal
RRO: fed back ring oscillators
S: Point of line
FR: Superparity signal
Start/stop: Control input
t: Time
T1: Time
T: Run time
TRNG: physical random number generator
U: Voltage
Ue: Input voltage
Ua: Output voltage
xor: Exclusive OR - /XOR gates with logical "1" at the output, if odd number of the inputs on logical "1"
xor1: Exclusive OR - /XOR gates with logical "1" at the output, if odd number of the inputs on logical "1"
xor2: Exclusive OR - /XOR gates with logical "1" at the output, if odd number of the inputs on logical "1"
Z: Number
E.G.: Coincidence bit
: Difference
: Sampling rate
max: maximum sampling rate
: Delay time

top

WAVELYNX EX. 1003, Pg. 1132
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Europäisches Patentamt
European Patent Office
Office européen des brevets

Claims of EP1643643	Print	Copy	Contact Us	Close

Result Page

Notice: This translation is produced by an automated process; it is intended only to make the technical content of the original document sufficiently clear in the target language. This service is not a replacement for professional translation services. The esp@cenet® Terms and Conditions of use are also applicable to the use of the translation tool and the results derived therefrom.

1. Methods to the generation of random numbers with periodicity generated different same of at least two ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) oscillatory digital outputs (A1, a2,..., aluminium) or become, whereby a logic state ("0", "1"), illustrative external parity signal (HP) becomes generated, which accurate takes then the logic state "1", if an odd number of outputs (A1, a2,..., aluminium) the logic state "1" exhibits, and which otherwise the logical State "0" takes,
characterised in that
the external parity signal (HP) is fed back on in each case an external parity entrance (36, 37, 38, 45, 46, 47) of the respective ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84).

2. Process according to claim 1,
characterised in that
to each ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) in each case a pre-determined logic state ("0", "1") an illustrative internal parity signal (P1, P2, P3, P4... PL) generated becomes, if entweder' the output (A1, a2.... Aluminium) of the respective ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) or the signal a predetermined logic state ("1"), fed back on the external parity entrance (36, 37, 38, 45, 46, 47) of the respective ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), takes.

top

3. Process according to claim 2,
characterised in that
a logic state ("0", "1") an illustrative other parity signal (PP) generated becomes, which accurate takes then the logic state "1", if an odd number of the internal parity signals (P1, P2, P3, P4... PL) the logic state "1" exhibits, and which otherwise the logic state "takes 0".

4. Process according to claim 3,
characterised in that
Signal transitions of the internal parity signals (P1, P2, P3, P4... Pz) before the parity signal generation counted become

5. Method after one of the preceding claims,
characterised in that
at least one of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) with the help of a respective input (start/stop) of the corresponding ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) a supplied start signal ("1") the oscillation excited becomes.

6. Process according to claim 5,
characterised in that
all ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), preferably simultaneous, with the help of the same start signal ("1") the oscillation excited become.

7. Method after one of the preceding claims,
characterised in that
the external parity signal (HP) before its feedback on at least one of the external parity entrances (47) inverted becomes.

8. Method after one of the preceding claims,
characterised in that
the external parity signal (HP) before its feedback on at least one of the external parity entrances (47) delayed becomes.

9. Process according to claim 8,
characterised in that
the external parity signal (HP) before its feedback on different external parity entrances (36, 37, 38, 45, 46, 47) around different periods () delayed becomes.

WAVELYNX EX. 1003, Pg. 1133
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

10. Process according to claim 9,
characterised in that the periodicities of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) and the deceleration time lasting of the external parity signal (HP) at the external parity entrances (36, 37, 38, 45, 46, 47) of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) in such a manner selected become that the sum some odd multiple one (c1, K2, K3,... KL) of a delay time of a gate amounting to periodicity one of the output generated of first of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) (A1, a2.... Aluminium) and some multiple one (M1, M2, M3,... ML) of the delay time of a gate amounting to deceleration time duration of the external parity signal (HP) at the external parity entrance (36, 37, 38, 45, 46, 47) first of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) an odd multiple one of the delay time of a gate is and that the sum some odd multiple one (c1, K2, K3,... KL) of the delay time of a gate amounting to periodicity one of the output generated of second of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) (A1, a2.... Aluminium) and some multiple one (M1, M2, M3,... ML) of the delay time of a gate amounting to deceleration time duration of the external parity signal (HP) at the external parity entrance (36, 37, 38, 45, 46, 47) second of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) an even multiple one of the delay time of a gate is.

11. Method after one of the preceding claims,
characterised in that
the external parity signal (HP) to the generation of coincidence bits (78) with predetermined rats (v) a scanned will or that the other parity signal (PP) becomes the generation of coincidence bits (78) with predetermined rats (v) a scanned.

12. Method after one of the preceding claims,
characterised in that
several external, in particular scanned, parity signals (HP) generated become and that a logic state ("0", "1") an illustrative superparity signal (FR) becomes generated, which accurate takes then the logic state "1", if an odd number external, in particular scanned, parity signals (HP) the logic state "1" exhibits, and which takes otherwise the logic state "0" or that several other, in particular scanned, parity signals generated become and that a logic state ("0", "1") an illustrative superparity signal (FR) becomes generated, which accurate then the logic state "1" takes, if an odd number exhibits other, in particular scanned, parity signals the logic state "1", and which otherwise the logic state "0" takes.

13. Process according to claim 12,
characterised in that
the external or the other parity signals (HP) to the generation of coincidence bits (E.G.) with predetermined rats (v) a synchronous scanned will or that the superparity signal (FR) becomes the generation of coincidence bits (E.G.) with predetermined rats (v) a scanned.

top

14. Process according to one of claims 11 to 13,
characterised in that
the sample in random, uniform sampling intervals performed does not become, in particular the fact that the sample becomes performed if after one of the methods after the claims 1 to 12 random generated coincidence bits (E.G.) takes a pre-determined logic state ("1").

15. Random number generator with at least two ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), in particular from independent freerunning fed back inverter chains with an odd number of (C) at connected in series inverters (inv1,2, inv2,1, inv3,1,... invi, j,... invL, KL), which oscillatory digital outputs (A1, a2,.... Aluminium) different periodicity produces, and with first parity signal generation means (XOR), which produce a pre-determined logic state ("0", "1") an illustrative external parity signal (HP), which accurate takes then the logic state "1", if an odd number of the outputs (A1, a2.... Aluminium) the logic state "1" exhibits, and which otherwise the logic state "takes 0",
characterised in that
Feeding back means (xor1, xor2, xor3, xor4... xorL) provided are, which feed the external parity signal back (HP) on in each case an external parity entrance (36, 37, 38, 45, 46, 47) of the respective ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84).

16. Random number generator according to claim 15,
characterised in that
the first parity signal generation means a XOR gate (XOR) cover, at its inputs the outputs (A1, a2,....) Lie close to aluminium.

17. Random number generator after one of the claims 15 or 16,
characterised in that
second parity signal generation means (xor1, xor2, xor3,... xorL) provided are, which to each ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) in each case a predetermined logic state ("1") an illustrative internal parity signal (P1, P2, P3, P4... PL) produce, which accurate takes then the logic state "1", if either the output (A1, a2.... Aluminium) of the respective ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) or the signal a predetermined logic state ("1"), fed back on the external parity entrance (36, 37, 38, 45, 46, 47) of the respective ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), takes.

18. Random number generator according to claim 17,
characterised in that
the second parity signal generation means XOR gate (xor1, xor2, xor3,... cover xorL) with in each case an external parity entrance and an output signal input, whereby at the parity entrance a signal and at the output signal input the respective

WAVELYNX EX. 1003, Pg. 1134
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

output (A1, a2, derived of the external parity signal (HP),…. Aluminium) of the respective ring oscillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) lies close.

19. Random number generator according to claim 18,
characterised in that
third parity signal generation means provided are, which produce a logic state ("0", "1") an illustrative other parity signal (WP), which accurate takes then the logic state "1", if an odd number of the internal parity signals (P1, P2, P3, P4… PL) the logic state "1" exhibits, and which otherwise the logic state "takes 0".

20. Random number generator according to claim 19,
characterised in that
Counting means (881, 882,… 88L) provided are, which signal transitions of the internal parity signals (P1, P2, P3,… PL) before the parity signal generation count.

21. Random number generator according to claim 20,
characterised in that
the counting means a binary counter (881, 882,… 88L), in particular a chain with flip-flops, preferably JK-flip-flop (JK1, JK2,… JKZ) cover.

22. Random number generator after one of the claims 15 to 21,
characterised in that
Starting means provided are, which a start signal ("1") produce and an input (start/stop) of at least one of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) supply, so that this becomes the oscillation excited.

23. Random number generator according to claim 22,
characterised in that
that at least one of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) in place of a input inverter (inv1) a Nand gate (nand1, nand1,1, nand2,1, nand3,1,… nandi, 1,… nandL, 1) with the input (start/stop) to supplies of the start signal ("1") covers.

24. Random number generator after one of the claims 22 or 23,
characterised in that
the starting means in such a manner formed are that all ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) become, preferably simultaneous, excited with the help of the same start signal ("1") the oscillation.

top

25. Random number generator according to claim 24,
characterised in that
all ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) in place of a input inverter (inv1) in each case a Nand gate (nand1, nand1,1, nand2,1, nand3,1,… nandi, 1,… nandL, 1) with in each case an input (start/stop) cover, which to supplies of the start signal ("1") are connected with one another.

26. Random number generator after one of the claims 15 to 25,
characterised in that
at least an external parity entrance (47) an inverter (inv3, -1, inv1, - M1…. inv1, -1,… invL, - ML,… invL, -1) upstream is, which becomes the external parity signal (HP) supplied.

27. Random number generator according to claim 26,
characterised in that
all external parity entrances inverter chains with a different number (M1, M2,… ML) at inverters (inv1, - M1… inv1, -1,… invL, - ML, invL, -1) upstream are, which become the external parity signal (HP) supplied.

28. Random number generator according to claim 27,
characterised in that the sum some odd multiple one (c1, K2, K3,… KL) of a delay time of a gate amounting to periodicity one of the output generated of first of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) (A1, a2…. Aluminium) and some multiple one (M1, M2, M3,… ML) of the delay time of a gate amounting to deceleration time duration of the external parity signal (HP) at the external parity entrance (36, 37, 38, 45, 46, 47) first of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) an odd multiple one of the delay time of a gate is and that the sum some odd multiple one (c1, K2, K3,… KL) of the delay time of a gate amounting to periodicity one of the output generated of second of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) (A1, a2…. Aluminium) and some multiple one (M1, M2, M3,… ML) of the delay time of a gate amounting to deceleration time duration of the external parity signal (HP) at the external parity entrance (36, 37, 38, 45, 46, 47) second of the ring oscillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) an even multiple one of the delay time of a gate is.

29. Random number generator after one of the claims 15 to 28,
characterised in that
Scanning means provided are, which it scans the external parity signal (HP) to the generation of coincidence bits (E.G.) with predetermined rats () and/or that
Scanning means provided are, which scan the other parity signal (PP) to the generation of coincidence bits (E.G.) with

WAVELYNX EX. 1003, Pg. 1135
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

predetermined rats ().

30. Random number generator after one of the claims 15 to 29,
characterised in that
several random number generators after one of the claims 15 to 29 provided are, which external, in particular scanned produce, parity signals (HP) and that superparity signal generation means provided are, which produce a logic state ("0", "1") an illustrative superparity signal (FR), which accurate takes then the logic state "1", if an odd number external, in particular scanned, parity signals (HP) the logic state "1" exhibits, and which takes otherwise the logic state "0" and/or that several random number generators are after one of the claims 15 to 29 provided, which other, in particular scanned, parity signals (PP) produce and that Superparity signal generation means provided are, which produce a logic state ("0", "1") an illustrative superparity signal (FR), which accurate takes then the logic state "1", if an odd number other, in particular scanned, parity signals (PP) the logic state "1" exhibits, and which otherwise the logic state "0" takes.

31. Random number generator according to claim 30,
characterised in that
Scanning means provided are, which scan the external parity signals (HP) or the other parity signals (PP) to the generation of coincidence bits (E.G.) with predetermined rats () a synchronous and/or that scanning means provided are, which scan the superparity signal (FR) to the generation of coincidence bits (E.G.) with predetermined rats ().

32. Random number generator after one of the claims 29 to 31,
characterised in that the scanning means arranged are, a sample in random to accomplish not uniform sampling intervals and to make in particular a sample if from one of the random number generators after the claims 15 to 31 random generated coincidence bits (E.G.) takes a pre-determined logic state ("1").

33. Random number generator after one of the claims 29 to 32,
characterised in that
the scanning means a D-flip-flop (881, 882,... 88L) cover, which in a clock (Cp) of a clock generator, in particular of an astable multivibrator (87, 871, 872,... 87L) or of a fed back ring oscillator (RRO), driven becomes.

top

WAVELYNX EX. 1003, Pg. 1136
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 643 643 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
05.04.2006 Patentblatt 2006/14

(51) Int Cl.:
H03K 3/84 *(2006.01)* ***G06F 7/58*** *(2006.01)*

(21) Anmeldenummer: **05020294.4**

(22) Anmeldetag: **16.09.2005**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA HR MK YU

(30) Priorität: **28.09.2004 DE 102004047425**

(71) Anmelder: **Micronas GmbH**
79108 Freiburg i. Br. (DE)

(72) Erfinder:
- **Lazich, Dejan, Dr.**
76297 Stutensee (DE)
- **Alrutz, Herbert, Dr.**
79102 Freiburg (DE)
- **Temerinac, Miodrag, Dr.**
79194 Gundelfingen (DE)
- **Schober, Steffen, Dipl. Inform.**
76185 Karlsruhe (DE)

(74) Vertreter: **Patentanwälte**
Westphal, Mussgnug & Partner
Am Riettor 5
78048 Villingen-Schwenningen (DE)

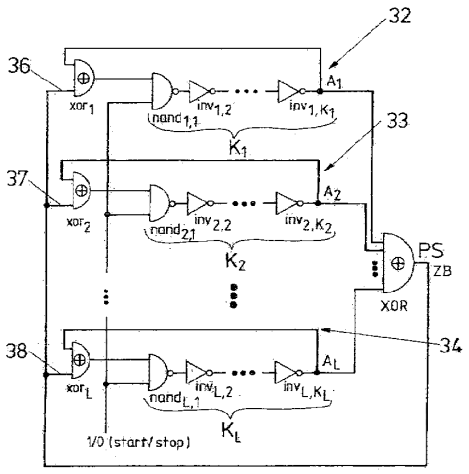
(54) Zufallszahlengenerator sowie Verfahren zur Erzeugung von Zufallszahlen

(57) Die Erfindung betrifft ein Verfahren zur Erzeugung von Zufallszahlen bei dem von wenigstens zwei Ringoszillatoren (32, 33, 34) oszillierende digitale Ausgangssignale (A_1, A_2, ... A_L) unterschiedlicher oder gleicher Periodizität erzeugt werden, wobei ein einen logischen Zustand ("0", "1") darstellendes externes Paritätssignal (PS) erzeugt wird, wenn eine ungerade Anzahl der Ausgangssignale (A_1, A_2 .... A_L) einen vorgegebenen logischen Zustand ("1") einnimmt. Erfindungsgemäß ist vorgesehen, dass das externe Paritätssignal (PS) auf jeweils einen externen Paritätseingang (36, 37, 38) der jeweiligen Ringoszillatoren (32, 33, 34) rückgekoppelt wird.

Die Erfindung betrifft ferner einen Zufallszahlengenerator mit wenigstens zwei Ringoszillatoren (32, 33, 34), insbesondere aus unabhängig freischwingenden rückgekoppelten Inverterketten mit einer ungeraden Anzahl (K) an hintereinandergeschalteten Invertern ($inv_{1,2}$, $inv_{2,1}$, $inv_{3,1}$, ... $inv_{i,j}$, ... $inv_{L,KL}$), welche oszillierende digitale Ausgangssignale (A_1, A_2, ... A_L) unterschiedlicher oder gleicher Periodizität erzeugen, und mit ersten Paritätssignalerzeugungsmitteln (XOR), welche ein einen logischen Zustand ("0", "1") darstellendes externes Paritätssignal (PS) erzeugen, wenn eine ungerade Anzahl der Ausgangssignale (A_1, A_2 .... A_L) einen vorgegebenen logischen Zustand ("1") einnimmt. Erfindungsgemäß sind Rückkoppelmittel (xor_1, xor_2, xor_3, xor_4 ... xor_L) vorgesehen, welche das externe Paritätssignal (PS) auf jeweils einen externen Paritätseingang (36, 37, 38) der jeweiligen Ringoszillatoren (32, 33, 34) rückkoppeln.

In dieser Erfindung ist das Zusammenwirken der chaotischen Dynamik (Rückkopplung des Paritätssignals) und echtem Zufall (Jitter als Folge des thermischen Rauschens) in digitalen Schaltungen, ein neues theoretisches Prinzip für die Erzeugung von Zufallszahlen, in eine effiziente praktische Lösung umgesetzt worden.

FIG 1



EP 1 643 643 A1

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1137
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Beschreibung

[0001] Die Erfindung betrifft einen Zufallsgenerator gemäß dem Oberbegriff des Patentanspruchs 14 sowie ein Verfahren zur Erzeugung von Zufallszahlen nach dem Oberbegriff des Patentanspruchs 1.

[0002] Zufallszahlengeneratoren (engl. Random Number Generators - RNGs) dienen der automatischen Erzeugung von zufälligen binären oder mehrwertigen Zahlen (Zufallszahlen). Zufallszahlengeneratoren werden in einer Vielzahl von Anwendungsbereichen benötigt. Hierzu gehören zum Beispiel:

- Kryptografische Anwendungen,
- Stochastische Simulationen,
- Testen von Software und Hardware,
- Computerspiele.

[0003] Im Folgenden werden ausschließlich kryptografische Anwendungen von Zufallszahlengeneratoren betrachtet. Zu diesen Anwendungen gehören beispielsweise:

- Für Authentifikation:
  - Challenge-Response-Protokolle,
  - Zero-Knowledge-Beweise.
- Für Schlüsselaustausch-Protokolle:
  - Diffie-Hellmann-Verfahren,
- Zur Schlüsselerzeugung,
  - Sitzungsschlüssel für symmetrische Verschlüsselungsverfahren,
  - Schlüsselerzeugung für asymmetrische Verschlüsselungsverfahren (Public-Key-Verfahren),
  - Erzeugung von binärem Rauschen (Onetime-Pad, Mc-Eleice Public-Key-Verfahren),
  - Parametererzeugung für Public-Key-Verfahren (z. B. die Erzeugung zufälliger Primzahlen).
- Für andere kryptografische Anwendungen:
  - Passworterzeugung,
  - Initialwerte (engl. Seeds) für deterministische Zufallszahlengeneratoren (Pseudo-Zufallszahlengeneratoren),
  - Ergänzung von Klartext-Blöcken (engl. Padding),
  - Sicheres Löschen von Speichermedien (durch mehrfaches Überschreiben mit zufälligen Bitmustern).

[0004] Im Allgemeinen werden zwei Hauptarten von Generatoren unterschieden, die deterministischen (engl. Pseudo Random Number Generator - PRNG) und die physikalischen Zufallszahlengeneratoren (engl. True Random Number Generator - TRNG). Bei deterministischen Generatoren handelt es sich um algorithmische Verfahren, welche aus einem zufällig gewählten Initialwert (engl. Initial Value - IV) eine viel längere Folge von Zahlen erzeugen, die zufällig erscheint. Natürlich kann diese Folge, durch den deterministischen Charakter der Erzeugungsmethode, per se nicht echt zufällig sein.

[0005] Um tatsächlich zufällige Folgen von Zahlen erzeugen zu können, muss daher ein so genannter physikalischer Zufallszahlengenerator verwendet werden. Dieser nutzt zur Erzeugung der Zufallszahlen entweder nichtdeterministische oder chaotische physikalische Prozesse. Durch Messung und Bearbeitung von bestimmten Prozessmessgrößen (z. B. Spannung des thermischen Rauschens an einem Widerstand), werden dann die Zufallszahlen erzeugt.

[0006] Ziel dieser Erfindung ist, einen physikalischen Zufallszahlengenerator zu realisieren, welcher in integrierten Schaltkreisen (Integrated Circuits = ICs) eingesetzt (eingebettet) werden kann und die folgenden kryptografischen und wirtschaftlich relevanten Gütekriterien erfüllt:

- Implementierbar ausschließlich unter Verwendung standardisierter Bauelemente der herkömmlichen hochintegrierten Schaltkreise (z. B. logische Gatter),
- Aufgebaut unter Nutzung möglichst weniger Bauelemente (kostengünstig, mit kleiner Oberfläche und geringem Stromverbrauch),
- Eingebettet als eigenständige, unabhängige, vor dem Einfluss anderer Einheiten geschützte Einheit auf dem IC
- Ein- und Ausschalten unabhängig von den übrigen Einheiten auf dem IC
- Schnelles Wiederherstellen der Funktionalität nach dem Einschalten (kurze Einwärme-Zeit)
- Möglichst hohe Anzahl von erzeugten Zufallbits pro Zeit (hohe Rate)
- Robustheit gegenüber Umgebungsbedingungen (Temperatur, elektromagnetische Störungen, Änderungen der Speisespannung, etc.)
- Robustheit gegenüber invasiven und nichtinvasiven Manipulationsversuchen (Angriffen)
  - Passive Angriffe
  - Aktive Angriffe
- Erfüllung statistischer Tests, welche die Qualität des Zufalls beider erzeugten Bits beurteilen

WAVELYNX EX. 1003, Pg. 1138
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- Möglichst wenig deterministische Nachbearbeitung der erzeugten Zufallszahlen

- Möglichkeit einer Funktionalitäts- und Qualitätsprüfung während des Betriebs (Online-Test).

[0007] Im Folgenden wird davon ausgegangen, dass ein kryptografischer Zufallszahlengenerator als Bitquelle realisiert ist. Je nach Anwendung werden die einzelnen Bits zu Blöcken zusammengefasst (z. B. 56 Bits für einen Schlüssel des Data Encryption Standard - DES). Im Allgemeinen ist davon auszugehen, dass die durch einen kryptografischen Zufallszahlengenerator erzeugten Bitfolgen (z. B. ein Schlüssel) geheim bleiben müssen, um die Sicherheit des Kryptosystems nicht zu kompromittieren (in den im vorigen Abschnitt aufgeführten Anwendungen gilt dies für alle Verfahren, bis auf Challenge-Response-Protokolle und Zero-Knowledge-Beweise). In diesen Fällen erzeugt der Zufallszahlengenerator das Geheimnis (engl. Secret) des jeweiligen Kryptoverfahrens. Mithilfe dieses Geheimnisses werden nun z. B. Klartexte chiffriert. Falls dem Angreifer das Geheimnis unbekannt ist, hat er immer die Wahl alle möglichen Bitfolgen durchzuprobieren (vollständige Suche). Im obigen Beispiel würde dies bedeuten, dass der Angreifer, welcher ein mit dem unbekannten Schlüssel chiffrierten Klartext beobachtet hat, im (statistischen) Mittel 2^{55} mögliche Schlüssel durchprobieren muss, bis er erwarten kann, den tatsächlich erzeugten Schlüssel gefunden zu haben. Dieser Angriff ist aus Sicht des Angreifers der schlechtest mögliche Fall. Um ein System erfolgreich anzugreifen, muss der Angreifer in der Lage sein, eine Vorhersage über eine bestimmte Anzahl von Bits zu treffen, die ein Generator zu einem bestimmten Zeitpunkt erzeugt. Dies kann ohne Kenntnis anderer vom Generator erzeugten Bitfolgen geschehen oder unter Kenntnis von Bitfolgen, die der Generator vor oder nach der unbekannten Bitfolge erzeugt hat. Der Angreifer kann entweder versuchen die erzeugte Bitfolge komplett oder nur zu Teilen zu erraten. Im letzteren Fall kann er die verbleibenden Bits durch eine vollständige Suche finden.

[0008] Um eine solche Vorhersage zu treffen, stehen dem Angreifer alle bekannten technischen und wissenschaftlichen Mittel zur Verfügung. Er ist nur hinsichtlich der für den Angriff aufzuwendenden Kosten eingeschränkt. Man kann davon ausgehen, dass diese unter einer festgelegen Kostengrenze zu liegen haben (ein ökonomisches Argument: Der zu erwartende Gewinn durch den Angriff sollte die Kosten für den Angriff nicht überschreiten).

[0009] Je nach Höhe der Kostengrenze kann die Bitquelle in verschiedene Sicherheitsstufen eingeteilt werden. Widersteht eine Bitquelle für eine gegebene Kostengrenze allen Angriffen, so soll sie, bezüglich dieser Kostengrenze, als praktisch sichere Bitquelle bezeichnet werden.

[0010] Die Figur 14 zeigt ein Modell eines physikalischen Zufallszahlengenerators TRNG in Form einer physikalischen Bitquelle. Wesentlicher Bestandteil der Quelle ist ein physikalisches dynamisches, unvorhersagbares System, die so genannte Zufallsquelle 1. Mit dieser Zufallsquelle 1 kann ein interner (zeitabhängiger) Zustand assoziiert werden. In zeitlichen Abständen wird der Wert des Zustands der Zufallsquelle 1 gemessen und bearbeitet (Werteermittlung 2) und hieraus ein oder mehrere Zufalls-Bit erzeugt (Zufalls-Bit-Erzeugung 3). Folgen dieser derart erzeugten Zufallsbits werden als interne Zufallsbits bezeichnet. Diese können anschließend einer algorithmischen Nachbearbeitung 5 unterzogen werden. Die mathematische Nachbearbeitung 5 dient im Allgemeinen dem Zweck, die Qualität der internen Zufallszahlen zu verbessern (ein Maß für die Qualität von Zufallszahlen muss hierbei noch definiert werden. Näheres hierzu im folgenden Abschnitt). Im Allgemeinen spricht man von Zufallsextraktion 5. Hierunter ist die Beseitigung von Abhängigkeiten zwischen aufeinander folgenden erzeugten Bits und der Beseitigung eines oftmals vorhandenen Bias (Ungleichverteilung der Nullen und Einsen) zu verstehen. Die hierbei erzeugten Zufallsbits werden in einem weiteren Schritt ausgegeben und gegebenenfalls in einem Ausgabespeicher hinterlegt (Zufalls-Bit-Ausgabe 5).

[0011] Wie in Figur 14 dargestellt, ist ein physikalischer Zufallszahlengenerator TRNG kein isoliertes System, sondern eingebettet in eine physikalische Umgebung 6. Es ist davon auszugehen, dass der gemessene Zustand und damit auch die erzeugten Zufallsbits von bestimmten physikalischen Größen der Umgebung 6 abhängig sind. Hierzu gehören Größen, wie z. B. die an das Gerät gelieferte Versorgungsspannung, die Umgebungstemperatur oder elektromagnetische Felder.

[0012] Anhand der Art des physikalischen Systems können verschiedene Arten von Generatoren unterschieden werden. Es können zwei wesentliche Arten der verwendeten physikalischen Systeme ausgemacht werden:

- Quantenphysikalische Systeme,
- Klassisch physikalische Systeme.

[0013] Unter einem quantenphysikalischen System versteht man ein System, welches durch die Gesetze der Quantenmechanik beschrieben wird. Nach der derzeitigen allgemeinen wissenschaftlichen Ansicht sind die hierbei auftretenden Phänomene, auf welche sich dann die Zufallserzeugung abstützt, echt zufällig. Beispiele hierfür sind Zerfallsprozesse von radioaktiven Materialien.

[0014] Klassisch physikalische Systeme hingegen werden durch die deterministischen Gesetze der (klassischen) Physik beschrieben. Dass diese Systeme trotzdem unvorhersagbar sein können, kann verschiedene Gründe haben. Für Systeme mit vielen Freiheitsgraden sind die auftretenden Wechselwirkungen innerhalb des Systems oft zu komplex um sie exakt vorherzusagen. Hinzu kommt, dass der Anfangszustand des Systems oft

WAVELYNX EX. 1003, Pg. 1139
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

nicht exakt bestimmt werden kann. Dieser Umstand hat im Falle so genannter chaotischer Systeme weitere Auswirkungen. In solchen Systemen führen kleinste Änderungen im Anfangszustand, im Laufe der Zeit, zu sich stark unterscheidenden, nicht vorhersagbaren Systemzuständen.

[0015] Um eine kryptografische Bitquelle zu beurteilen, muss sie mit den Eigenschaften der vorstehend vorgestellten praktisch sicheren kryptografischen Bitquelle verglichen werden. Hierzu gehören eine statistische Beurteilung der erzeugten Bitfolgen und eine Prüfung der Möglichkeiten der so genannten Seitenkanalangriffe. Beim Einsatz von Zufallszahlengeneratoren in eingebetteten Systemen kommt diesen Angriffen tatsächlich eine große Bedeutung zu. Unter einem Seitenkanalangriff ist ein Versuch zu verstehen, die vom Generator erzeugten Zahlen vorherzusagen, bzw. ihre Erzeugung zu beeinflussen. Dies geschieht nicht-invasiv durch Ermittlung von Messwerten aus der Umgebung des Generators (passive Angriffe), bzw. durch eine gezielte Beeinflussung der Umgebung (aktive Angriffe). Eine weitere Verschärfung eines solchen Angriffs stellen die invasiven Seitenkanalangriffe dar (zum Beispiel könnte der IC aufgebohrt werden, um dort Signale zu messen). Typische passive, nicht-invasive Angriffe sind zum Beispiel die Messung der elektromagnetischen Abstrahlung oder des Stromverbrauchs des Generators.

[0016] Für die statistische Beurteilung der, durch einen Generator generierten Bitfolgen stehen verschiedene statistische Tests zur Verfügung (z. B. Killmann, Wolfgang; Schindler, Werner: "Ein Vorschlag zu: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren", Bundesamt für Sicherheit in der Informationstechnik, 2001; / Marsaglia, G. Diehard: "A Battery of Tests for Randomness", URL http://stat.fsu.edu/pub/diehard/. 1996; / Ruhkin, A.L.; Sotot, J.; Nechvatal, J.; Smid, M.; Levenson, M.; Banks, D.; Vangle, M.; Leigh, S.; Vo, S.; Dray, J.: "A Statistical Test Suite for the Validation of Cryptography Random Number Generators", National Institute of Standards and Technology, Gaithersburg, MD, 2000; / Schindler, Werner: "Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applictions", in: Jr., Burton S.K. (Hrsg.); Kaya Koc, Cetin (Hrsg.); Paar, Christof (Hrsg.): "Cryptographic Hardware and Embedded Systems - CHES 2002", 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers. BD. 2523. Springer, 2003 (Lecture Notes in Computer Science). - ISBN 3-540-00409-2, S. 1-2.).

[0017] Prinzipiell steht man bei der Beurteilung dieser endlichen Bitfolgen vor dem Problem der Definition des Begriffs einer zufälligen endlichen Sequenz. Nach Kolmogorov (Kolmogorov, Andrei N.: "Three approaches to the quantitative definition of information", in: "Problems in Information Transmission 1" (1965), Nr. 1) ist eine endliche Sequenz zufällig, falls sie nicht komprimiert werden kann. Dies bedeutet, dass die Länge ihrer kürzesten algorithmischen Beschreibung, bezüglich eines ausgewählten Rechnermodells, von der gleichen Größenordnung ist, wie die Länge der Sequenz selbst (dies ist die so genannte Kolmogorov-Komplexität einer Folge, mit der Turning-Maschine als Rechnermodell). Der Grundgedanke hierbei ist, dass eine Folge, welche komprimierbar ist, Regelmäßigkeiten aufweisen muss, um die Kompression zu ermöglichen. Zufällige Folgen weisen also in diesem Sinne keinerlei Regelmäßigkeiten auf. Leider lassen sich aus diesem Konzept keine direkten Tests für die Zufälligkeit von Folgen ableiten, da die Kolmogorov-Komplexität im Sinne der Berechenbarkeitstheorie nicht berechenbar ist.

[0018] Die statistischen Tests sind nur in der Lage eine Bitfolge bezüglich bestimmter Eigenschaften zu prüfen, welche man zufälligen (endlichen) Bitfolgen zuweist. Diese Eigenschaften leiten sich oft aus intuitiven Vorstellungen ab, welche man nach allgemeiner Auffassung vom Zufall hat. Tatsächlich konnte von einer Reihe Tests gezeigt werden, dass sie, von im Sinne Kolmogorov zufälligen Bitfolgen, bestanden werden (Li, Ming; Vitannyi, Paul: "An Introduction to Kolmogorov Complexity and its Applications", Springer-Verlag, 1993, - ISBN 0-387-94053-7).

[0019] Aus dem Stand der Technik sind nunmehr physikalische Zufallszahlengeneratoren in einer Vielzahl von Abwandlungen bekannt. Zu Beginn der Zufallszahlengeneratorenentwicklung wurden vorwiegend externe, d. h. nicht in ICs eingebettete Zufallszahlengeneratoren entwickelt. Hierfür steht eine größere Auswahl an verwendeten Zufallsquellen zur Verfügung. In heutigen, externen Zufallszahlengeneratoren werden eine Vielzahl von Zufallsquellen verwendet, beispielsweise radioaktive Quellen, elektronisches, thermisches Rauschen in Widerständen oder zufällige Ereignisse in der Umgebung (z. B. Zeitintervalle zwischen Tastendrucken auf einer Tastatur).

[0020] Erst in jüngster Zeit werden in kommerziellen ICs Zufallszahlengeneratoren eingebettet. Hier spielen nun die Art der Zufallsquelle, deren Oberflächengröße auf dem IC, die technische Realisierung und Miniaturisierung eine wichtige Rolle. Allerdings wird bis heute die Immunität der Zufallszahlengeneratoren gegen Seitenkanalangriffe kaum beachtet. Beispiele für realisierte eingebettete Zufallszahlengeneratoren finden sich in DE 101 17 362 A1; Cryptography Research, Inc. "Evaluation of the VIA C3 Nehemiah Random Number Generator", URL http://www.cryptography.com/resources/whitepapers/VIA_rng.pdf; Cryptography Research, Inc. "The Intel Random Number Generator" URL http://www.cryptography.com/resources/whitepapers/ IntelRNG.pdf; US 2002/0186 086 A1; US 4,855,690; DE 101 03 071 A1; Fischer, Viktor; Drutarovsky, Milos: "True Random Number Generator Embedded in Reconfigurable Hardware", in: Jr., Burton S.K. (Hrsg.); Kaya Koc, Cetin (Hrsg.); Paar, Christof (Hrsg.): "Cryptographic Hardware and Embedded Systems - CHES 2002", 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers. BD. 2523. Springer, 2003 (Lecture Notes in

WAVELYNX EX. 1003, Pg. 1140
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Computer Science). - ISBN 3-540-00409-2, S. 415-430,US 5,706,218; WO 03/081417, DE 102 13 269 A1; US 2003/ 0185392 A1; EP 1 343 073 A2; Tkacik, Thomas E.: "A Hardware Random Number Generator", in: Jr., Burton S.K. (Hrsg.); Kaya Koc, Cetin (Hrsg.); Paar, Christof (Hrsg.): "Cryptographic Hardware and Embedded Systems - CHES 2002", 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers. BD. 2523. Springer, 2003 (Lecture Notes in Computer Science), - ISBN 3-540-00409-2, S. 450-453.

[0021] Die Erfindung geht von einem sogenannten Inverterketten-Zufallszahlengenerator aus, wie er gemäß dem Stand der Technik in unterschiedlichster Ausführung beschrieben ist. Beispielhaft wird auf die DE 102 13 269 A1 verwiesen.

[0022] Grundbaustein dieser Zufallszahlengeneratoren ist ein so genannter Ringoszillator 8. Er besteht aus der seriellen Verbindung von einer ungeraden Anzahl K von Invertern inv_1, inv_2, ...inv_K (logischen NOT-Gattern), wobei der Ausgang des letzten Inverters inv_K mit dem Eingang des ersten Inverters inv_1 verbunden ist (siehe Fig. 15a). Durch die Verzögerungszeiten der einzelnen Inverter inv_1, inv_2, .. inv_K kommt es nur bei einer ungeraden Anzahl K von Gattern inv_1, inv_2, ...inv_K zu einer periodischen Schwingung.

[0023] Um diese Schwingung zu starten bzw. zu stoppen, kann der erste Inverter inv_1 durch ein NAND-Gatter $nand_1$ mit Steuereingang start/stop ersetzt werden (siehe Fig. 15b). Wird dieser Steuereingang start/stop auf logisch Eins ("1") gesetzt, beginnt der Ringoszillator 9 zu schwingen.

[0024] Fig. 16a zeigt einen Ringoszillator 10 für K=3 mit zwei Invertern inv_2, inv_3 und einem NAND-Gatter $nand_1$. Fig. 16b zeigt einen idealisierten Signalverlauf am Eingang 11 und Ausgang 12 eines Inverters inv, dessen Verzögerungszeit τ beträgt. Nimmt man an, das die Gatter $nand_1$, inv_2, inv_3 im Ringoszillator 10 nach Fig. 16a ein derartig idealisiertes Verhalten aufweisen, so zeigt Fig. 16c den idealisierten Signalverlauf des Ringoszillators 10 gemäß der Figur 16a an den Punkten S, B, C und A=A', nachdem der Eingang S für eine Laufzeit T auf "1" gesetzt wurde.

[0025] Für eine technische Realisierung des Ringoszillators 10 mit K=3 mit dem CMOS-Baustein 74HCT04 (ohne Eingangs-NAND-Gatter, Fig. 17a), ist ein mit einem Oszilloskop aufgenommener Signalverlauf 14 am Punkt A' in Fig. 17b darstellt. Wie sich aus der Ausschnittsvergrößerung des Signalverlaufs 14 (in Fig. 17b) ergibt, wird durch thermische Bewegung der Elektronen in den Leitungen des Schaltkreises 74HCT04 ein thermisches Rauschsignal aufaddiert. Fig. 17c zeigt die Hüllkurve 15 des verrauschten Schwingungssignals 14 beobachtet über ein längeres Zeitintervall t. Wie zu bemerken ist, führt das Rauschen in den Flanken des Signals 14 zu einer früheren oder späteren Überschreitung des Entscheidungspegels relativ zum rauschfreien Signal. Diese zeitlich zufällige Verschiebung der Flanken wird als Jitter bezeichnet. Die Differenz zwischen den maximal möglichen Flankenverschiebungen, beobachtet bezüglich eines fixen Zeitpunktes t_1 (Fig. 17c), ist mit dem Bezugszeichen Δ bezeichnet. Der Betrag dieser Differenz Δ nimmt zu, je weiter die Flanke von dem Bezugszeitpunkt t_1 entfernt ist. Dieses Phänomen ist als Jitter-Akkumulation bekannt.

[0026] In Fig. 18 ist ein Schwingungssignal 14 des Ringoszillators 10 aus Fig. 17a, mit einer Frequenz f von ca. 25 MHz, 512 mal über die Dauer von 0,2 s gemittelt, dargestellt. Die Einhüllende 13 dieses gemittelten Signals zeigt den Verlauf der Autokorrelation für verschiedene zeitliche Abstände vom Triggerpunkt an. Wie man aus Fig. 18 sehen kann, wird das Signal 14 erst nach ca. 0,28 s durch akkumulierten Jitter vollständig dekorreliert. Dies bedeutet, dass die erzeugten Bits erst bei einer Abtastungsrate ν von 3 Hz (oder kleiner) dekorreliert wären und somit für eine Zufallsbitquelle genutzt werden könnten. Um die maximal mögliche Rate ν_{max} der erzeugten Zufallsbits zu erhöhen, kann man mehrere Ringoszillatoren mit verschiedenen Perioden (d.h. mit verschiedenen Werten für K) kombinieren. Figur 19 zeigt zwei Ausführungsbeispiele für Schaltungsanordnungen basierend auf einer Anzahl L von Ringoszillatoren 17, 18, 19, 20, 21, 22. Hierbei wird jeweils eine Paritätsprüfung (sogenanntes XORing) der Ausgänge durchgeführt. Konkret bedeutet dies, dass die Ausgänge der jeweiligen Ringoszilatoren 17, 18, 19, 20, 21, 22 mit den Eingängen eines XOR-Gatters xor verbunden werden, so dass an dessen Ausgang genau dann ein "1"-Signal erzeugt wird, wenn an den Ausgängen der Ringoszilatoren 17, 18, 19, 20, 21, 22 eine ungerade Anzahl von logischen "1" anliegt. Eine gerade Anzahl von logischen "1" wird am Ausgang des XOR-Gatters xor ein "0"-Signal erzeugen. Deshalb wird das Signal am Ausgang des XOR-Gatters xor nachfolgend als Paritätssignal PS bezeichnet.

[0027] Die beiden Schaltungen gemäß den Figuren 19a bzw. 19b unterscheiden sich lediglich in der Beschaffung der start/stop-Eingänge der Ringoszillatoren 17, 18, 19, 20, 21, 22. Bei der ersten Ausführungsvariante gemäß der Fig. 19a werden die start/stop-Eingänge der einzelnen Ringoszillatoren 17, 18, 19 gemeinsam angesteuert. Die zweite in Fig. 19b dargestellte Möglichkeit besteht darin, die Eingänge separat anzusteuern, um damit die Anfangsphasen der einzelnen Schwingungssignale gegeneinander zu verschieben.

[0028] In Fig. 20a ist eine Schaltung mit Paritätsprüfung von zwei Ringoszillatoren 24, 25 mit gemeinsamem start/stop Signal dargestellt. Wie in Fig. 20b und 20c zu sehen ist, bleibt die Periode P des Paritätssignals PS, 29 konstant. Durch langsame Phasenverschiebungen der einzelnen Ringoszillator-Signale 27, 28 ändert sich der Signalverlauf 29 des Paritätssignals PS, innerhalb einer Periode P über größere Zeitabstände, was in Fig. 21a deutlich zu sehen ist. Die Einhüllende 30 des Paritätssignals PS, 29 über einen Zeitraum von ca. 0,2.s in Fig. 21b zeigt eine variablere Autokorrelation, die kleiner ist, als die Autokorrelation der einzelnen Komponenten (siehe Fig. 18). Diese Paritätsprüfung von Ringoszillato-

WAVELYNX EX. 1003, Pg. 1141
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ren wird in vielen Realisierungen von Zufallszahlengeneratoren benutzt. Mit dieser Technik kann man die Korrelationen nicht komplett entfernen und daher wird eine zusätzliche, die Rate herabsetzende, deterministische Nachbearbeitung unvermeidbar.

[0029] Die Aufgabe der Erfindung besteht nunmehr darin, einen Zufallszahlengenerator der gattungsgemäßen Art sowie ein Verfahren zur Erzeugung einer Zufallszahlenfolge, wie es aus dem Stand der Technik bekannt ist, derart auszuführen bzw. weiterzubilden, dass eine deterministische Nachbearbeitung nicht mehr notwendig ist.

[0030] Diese Aufgabe wird durch einen Zufallszahlengenerator mit den Merkmalen des Patentanspruchs 14 sowie durch ein Verfahren mit den Merkmalen des Patentanspruchs 1 gelöst.

[0031] Vorteilhafte Ausführungen und Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben.

[0032] Die Erfindung geht von einem Verfahren zur Erzeugung von Zufallszahlen aus, bei dem von wenigstens zwei Ringoszillatoren oszillierende digitale Ausgangssignale gleicher oder unterschiedlicher Periodizität erzeugt werden und bei dem ein einen logischen Zustand, nämlich logisch "0" oder "1", darstellendes externes Paritätssignal erzeugt wird, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der Äusgangssignale den logischen Zustand "1" hat, und ansonsten den logischen Zustand "0" einnimmt. Erfindungsgemäß ist vorgesehen, dass das externe Paritätssignal auf jeweils einen externen Paritätseingang der jeweiligen Ringoszillatoren rückgekoppelt wird. Wie aus dem Stand der Technik bekannt ist kann das externe Paritätssignal zur Erzeugung von Zufallsbits verwendet werden, indem es abgetastet wird. Aufgrund der Rückkopplung des Paritätssignals auf den (externen Paritäts-) Eingang des jeweiligen Ringoszillators wird die Autokorrelation des Paritätssignals gegenüber dem aus dem Stand der Technik bekannten Verfahren ohne Rückkopplung signifikant reduziert. Daher kann mit dem erfindungsgemäßen Verfahren die Rate der erzeugten Zufallsbits deutlich erhöht werden.

[0033] Ein Zufallszahlengenerator gemäß der Erfindung umfasst in entsprechender Weise wenigstens zwei vorzugsweise aus unabhängig freischwingenden rückgekoppelten Inverterketten mit einer ungeraden Anzahl an hintereinandergeschalteten Invertern aufgebaute Ringoszillatoren, welche die vorstehend genannten oszillierenden digitalen Ausgangssignale gleicher oder unterschiedlicher Periodizität erzeugen, sowie erste, vorzugsweise durch ein Exklusiv-ODER-Gatter gebildete, Paritätssignalerzeugungsmittel, welche das vorerwähnte externe Paritätssignal erzeugen. Erfindungsgemäß sind beispielsweise durch Exklusiv-ODER-Gatter gebildete Rückkoppelmittel vorgesehen, welche dieses externe Paritätssignal auf den jeweils einen externen Paritätseingang der jeweiligen (aus Inverterketten gebildeten) Ringoszillatoren zurückkoppeln.

[0034] Erfindungsgemäß ist in einer bevorzugten Ausführungsvariante vorgesehen, dass zu jedem Ringoszillator jeweils ein einen vorgegebenen logischen Zustand (z.B. "1") darstellendes internes Paritätssignal erzeugt wird, wenn entweder das Ausgangssignal des jeweiligen Ringoszillators oder das auf den externen Paritätseingang des jeweiligen Ringoszillators rückgekoppelte Signal einen vorgegebenen logischen Zustand (z.B. "1") einnimmt. Diese internen Paritätssignale können wiederum durch weitere Paritätssignalbildung der vorstehend beschriebenen Art in ein weiteres Paritätssignal überführt werden, welches in vorstehend beschriebener Weise zur Erzeugung von Zufallsbits verwendet werden kann, indem es abgetastet wird. Durch diese weitere Paritätsbildung ergibt sich ein Signal, dessen Autokorrelation gegenüber dem externen Paritätssignal noch einmal signifikant reduziert ist. Damit einhergehend kann auf diese Weise die mögliche Abtastrate zur Erzeugung der Zufallsbits noch einmal deutlich erhöht werden.

[0035] Der erfindungsgemäße Zufallszahlengenerator umfasst demgemäss zur Erzeugung der inneren Paritätssignale entsprechende Paritätssignalerzeugungsmittel. Diese umfassen vorzugsweise Exklusiv-ODER-Gatter mit jeweils einem externen Paritätseingang und einem Ausgangssignal-Eingang. An dem externen Paritätseingang liegt ein vom externen Paritätssignal abgeleitetes Signal, z.B. das Paritätssignal selbst oder ein Signal, dessen Erzeugung nachfolgend im Detail beschrieben wird, an. An dem Ausgangssignal-Eingang liegt das jeweilige Ausgangssignal des jeweiligen Ringoszillators an. Zur Erzeugung des weiteren Paritätssignals umfasst der erfindungsgemäße Zufallszahlengenerator weitere Paritätssignalerzeugungsmittel, welche das einen logischen Zustand "0" oder "1" darstellende weitere Paritätssignal erzeugen, wenn eine ungerade Anzahl der internen Paritätssignale einen vorgegebenen logischen Zustand (z.B. "1") einnimmt. Auch diese Mittel umfassen in entsprechender Art und Weise vorzugsweise ein Exklusiv-ODER-Gatter (XOR-Gatter) an dessen Eingängen die internen Paritätssignale anliegen.

[0036] Wie vorstehend bereits erwähnt wurde, kann insbesondere bei aus Inverterketten gebildeten Ringoszillatoren ein Startproblem auftreten. Um dieses Problem zu vermeiden sind erfindungsgemäß bei dem Zufallszahlengenerator gemäß der Erfindung Startmittel vorgesehen, welche ein Startsignal (z.B. eine logische "1") erzeugen und einem start/stop-Eingang wenigstens eines der Ringoszillatoren zuführen, so dass dieser zur Oszillation angeregt wird. Hierzu weist dieser beispielsweise anstelle eines eingangsseitigen Inverters ein NAND-Gatter mit zwei Eingängen auf. Der eine Eingang und der Ausgang dieses NAND-Gatters sind anstelle des Eingangs und des Ausgangs des herausgenommenen Inverters mit der verbleibenden Inverterkette verschaltet. Der andere Eingang bildet den vorerwähnten start/stop-Eingang zum Zuführen des Startsignals.

[0037] Es können grundsätzlich sämtliche Ringoszillatoren separat über entsprechende start/stop-Eingänge

WAVELYNX EX. 1003, Pg. 1142
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

gestartet werden. Es hat sich jedoch in vielen Fällen als günstig erwiesen, wenn alle Ringoszillatoren, vorzugsweise gleichzeitig, mit Hilfe desselben Startsignals (z.B. logisch "1") zur Oszillation angeregt werden. Zu diesem Zweck sind beispielsweise alle Ringoszillatoren anstelle eines eingangsseitigen Inverters jeweils mit einem NAND-Gatter versehen, deren start/stop-Eingänge zum Zuführen des Startsignals (z.B. einer logischen "1") miteinander verbunden sind.

[0038] Je nach Konstellation kann auch jetzt noch ein Startproblem auftreten. Dieses Startproblem lässt sich dadurch beseitigen, dass wenigstens einem externen Paritätseingang ein Inverter vorgeschaltet ist, dem das externe Paritätssignal zugeführt wird. Zum einen tritt durch diesen Inverter eine Verzögerung des Signals an diesem externen Paritätseingang und zum anderen tritt eine Polaritätsumkehr des Signals an diesem externen Paritätseingang mit vorgeschaltetem Inverter ein. Letzteres führt zu einer Polaritätsumkehr am Eingang des entsprechenden Ringoszillators und damit zu einem Ingangsetzen der Oszillation in diesem Ringoszillator. In der Folge werden auch die anderen angeschlossenen Ringoszillatoren zur Schwingung angeregt.

[0039] In bestimmten Anwendungsfällen hat es sich als vorteilhaft herausgestellt, wenn allen externen Paritätseingängen Inverterketten mit einer unterschiedlichen Anzahl an Invertern vorgeschaltet sind, denen das externe Paritätssignal zugeführt wird. Eine Schwingung der Schaltungsanordnung kommt dann zustande, wenn die Summe der ein ungeradzahliges Vielfaches einer Verzögerungszeit eines Gatters (Inventer, NAND-Gatter, XOR-Gatter) betragenden Periodizität eines der von einem ersten der Ringoszillatoren erzeugten Ausgangssignals und der ein Vielfaches der Verzögerungszeit betragenden Verzögerungszeitdauer des externen Paritätssignals an dem externen Paritätseingang des ersten der Ringoszillatoren ein ungeradzahliges Vielfaches der Verzögerungszeit ist und wenn die Summe der ein ungeradzahliges Vielfaches der Verzögerungszeit betragenden Periodizität eines der von einem zweiten der Ringoszillatoren erzeugten Ausgangssignals und der ein Vielfaches der Verzögerungszeit betragenden Verzögerungszeitdauer des externen Paritätssignals an dem externen Paritätseingang des zweiten der Ringoszillatoren ein geradzahliges Vielfaches der Verzögerungszeit ist.

[0040] Wie vorstehend bereits erwähnt wurde können sowohl das externe Paritätssignal als auch das weitere Paritätssignal zur Erzeugung von Zufallsbits verwendet werden. Der Zufallszahlengenerator gemäss der Erfindung kann daher Abtastmittel aufweisen, welche das externe Paritätssignal zur Erzeugung von Zufallsbits mit einer vorgegebenen Rate abtasten und/oder Abtastmittel, welche das weitere Paritätssignal zur Erzeugung von Zufallsbits mit einer vorgegebenen Rate abtasten.

[0041] Die maximale Abtastrate kann weiter erhöht werden, wenn mehrere Zufallszahlengeneratoren der vorstehend beschriebenen Art kombiniert werden. Ausgehend von Zufallszahlengeneratoren, welche externe, insbesondere abgetastete, Paritätssignale erzeugen und/oder welche weitere, insbesondere abgetastete, Paritätssignale erzeugen lassen sich durch nochmalige bzw. wiederholte Paritätsbildung aus diesen Paritätssignalen (es sind beliebige Variationen von Paritätssignalbildungen möglich) Zufallszahlengeneratoren bilden bei denen das zur Zufallszahlenerzeugung vorgesehene (Super-)Paritätssignal eine nahezu beliebig reduzierte Autokorrelation aufweist.

[0042] Die weitere Zufallszahlengeneration erfordert eine Abtastung. Hierbei spielt es keine Rolle, ob die externen Paritätssignale oder die weiteren Paritätssignale oder sonstige Paritätssignale niederer Ordnung zur Erzeugung von Zufallsbits mit einer vorgegebenen Rate synchron abgetastet werden oder das (Super-) Paritätssignal höchster Ordnung zur Erzeugung von Zufallsbits mit der vorgegebenen Rate abgetastet wird.

[0043] Die Abtastung kann in zeitlich konstanten Abständen erfolgen, erfindungsgemäß ist jedoch auch vorgesehen, eine Abtastung in zufälligen, nicht uniformen Abtastintervallen durchzuführen. Beispielsweise lässt sich eine zufällige Abtastung erreichen, wenn die Abtastung zu einem Zeitpunkt durchgeführt wird, wenn ein von einem der vorstehend beschriebenen Zufallsgeneratoren zufällig erzeugtes Zufallsbit einen vorbestimmten logischen Zustand (z.B. "1") einnimmt.

[0044] Die Abtastung kann beispielsweise mittels eines D-Flip-Flops erfolgen, welches in einem Takt von einem Taktgeber, insbesondere von einem astabilen Multivibrator (bei zeitlich konstanten Abtastintervallen) oder von einem rückgekoppelten Ringoszillatoren der vorstehend beschriebenen Art (bei zeitlich zufälligen Abtastintervallen), angesteuert wird.

[0045] Die Erfindung wird nunmehr anhand der Zeichnungen näher beschrieben. Es zeigen:

Figur 1 Ringoszillatoren mit rückgekoppeltem Paritätssignal.

Figur 2 ein Beispiel des Startproblems bei rückgekoppelten Ringoszillatoren:

a) vor dem Start;
b) nach dem Start.

Figur 3 eine Lösung des Startproblems aus Figur 2;

a) vor dem Start;
b) nach dem Start.

Figur 4 den Signalverlauf des Paritätssignals PS in der Schaltung aus Fig. 3 in einer Zeitspanne von:

a) 10ns;
b) 40ns;
c) 200ns;
d) 400ns;
e) 1000ns;

WAVELYNX EX. 1003, Pg. 1143
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

f) 2000ns.

Figur 5 ein gemitteltes Paritätssignal der Schaltung aus Fig. 3.

Figur 6 ein allgemeines Schaltbild von rückgekoppelten Ringoszillatoren (RRO).

Figur 7 einen Schaltkreis von RRO (4; 1, 3, 4, 5; 3, 2, 1, 0).

Figur 8 interne Paritätssignale des RRO (4; 1, 3, 4, 5; 3, 2, 1, 0) nach der Figur 7 in den Punkten P_1, P_2, P_3 und P_4.

Figur 9 einen Zufallsbitgenerator realisiert mit RROs.

Figur 10 ein Beispiel eines Zufallszahlengenerators mit RRO (4; 1, 3, 4, 5; 3, 2, 1, 0).

Figur 11 einen Zufallszahlengenerator mit einer Anzahl N RROs und abgetastetem Superparitätssignal.

Figur 12 einen Zufallszahlengenerator mit einer Anzahl N abgetasteten RROs und abgetastetem Superparitätssignal.

Figur 13 einen Zufallszahlengenerator mit einer Anzahl N synchronisiert, abgetasteten RROs und abgetastetem Superparitätssignal.

Figur 14 ein Modell eines physikalischen Zufallsgenerators (Stand der Technik).

Figur 15 Ring-Oszillatoren gemäß dem Stand der Technik

a) Inverterketten-Ring Oszillator;
b) Inverterketten-Ring Oszillator mit Steuereingang.

Figur 16 ein Beispiel für die Funktionsweise eines Ring-Oszillators nach dem Stand der Technik

a) einen Ring Oszillator für K=3 (Stand der Technik);
b) eine idealisierte Verzögerung eines Inverters;
c) einen Verlauf eines Schwingsignals.

Figur 17 ein Beispiel für die praktische Realisierung des Ring-Oszillators nach Figur 16

a) Realisierung eines Ring Oszillator für K=3 mit dem Baustein 74HCT04,
b) Verlauf seines Schwingungssignals mit aufaddiertem thermischen Rauschen;
c) Hüllkurve des verrauschten Schwingungssignals.

Figur 18 ein gemitteltes Schwingungssignal des Ringoszillators aus Fig. 17a.

Figur 19 ein Beispiel für die Durchführung einer sogenannten Paritätsprüfung (Stand der Technik)

a) eine Schaltung für die Paritätsprüfung von L Ringoszillatoren mit gemeinsam angesteuertem start/stop-Signal;
b) eine Schaltung für die Paritätsprüfung von L Ringoszillatoren mit getrennt angesteuertem start/Stopp-Signal.

Figur 20 ein Beispiel für die praktische Durchführung der Paritätsprüfung nach der Fig. 19a

a) ein Beispiel für eine Schaltung für Paritätsprüfung von zwei Ringoszillatoren mit gemeinsam angesteuertem start/Stopp-Signal
b) Signale der einzelnen Komponenten und Verlauf des Paritätssignals.
c) Signale der einzelnen Komponenten und Verlauf des Paritätssignals.

Figur 21 ein Beispiel für die praktische Durchführung der Paritätsprüfung nach der Figur 19a

a) Signale der einzelnen Komponenten und Verlauf des Paritätssignals;
b) ein gemitteltes Paritätssignal der Schaltung aus Fig. 20a.

Figur 22 einen RRO mit neutralisiertem Restbias

[0046] Die grundsätzliche Idee der Erfindung besteht, wie vorstehend dargelegt wurde, in der Rückkopplung des Paritätssignals auf die Eingänge der einzelnen Ringoszillatoren.

[0047] Die Fig. 1 zeigt ein erstes Ausführungsbeispiel eines erfindungsgemäßen Zufallsgenerators basierend auf einer Anzahl L von Ringoszillatoren 32, 33, 34, deren Ausgänge entsprechenden Eingängen eines XOR-Gatters xor zugeführt werden, an dem ein Paritätssignal PS gebildet wird.

[0048] Wie Fig. 1 zeigt, wird die Zuführung des rückgekoppelten Paritätssignals PS auf die einzelnen Eingänge der Ringoszillatoren 32, 33, 34 durch eine Anzahl logischer XOR-Gatter xor_1, xor_2, ... xor_L erreicht. Der jeweilige Eingang, an dem das Paritätssignal PS anliegt, soll als externer Paritätseingang 36, 37, 38 bezeichnet werden.

[0049] Wichtig ist zu bemerken, dass nicht für alle Wert-Kombinationen der Parameter L, K_1, ..., K_L eine Schwingung dieser Schaltung zustande kommt, wie das Beispiel in Fig. 2 für L=3, K1=3, K2=5 und K3=7 zeigt und wie nachfolgend im Detail beschrieben wird.

[0050] In Fig. 2a ist der logische Zustand der ausgeschalteten Schaltung dargestellt. Fig. 2b zeigt den Zu-

WAVELYNX EX. 1003, Pg. 1144
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

stand der Schaltung nach dem Einschalten (d.h. nach dem Setzen des Start/Stop-Signals auf logisch "1"). Wie zu bemerken ist, befindet sich die Schaltung immer noch in einem statischen (nicht schwingenden) Zustand, da sich alle Ausgänge der NAND-Gatter $nand_{i,1}$ für i=1, 2, 3 nicht geändert haben. Dieses Startproblem kann durch Einfügen eines weiteren Inverters $inv_{3,-1}$ vor dem externen Paritätseingang 47 des XOR-Gatters behoben werden (siehe Fig. 3).

[0051] Das Paritätssignal PS dieser nun schwingenden Schaltung ist in Fig. 4 für verschiedene Zeitintervalle dargestellt. Es ist eindeutig zu sehen, dass die Rückkopplung für eine geeignete (schwingende) Parameterkombination zu einer sehr unregelmäßigen Form des Paritätssignals PS führt. Das gemittelte Paritätssignal PS zeigt eine sehr geringe und konstante Autokorrelation (siehe Fig. 5). Im Vergleich zu Fig. 21b ist dies eine signifikante Verbesserung, die es erlaubt, die Rate v der erzeugten Zufallsbits deutlich zu erhöhen.

[0052] Um das Startproblem generell zu lösen, und um zusätzliche Jitter-Akkumulation einzuführen, werden vor den XOR-Gattern xor_i i=1, ...,L, Ketten von Invertern $inv_{i,-j}$, i=1...L, j=1, ...M_i eingeführt. Die Länge der einzelnen Ketten M_1,...M_L variiert hierbei. Um sicher zu stellen, dass das Start/Stop-Problem nicht auftritt, müssen die Parameter M_i und K_i speziell gewählt werden. Es muss gelten, dass mindestens ein Paar i, j mit i, j, $\in$ {1, ...L} x {1,..., L} existiert, so dass eine der beiden Summen $M_i + K_i$ und $M_j + K_j$ ungerade und die andere gerade ist.

[0053] Fig. 6 zeigt ein generelles Schaltbild mit rückgekoppeltem Paritätssignal PS. Diese Schaltung soll im Folgenden als rückgekoppelter Ring-Oszillatoren RRO bezeichnet werden. Die Signale an den Ausgängen P_1 bis P_L, der XOR-Gatter xor_1 bis xor_L, prüfen die Parität ihrer Eingangssignale und werden daher als interne Paritätssignale bezeichnet. Zur Unterscheidung soll das Paritätssignal PS am Ausgang des XOR-Gatters XOR als externes Paritätssignal bezeichnet werden.

[0054] Fig. 7 zeigt eine Instanz des RRO mit den Parametern L=4, K_1=1, K_2=3, K_3=4, K_4=5 ; M_1=3, M_2=2, M_3=1, M_4=0. Als Kurzschreibweise wird RRO (4; 1,3,4,5; 3,2,1,0) verwendet. Die inneren Paritätssignale sind durch die Konstruktion des RRO sehr unterschiedlich, wie dies die Fig. 8 zeigt, und können zur Erzeugung von Zufallsbits benutzt werden.

[0055] Durch eine weitere Paritätsprüfung PP der inneren Paritätssignale P_1, P_2,...P_L, bei der ein weiteres Paritätssignal PP erzeugt wird, wird die Qualität weiter verbessert und kann nach Abtastung als Zufallsbitfolge ZB verwendet werden, wie dies in Fig. 9 dargestellt ist. Die Abtastung erfolgt durch ein D-Flip-Flop 85, welches durch ein periodisches Taktsignal C_p angesteuert wird. Das Taktsignal C_p kann von einem astabilen Multivibrator 87 erzeugt werden und seine Periode (uniformes Abtastungsintervall) durch einen binären Zähler 86 bestimmt werden. Um zufällige, nicht uniforme Abtastintervalle zu erhalten, kann der astabile Multivibrator 87 durch einen RRO ersetzt werden. In Fig. 10 ist ein Zufallzahlengenerator mit der RRO-Instanz RRO (4; 1,3,4,5; 3,2,1,0) mit uniformer Abtastung dargestellt. Statistische Tests dieses Zufallszahlengenerators haben eine geringe Ungleichverteilung (Bias) und eine kleine Korrelation der Bits 7 gezeigt.

[0056] Um diese zu beseitigen, wurden mehrere RROs durch eine weitere (Super-)Paritätsprüfung SP gekoppelt. Diese Kopplung kann auf verschiedene Weise durchgeführt werden. In Fig. 11 erfolgt die uniforme Abtastung nach der Paritätsprüfung PP, wohingegen in Fig. 12 die einzelnen RROs vor der (Super)Paritätsprüfung SP abgetastet werden. Da dies asynchron geschieht, muss, um Zufallsbits 7 gleicher Dauer zu erhalten, das Superparitätssignal SP nochmals abgetastet werden. Um dies zu vermeiden kann die Abtastung auch synchron durchgeführt werden, wie in Fig. 13 gezeigt wird.

[0057] Oft zeigt sich in der Praxis ein kleines aber immer noch störendes Bias. Dementsprechend wird eine Zufallsbitfolge erzeugt, die nicht gut genug ist. Auch andere elektronisch realisierte TRNGs besitzen diesen Mangel, der meistens durch die unangepassten Arbeitspunkte der benutzten aktiven Halbleiterkomponenten bedingt ist. Um dieses Restbias zu neutralisieren, werden in bisheriger Praxis verschiedene deterministische Nachbearbeitungen nach der Abtastung (auf digitaler Ebene) durchgeführt, wie z.B. die oft benutzte von Neuman-Methode. Alle diese Algorithmen vermindern die Rate der erzeugten Zufallsbits wesentlich.

[0058] Dennoch, bei rückgekoppelten Ringoszillatoren RRO kann dieses Restbias schon vor der Abtastung neutralisiert werden, wenn an den Ausgängen P_1, P_2, ..., P_L der Ringoszillatoren RRO (siehe Fig. 9) binäre Zähler 88_1, 88_2, ...88_L der Länge Z (hier mit einer Anzahl Z JK-Flip-Flops JK_1, JK_2 ... JK_Z) angeschlossen werden. Die Ausgänge dieser Zähler 88_1, 88_2,... 88_L werden an die Eingänge des XOR-Gatters, welches weitere Paritätssignal PP liefert, angeschlossen (Fig. 22). Durch Zählen der Signalübergänge zwischen beiden Signalzuständen (Hoch und Niedrig mit ungleicher Dauer) erhält man neue (längere) Signalzustände. Diese neuen Signalzustände sind einander dauermäßig ähnlicher, als die Signalzustände des ursprünglichen Signals. Je größer die Anzahl Z ist, desto bessere Ausgleichungen der Signalzustandsdauern kann man erreichen und damit das Restbias auf beliebig kleine Werte unterdrücken. Schon bei Z=1 erreicht man gute Ergebnisse.

Bezugszeichenliste / Abkürzungen

[0059]

1	Zufallsquelle
2	Wertermittlung
3	Zufalls-Bit-Erzeugung
4	algorithmische Nachbearbeitung/Zufallsextraktion
5	Zufalls-Bit-Ausgabe
6	physikalische Umgebung

WAVELYNX EX. 1003, Pg. 1145
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

8	Ringoszillator
9	Ringoszillator mit Steuereingang
10	Ringoszillator
11	Eingangssignal
12	Ausgangssignal
13	Signaleinhüllende
14	Signalverlauf an Leitungspunkt A'
15	Hüllkurve
17	Ringoszillator
18	Ringoszillator
19	Ringoszillator
20	Ringoszillator
21	Ringoszillator
22	Ringoszillator
24	Ringoszillator
25	Ringoszillator
27	erstes Eingangssignal des XOR-Gatters
28	zweites Eingangssignal des XOR-Gatters
29	Paritätssignal
30	Einhüllende des gemittelten Paritätssignals
32	Ringoszillator
33	Ringoszillator
34	Ringoszillator
36	externer Paritätseingang
37	externer Paritätseingang
38	externer Paritätseingang
41	Ringoszillator
42	Ringoszillator
43	Ringoszillator
45	externer Paritätseingang
46	externer Paritätseingang
47	externer Paritätseingang
47°	externer Paritätseingang
71	Ringoszillator
72	Ringoszillator
73	Ringoszillator
81	Ringoszillator
82	Ringoszillator
83	Ringoszillator
84	Ringoszillator
85	D-Flip-Flop
85_1	D-Flip-Flop
... 86	binärer Zähler
86_1	binärer Zähler
... 87	astabiler Multivibrator
87_1	astabiler Multivibrator
... 88_1	binärer Zähler
... A	Leitungspunkt
B	Leitungspunkt
C	Leitungspunkt
A'	Leitungspunkt
DES	Data Encryption Standard
f	Frequenz
inv	Inverter
inv_1	Inverter/NOT-Gatter
inv_2	Inverter/NOT-Gatter
...	
inv_k	Inverter/NOT-Gatter
JK_1	JK-Flip-Flop
JK_2	JK-Flip-Flop
...	
JK_z	JK-Flip-Flop
K	Anzahl der Gatter
K_1	Anzahl der Gatter
K_1	Anzahl der Gatter
K_2	Anzahl der Gatter
K_3	Anzahl der Gatter
...	
K_L	Anzahl der Gatter
L	Anzahl der Ringoszillatoren
M	Anzahl der Gatter
M_1	Anzahl der Gatter
M_2	Anzahl der Gatter
M_3	Anzahl der Gatter
M_4	Anzahl der Gatter
...	
M_L	Anzahl der Gatter
N	Anzahl der Ringoszillatoren
$nand_1$	NAND-Gatter
$nand_2$	
...	
P	Periode
P_1	internes Paritätssignal
P_2	internes Paritätssignal
...	
P_L	internes Paritätssignal
PRNG	deterministischer Zufallsgenerator

WAVELYNX EX. 1003, Pg. 1146
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PS	externes Paritätssignal
RRO	rückgekoppelte Ringoszillatoren
S	Leitungspunkt
SP	Superparitätssignal
Start/Stop	Steuereingang
t	Zeit
t_1	Zeitpunkt
T	Laufzeit
TRNG	physikalischer Zufallsgenerator
U	Spannung
U_e	Eingangsspannung
U_a	Ausgangsspannung
xor	Exklusiv ODER -/XOR-Gatter mit logisch "1" am Ausgang, wenn ungerade Anzahl der Eingänge auf logisch "1"
xor_1	Exklusiv ODER -/XOR-Gatter mit logisch "1" am Ausgang, wenn ungerade Anzahl der Eingänge auf logisch "1"
xor_2	Exklusiv ODER -/XOR-Gatter mit logisch "1" am Ausgang, wenn ungerade Anzahl der Eingänge auf logisch "1"
Z	Anzahl
ZB	Zufallsbit
Δ	Differenz
ν	Abtastrate
ν_{max}	maximale Abtastrate
τ	Verzögerungszeit

Patentansprüche

1. Verfahren zur Erzeugung von Zufallszahlen bei dem von wenigstens zwei Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) oszillierende digitale Ausgangssignale (A1, A2, ..., AL) gleicher oder unterschiedlicher Periodizität erzeugt werden, wobei ein einen logischen Zustand ("0", "1"), darstellendes externes Paritätssignal (PS) erzeugt wird, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl von Ausgangssignalen (A1, A2, ..., AL) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt,
dadurch gekennzeichnet, dass
das externe Paritätssignal (PS) auf jeweils einen externen Paritätseingang (36, 37, 38, 45, 46, 47) der jeweiligen Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) rückgekoppelt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
zu jedem Ringoszillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) jeweils ein einen vorbestimmten logischen Zustand ("0", "1") darstellendes internes Paritätssignal (P_1, P_2, P_3, P_4 ... P_L) erzeugt wird, wenn entweder' das Ausgangssignal (A_1, A_2 .... A_L) des jeweiligen Ringoszillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) oder das auf den externen Paritätseingang (36, 37, 38, 45, 46, 47) des jeweiligen Ringoszillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) rückgekoppelte Signal einen vorgegebenen logischen Zustand ("1") einnimmt.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, dass
ein einen logischen Zustand ("0", "1") darstellendes weiteres Paritätssignal (PP) erzeugt wird, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der internen Paritätssignale (P_1, P_2, P_3, P_4 ... P_L) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt.

4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet, dass
Signalübergänge der internen Paritätssignale (P_1, P_2, P_3, P_4 ... P_z) vor der Paritätssignalerzeugung gezählt werden

5. Verfahren nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet, dass
wenigstens einer der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) mit Hilfe eines einem entsprechenden Eingang (Start/Stop) des entsprechenden Ringoszillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) zugeführten Startsignals ("1") zur Oszillation angeregt wird.

6. Verfahren nach Anspruch 5,
dadurch gekennzeichnet, dass
alle Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), vorzugsweise gleichzeitig, mit Hilfe desselben Startsignals ("1") zur Oszillation angeregt werden.

7. Verfahren nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet, dass
das externe Paritätssignal (PS) vor dessen Rückkopplung auf wenigstens einen der externen Paritätseingänge (47) invertiert wird.

8. Verfahren nach einem der vorangegangenen An-

WAVELYNX EX. 1003, Pg. 1147
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

sprüche,
dadurch gekennzeichnet, dass
das externe Paritätssignal (PS) vor dessen Rückkopplung auf wenigstens einen der externen Paritätseingänge (47) verzögert wird.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass
das externe Paritätssignal (PS) vor dessen Rückkopplung auf unterschiedliche externe Paritätseingänge (36, 37, 38, 45, 46, 47) um unterschiedliche Zeitdauern (τ) verzögert wird.

10. Verfahren nach Anspruch 9,
dadurch gekennzeichnet, dass die Periodizitäten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) und die Verzögerungszeitdauern des externen Paritätssignals (PS) an den externen Paritätseingängen (36, 37, 38, 45, 46, 47) der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) derart gewählt werden, dass die Summe der ein ungeradzahliges Vielfaches (K_1, K_2, K_3, ... K_L) einer Verzögerungszeit eines Gatters betragenden Periodizität eines der von einem ersten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) erzeugten Ausgangssignals (A_1, A_2 .... A_L) und der ein Vielfaches (M_1, M_2, M_3, ... M_L) der Verzögerungszeit eines Gatters betragenden Verzögerungszeitdauer des externen Paritätssignals (PS) an dem externen Paritätseingang (36, 37, 38, 45, 46, 47) des ersten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) ein ungeradzahliges Vielfaches der Verzögerungszeit eines Gatters ist und dass die Summe der ein ungeradzahliges Vielfaches (K_1, K_2, K_3, ... K_L) der Verzögerungszeit eines Gatters betragenden Periodizität eines der von einem zweiten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) erzeugten Ausgangssignals (A_1, A_2 .... A_L) und der ein Vielfaches (M_1, M_2, M_3, ... M_L) der Verzögerungszeit eines Gatters betragenden Verzögerungszeitdauer des externen Paritätssignals (PS) an dem externen Paritätseingang (36, 37, 38, 45, 46, 47) des zweiten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) ein geradzahliges Vielfaches der Verzögerungszeit eines Gatters ist.

11. Verfahren nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet, dass
das externe Paritätssignal (PS) zur Erzeugung von Zufallsbits (78) mit einer vorgegebenen Rate (v) abgetastet wird oder dass das weitere Paritätssignal (PP) zur Erzeugung von Zufallsbits (78) mit einer vorgegebenen Rate (v) abgetastet wird.

12. Verfahren nach einem der vorangegangenen Ansprüche,
dadurch gekennzeichnet, dass
mehrere externe, insbesondere abgetastete, Paritätssignale (PS) erzeugt werden und dass ein einen logischen Zustand ("0", "1") darstellendes Superparitätssignal (SP) erzeugt wird, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der externen, insbesondere abgetasteten, Paritätssignale (PS) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt oder dass mehrere weitere, insbesondere abgetastete, Paritätssignale erzeugt werden und dass ein einen logischen Zustand ("0", "1") darstellendes Superparitätssignal (SP) erzeugt wird, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der weiteren, insbesondere abgetasteten, Paritätssignale den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt.

13. Verfahren nach Anspruch 12,
dadurch gekennzeichnet, dass
die externen oder die weiteren Paritätssignale (PS) zur Erzeugung von Zufallsbits (ZB) mit einer vorgegebenen Rate (v) synchron abgetastet werden oder dass das Superparitätssignal (SP) zur Erzeugung von Zufallsbits (ZB) mit einer vorgegebenen Rate (v) abgetastet wird.

14. Verfahren nach einem der Ansprüche 11 bis 13,
dadurch gekennzeichnet, dass
die Abtastung in zufälligen, nicht uniformen Abtastintervallen durchgeführt wird, insbesondere dass die Abtastung dann durchgeführt wird, wenn ein nach einem der Verfahren nach den Ansprüchen 1 bis 12 zufällig erzeugtes Zufallsbit (ZB) einen vorbestimmten logischen Zustand ("1") einnimmt.

15. Zufallszahlengenerator mit wenigstens zwei Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), insbesondere aus unabhängig freischwingenden rückgekoppelten Inverterketten mit einer ungeraden Anzahl (K) an hintereinandergeschalteten Invertern ($inv_{1,2}$, $inv_{2,1}$, $inv_{3,1}$, ... $inv_{i,j}$, ... $inv_{L,KL}$), welche oszillierende digitale Ausgangssignale (A_1, A_2, ... A_L) unterschiedlicher Periodizität erzeugen, und mit ersten Paritätssignalerzeugungsmitteln (XOR), welche ein einen vorbestimmten logischen Zustand ("0", "1") darstellendes externes Paritätssignal (PS) erzeugen, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der Ausgangssignale (A_1, A_2 .... A_L) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt,
dadurch gekennzeichnet, dass
Rückkoppelmittel (xor_1, xor_2, xor_3, xor_4 ... xor_L) vorgesehen sind, welche das externe Paritätssignal (PS) auf jeweils einen externen Paritätseingang (36, 37, 38, 45, 46, 47) der jeweiligen Ringoszillatoren

WAVELYNX EX. 1003, Pg. 1148
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) rückkoppeln.

16. Zufallszahlengenerator nach Anspruch 15,
dadurch gekennzeichnet, dass
die ersten Paritätssignalerzeugungsmittel ein XOR-Gatter (XOR) umfassen, an dessen Eingängen die Ausgangssignale (A_1, A_2, ... A_L) anliegen.

17. Zufallszahlengenerator nach einem der Ansprüche 15 oder 16,
dadurch gekennzeichnet, dass
zweite Paritätssignalerzeugungsmittel (xor_1, xor_2, xor_3, ... xor_L) vorgesehen sind, welche zu jedem Ringoszillator (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) jeweils ein einen vorgegebenen logischen Zustand ("1") darstellendes internes Paritätssignal (P_1, P_2, P_3, P_4 ... P_L) erzeugen, welches genau dann den logischen Zustand "1" einnimmt, wenn entweder das Ausgangssignal (A_1, A_2 .... A_L) des jeweiligen Ringoszillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) oder das auf den externen Paritätseingang (36, 37, 38, 45, 46, 47) des jeweiligen Ringoszillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) rückgekoppelte Signal einen vorgegebenen logischen Zustand ("1") einnimmt.

18. Zufallszahlengenerator nach Anspruch 17,
dadurch gekennzeichnet, dass
die zweiten Paritätssignalerzeugungsmittel XOR-Gatter (xor_1, xor_2, xor_3, ... xor_L) mit jeweils einem externen Paritätseingang und einem Ausgangssignal-Eingang umfassen, wobei an dem Paritätseingang ein vom externen Paritätssignal (PS) abgeleitetes Signal und an dem Ausgangssignal-Eingang das jeweilige Ausgangssignal (A_1, A_2 .... A_L) des jeweiligen Ringoszillators (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) anliegt.

19. Zufallszahlengenerator nach Anspruch 18,
dadurch gekennzeichnet, dass
dritte Paritätssignalerzeugungsmittel vorgesehen sind, welche ein einen logischen Zustand ("0", "1") darstellendes weiteres Paritätssignal (WP) erzeugen, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der internen Paritätssignale (P_1, P_2, P_3, P_4 ... P_L) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt.

20. Zufallszahlengenerator nach Anspruch 19,
dadurch gekennzeichnet, dass
Zählmittel (88_1, 88_2, ...88_L) vorgesehen sind, welche Signalübergänge der internen Paritätssignale (P_1, P_2, P_3, ... P_L) vor der Paritätssignalerzeugung zählen.

21. Zufallszahlengenerator nach Anspruch 20,
dadurch gekennzeichnet, dass
die Zählmittel einen Binärzähler (881, 882, ... 88L), insbesondere eine Kette mit Flip-Flops, vorzugsweise JK-Flip-Flops (JK_1, JK_2, ...JK_Z) umfassen.

22. Zufallszahlengenerator nach einem der Ansprüche 15 bis 21,
dadurch gekennzeichnet, dass
Startmittel vorgesehen sind, welche ein Startsignal ("1") erzeugen und einem Eingang (start/stop) von wenigstens einem der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) zuführen, so dass dieser zur Oszillation angeregt wird.

23. Zufallszahlengenerator nach Anspruch 22,
dadurch gekennzeichnet, dass
der wenigstens eine der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) anstelle eines eingangsseitigen Inverters (inv_1) ein NAND-Gatter ($nand_1$, $nand_{1,1}$, $nand_{2,1}$, $nand_{3,1}$, ... $nand_{i,1}$, ... $nand_{L,1}$) mit dem Eingang (start/stop) zum Zuführen des Startsignals ("1") umfasst.

24. Zufallszahlengenerator nach einem der Ansprüche 22 oder 23,
dadurch gekennzeichnet, dass
die Startmittel derart ausgebildet sind, dass alle Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84), vorzugsweise gleichzeitig, mit Hilfe desselben Startsignals ("1") zur Oszillation angeregt werden.

25. Zufallszahlengenerator nach Anspruch 24,
dadurch gekennzeichnet, dass
alle Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) anstelle eines eingangsseitigen Inverters (inv_1) jeweils ein NAND-Gatter ($nand_1$, $nand_{1,1}$, $nand_{2,1}$, $nand_{3,1}$, ... $nand_{i,1}$, ... $nand_{L,1}$) mit jeweils einem Eingang (start/stop) umfassen, welche zum Zuführen des Startsignals ("1") miteinander verbunden sind.

26. Zufallszahlengenerator nach einem der Ansprüche 15 bis 25,
dadurch gekennzeichnet, dass
wenigstens einem externen Paritätseingang (47) ein Inverter ($inv_{3,-1}$, $inv_{1,-M1}$ .... $inv_{1,-1}$, ... $inv_{L,-ML}$, ... $inv_{L,-1}$) vorgeschaltet ist, dem das externe Paritätssignal (PS) zugeführt wird.

27. Zufallszahlengenerator nach Anspruch 26,
dadurch gekennzeichnet, dass
allen externen Paritätseingängen Inverterketten mit einer unterschiedlichen Anzahl (M_1, M_2,... M_L) an Invertern ($inv_{1,-M1}$... $inv_{1,-1}$, ... $inv_{L,-ML}$, $inv_{L,-1}$) vorgeschaltet sind, denen das externe Paritätssignal (PS) zugeführt wird.

WAVELYNX EX. 1003, Pg. 1149
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

28. Zufallszahlengenerator nach Anspruch 27, **dadurch gekennzeichnet, dass** die Summe der ein ungeradzahliges Vielfaches (K_1, K_2, K_3, ... K_L) einer Verzögerungszeit eines Gatters betragenden Periodizität eines der von einem ersten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) erzeugten Ausgangssignals (A_1, A_2 .... A_L) und der ein Vielfaches (M_1, M_2, M_3, ... M_L) der Verzögerungszeit eines Gatters betragenden Verzögerungszeitdauer des externen Paritätssignals (PS) an dem externen Paritätseingang (36, 37, 38, 45, 46, 47) des ersten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) ein ungeradzahliges Vielfaches der Verzögerungszeit eines Gatters ist und dass die Summe der ein ungeradzahliges Vielfaches (K_1, K_2, K_3, ... K_L) der Verzögerungszeit eines Gatters betragenden Periodizität eines der von einem zweiten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) erzeugten Ausgangssignals (A_1, A_2 .... A_L) und der ein Vielfaches (M_1, M_2, M_3, ... M_L) der Verzögerungszeit eines Gatters betragenden Verzögerungszeitdauer des externen Paritätssignals (PS) an dem externen Paritätseingang (36, 37, 38, 45, 46, 47) des zweiten der Ringoszillatoren (32, 33, 34, 41, 42, 43, 71, 72, 73, 81, 82, 83, 84) ein geradzahliges Vielfaches der Verzögerungszeit eines Gatters ist.

29. Zufallszahlengenerator nach einem der Ansprüche 15 bis 28,
dadurch gekennzeichnet, dass
Abtastmittel vorgesehen sind, welche das externe Paritätssignal (PS) zur Erzeugung von Zufallsbits (ZB) mit einer vorgegebenen Rate (ν) abtasten und/oder dass
Abtastmittel vorgesehen sind, welche das weitere Paritätssignal (PP) zur Erzeugung von Zufallsbits (ZB) mit einer vorgegebenen Rate (ν) abtasten.

30. Zufallszahlengenerator nach einem der Ansprüche 15 bis 29,
dadurch gekennzeichnet, dass
mehrere Zufallszahlengeneratoren nach einem der Ansprüche 15 bis 29 vorgesehen sind, welche externe, insbesondere abgetastete, Paritätssignale (PS) erzeugen und dass Superparitätssignalerzeugungsmittel vorgesehen sind, welche ein einen logischen Zustand ("0", "1") darstellendes Superparitätssignal (SP) erzeugen, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der externen, insbesondere abgetasteten, Paritätssignale (PS) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt und/oder dass mehrere Zufallszahlengeneratoren nach einem der Ansprüche 15 bis 29 vorgesehen sind, welche weitere, insbesondere abgetastete, Paritätssignale (PP) erzeugen und dass Superparitätssignalerzeugungsmittel vorgesehen sind, welche ein einen logischen Zustand ("0", "1") darstellendes Superparitätssignal (SP) erzeugen, welches genau dann den logischen Zustand "1" einnimmt, wenn eine ungerade Anzahl der weiteren, insbesondere abgetasteten, Paritätssignale (PP) den logischen Zustand "1" aufweist, und welches ansonsten den logischen Zustand "0" einnimmt.

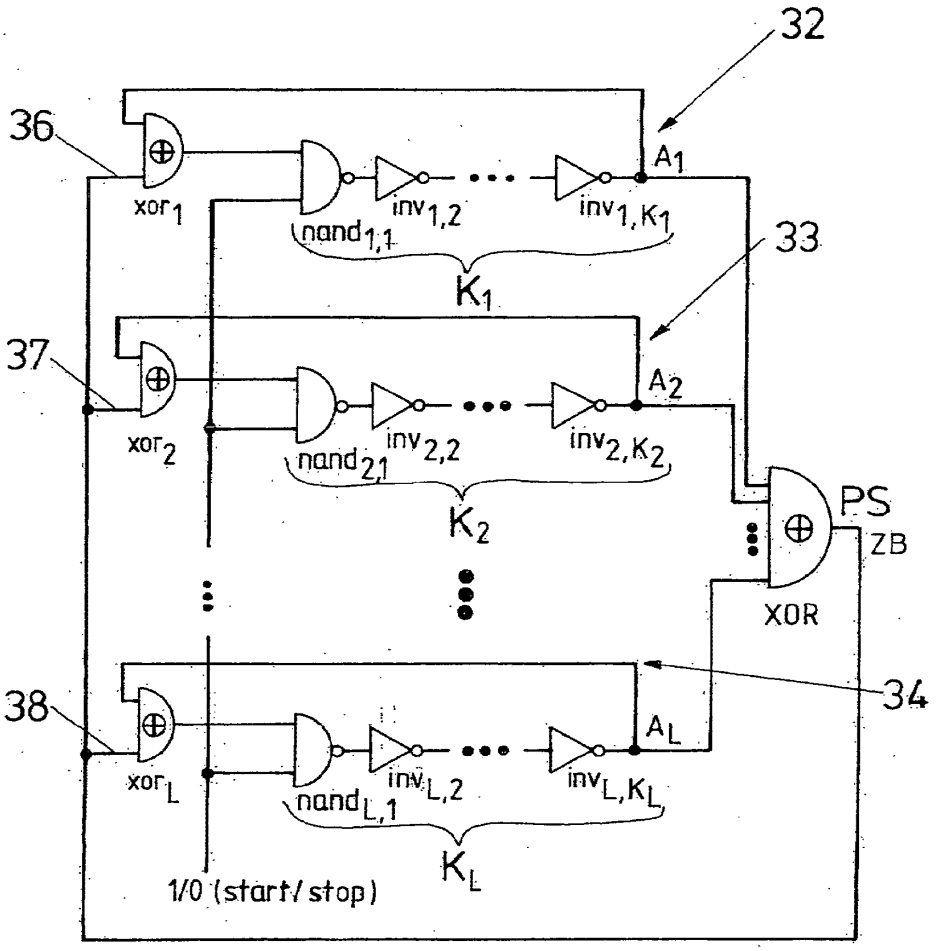
31. Zufallszahlengenerator nach Anspruch 30,
dadurch gekennzeichnet, dass
Abtastmittel vorgesehen sind, welche die externen Paritätssignale (PS) oder die weiteren Paritätssignale (PP) zur Erzeugung von Zufallsbits (ZB) mit einer vorgegebenen Rate (ν) synchron abtasten und/oder dass Abtastmittel vorgesehen sind, welche das Superparitätssignal (SP) zur Erzeugung von Zufallsbits (ZB) mit einer vorgegebenen Rate (ν) abtasten.

32. Zufallszahlengenerator nach einem der Ansprüche 29 bis 31,
dadurch gekennzeichnet, dass die Abtastmittel eingerichtet sind, eine Abtastung in zufälligen, nicht uniformen Abtastintervallen durchzuführen und insbesondere dann eine Abtastung vorzunehmen, wenn ein von einem der Zufallsgeneratoren nach den Ansprüchen 15 bis 31 zufällig erzeugtes Zufallsbit (ZB) einen vorbestimmten logischen Zustand ("1") einnimmt.

33. Zufallszahlengenerator nach einem der Ansprüche 29 bis 32,
dadurch gekennzeichnet, dass
die Abtastmittel ein D-Flip-Flop (88_1, 88_2, ... 88_L) umfassen, welches in einem Takt (C_p) von einem Taktgeber, insbesondere von einem astabilen Multivibrator (87, 87_1, 87_2, ... 87_L) oder von einem rückgekoppelten Ringoszillator (RRO), angesteuert wird.

WAVELYNX EX. 1003, Pg. 1150
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 1



WAVELYNX EX. 1003, Pg. 1151
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 2a

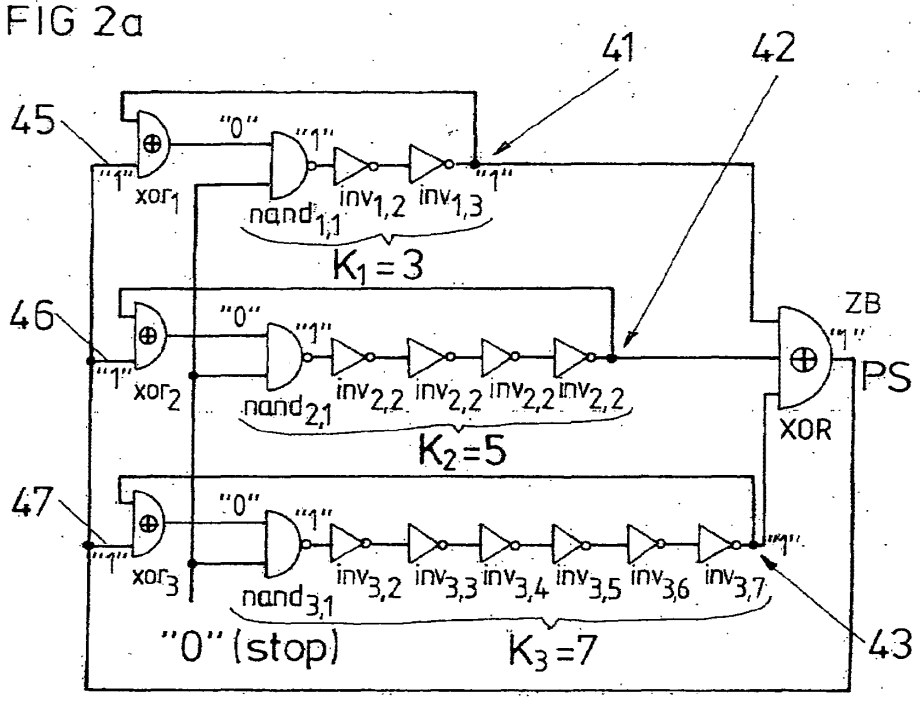
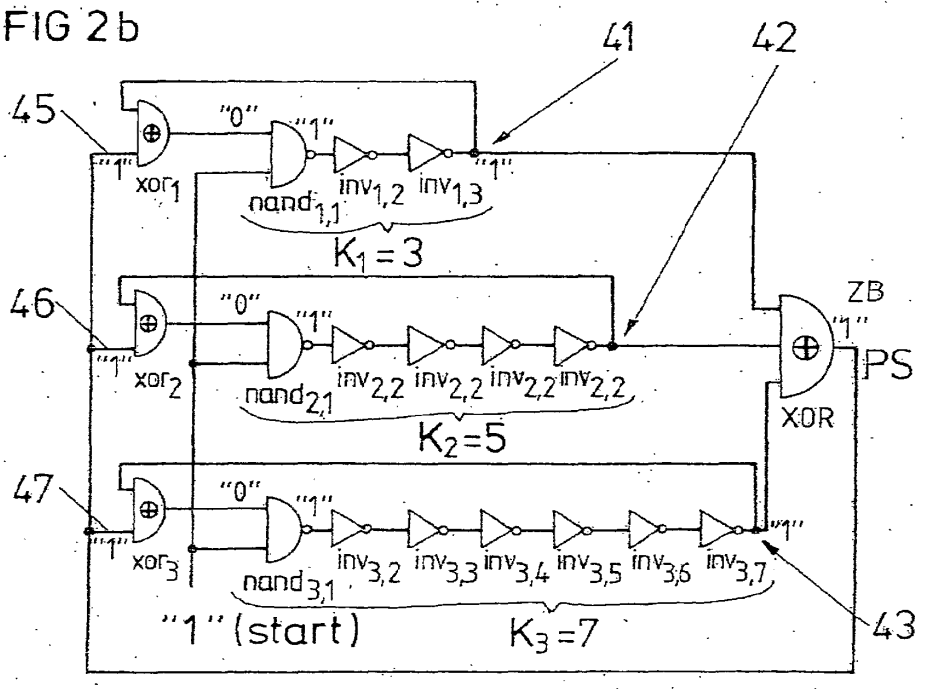


FIG 2b



WAVELYNX EX. 1003, Pg. 1152
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 3a

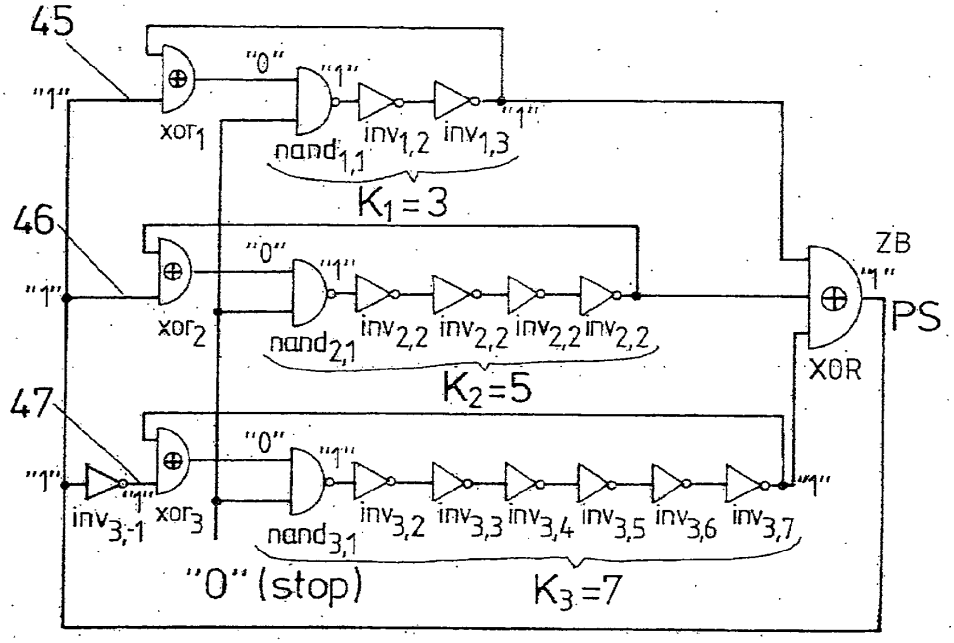
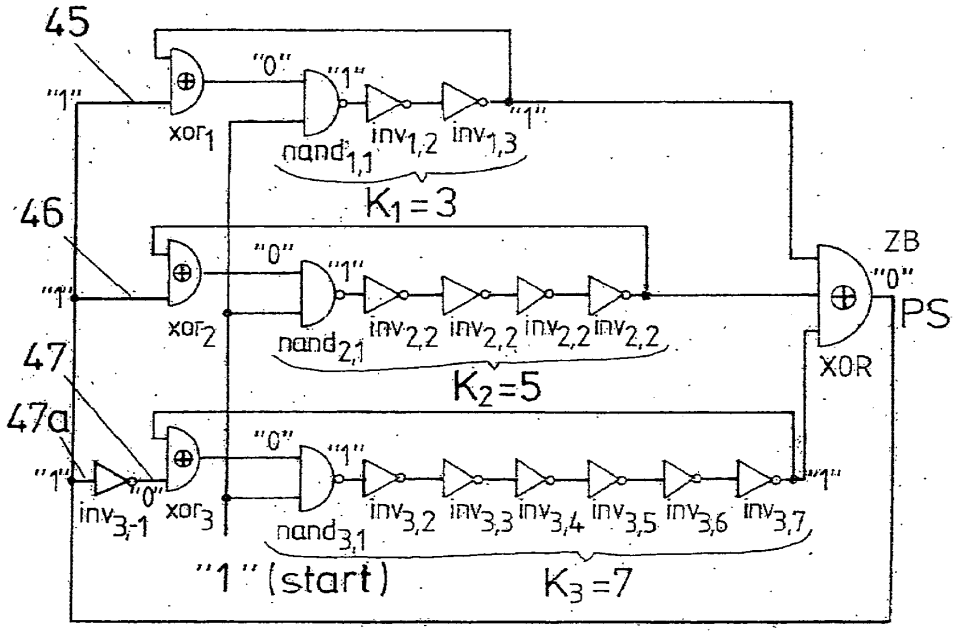


FIG 3b



WAVELYNX EX. 1003, Pg. 1153
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 4a

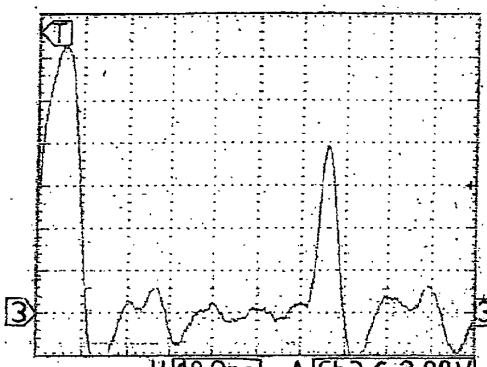


FIG 4b

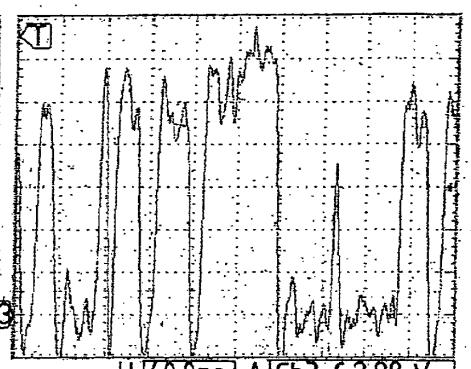


FIG 4c

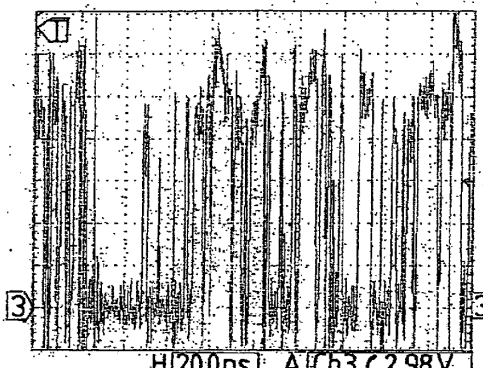


FIG 4d

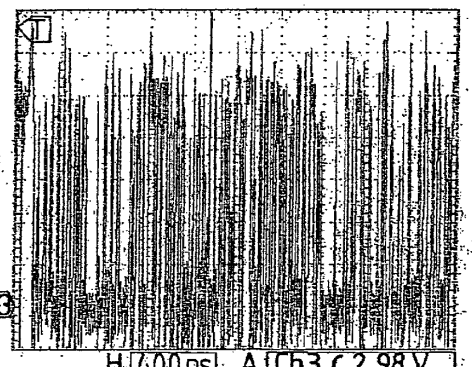


FIG 4e

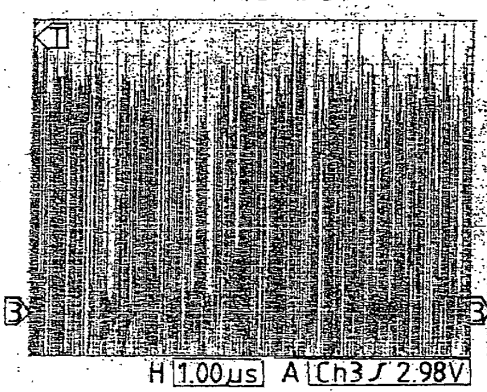
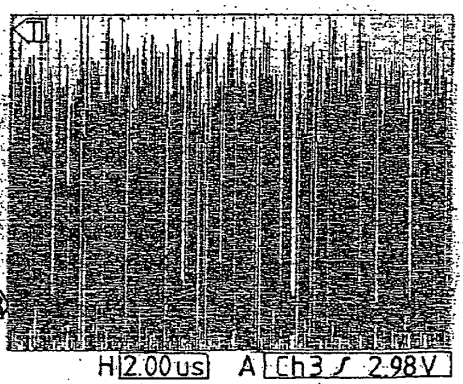


FIG 4f



WAVELYNX EX. 1003, Pg. 1154
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

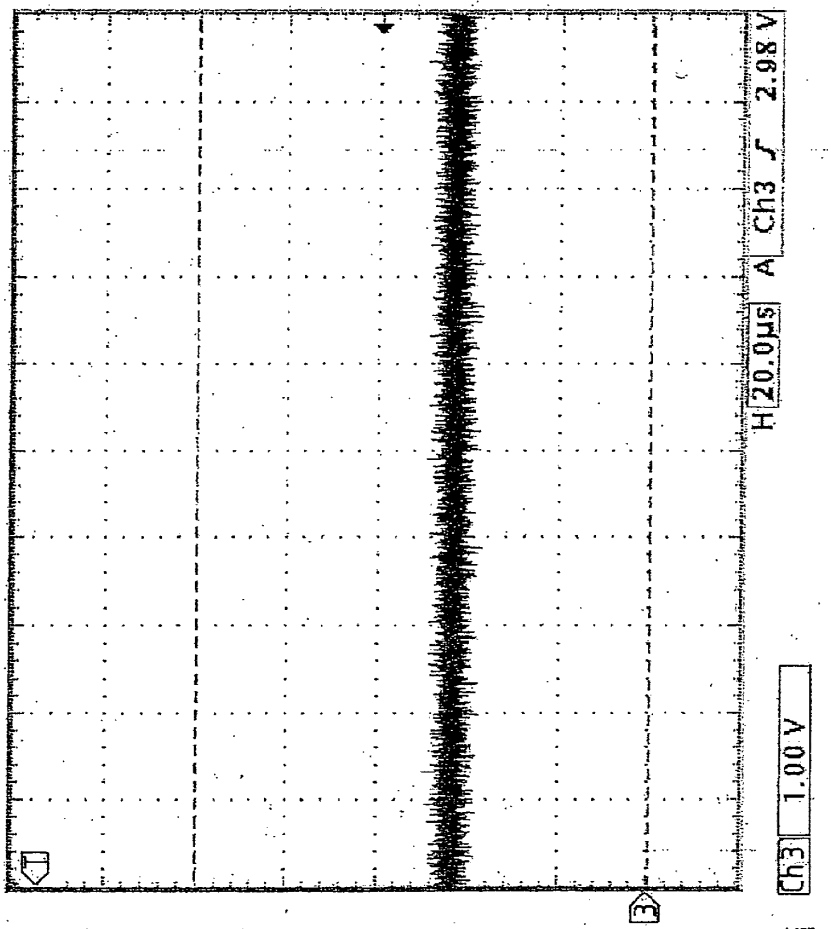


FIG 5

WAVELYNX EX. 1003, Pg. 1155
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

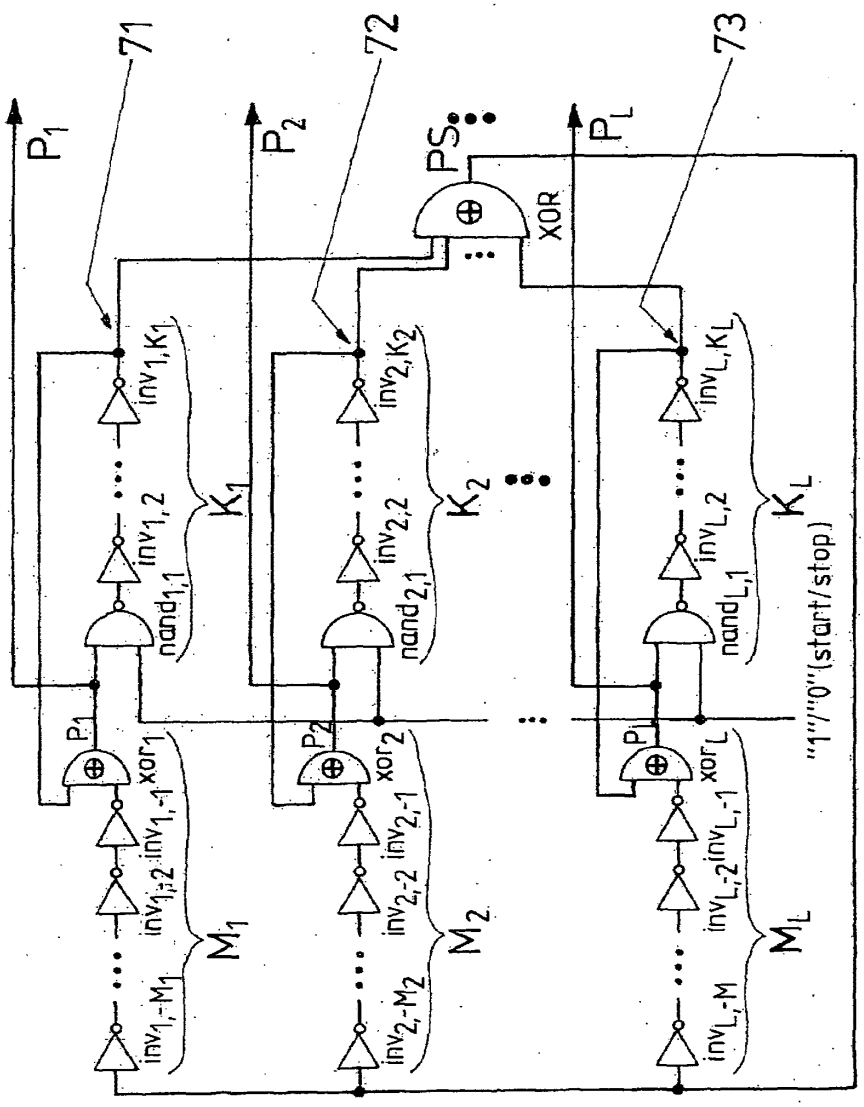


FIG 6

WAVELYNX EX. 1003, Pg. 1156
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

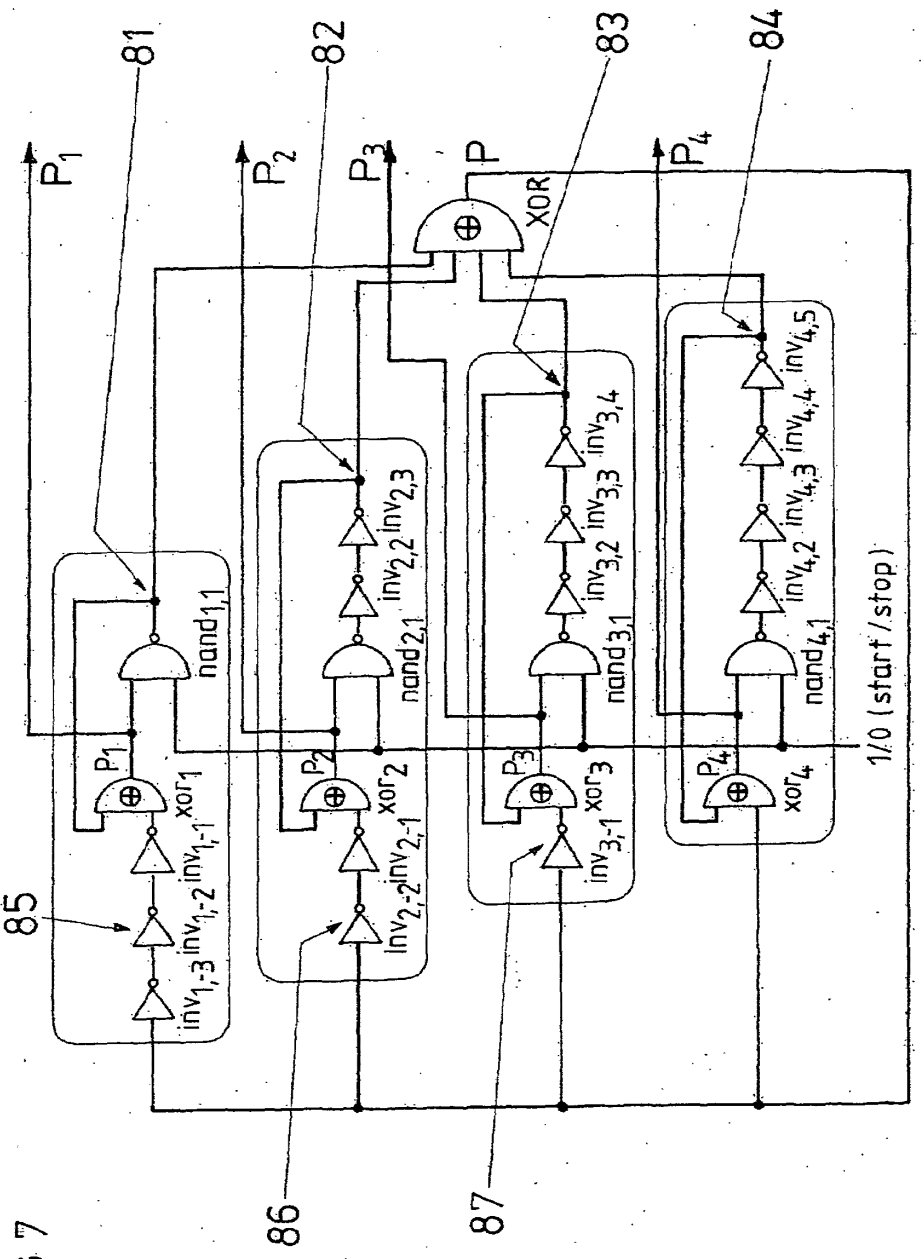


FIG 7

WAVELYNX EX. 1003, Pg. 1157
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

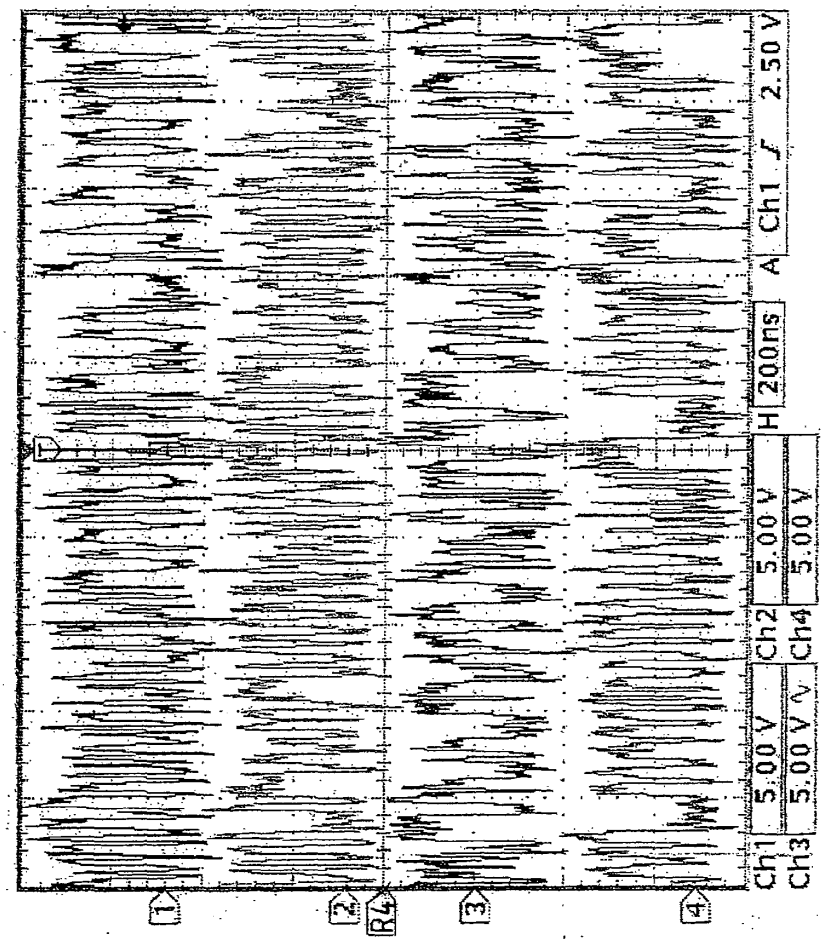


FIG 8

WAVELYNX EX. 1003, Pg. 1158
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

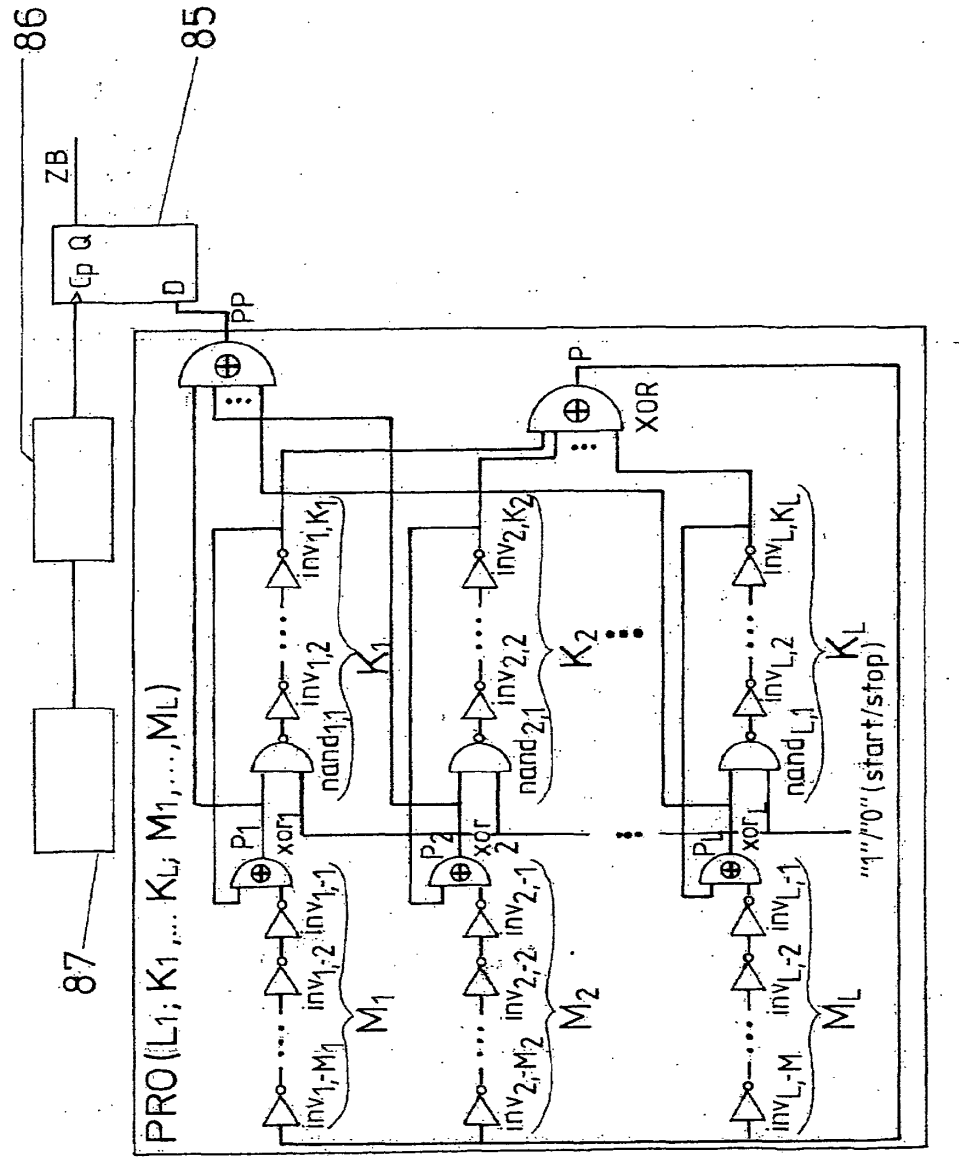


FIG 9

WAVELYNX EX. 1003, Pg. 1159
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

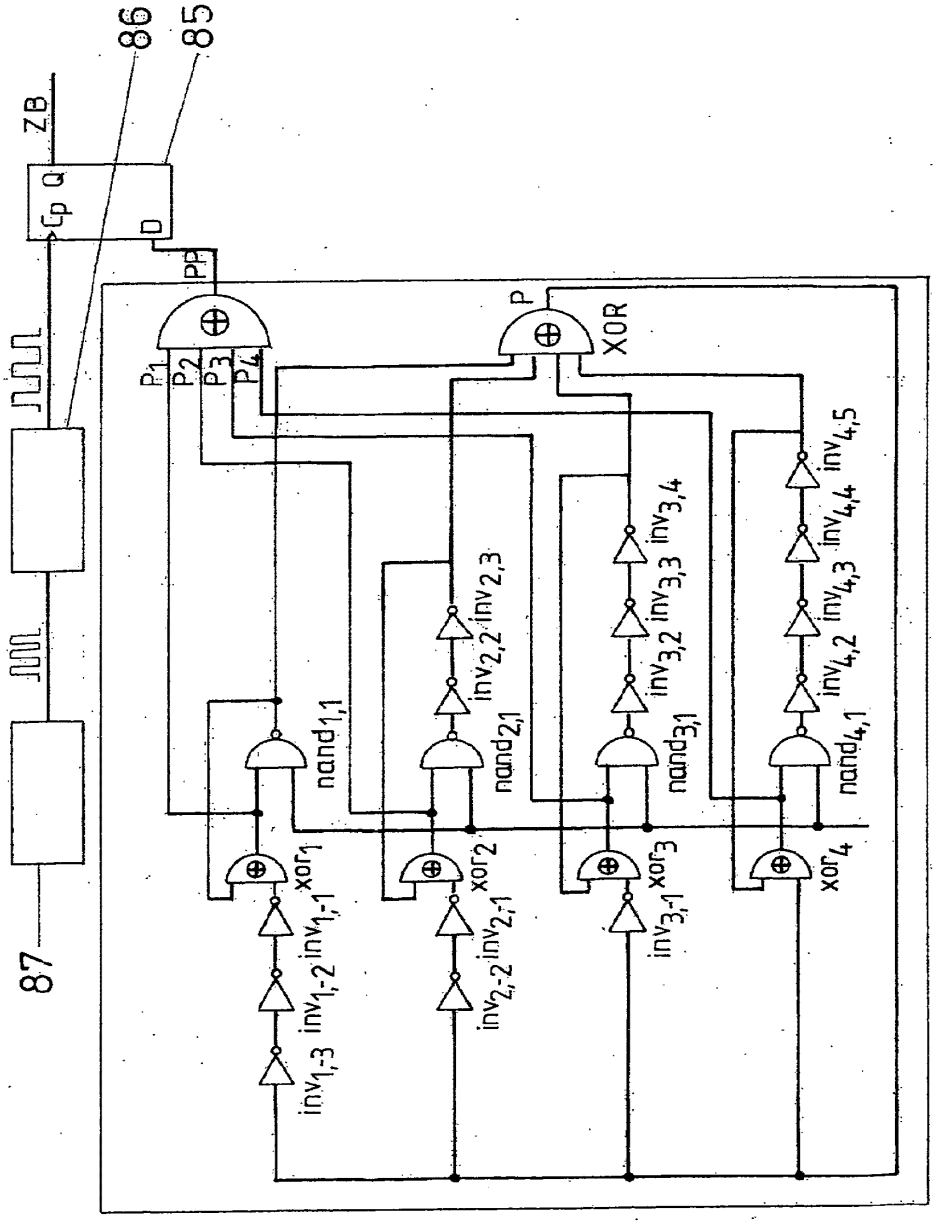


FIG 10

WAVELYNX EX. 1003, Pg. 1160
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

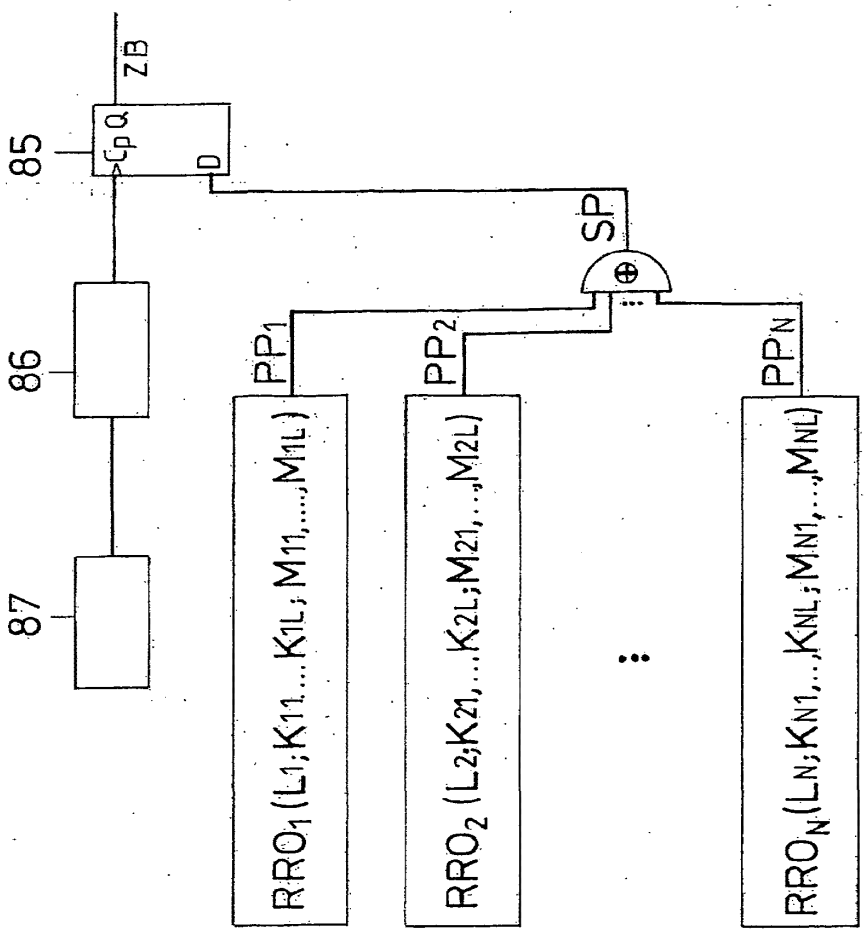


FIG 11

WAVELYNX EX. 1003, Pg. 1161
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

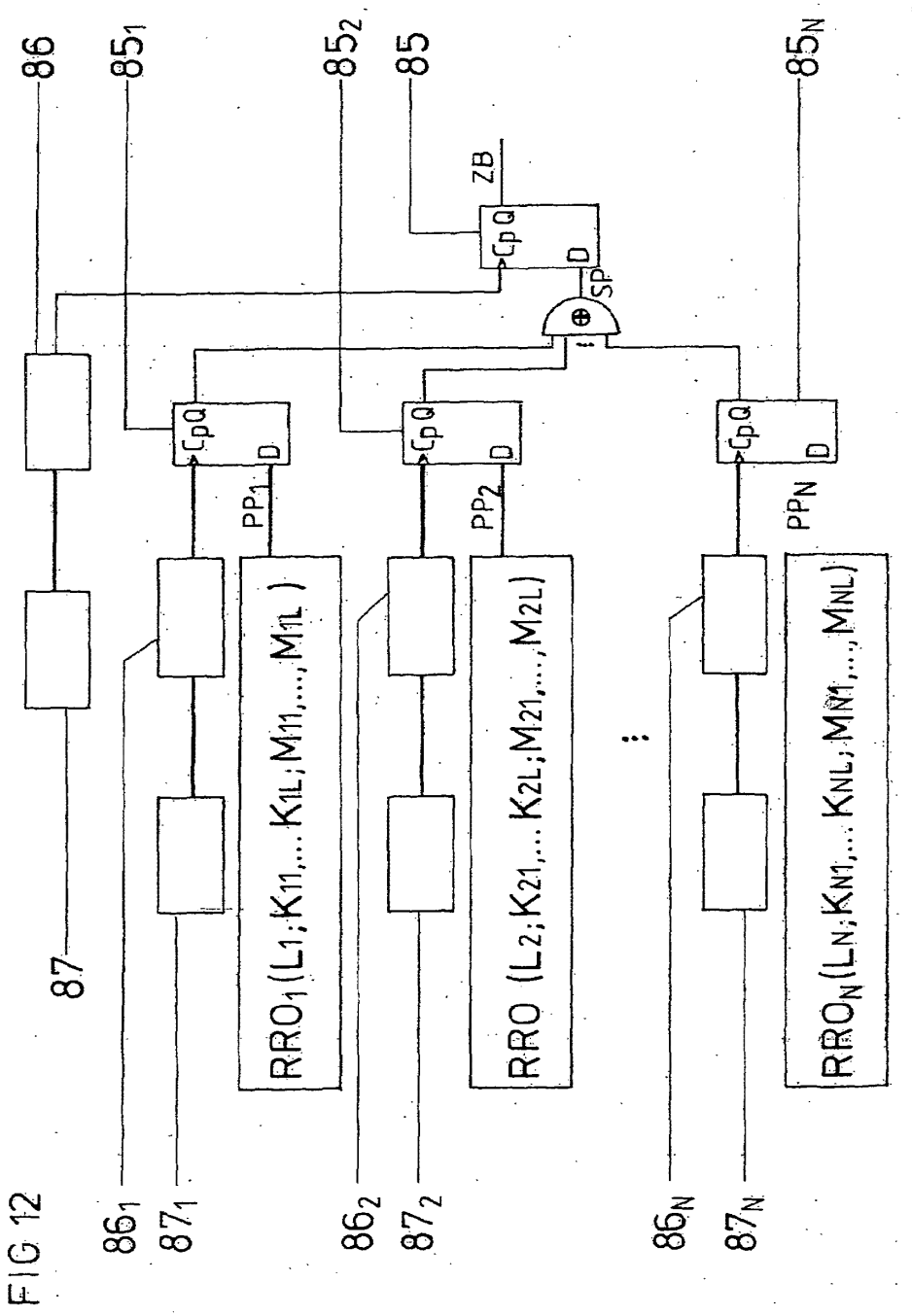


FIG 12

WAVELYNX EX. 1003, Pg. 1162
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

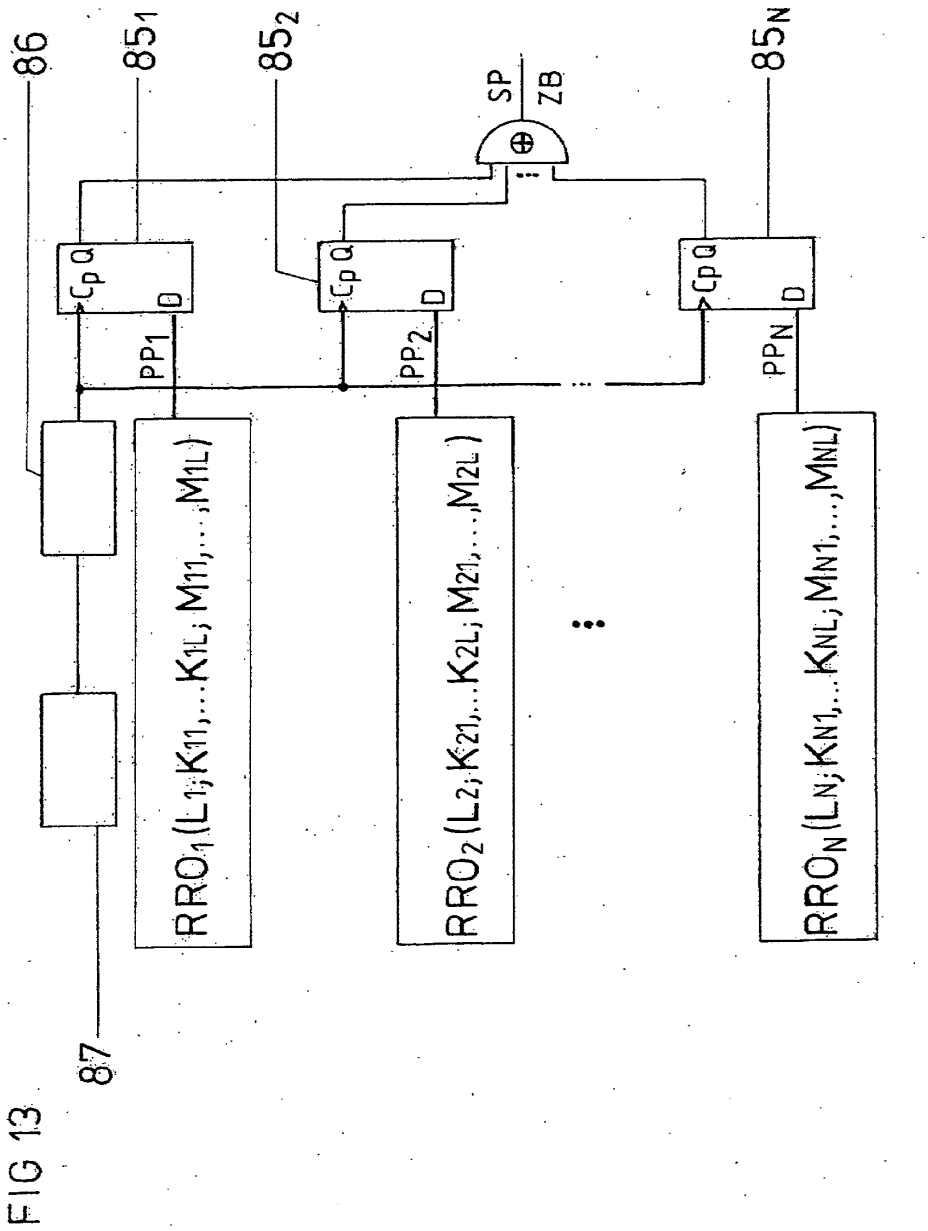
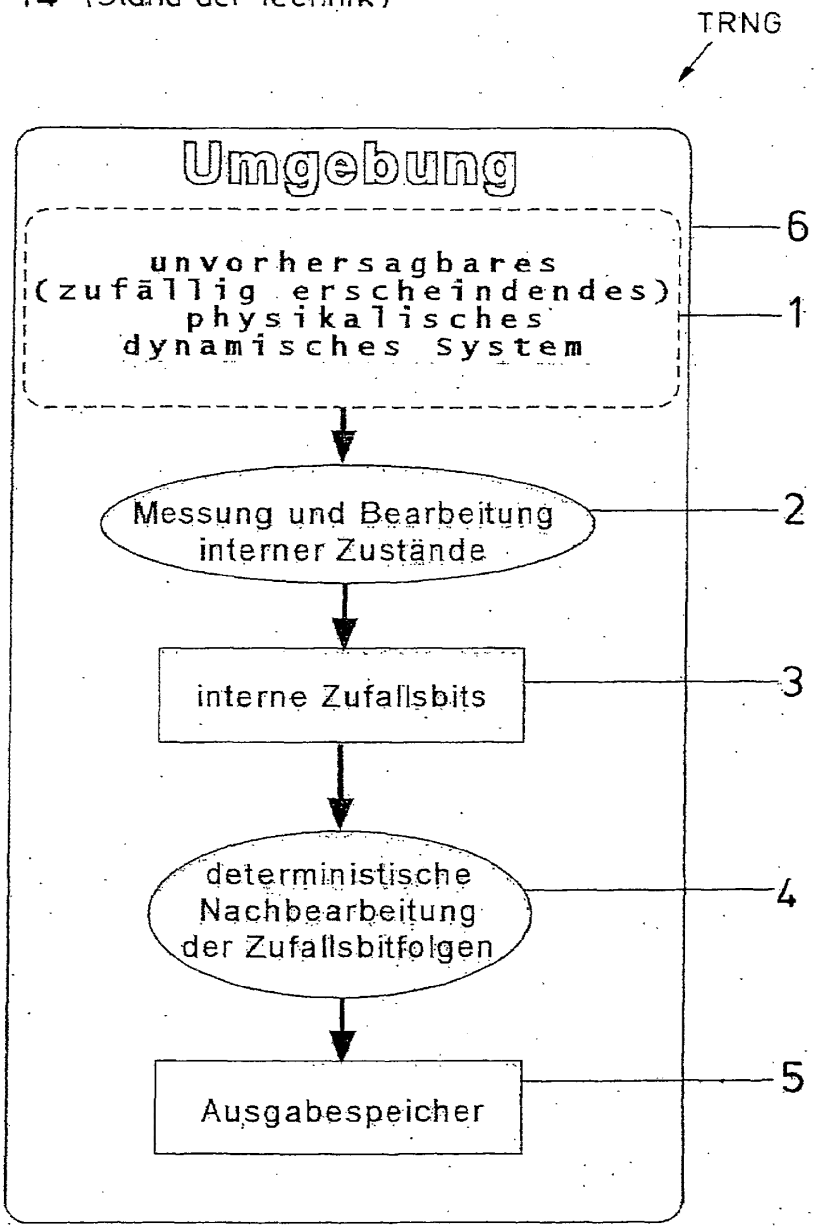


FIG 13

WAVELYNX EX. 1003, Pg. 1163
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 14 (Stand der Technik)



WAVELYNX EX. 1003, Pg. 1164
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 15a (Stand der Technik)

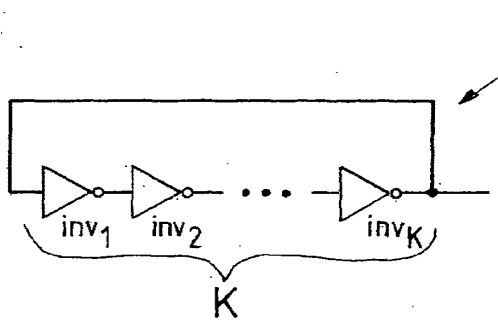
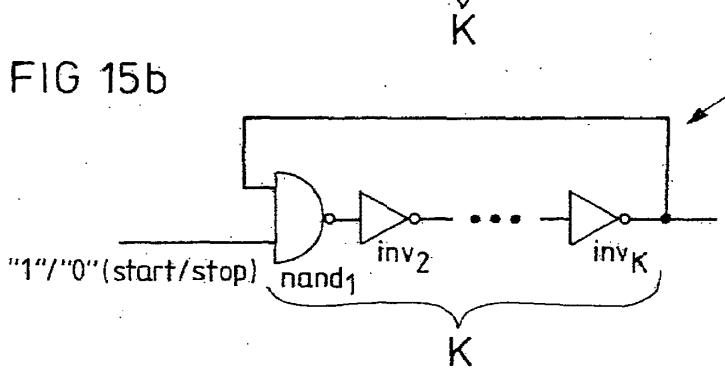


FIG 15b



K = ungerade Zahl

WAVELYNX EX. 1003, Pg. 1165
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 16a

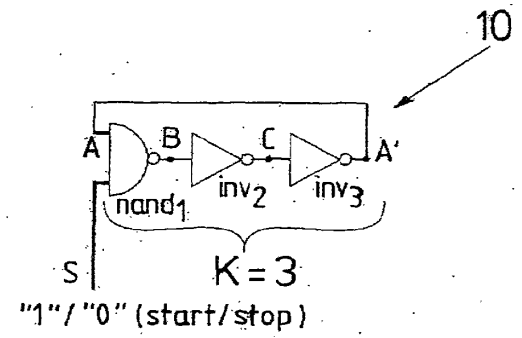


FIG 16b

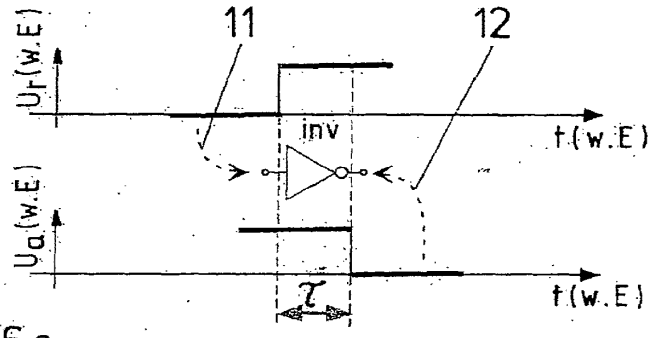
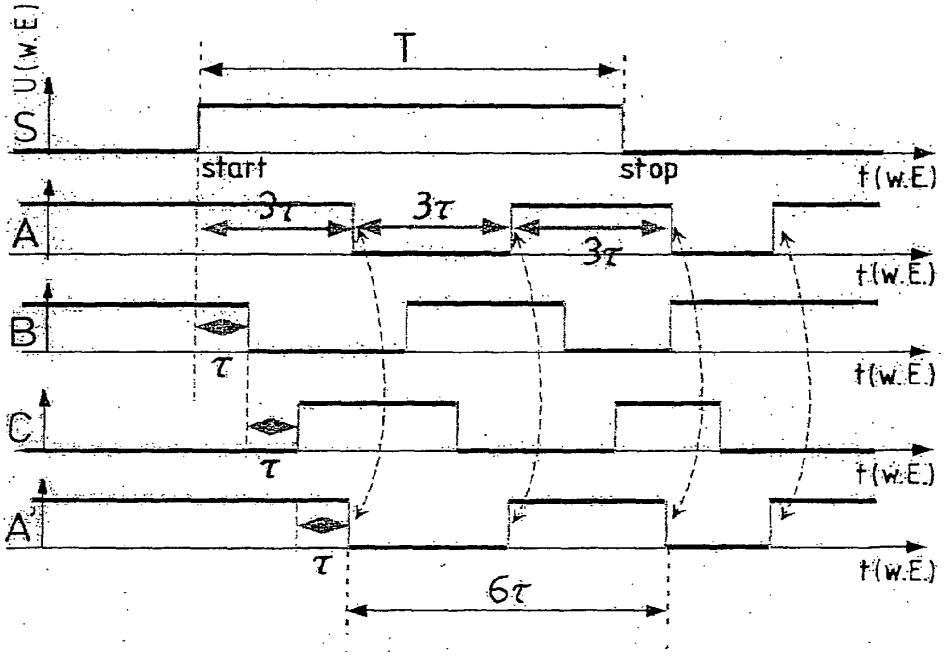


FIG 16c



WAVELYNX EX. 1003, Pg. 1166
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 17a (Stand der Technik)

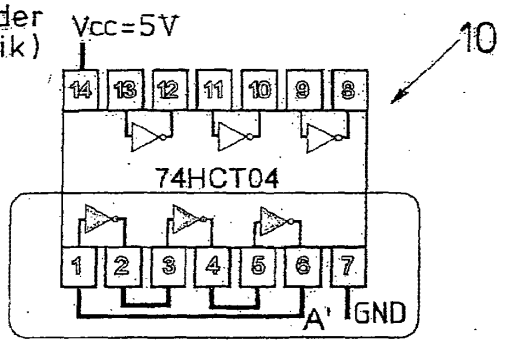


FIG 17b

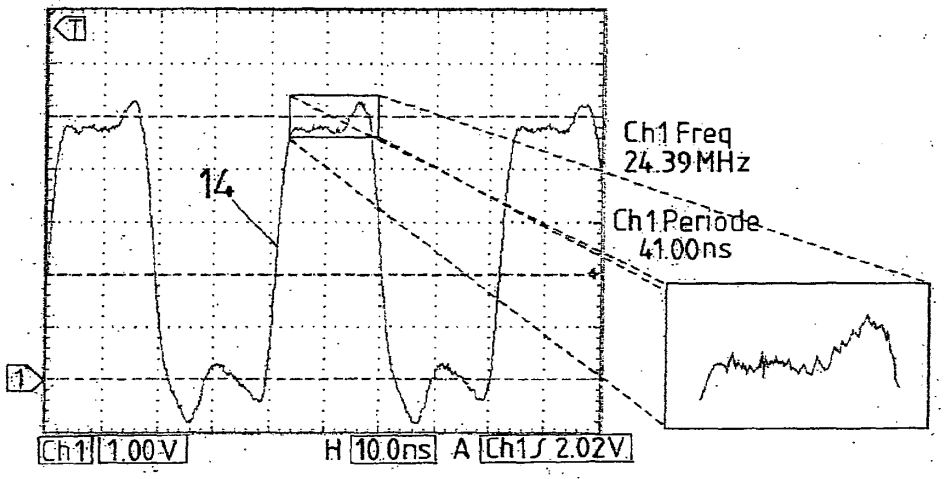
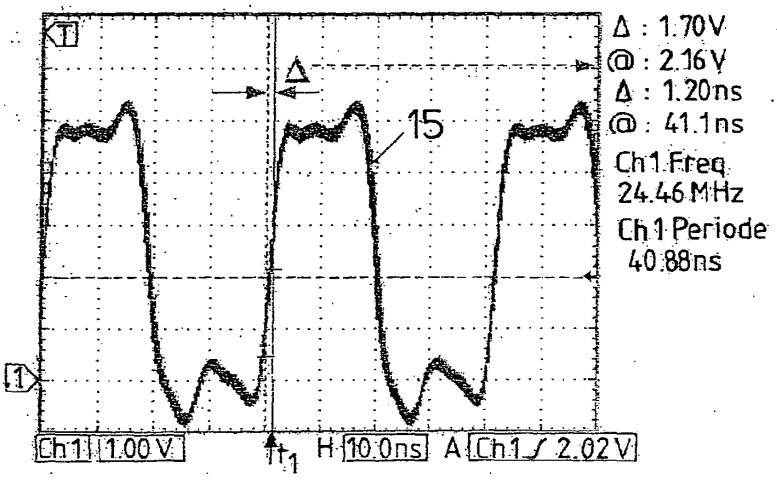


FIG 17c



WAVELYNX EX. 1003, Pg. 1167
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

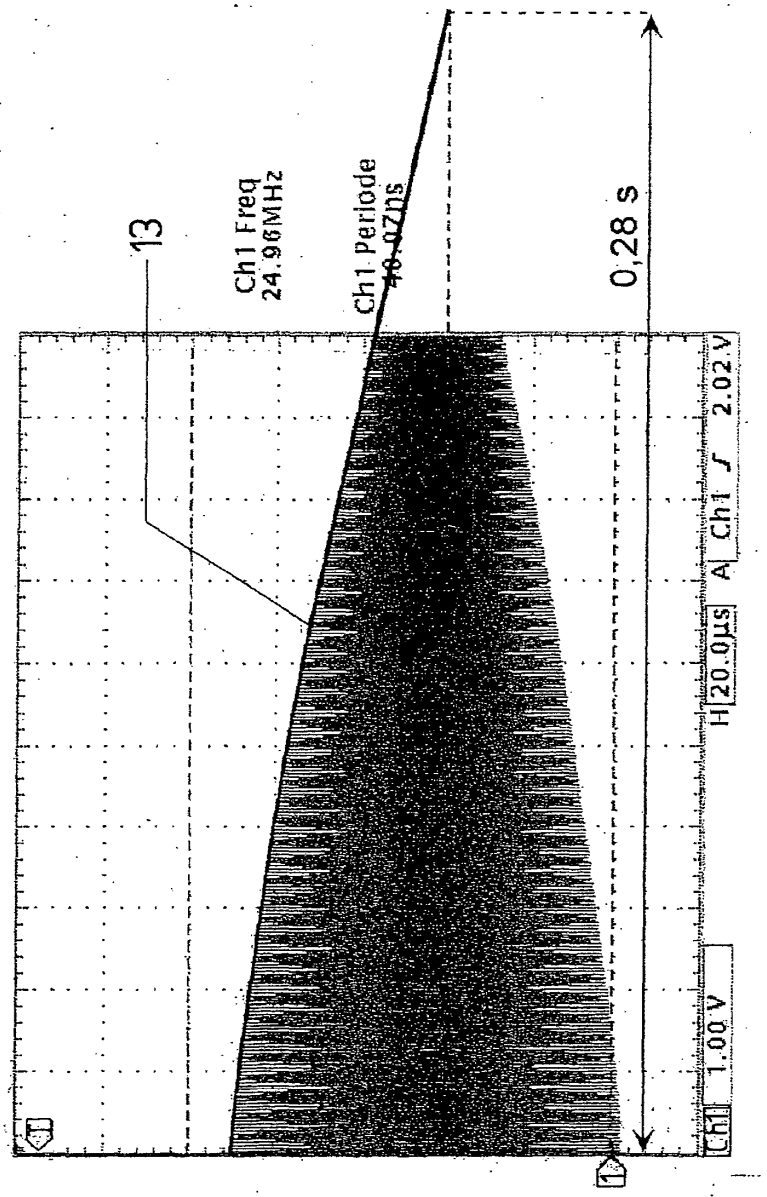


FIG 18 (Stand der Technik)

WAVELYNX EX. 1003, Pg. 1168
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 19b

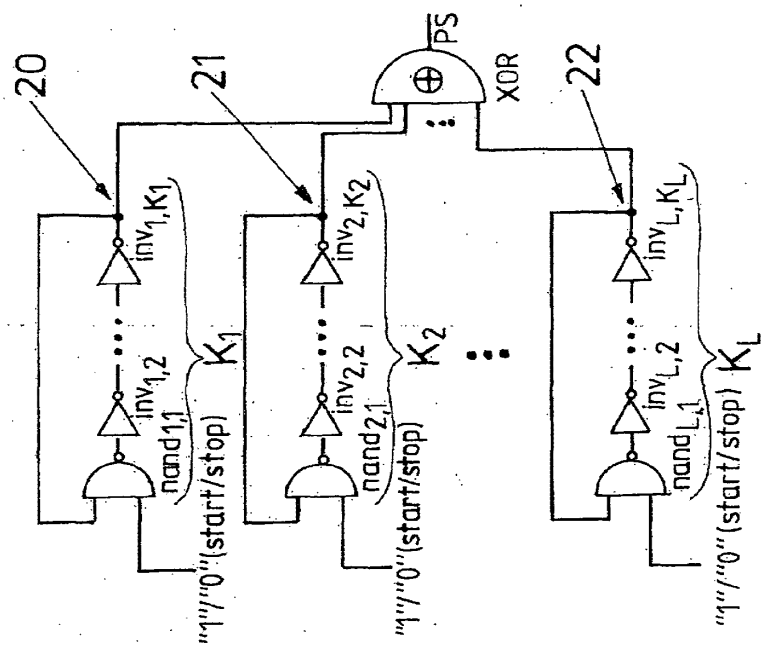
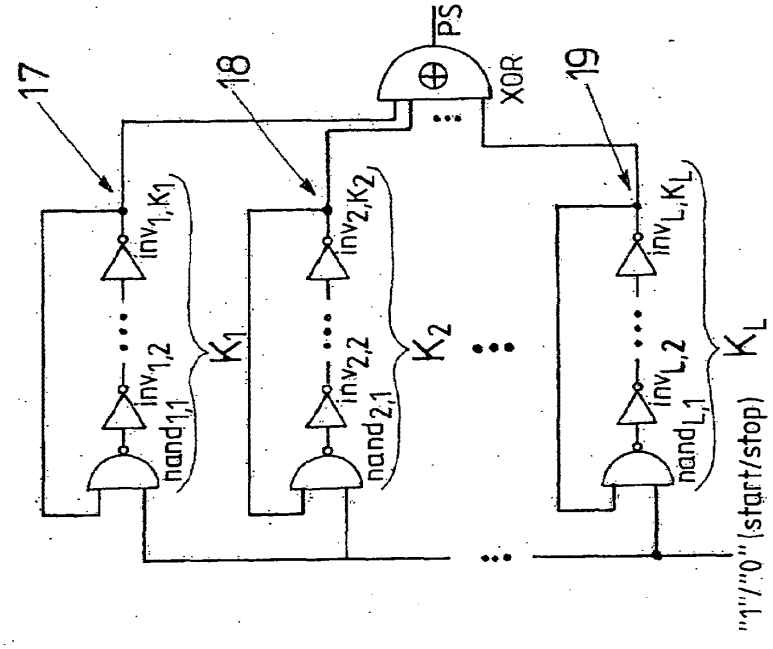


FIG 19a (Stand der Technik)



WAVELYNX EX. 1003, Pg. 1169
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 20a

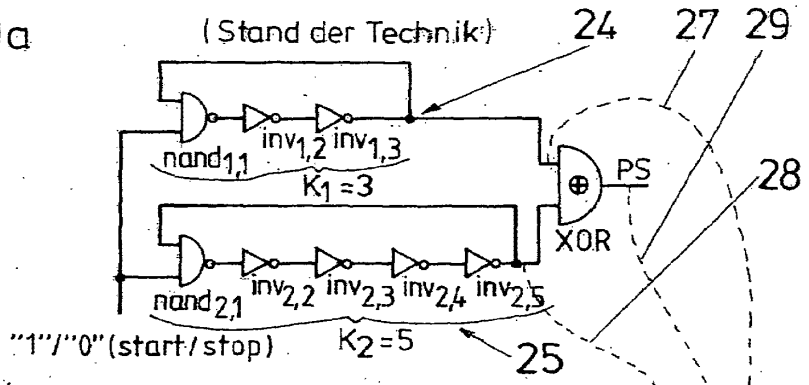


FIG 20b

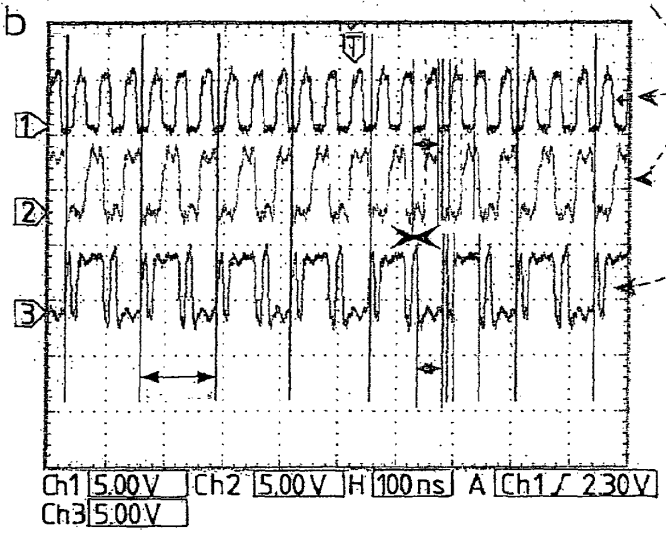
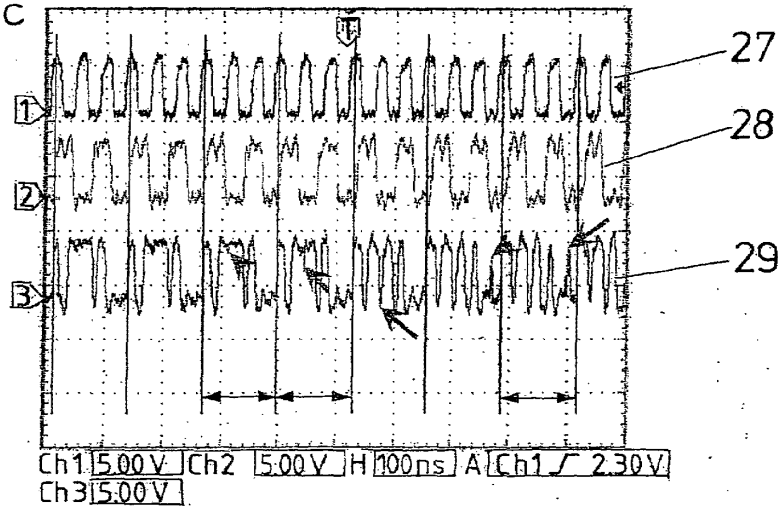


FIG 20c



WAVELYNX EX. 1003, Pg. 1170
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 21a (Stand der Technik)

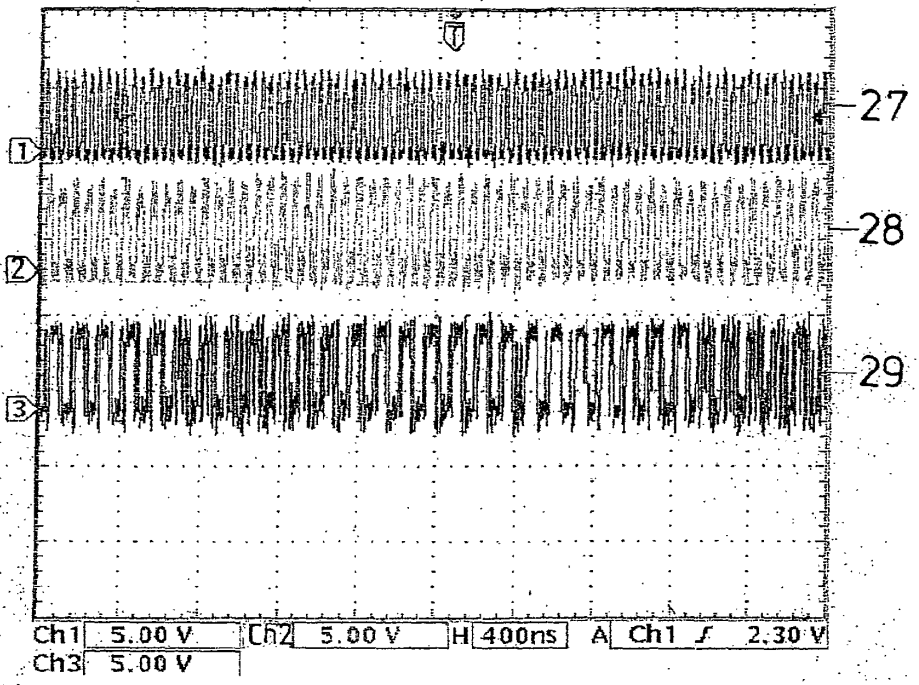
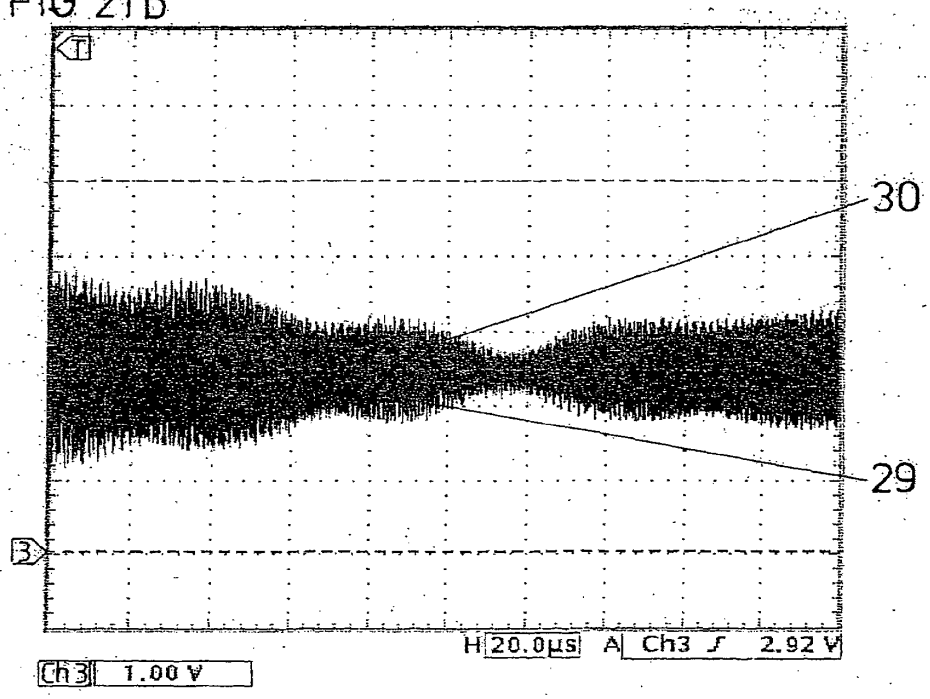


FIG 21b



WAVELYNX EX. 1003, Pg. 1171
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

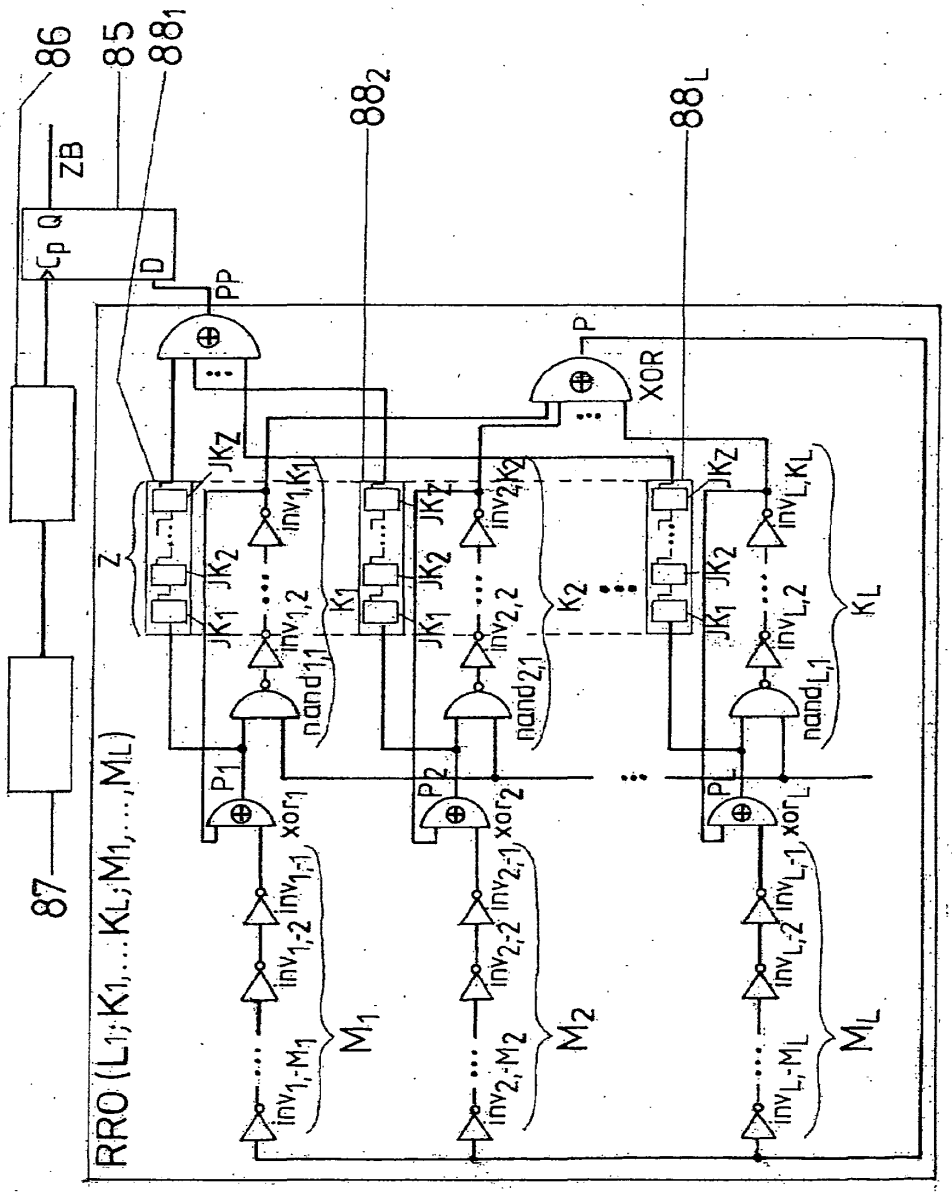


FIG 22

WAVELYNX EX. 1003, Pg. 1172
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 05 02 0294

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
A	US 5 963 104 A (BUER ET AL) 5. Oktober 1999 (1999-10-05) * Spalte 4, Zeile 29 - Spalte 11, Zeile 53; Abbildungen 1-4b,5a-5b * -----	1-33	H03K3/84 G06F7/58
D,A	WO 03/081417 A (INFINEON TECHNOLOGIES AG; JANSSEN, NORBERT; SEIFERT, JEAN-PIERRE) 2. Oktober 2003 (2003-10-02) * Seite 3, Zeile 29 - Seite 6, Zeile 4 * * Seite 6, Zeile 24 - Seite 7, Zeile 14; Abbildungen 1,2,4 * -----	1-33	
A	US 5 961 577 A (SOENEN ET AL) 5. Oktober 1999 (1999-10-05) * Zusammenfassung; Abbildung 2 * -----	1-33	

RECHERCHIERTE SACHGEBIETE (IPC)

H03K
G06F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	14. Februar 2006	Kassner, H

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

WAVELYNX EX. 1003, Pg. 1173
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 05 02 0294

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

14-02-2006

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5963104 A	05-10-1999	KEINE	
WO 03081417 A	02-10-2003	AU 2003215646 A1	08-10-2003
		DE 10213269 A1	23-10-2003
US 5961577 A	05-10-1999	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

WAVELYNX EX. 1003, Pg. 1174
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 696 360 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.08.2006 Bulletin 2006/35

(51) Int Cl.:
G06F 21/00 (2006.01)

(21) Application number: **06250865.0**

(22) Date of filing: **17.02.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **23.02.2005 KR 2005014881**

(71) Applicant: **Samsung Electronics Co., Ltd.**
Yeongtong-gu
Suwon-si, Gyeonggi-do (KR)

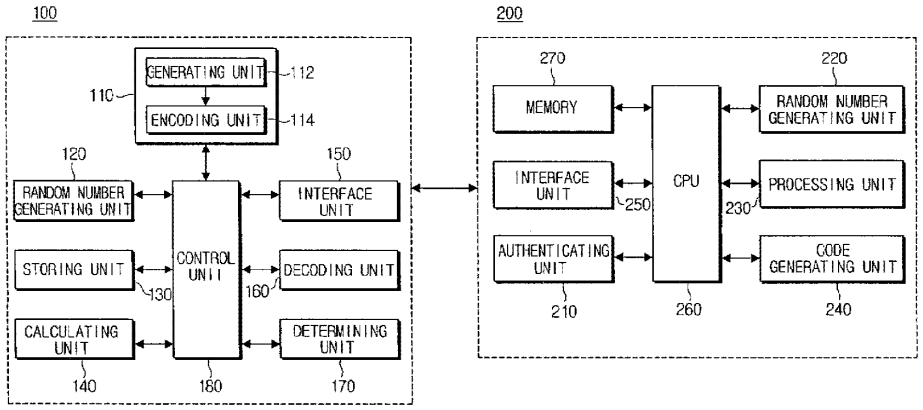
(72) Inventors:
- **Korkishko, Tymur,**
  407-501, Cheongmyeong-maeul
  Suwon-si
  Gyeonggi-do (KR)
- **Lee, Kyung-hee**
  Yongin-si
  Gyeonggi-do (KR)

(74) Representative: **Ertl, Nicholas Justin**
Elkington and Fife LLP,
Prospect House,
8 Pembroke Road
Sevenoaks,
Kent TN13 1XR (GB)

(54) Apparatus and system for remotely verifying integrity of memory for mobile platform, and method therefor

(57) A verification apparatus for a mobile platform for remotely verifying the integrity of a device that is connected to a network and has a shared private key includes a verifying unit that determines whether the device shares a private key with the verification apparatus by checking whether the authentication code generated by the verification apparatus matches the authentication code generated by the device; a calculating unit that generates a local check code that verifies the integrity of the memory; an interface unit that transmits, to the device, the information that the verification apparatus uses to generate an authentication code and the integrity check parameter used to generate a remote check code, and receives the authentication code and the remote check code from the device; and a determining unit that verifies the integrity of the memory if the local check code matches the remote check code.

FIG. 2



EP 1 696 360 A1

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1175
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

[0001] The present invention relates to an apparatus, system, and method for remotely verifying the integrity of a device for a mobile platform. When both the device and the verification apparatus, which is connected to the device via a network, share private information, the apparatus and system can remotely check the integrity of the device by authenticating the device by comparing a check code generated by a verification apparatus with a check code generated by the device and determining whether the two check codes match each other.

[0002] FIG. 1 illustrates a conventional method for verifying the integrity of a device.

[0003] Referring to FIG. 1, television set-top boxes, mobile telephones, local area network (LAN)-based or wide area network (WAN)-based personal computers (PCs) and remote network equipment, such as small-sized sensors, are susceptible to attacks from hackers since network hosts or service providers have limited capabilities in controlling user access to devices. Furthermore, it is difficult for network hosts or service providers to check remote devices physically and determine whether the remote devices have been changed, for example, whether unauthorized users have accessed software applications on a network. Therefore, there is a need for a technique to verify the integrity of a memory in a remote device in a network environment. Here, integrity refers to the certainty that only authorized people are allowed to access or change the information on data and the certainty of network security.

[0004] Conventional methods of verifying the integrity of a memory in a device include comparing a digest value for selected software with a hash value for a memory area in a remote device.

[0005] The conventional method of verifying the integrity using a hash value for a memory area in a device is disclosed in U.S. Patent Publication No. 2002/0138544. In this method, a random seed is inserted into a memory area to obtain a hash value. And then the random seed, a hash function and the information about the memory area to be tested are sent to the device. The device produces the hash value of the memory area using the information received from a verification apparatus and sends the generated hash value to the verification apparatus. The verification apparatus compares its generated hash value for the memory area with the hash value generated by the device and checks the integrity of the memory area based on a comparison result.

[0006] This method uses the hash value for a memory area to verify the integrity. For this reason, if a malicious code such as virus changes its position and attacks different parts of the memory, the integrity check will be successful when it should not be successful. As a result, the verification apparatus cannot correctly verify the integrity of the device.

[0007] The conventional method of verifying the integrity of a device using a digest value of selected software is disclosed in U.S. Patent No. 6,748,538. In this method, the digest value for the software installed in the device is stored with a signature in a memory. The integrity of the software is checked by comparing the signed digest value with the digest value obtained by applying a separate hash function to the selected software. However, this method has a limitation in that it can verify only the integrity of the software stored in the device.

[0008] U.S. Patent No. US 6,138,236 discloses a method of verifying the integrity of software with a code stored in a programmable read only memory (PROM) which checks the signature of the software during booting. However, this method can internally check the integrity of software only during booting. A separate secure mechanism is needed to externally check the integrity of software since it is impossible to correctly check the integrity when an attacker changes the contents of a PROM and creates a valid check code.

[0009] Accordingly, there is a need for an integrity verification method capable of coping with a malicious code that attacks different parts of a memory and externally verifying the integrity of a device during runtime as well as during booting of the device.

[0010] The present invention provides an apparatus for verifying the integrity of a device that is connected to a network and has a shared private key. The apparatus includes a verifying unit that determines whether the device has a shared private key by determining whether an authentication code generated by the verification apparatus matches an authentication code generated by the device; a calculating unit that, when the device has the shared private key, fills the empty areas of a memory in the device with random numbers based on a pre-stored memory filling map and generates a local check code that is a message authentication code (MAC) for verifying the integrity of the memory; an interface unit that transmits, to the device, the information on the authentication code generated by the verification apparatus and the integrity check parameter used to produce a remote check code that is a MAC generated by the device, and receives the authentication code and the remote check code from the device; and a determining unit that verifies the integrity of the memory -by checking whether the local check code matches the remote check code.

[0011] In an exemplary embodiment, the verifying unit may include a generating unit that produces a random number used to generate an authentication code; and an encoding unit that encrypts the random number and the shared private key and determines whether the authentication code generated by the verification apparatus matches the authentication code generated by the device.

[0012] In an exemplary embodiment, the apparatus may further include a storing unit that stores the contents of the memory in the device, the random numbers, the memory filling map, the shared private key, and a generating function used to generate a MAC.

WAVELYNX EX. 1003, Pg. 1176
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0013] In an exemplary embodiment, the apparatus may further include a random number generating unit that, using a random function, generates random numbers to fill the empty areas of the memory.

[0014] The calculating unit in the apparatus produces a local check code by reading the contents of the memory in a reverse order and applying a MAC generating function to the contents.

[0015] In an exemplary embodiment, the apparatus may further include a decoding unit that decodes the remote check code encoded using the shared private key.

[0016] The device may include an interface unit that receives an integrity check parameter and the information on an authentication code generated by the verification apparatus, and transmits the authentication code generated by the device and the generated remote check code to the verification apparatus; an authenticating unit that generates an authentication code using the random number and the information on the authentication code generated by the verification apparatus; a code generating unit that produces a remote check code using the received integrity check parameter and a MAC generating function; and a central processing unit (CPU) that stores the MAC generating function and the shared private key.

[0017] In this case, the integrity check parameter may comprise the memory filling map and the information on the random number used to generate the local check code.

[0018] In an exemplary embodiment, the apparatus may further comprise a random number generating unit that generates the random number used to produce a remote check code by applying a random function and the information on the random number used to generate a local check code.

[0019] The code generating unit generates a remote check code by filling the empty areas of the memory in the device with the random numbers generated based on the memory filling map, reading the contents of the memory in a reverse order and applying the MAC generating function to the contents.

[0020] In accordance with another aspect of the present invention, a system comprises a device with a shared private key and a verification apparatus communicably connected to the device over a network to remotely verify the integrity of a memory in the device. Further, the system comprises the verification apparatus that determines whether the device has a shared private key by checking whether an authentication code generated by the device matches an authentication code generated by the verification apparatus, generates a local check code that is a MAC by filling the empty areas of a memory in the device with random numbers and verifies the integrity of the device by determining whether the remote check code generated by the device, which is a MAC for verifying the integrity of the device, matches the local check code; and the device that generates an authentication code using the information on the authentication code produced by the verification apparatus and creates a remote check code based on the information used to generate a local check code.

[0021] The verification apparatus may include a verifying unit that determines whether the device has a shared private key by checking whether the authentication code generated by the verification apparatus matches the authentication code generated by the device; a calculating unit that, when the device has a shared private key, fills the empty areas of a memory in the device with random numbers based on a pre-stored memory filling map and generates a local check code that is a MAC for verifying the integrity of the memory; an interface unit that transmits, to the device, the information on the authentication code generated by the verification apparatus and the integrity check parameter that the device uses to generate a remote check code, which is a MAC for verifying the integrity of the memory, and receives the authentication code and the remote check code from the device; and a determining unit that verifies the integrity of the memory by checking if the local check code matches the remote check code.

[0022] The device may include an interface unit that receives the integrity check parameter and the information that the verification apparatus uses to generate an authentication code, and transmits the authentication code and the remote check code generated by the device to the verification apparatus; an authenticating unit that generates an authentication code using the random number and the information that the verification apparatus uses to create the authentication code; a code generating unit that generates a remote check code using the received integrity check parameter and a MAC generating function; and a CPU that stores the MAC generating function and the shared private key.

[0023] In accordance with yet another aspect of the present invention, there is provided a method for verifying the integrity of a device that is connected to a verification apparatus over a network and has a shared private key. The method includes determining whether the device has the shared private key by checking whether the authentication code generated by the verification apparatus matches the authentication code generated by the device; when the device has the shared private key, filling the empty areas of a memory in the device with random numbers based on a pre-stored memory filling map and generating a local check code that is a MAC for verifying the integrity of the memory; transmitting, to the device, the information that the verification apparatus uses to generate the authentication code and the integrity check parameter that the device uses to create a remote check code, which is a MAC for verifying the integrity of a memory, and receiving the authentication code and the remote check code from the device; and verifying the integrity of the memory by checking if the local check code matches the remote check code.

[0024] The determining operation may include generating a random number used to create an authentication code, encoding the random number and the shared private key and determining whether the authentication code generated

WAVELYNX EX. 1003, Pg. 1177
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

by the verification apparatus matches the authentication code generated by the device.

[0025] In an exemplary embodiment, the method may further include storing the contents of the memory in the device, the random numbers, the memory filling map, the shared private key and the generating function that is used to create a MAC.

[0026] In an exemplary embodiment, the method may further include generating random numbers to fill the empty areas of the memory using a random function.

[0027] The operation of generating a local check code may comprise reading the contents of the memory in a reverse order and generating a local check code by applying a MAC generating function to the contents.

[0028] In an exemplary embodiment, the method may further include decoding a remote check code if it is encoded using a shared private key.

[0029] The operation of generating a local check code may include generating an authentication code using the random number and the information that the verification apparatus uses to generate an authentication code; generating a remote check code using the received integrity check parameter and a MAC generating function; and transmitting the authentication code generated by the device and the generated remote check code to the verification apparatus.

[0030] An integrity check parameter may include the memory filling map and the information on the random number used to generate a local check code.

[0031] In an exemplary embodiment, the method may further include generating the random number used to produce a remote check code by applying the random function and the information on the random number used to generate a local check code.

[0032] The operation of generating a remote check code may include filling the empty areas of the memory in the device with the generated random numbers based on the memory filling map, reading the contents of the memory in a reverse order, applying the MAC generating function to the contents and creating a remote check code.

[0033] In accordance with yet another aspect of the present invention, there is provided a method based on the system that includes a device and a verification apparatus communicably connected to the device over a network for remotely verifying the integrity of a memory in the device. The method comprises determining whether the device has a private key shared with the verification apparatus by checking whether the authentication code generated by the device matches the authentication code generated by the verification apparatus; filling the empty areas of a memory in the device with the random numbers based on a pre-stored memory filling map and generating a local check code that is a MAC for verifying the integrity of the memory; transmitting, to the device, the integrity check parameter used to generate a remote check code that is a MAC generated by the device to verify the integrity of a memory; generating a remote check code using the received integrity check parameter and transmitting the remote check code generated by the device to the verification apparatus; and verifying the integrity of the memory in the device by checking whether the local check code matches the remote check code.

[0034] The present invention thus provides an apparatus and system that remotely verifies the integrity of a device for a mobile platform and a method capable of remotely authenticating the device and checking the integrity of the device simultaneously.

[0035] The present invention also provides an apparatus and system for remotely verifying the integrity of a device for a mobile platform and a method capable of correctly checking the integrity of the device by authenticating the device, comparing a check code generated by a verification apparatus with a check code generated by the device and determining whether the two check codes match with each other when both the device and the verification apparatus share private information.

[0036] The above aspects and features of the present invention will be more apparent by describing certain exemplary embodiments of the present invention with reference to the accompanying drawings, in which:

FIG. 1 illustrates a conventional method by which the integrity of a device is verified;

FIG. 2 illustrates a system that remotely verifies the integrity of a memory for a mobile platform according to an exemplary embodiment of the present invention;

FIGS. 3A to 3D illustrate the process of generating a local check code in a system that remotely verifies the integrity of a memory for a mobile platform according to an exemplary embodiment of the present invention; and

FIGS. 4A and 4B illustrate a method by which the integrity of a memory for a mobile platform is remotely verified according to an exemplary embodiment of the present invention.

[0037] Hereinafter, the present invention will be described in detail with reference to the accompanying drawings.

[0038] FIG. 2 illustrates a system that remotely verifies the integrity of a memory for a mobile platform according to an exemplary embodiment of the present invention.

[0039] Referring to FIG. 2, the system comprises a device 200 and a verification apparatus 100 that can communicate with the device 200 over a network.

[0040] The verification apparatus 100 comprises a verifying unit 110, a random number generating unit 120, a storing

WAVELYNX EX. 1003, Pg. 1178
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

unit 130, a calculating unit 140, an interface unit 150, a decoding unit 160, a determining unit 170 and a control unit 180.

[0041] The verifying unit 110 comprises a generating unit 112 and an encoding unit 114. The verifying unit 110 determines whether a device to be tested shares private information with the verification apparatus 100 by comparing the authentication code generated by the verifying unit 100 with the authentication code generated by the device 200. The generating unit 112 creates a random number used to generate an authentication code using the private key that is the shared private information. Here, the generating unit 112 may use a random function to generate the random number.

[0042] The encoding unit 114 is equipped with the first and second encryption algorithms. The encoding unit 114 creates the encoded random number produced by the generating unit 112 using the random number, the shared key and the first encryption algorithm. The encoding unit 114 further creates an encoded shared key using the generated random number, the shared key and the second encryption algorithm.

[0043] Using a pre-stored random function, the random number generating unit 120 generates random numbers that will fill the empty areas of the memory 270 in the device 200.

[0044] The storing unit 130 stores the random function used by the random number generating unit 120, the contents of the memory 270 in the device 200 of which the integrity is to be tested, the memory filling map used to fill the empty areas of the memory 270 in the device 200 with the random numbers, the MAC generating function used to generate a local check code that is a MAC for verifying the integrity of the device 200, and the shared key that is the private information shared with the device 200, the first, second and third encryption algorithms for encoding data, and a decoding algorithm for decoding an encoded remote check code.

[0045] The storing unit 130 stores the contents of the memories in the devices of which the integrity will be verified by the verification apparatus 100. The memory filling map may refer to the method by which the empty areas of a memory 270 are filled with random numbers, and the method can be either sequential or random.

[0046] The calculating unit 140 fills the empty areas of the memory 270 with random numbers based on the memory filling map, reads the contents of the filled memory in a reverse order and generates a local check code to verify the integrity of the device 200 using the MAC generating function stored in the storing unit 130. The MAC generating function produces a code attached to data, which is used to check data alteration, such as modification, deletion and insertion of data. One example of a MAC generating function may be a hash function.

[0047] The interface unit 150 transmits, to the device 200, the random number generated by the generating unit 112, i.e., a random number used to generate an authentication code by the encoding unit 114 of the verifying unit 110 and receives an encoded random number that is an authentication code from the device 200.

[0048] The interface unit 150 transmits data to and receives data from the device 200. The interface unit 150 receives an encoded remote check code from the device 200, and transmits the encoded integrity check parameter used to generate a remote check code. An encoded integrity check parameter refers to a value obtained by applying the third encryption algorithm to the memory filling map stored in the storing unit 130 and the encoded shared key.

[0049] The decoding unit 160 decodes the encoded remote check code received from the device 200 using the decoding algorithm stored in the storing unit 130 and the shared key encoded by the encoding unit 114.

[0050] The determining unit 170 determines whether the remote check code decoded by the decoding unit 160 matches the local check code generated by the calculating unit 140. If the remote check code matches the local check code, the determining unit 170 concludes that the integrity check for the device 200 is successful. If the remote check code does not match the local check code, the determining unit 170 determines that the integrity check for the device 200 has failed.

[0051] The control unit 180 controls all of the components of the verification apparatus 100. The control unit 180 first selects a memory 270 in the device 200 of which the integrity will be checked. If the selected device 200 has the private key shared with the verification apparatus 100, the control unit 180 controls the interface unit 150 so that the interface unit 150 transmits the encoded integrity check parameter to the device 200 that contains the selected memory contents.

[0052] The device 200 includes an authenticating unit 210, a random number generating unit 220, a processing unit 230, a code generating unit 240, an interface unit 250, a CPU 260 and the memory 270.

[0053] The interface unit 250 of the device 200 transmits data to and receives data from the verification apparatus 100. The interface unit 250 transmits the encoded remote check code generated by the code generating unit 240 to the interface unit 150 of the verification apparatus 100 and receives the encoded integrity check parameter used to generate a remote check code from the interface unit 150.

[0054] The authenticating unit 210 receives the random number used to generate the authentication code from the verifying unit 110 of the verification apparatus 100 and generates the encoded private key by applying the second encryption algorithm to the private key and the random number. The authenticating unit 210 applies the first encryption algorithm to the received random number and the shared private key to generate an encoded random number, and then transmits the generated encoded random number to the verification apparatus 100.

[0055] The random number generating unit 220 generates random numbers that will fill the empty areas of the memory 270 in the device 200 using the pre-stored random function.

[0056] The processing unit 230 decodes the encoded integrity check parameter received via the interface unit 250 of

WAVELYNX EX. 1003, Pg. 1179
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the device 200 using the same algorithm as the decoding algorithm used by the determining unit 170 of the verification apparatus 100.

[0057] The code generating unit 240 generates a remote check code using the memory filling map received from the verification apparatus 100 and the random numbers generated by the random number generating unit 220. The code generating unit 240 creates an encoded remote check code by applying the third encryption algorithm that the verification apparatus 100 uses to encode the integrity check parameter to the generated remote check code and the private key shared with the verification apparatus 100 .

[0058] Specifically, the code generating unit 240 fills the empty areas of the memory 270 with the random numbers generated by the random number generating unit 220 based on the received memory filling map, as in the calculating unit 140 of the verification apparatus 100. The code generating unit 240 generates an encoded remote check code by applying the encryption algorithm to the contents of the memory 270 completely filled with the random numbers.

[0059] The CPU 260 controls all the components of the device 200. The CPU 260 stores a MAC generating function used when the code generating unit 240 generates a remote check code and a shared private key. The CPU 260 stores the first and second encryption algorithms that are used when the authenticating unit 210 generates an encoded random number and an encoded shared key. These algorithms are identical to the encryption algorithms used by the verifying unit 110 of the verification apparatus 100. The CPU 260 also stores a decoding algorithm that is identical to the decoding algorithm used when the decoding unit 160 decodes a remote check code.

[0060] FIGS. 3A to 3D illustrate the process of generating a local check code in a system for remotely verifying the integrity of a memory in a device according to an exemplary embodiment of the present invention. FIG. 3A illustrates a random number sequence generated by the random number generating unit 120. FIG. 3B illustrates the contents of the memory 270 in the device 200 of which the integrity will be tested. FIG. 3C illustrates the empty areas of the memory 270 in the device 200 filled with the random numbers, and FIG. 3D illustrates the operation of which the calculating unit 140 generates a local check code.

[0061] Referring to FIG. 3A, the random number generating unit 120 produces a random number sequence using a random function.

[0062] Referring to FIG. 3B, "A" areas indicate the areas of the memory 270 where contents such as software are stored, and "B" areas represent the empty areas of the memory 270.

[0063] Referring to FIG. 3C, the random numbers as shown in FIG. 3A fills the empty areas of the memory 270 in a predetermined manner using the memory filling map that is one of the integrity check parameters received from the verification apparatus 100. FIG. 3C illustrates the operation where the empty spaces of the memory 270 are sequentially filled with the random numbers using the memory filling map.

[0064] Referring to FIG. 3D, the data in the memory of which the empty spaces are completely filled with the random numbers is read in a reverse order, and a local check code is generated using a MAC generating function such as a hash function. This method increases security.

[0065] FIGS. 4A and 4B illustrate a method for remotely verifying the integrity of a memory for a mobile platform according to an exemplary embodiment of the present invention.

[0066] Referring to FIGS. 4A and 4B, in operation S901, it is determined whether the authentication code generated by the device 200 matches the authentication code generated by the verification apparatus 100 in order to determine whether the device 200 shares the private key with the verification apparatus 100. Specifically, the verification apparatus 100 generates an authentication code that is the encoded random number SRAND-1 by applying the first encryption algorithm E1 to the random number RAND and the shared private key K. The verification apparatus 100 also generates an encoded shared private key K1 by applying the second encryption algorithm E2 to the random number RAND and the shared private key K. Here, the encoded shared private key K1 is used to encrypt the integrity check parameter used to generate a remote check code, and also to decode the encoded remote check code.

[0067] The verification apparatus 100 transmits the random number used to generate the authentication code to the device 200. The device 200 creates the authentication code SRAND-2 by applying the first encryption algorithm E1 to the received random number RAND and the shared private key K. The device 200 generates the encoded shared private key K1 by applying the second encryption algorithm E2 to the random number RAND and the shared private key K. The device 200 transmits the generated authentication code SRAND-2 to the verification apparatus 100.

[0068] The verification apparatus 100 compares the generated authentication code SRAND-1 with the authentication code SRAND-2 received from the device 200. If SRAND-1 and SRAND-2 match each other, the verification apparatus 100 concludes that the device 200 has the shared private key K.

[0069] The verification apparatus 100 then fills the empty areas of the memory 270 in the device 200 with the random numbers generated by the random number generating unit 120 based on the pre-stored memory filling map (S903).

[0070] The verification apparatus 100 then generates a local check code that is a MAC for verifying the integrity of the memory 270 (S905). In this case, the verification apparatus 100 reads the contents of the completely filled memory 270 in a reverse order and produces a local check code by applying a MAC generating function, such as a hash function.

[0071] The verification apparatus 100 then transmits, to the device 200, the integrity check parameter used to generate

WAVELYNX EX. 1003, Pg. 1180
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

a remote check code, which is the MAC generated by the device 200 for verifying the integrity of the memory 270 (S907). The integrity check parameter is encrypted using the encoded shared private key and transmitted from the verification apparatus 100 to the device 200. Here, the integrity check parameter includes the memory filling map, the information on the random number used to generate the local check code, etc.

[0072] The device 200 generates a remote check code using the received integrity check parameter and transmits the generated remote check code to the verification apparatus 100 (S909). The device 200 decodes the received encoded integrity check parameter using the shared private key. The device 200 fills the empty areas of the memory 270 in the device with the random numbers based on the memory filling map of the decoded integrity check parameter and generates a remote check code by applying the MAC generating function to the memory contents in a reverse order. The generated remote check code is encoded using the shared private key. Here, the random numbers used to fill the empty areas of the memory 270 are the numbers that the device 200 generates based on the information on the random numbers used to produce the local check code.

[0073] The device 200 then decodes the received encoded remote check code using the encoded shared private key (S911).

[0074] The device 200 then checks whether the local check code matches the decoded remote check code (S913). If the local check code matches the decoded remote check code, the device 200 determines that the integrity check of the memory 270 is successful (S915). If the local check code does not match the decoded remote check code, the device 200 concludes that the integrity check of the memory 270 has failed (S917).

[0075] As described above, it is possible to remotely authenticate the device and check the integrity of the device simultaneously according to an exemplary embodiment of the present invention.

[0076] It is also possible to accurately check the integrity of a device when the device and the verification apparatus have a shared private key by authenticating the device and then comparing the check code generated by the verification apparatus with the check code generated by the device.

[0077] It is also possible to correctly verify the integrity, even when a malicious code, such as virus, changes its position and attacks different parts of the memory, by filling the empty areas of the memory in the device with random numbers and generating a MAC. In addition, it is possible to remotely verify the integrity of the device even during runtime as well as during booting of the device

[0078] The foregoing embodiment and advantages are merely exemplary and are not to be construed as limiting the present invention. The present teaching can be readily applied to other types of apparatuses. Also, the description of the embodiments of the present invention is intended to be illustrative and not to limit the scope of the claims. Many alternatives, modifications and variations will be apparent to those skilled in the art.

Claims

1. A verification apparatus for verifying an integrity of a device that is connected to a network, the verification apparatus comprising:

   a verifying unit arranged to determine whether the device has a shared private key with the verification apparatus by checking whether a first authentication code generated by the verification apparatus matches a second authentication code generated by the device;
   a calculating unit arranged to, when the device has the shared private key with the verification apparatus, fill empty areas of a memory of the device with first random numbers based on a pre-stored memory filling map and generate a local check code that verifies the integrity of the memory;
   an interface unit arranged to transmit, to the device, information on the first authentication code generated by the verification apparatus and an integrity check parameter used to generate a remote check code generated by the device that verifies the integrity of the memory, and receive the second authentication code and the remote check code from the device; and
   a determining unit arranged to verify the integrity of the memory by checking if the local check code matches the remote check code.

2. The apparatus as claimed in claim 1, wherein the verifying unit comprises:

   a generating unit arranged to produce a second random number used to generate the first authentication code; and
   an encoding unit arranged to encrypt the second random number and the shared private key and determine whether the first authentication code generated by the verification apparatus matches the second authentication code generated by the device.

WAVELYNX EX. 1003, Pg. 1181
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

3. The apparatus as claimed in claim 1 or 2, further comprising a storing unit arranged to store contents of the memory in the device, the first random numbers to fill the empty areas of the memory, the memory filling map, the shared private key and a generating function used to generate at least one of the local check code and the remote check code.

4. The apparatus as claimed in any preceding claim, further comprising a random number generating unit arranged to, using a random function, generate the first random numbers to fill the empty areas of the memory.

5. The apparatus as claimed in any preceding claim, wherein the calculating unit arranged to produce the local check code by reading contents of the memory in a reverse order and applying a message authentication code generating function to the contents.

6. The apparatus as claimed in any preceding claim, the verification apparatus further comprising a decoding unit arranged to decode the remote check code encoded by the device by using the shared private key.

7. A device which is connected to the verification apparatus via a network, the device comprising:

an interface unit arranged to receive an integrity check parameter and information on a first authentication code generated by the verification apparatus, and transmit a second authentication code generated by the device and a generated remote check code to the verification apparatus;
an authenticating unit arranged to generate the second authentication code using a second random number and the information on the first authentication code generated by the verification apparatus;
a code generating unit arranged to produce the remote check code using a received integrity check parameter and a message authentication code generating function; and
a central processing unit that stores the message authentication code generating function and a shared private key.

8. The device as claimed in claim 7, wherein the integrity check parameter comprises a memory filling map, and information on the second random number used to generate a local check code.

9. The device as claimed in claim 8, further comprising a random number generating unit arranged to generate the second random number used to produce the remote check code by applying a random function and the information on the second random number used to generate the local check code.

10. The device as claimed in claim 9, wherein the code generating unit generates the remote check code by filling the empty areas of a memory in the device with the generated first random numbers based on the memory filling map, reading contents of the memory in a reverse order and applying the message authentication code generating function to the contents.

11. The device as claimed in any of claims 7 to 10, wherein the device shares the private key with the verification apparatus.

12. An arrangement comprising the apparatus as claimed in any of claims 1 to 6 and the device as claimed in any of claims 7 to 10.

13. A system comprising a device and a verification apparatus which is communicably connected to the device over a network, for remotely verifying an integrity of a memory in the device, the system comprising:

the verification apparatus, arranged to determine whether the device has the shared private key with the verification apparatus by checking whether a second authentication code generated by the device matches a first authentication code generated by the verification apparatus, generate a local check code by filling empty areas of the memory in the device with first random numbers, and verify the integrity of the device by determining whether the local check code matches the remote check code; and
the device, arranged to generate the second authentication code using the information on the first authentication code produced by the verification apparatus and create the remote check code based on the information used to generate the local check code.

14. The system as claimed in claim 13, wherein the verification apparatus comprises the apparatus as claimed in any of claims 1 to 6.

WAVELYNX EX. 1003, Pg. 1182
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

15. The system as claimed in claim 13 or 14, wherein the device comprises the device as claimed in any of claims 7 to 10.

16. The apparatus, device, arrangement or system as claimed in any preceding claim, wherein at least one of said local check code and said remote check code is a message authentication code.

17. A method for verifying the integrity of a device that is connected to a verification apparatus over a network, the method comprising:

determining whether the device has a shared private-key with the verification apparatus by checking whether a first authentication code generated by the verification apparatus matches a second authentication code generated by the device;
when the device has the shared private key with the verification apparatus, filling empty areas of a memory in the device with first random numbers based on a pre-stored memory filling map and generating a local check code that verifies an integrity of the memory;
transmitting, to the device, information on the first authentication code generated by the verification apparatus and an integrity check parameter used to create a remote check code, that verifies the integrity of the memory, and receiving the second authentication code and the remote check code from the device; and
verifying the integrity of the memory by checking if the local check code matches the remote check code.

18. The method as claimed in claim 17, wherein the determining operation comprises:

generating a second random number used to create the second authentication code; and
encoding the second random number and the shared private key and determining whether the first authentication code generated by the verification apparatus matches the second authentication code generated by the device.

19. The method as claimed in claim 17 or 18, further comprising storing contents of the memory in the device, the first random numbers to fill the empty areas of the memory, the memory filling map, the shared private key and a generating function that is used to create at least one of the local check code and the remote check code.

20. The method as claimed in any of claims 17 to 19, further comprising generating the first random numbers to fill the empty areas of the memory using a random function.

21. The method as claimed in any of claims 17 to 20, wherein the generating the local check code comprises:

reading contents of the memory in a reverse order, and generating the local check code by applying a message authentication code generating function to the contents.

22. The method as claimed in any of claims 17 to 21, further comprising decoding the remote check code if the remote check code is encoded using the shared private key.

23. The method as claimed in any of claims 17 to 21, wherein the operation of generating the local check code comprises:

generating the second authentication code using a second random number and the information that the verification apparatus uses to generate the first authentication code;
generating the remote check code using the received integrity check parameter and a message authentication code generating function; and
transmitting the second authentication code generated by the device and the generated remote check code to the verification apparatus.

24. The method as claimed in claim 23, wherein the integrity check parameter comprises the memory filling map and information on the second random number used to generate the local check code.

25. The method as claimed in claim 23 or 24, further comprising generating a second random number used to produce the remote check code by applying a random function and information on the second random number used to generate the local check code.

26. The method as claimed in claim 25, wherein the operation of generating the remote check code comprises filling the empty areas of the memory in the device with the generated first random numbers based on the memory filling

WAVELYNX EX. 1003, Pg. 1183
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

map, reading contents of the memory in a reverse order, applying the message authentication code generating function to the contents and creating the remote check code.

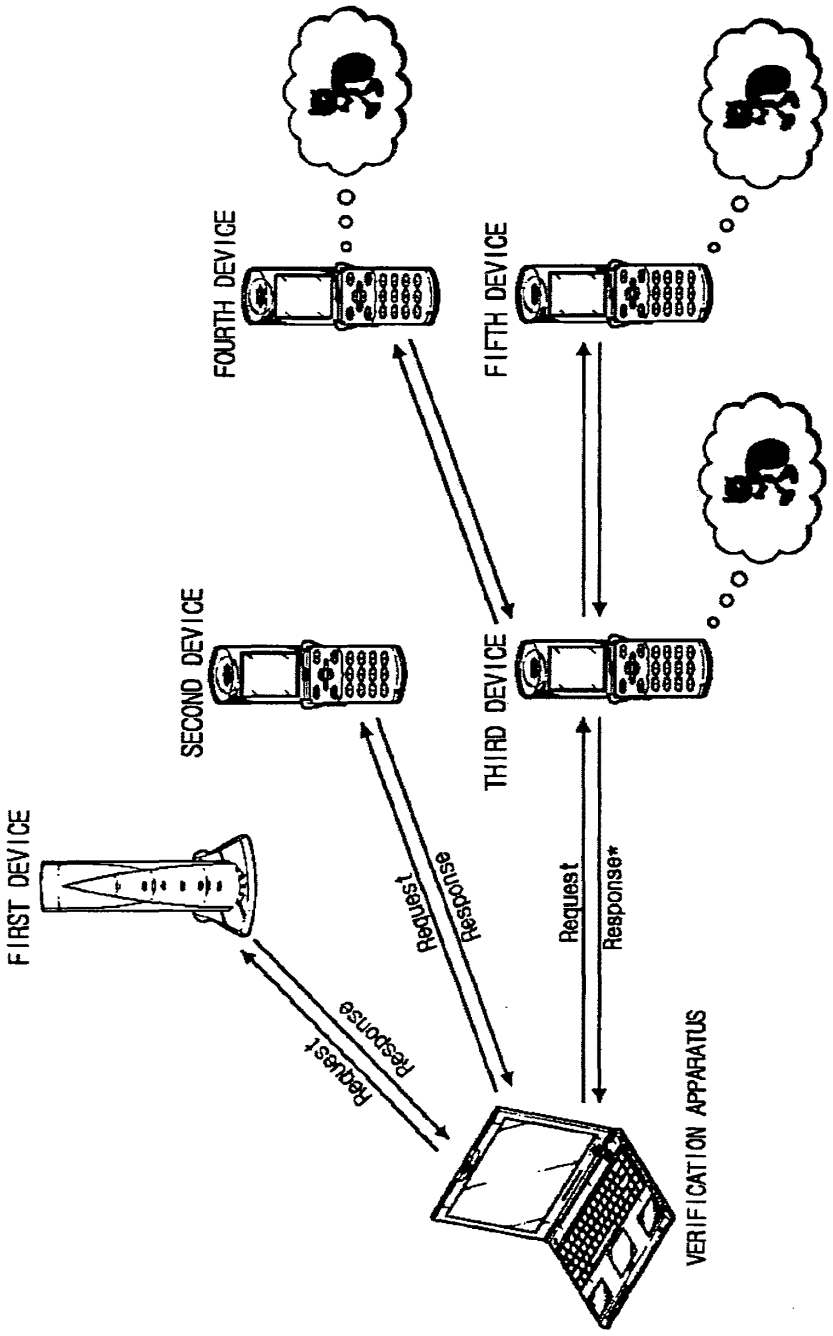
27. A method using a system comprising a device and a verification apparatus communicably connected to the device over a network that remotely verifies the integrity of a memory in the device, the method comprising:

determining whether the device has a private key shared with the verification apparatus by checking whether a first authentication code generated by the device matches a second authentication code generated by the verification apparatus;
the verification apparatus filling empty areas of the memory in the device with first random numbers based on a pre-stored memory filling map and generating a local check code that verifies the integrity of the memory;
the verification apparatus transmitting to the device an integrity check parameter used to generate a remote check code, generated by the device that verifies the integrity of the memory;
the device generating the remote check code using the received integrity check parameter and transmitting the remote check code generated by the device to the verification apparatus; and
verifying the integrity of the memory in the device by checking if the local check code matches the remote check code.

28. The method according to any of claims 17 to 27, wherein at least one of said local check code and said remote check code is a message authentication code.

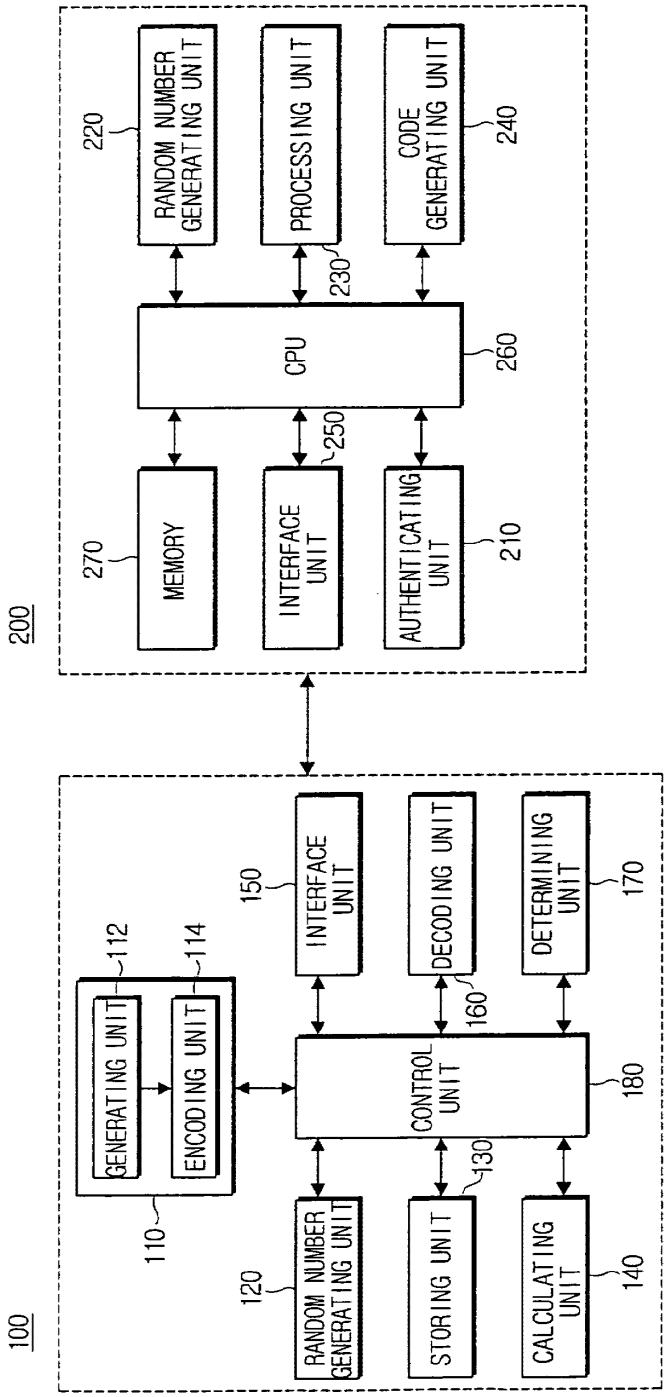
WAVELYNX EX. 1003, Pg. 1184
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 1



WAVELYNX EX. 1003, Pg. 1185
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 2



WAVELYNX EX. 1003, Pg. 1186
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 3A



FIG. 3B

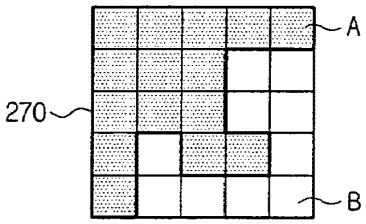


FIG. 3C

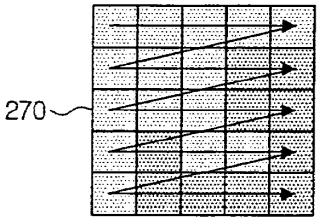
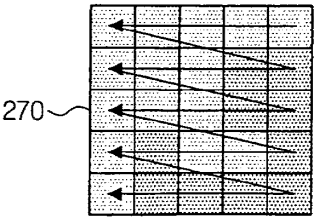
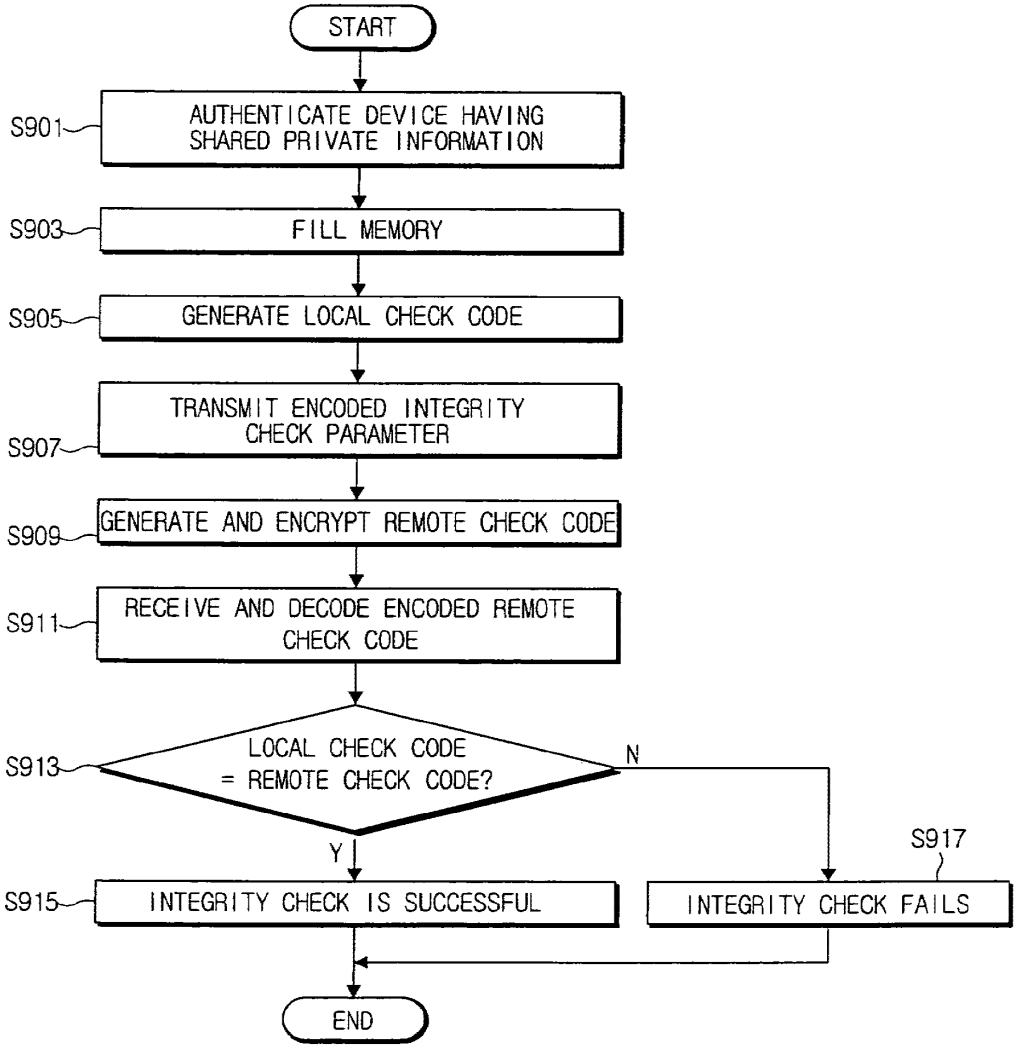


FIG. 3D



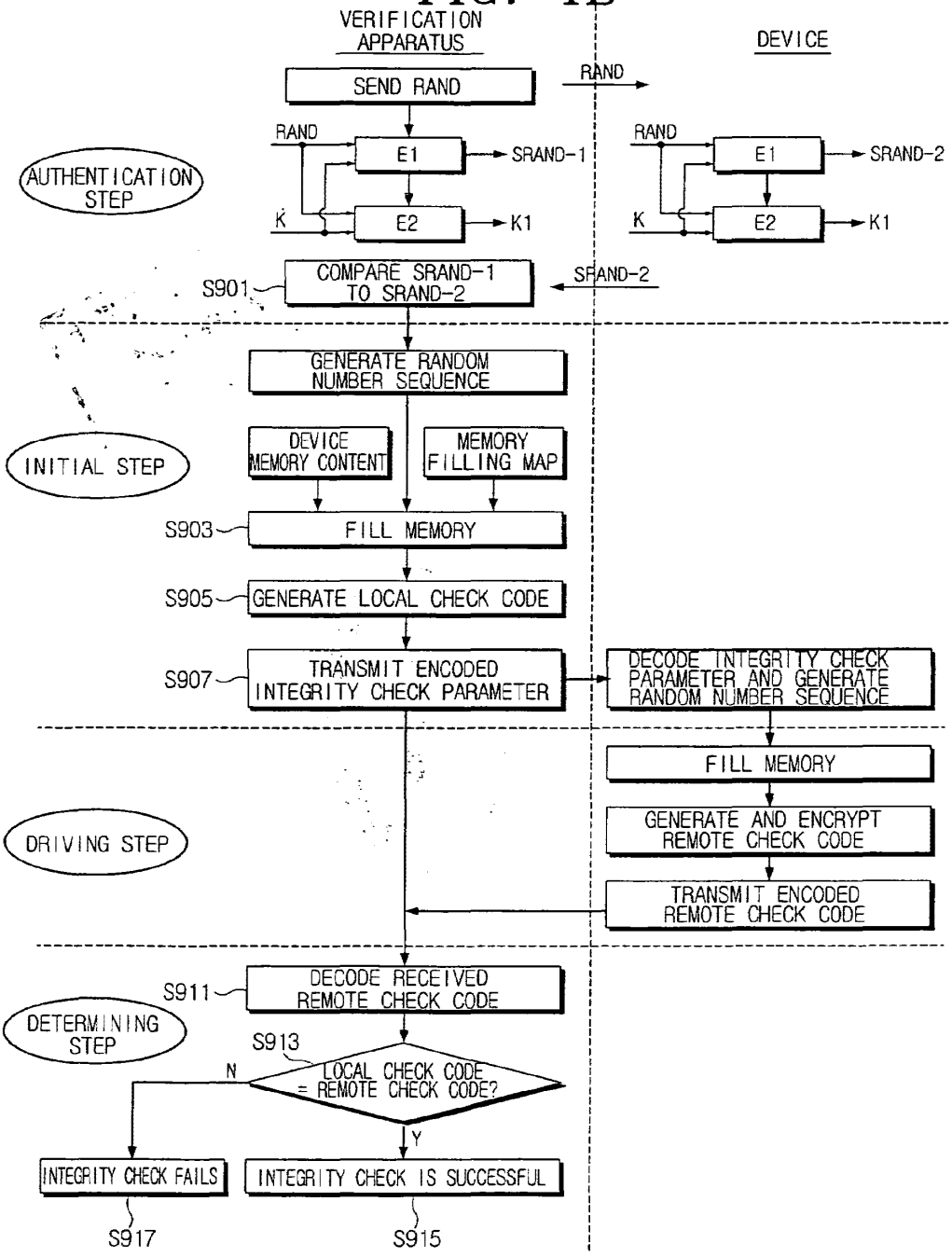
WAVELYNX EX. 1003, Pg. 1187
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 4A



WAVELYNX EX. 1003, Pg. 1188
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 4B



WAVELYNX EX. 1003, Pg. 1189
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 0865

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	SESHADRI A ET AL: "SWATT: SoftWare-based attestation for embedded devices" SECURITY AND PRIVACY, 2004. PROCEEDINGS. 2004 IEEE SYMPOSIUM ON BERKELEY, CA, USA 9-12 MAY 2004, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 9 May 2004 (2004-05-09), pages 272-282, XP010768051 ISBN: 0-7695-2136-3 * page 1 - page 5 * * page 6, left-hand column, last paragraph * * page 9, left-hand column, lines 14-23 *	7,11	INV. G06F21/00 H04L29/06
Y	MENEZES A J ET AL: "Handbook of Applied Cryptography , Chapter 10: Identification and Entity Authentication" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, 1997, pages 385-386,397-403, XP002386305 BOCA RATON, FL, CRC PRESS, US ISBN: 0-8493-8523-7 * page 385 * * page 397, paragraph 10.3 * * page 398 * * page 400, paragraph 10.3.2 - page 402 *	7,11	TECHNICAL FIELDS SEARCHED (IPC) H04L G06F
A	WO 02/065258 A (QUALCOMM INCORPORATED) 22 August 2002 (2002-08-22) * page 9, line 8 - page 11, line 19 *	1-28	
A	WO 02/03175 A (MARCONI COMMUNICATIONS LIMITED; SPARRY, ICARUS, WILLIAM, JOHN; WRAY, S) 10 January 2002 (2002-01-10) * page 2, line 14 - page 3, line 7 * * page 6, line 4 - page 8, line 22 * * page 11, lines 1-16 *	1-28	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	21 June 2006	Ruiz Sanchez, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1190
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 0865

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 02/17048 A (HEWLETT-PACKARD COMPANY; LEE, CALVIN, LAP-KEI; CHEN, LIQUN) 28 February 2002 (2002-02-28) * abstract * * page 10, lines 5-22 * * page 11, lines 21-31 * * page 14, lines 10-13 * * page 15, lines 4-11 * * page 18, lines 12-32 * -----	1-28	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	21 June 2006	Ruiz Sanchez, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1191
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 06 25 0865

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-06-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02065258 A	22-08-2002	AU 2001237019 A1	28-08-2002
WO 0203175 A	10-01-2002	AT 306099 T	15-10-2005
		AU 6622801 A	14-01-2002
		CN 1449515 A	15-10-2003
		DE 60113844 D1	10-11-2005
		DE 60113844 T2	16-03-2006
		EP 1299789 A2	09-04-2003
		GB 2364404 A	23-01-2002
		JP 2004503006 T	29-01-2004
		US 2003159090 A1	21-08-2003
WO 0217048 A	28-02-2002	EP 1352306 A2	15-10-2003
		JP 2004508619 T	18-03-2004
		US 2004243801 A1	02-12-2004

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

WAVELYNX EX. 1003, Pg. 1192
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 760 985 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.03.2007 Bulletin 2007/10

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***G06K 19/10*** *(2006.01)*

(21) Application number: **06119388.4**

(22) Date of filing: **23.08.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **31.08.2005 US 713528**
16.08.2006 US 464912

(71) Applicant: **Assa Abloy Identification Technology Group AB**
107 23 Stockholm (SE)

(72) Inventors:
- **Davis, Michael L.**
AMHERT, NY 14228 (US)
- **Hulusi, Tam**
IRVINE, CA 92618 (US)

(74) Representative: **Grosfillier, Philippe**
Andre Roland S.A.
Intellectual Property Services
Avenue Tissot 15
P.O. Box 1255
1001 Lausanne (CH)

(54) Device authentication using a unidirectional protocol

(57) The present invention is directed toward secure access systems. Specifically, a method and system is provided that allows a control panel (104) of a secure access system to verify the authenticity and fidelity of a reader (112) within the secure access system by utilizing a rolling code agreed upon by the reader and the control panel.

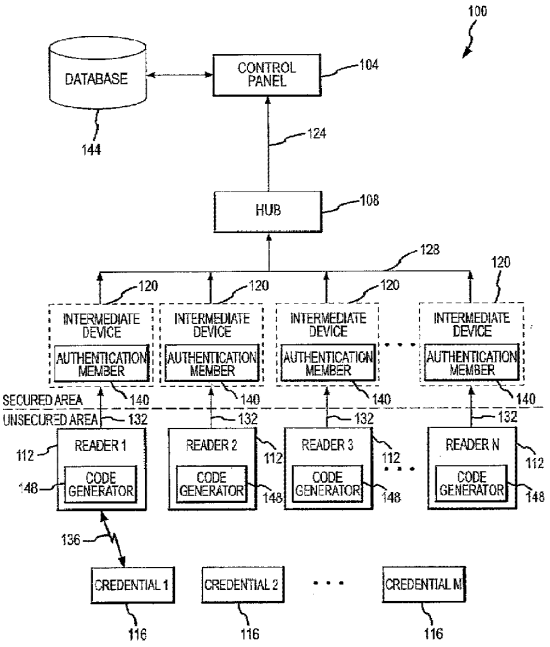


FIG.1

Printed by Jouve, 75001 PARIS (FR)

EP 1 760 985 A2

WAVELYNX EX. 1003, Pg. 1193
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

[0001] This application claims benefit of United States Provisional Patent Application serial number 60/713,528, filed August 31, 2005, which is herein incorporated by this reference in its entirety.

FIELD OF THE INVENTION

[0002] The present invention is generally directed to authentication of a reader in a secure access system. More specifically, the present invention provides a reader signal protocol used to protect and differentiate authorized, authentic readers from non-authorized, non-authentic readers in a secure access system.

BACKGROUND

[0003] Limiting or securing access to designated or sensitive areas is an important issue. As such, there is a current focus on technological systems for controlling access to designated areas in both the private and public venues. Such systems must be made highly impervious to attack by those wishing to gain unauthorized access to the secured area.

[0004] In access control systems, Radio Frequency Identification Devices (RFIDs) or other security credentials are typically used to store data that uniquely identify a holder of the RFID device or the holder's access authorizations. In order to gain access to an asset, such as a building, room, safe, computer, files, information, etc., a holder presents the RFID device to a reader that reads the data and subsequently transmits the data to a panel, processor, or a host system where a decision is made to either grant access to the subject asset or not. There are also readers that combine the functionality of a panel/host and the physical reader into a single unit that makes the access decision. This type of device is sometimes referred to as a stand-alone reader.

[0005] Attention has been focused on the security mechanisms employed by RFID cards to protect and secure the data exchange between the RFID device and the reader. Some of these techniques include the use of cryptography, mutual key authentication, secure channels, and even protection of the chip on the RFID device against physical and electrical attacks. However, little attention has been given to ensuring the integrity of the communications between the reader and its host/control panel as well as insuring the integrity of the reader itself.

[0006] A working assumption thus far has been that RFID device readers are trustworthy devices, when in fact this may not be the case. In many building access control applications, a reader is mounted on the unsecured side of a door in a location that is not under continuous scrutiny. In such a case, compromise of a single reader could result in a compromise of RFID device security if any secret information, such as keys, authorization codes and the like, were somehow extracted from the reader.

[0007] In addition, without knowing the authenticity of the reader an unauthorized or rogue reader could be used to replace an existing legitimate reader in a security system. This rogue reader can actually be any reader or data reply device capable of outputting data in the same format as the replaced reader.

[0008] In the access control industry, one of the most popular communication protocols used between a reader and a panel is the Wiegand protocol. Due to its popularity, the Wiegand protocol has become a de-facto industry standard. It is estimated that the majority of today's access control panels support the Wiegand protocol as the primary method to connect readers to the panel. It should be noted that several companies use their own proprietary communications protocols, but they still support the Wiegand protocol due to its popularity and widespread use. Because of this, a variety of non-RFID machine readable ID readers and other devices have standardized on the Wiegand protocol. Examples of these readers support smart card, proximity, magnetic stripe, bar code, barium ferrite, etc. There are also keypads, biometric devices, wireless Wiegand protocol extenders, protocol converters, and even robots that utilize the Wiegand protocol. The Security Industry Association (SIA) also recognizes the Wiegand protocol as an important standard in the access control industry. The Wiegand protocol has become so important that it has been published as an industry standard.

[0009] The Wiegand protocol is essentially a unidirectional protocol that only provides for data transmission from a reader to an upstream device (*e.g.,* a control panel, host, or processor). Although there is a signal sent back from the upstream device to the reader, this signal is essentially a logic signal used to convey status to a cardholder by controlling a reader's LED. A superset of the Wiegand protocol adds additional logic signals to control an audible device in the reader and provides for additional reader LED colors. These are not bi-directional protocols because substantive data is still sent in only one direction. The host cannot give the reader a command. Only simple signals are sent from the host to the reader.

[0010] As popular as the Wiegand protocol has become, it has shortcomings. Examples of these shortcomings include the fact that the Wiegand protocol is susceptible to electrical noise, has distance limitations, and only allows data to be sent from a reader to an upstream device. Without bidirectional capabilities, it is very difficult to implement a modem protocol that provides for reader authentication.

[0011] Another issues is that the Wiegand protocol allows "party line" connections so that it is very easy to connect one or more additional devices to communication wires to monitor the communications between a card reader and a host in an attempt to harvest data streams to be used to compromise the system. Once a rogue device has been connected to monitor communications between the reader and control panel, an attacker could

WAVELYNX EX. 1003, Pg. 1194
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

merely note when the door has been unlocked and flag the most recent data stream as one that will open the door. Then, whenever illicit entry is desired, the attacker could just "replay" that data stream causing the door to unlock. The attacker need not even remove the device from the communication wires because the Wiegand communications utilize an "open collector" electrical interface, which allows both the monitoring of messages and generation of messages from that same connection.

[0012] There is typically little stopping an attacker from harvesting one or more valid messages to gain illicit entry using different cardholder's data so that no suspicions are aroused. Accessibility to the Wiegand communications wires is increased by the fact that a reader is typically located on the unsecured side of a wall or door and, because of the nature of access control, may be at a location that is not under continuous observation or scrutiny. Making matters worse, many access control readers do not employ a tamper mechanism so that the removal of a reader to access the internal wiring or even to replace the reader with another compromised reader or illicit Wiegand generating device is undetectable.

[0013] There have been some attempts to address the shortcomings of the Wiegand protocol. One example of an extension to the Wiegand protocol is described in U.S. Patent No. 6,988,203 to Davis et al., the contents of which are hereby incorporated herein by this reference. The '203 patent describes appending additional bits to the Wiegand data stream. This provides supplementary information from the reader to the upstream device as well as a CRC or other type of error detection and/or correction bits covering all of the data in the transmission. The '203 patent further describes transmitting data back to the reader from the upstream device via an LED control line.

[0014] Additionally, in PCT Application No. WO 2005/038729 to Merkert, which is herein incorporated by this reference, an access system that includes a signal generator located between a reader and a control panel is described. The reader utilizes a dynamic timing element that ensures a replay attack cannot be used to gain unauthorized access to an asset. The reader stamps any signal sent therefrom with a time stamp indicating when the message was generated. Then the control panel reads the time stamp to ensure that the message is authentic. An attempt to harvest a signal and resubmit that signal again at a later time will result in the control panel determining the signal is invalid. To ensure channel security between system elements, encryption and/or digital signatures are used. Unfortunately, this solution does not overcome most of the Wiegand deficiencies.

[0015] For instance, there is no way in the currently existing solutions that allows the control panel to continually monitor each reader in order to verify the fidelity of each reader. Thus, leaving open the possibility of having a valid reader replaced with a rogue reader without the system or system operator becoming aware of such actions.

SUMMARY

[0016] The present invention is generally directed toward a method, apparatus, and system that allows for authentication of readers in a secure access system. Although well suited for use in an access system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol.

[0017] In accordance with embodiments of the present invention, a method of checking authenticity of devices in a secure access system utilizing a unidirectional communication protocol is provided. The method comprises the steps of reading a credential with a reader, the reader generating a first message that includes credential data associated with the credential and a first code, transmitting the first message to an upstream device, and the upstream device analyzing the credential data in order to determine the authenticity of the credential and further analyzing the first code in order to determine the authenticity of the reader.

[0018] A valid reader employing the above-described method will be able to verify its authenticity to the upstream device by sending a valid code. A reader that is not enabled to generate a valid code may be identified by the upstream device as defective and/or fraudulent. By requiring the reader to send a valid code along with credential data, the upstream device can be confident that the reader is valid and has not been tampered with.

[0019] In accordance with further embodiments of the present invention, a method of maintaining a secure access system that utilizes a unidirectional communication protocol is provided. The method comprises the steps of providing a downstream device that is operable to transmit a valid rolling code as a part of a message and further providing an upstream device that is operable to receive the message and analyze the rolling code. The method can continue by determining a required first time of check in and requiring the downstream device to transmit a first message including a first valid rolling code at a first time related to the required time of check in. The method may then determine a required second time of check in that is after the required first time of check in, and require the downstream device to transmit a second message including a second valid rolling code at a second time related to the required second time of check in.

[0020] By requiring a downstream device to check in with the upstream device at a particular time schedule, the upstream device can continually update the state of the system. In other words, the upstream device can determine fairly quickly, depending on the amount of time between required check in times, whether a downstream device has been tampered with, replaced, and/or is malfunctioning. If the time between required check in messages is very short, like one second or less, it becomes very difficult for an attacker to perform any action that would interrupt communications between the upstream device and the downstream device.

WAVELYNX EX. 1003, Pg. 1195
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0021] In one embodiment of the present invention, certain thresholds may be set at the upstream device that allows for missed messages due to noise or the like. For example, a threshold of N missed messages may be allowed for a particular downstream device. Thus, if a downstream device misses one predetermined check in time, it is not necessarily identified as malfunctioning or having been tampered with. Rather, the downstream device is allowed to miss up to N check-ins, which may or may not be consecutive, before an error determination is made.

[0022] In accordance with other embodiments of the present invention, a secure access system utilizing a unidirectional communication protocol is provided. The system comprises a credential, a reader that is operable to read credential data from the credential upon presentation of the credential to the reader, generate a message including the credential data and rolling code data, and to transmit the message, and an upstream device that is operable to receive the message and upon receiving the message is operable to analyze the credential data in order to determine the authenticity of the credential and to analyze the rolling code data in order to determine the authenticity of the reader.

[0023] In accordance with still further embodiments of the present invention a device adapted for use in a secure access system utilizing a unidirectional communication protocol is provided. The device comprises an input that is adapted to receive a message from a reader, where the message includes a rolling code, an authentication member operable to determine the authenticity of the reader based upon an analysis of the rolling code, and an output operable to transmit the message to an upstream device in response to the authentication member determining the authenticity of the reader is valid.

[0024] The device may be an intermediate device that is used only to monitor the authenticity of readers in a given system. The intermediate device may also be adapted to analyze credential data received from the reader in order to make a determination about the authenticity of a credential that was presented to the reader. The intermediate device may be employed in order to ensure that communications between a rogue reader and a control panel do not occur, thus protecting the control panel from potentially harmful signals. This provides a provision for updating legacy systems with embodiments of the present invention without requiring the replacement of a reader or host.

[0025] These and other advantages will be apparent from the disclosure of the invention(s) contained herein. The above-described embodiments and configurations are neither complete nor exhaustive. As will be appreciated, other embodiments of the invention are possible using, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026]

Fig. 1 is a diagram depicting an exemplary system for authenticating credentials with legitimate readers in accordance with embodiments of the present invention;

Fig. 2 is a block diagram depicting an exemplary reader and control panel utilizing a unidirectional data transfer protocol in accordance with embodiments of the present invention;

Fig. 3 is a flow chart depicting a method of generating a message for transmission to an upstream device in accordance with embodiments of the present invention;

Fig. 4 is a flow chart depicting a method of receiving and processing a message at an upstream device in accordance with embodiments of the present invention;

Fig. 5 is a flow chart depicting a method of transmitting a message in order to verify authenticity of downstream device to an upstream device in accordance with embodiments of the present invention;

Fig. 6 is a flow chart depicting logic within an exemplary upstream device in order to verify the authenticity of downstream devices in a secure access system in accordance with embodiments of the present invention; and

Fig. 7 is a block diagram depicting a data structure that can be used by both the upstream and downstream device in order to maintain a secure access system in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

[0027] The present invention is generally directed toward a reader authentication method, device, and system. The invention advantageously addresses deficiencies of the prior art and may be utilized within the context of access control or security systems, as well as be equally efficiently utilized in a broad range of other applications using a unidirectional communications protocol where interactive computerized data acquisition techniques are used, both contactless or requiring a physical contact with a carrier of pre-programmed information (e.g., monitoring moving objects, tracking inventory, verifying credit cards, and the like).

[0028] Fig. 1 depicts an access network 100 used to verify the identity of at least one credential. In one embodiment of the present invention, the system 100 comprises a control panel 104, a hub 108, a plurality of readers 1121-n, and a plurality of credentials 1161-m such that n and m are integers wherein $n \geq 1$, $m \geq 1$, and typically m is greater than n. The plurality of readers 1121-n may include readers 112 of the same type, as well as readers of different types. For example, a subset of the plurality

WAVELYNX EX. 1003, Pg. 1196
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

of readers 1121-n may be legacy readers (e.g. readers using older transmission protocols). Whereas another subset of the plurality of readers 1121-n may be new readers utilizing more secure protocols including the protocols described herein.

[0029] Additionally, the system 100 may further comprise intermediate devices 120 connected between a reader 112 and the control panel 104. In the depicted embodiment, the readers 112 are coupled to an intermediate device 112 through interface 132. The intermediate devices 120 are coupled to the hub 108 through interface 128 and the hub is coupled to the control panel 104 via interfaces 124. In an alternate embodiment (not shown), the readers 112 may be coupled to the respective inputs/outputs of the control panel 104 without a device, like the hub 108 or intermediate device 120, existing there between. Interfaces 124, 128, and 132 between the readers 112, the intermediate devices 120, the hub 108, and the control panel 104 are generally unidirectional interfaces, which may selectively be implemented in a form of wired, wireless, fiber-optic communication links, or combinations thereof.

[0030] As can be appreciated by one of skill in the art, the interfaces 124, 128, and 132 may be implemented utilizing buses or other types of connections. For example, the I/O ports may be one or more of a USB port, parallel port, serial port, Small Computer Systems Interface (SCSI) port, modem, Ethernet, and/or an RF interface. The protocols used to communicate between the control panel 104 and the readers 112 may include one or more of the TCP/IP protocol, RS 232, RS 485, Current Loop, Power of Ethernet (POE), Bluetooth, ZigBee, GSM, WiFi, and other communication methods and protocols known in the art.

[0031] An exemplary intermediate device 120 comprises an input that is adapted to receive signals via interface 132, an output that is adapted to transmit signals via interface 128, and an authentication member 140. The authentication member 140 is operable to determine the authenticity of one or more readers 112 associated with the intermediate device 120 (*e.g* , determine whether the reader 112 is valid or not), based upon a rolling code that is transmitted from the reader 112 to the intermediate device 120.

[0032] The control panel 104 may be a general-purpose computer adapted for multi-task data processing and suitable for use in a various settings (*e.g.,* commercial, industrial, residential, and the like). A memory of the control panel 104 comprises software program(s) containing a database of records for the system 100. Alternatively, a database 144 may be separated from the control panel 104. The database 144 whether integral to the control panel 104, separate from the control panel 104, or both, maintains records associated with the readers 112, credentials 116 and their respective holders or users, algorithm(s) for acquiring, decoding, verifying, and modifying data contained in the readers 112, algorithm (s) for testing authenticity and validity of the credentials 116, and aigorithm(s) for implementing actions based on the results of these tests. The database 144 may further comprise a list of valid rolling codes and their corresponding required time of check in and/or algorithm(s) for generating valid rolling codes and comparing them with rolling codes received from a downstream device.

[0033] As used herein, in reference to an individual or an object associated with a credential 116, the terms a "holder" and a "user" are used interchangeably.

[0034] Each reader 112 is adapted for exchanging information with the control panel 104 and for requesting data from the credential 116 placed in the active zone of the reader. The reader 112 may also be adapted for processing at least a portion of the data acquired from the credential 116. Alternatively, processing of the acquired data may be performed using the control panel 104 exclusively. In one embodiment, the reader 112 generates signals facilitating execution of the results of interrogating the credential 116 (e.g., engages/disengages a locking mechanism, allows/disallows movement of a monitored article, temporarily disables itself, activates an alarm system, updates a database, and the like). Alternatively, the control panel 104 may generate such signals.

[0035] In accordance with embodiments of the present invention, a stand-alone reader 112 may be utilized to perform the functionality of both the reader 112 and the control panel 104. This stand-alone reader may include, or have access to, the database that contains data used to determine the authenticity of a credential and/or algorithm(s) used to make the determination of authenticity of the credential 116. A determination of authenticity for a credential is made at the receiving point rather than having to transmit data across a network from the reader to a control panel 104 in order to make a determination of authenticity. The stand-alone reader is further operable to execute instructions based upon the analysis of the credential 116.

[0036] Specific configurations of the control panel 104 are determined based on and compliant with computing and interfacing capabilities of the readers 112 and/or the hub 108.

[0037] At least a portion of the plurality of readers 112 further comprise a code generator 148. The code generator 148 is used by the reader 112 to generate a code, possibly a rolling code, in order to verify its authenticity to an upstream device. The code generator 148 may comprise a table, sequence, or data structure of valid rolling codes that the reader 112 can work through as update signals are generated. The code generator 148 may also comprise a code generating algorithm that creates a valid code based on certain criteria.

[0038] Interface 136 represents the communication interface that exists between a reader 112 and a credential 116. Interface 128 may represent an RF communication interface, a biometric communication interface, a keypad, a magnetic communication interface, an optical communication interface, or combinations thereof.

WAVELYNX EX. 1003, Pg. 1197
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0039] In operation a credential 116, for example a credential, is brought into an active zone of the reader 112 in order to establish the communication interface 136. For a credential, a Radio Frequency (RF) communication interface 136 between the reader 112 and the credential is typically automatically established when the credential is brought within an active zone of a reader/interrogator 112. The active zone of an RF reader 112 is defined as a three dimensional space where the intensity of RF signals emitted by the reader 112 exceeds a threshold of sensitivity of the credential and the intensity of RF signals emitted by the credential exceeds a threshold of sensitivity of the reader 112. When a credential is presented to most readers, such a communication interface 136 is established and the reader 112 and credential begin transmitting data back and forth.

[0040] The credential 116 may also be implemented in a number of other machine readable devices including, but not being limited to, contact smart card, a contactless smart card, a proximity card, a magnetic stripe card, a barium ferrite card, a bar code, a Wiegand card, a PDA, a cellular phone and any other type of device used to store and transmit data relating a particular application. The active zone for each type of credential 116 may vary based upon the type of communications used between the reader 112 and the credential 116. For example, a magnetic stripe card is placed in the active zone of the reader 112 when it is swiped through the reader 112. As can be appreciated by one of skill in the art, the interface 128 is created upon presentation of the credential 116 to the reader 112 such that communications between the two is facilitated.

[0041] The reader 112 takes the information that it retrieves from the credential 116 and generates a signal to send to the control panel 104. In generating the signal the reader 112 creates a credential part of the signal and a rolling code part of the signal. The code generator 148 is typically operable to generate the code part of the signal. The credential data relates to the credential that was read (*e.g.,* user name, social security number, title, access permissions, key, password, manufacturer ID, site code, customer code, unique ID, etc.) The code data or rolling code data is a number, letter, dataset, and/or identifier chosen from possibly a list of potential rolling codes. The rolling code sent from a valid reader 112 may possibly be a code previously agreed upon by the control panel 104 and reader 112. The reader 112 and control panel 104 may cycle through and agree upon a number of valid rolling codes as time progresses in order to provide a more secure system.

[0042] Once the control panel 104 receives the signal from the reader 112, the control panel 104 will analyze the credential data from the signal to determine if the credential 116 is authorized to gain access to the asset associated with the reader 112. Additionally, the control panel 104 will analyze the rolling code portion of the signal to determine if the reader 112 is authorized to send commands and has not been tampered with. In an alternative configuration, the signal is sent from the reader 112 to the intermediate device 120 where the rolling code data is analyzed by the authentication member 140 in order to determine if the reader 112 is still valid and has not been tampered with. The intermediate device 120 then forwards the signal on to the control panel 104 for verification of the credential 116. In still a further configuration, the reader 112 generates a signal containing only the credential data and forwards that signal on to the intermediate device 120. The intermediate device 120 then generates rolling code data and incorporates that into the signal from the reader 112. The intermediate device 120 then forwards the signal on to the control panel 104 for verification of the credential and rolling code data. As can be appreciated, any upstream device within the system 100 may perform the verification of the credential data and/or the rolling code data generated by a downstream device. However, it is advantageous to have the reader 112 verified by a device that resides in a secured area rather than an unsecured area so that the device verifying the authenticity of the reader 112 may not be as easily compromised.

[0043] Referring now to Fig. 2 a typical Wiegand protocol reader 112 and control panel 104 will be described. As noted above, the control panel 104 is located in a secure area remote from the Wiegand reader 112. The reader 112 may receive its power from the control panel 104 via the channel 204. The reader 112 is accessible to a user attempting to obtain access to an asset, like the secure area. In order to gain access, a user presents his/her credential (*e.g.,* smart card, RFID tag, magnetic stripe card, bar code card, PDA, cellphone, or the like) to the reader 112. The information received at the reader 112 is transmitted from the reader 112 to the control panel 104 via the data channels 208 and/or 212. The control panel 104 evaluates the information to determine whether the credential is authorized to gain access to an asset associated with reader 112. Depending upon the results of the evaluation, the control panel 104 either performs a valid credential action (*e.g.,* unlocks a door, unlocks a file, turns on a computer, opens a door, *etc.*) or performs an invalid credential action (*e.g.,* no action, denies access, sounds an alarm, notifies security personnel, *etc.*) Additionally the control panel 104 may send a signal to the reader 112 via the data channel 216 to flash a light on/off indicating to the credential holder the results of the evaluation. The communications protocol between the control panel 104 and the reader 112 is typically considered unidirectional because most often substantive data is sent from the reader 112 to the control panel 104 and not from the control panel 104 to the reader 112.

[0044] Referring now to Fig. 3 a method of generating a signal for transmission to an upstream device will be described in accordance with at least some embodiments of the present invention. Initially, the method begins when a credential, like an RFID device, is presented to and read by a reader 112 (step 304). The reader 112 processes the received signal and determines what credential

WAVELYNX EX. 1003, Pg. 1198
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

data is contained therein (step 308). Examples of credential data include, user name, social security number, title, access permissions, key, password, manufacturer ID, site code, customer code, and a unique ID. Once the credential data has been determined, a rolling code is determined and generated by the code generator 148 (step 312). A rolling code is generally selected from a list of rolling codes. After a predetermined amount of time the next rolling code from the list of rolling codes is selected by the reader 112. Alternatively, an algorithm for generating a proper code based upon certain criteria may be used. For example, a choosing algorithm for a rolling code may be created based upon the time of day, the number of credentials previously read at a given reader 112, the number of messages transmitted from the reader to the upstream device, a reader unique ID, reader manufacturer identification number, *etc.* If the reader 112 sends the wrong rolling code, then the control panel 104 will know something is wrong with the reader 112. The reader 112 and control panel 104 generally have their copies of the rolling code (or rolling code selection algorithms) synchronized upon installation. However, as can be appreciated by one of skill in the art, the reader 112 and control panel 104 may have their rolling codes synchronized based upon other known methods.

[0045] Alternatively, a valid rolling code may be generated arbitrarily, as long as the control panel 104 is in synchronization with the reader 112 in determining what the next valid code is in a rolling code sequence. For example, the reader 112 may use a pseudorandom code generator and the control panel 104 may use an exact copy of the generator. The system may be initiated such that each generator determines, creates, and agrees upon the same valid rolling code as each continues to operate properly. For example, the reader 112 and the control panel 104 may use a previously agreed upon sequence or list of valid rolling codes. The control panel 104, at any random time, may change the order in which the code generator 148 goes through the list. The control panel 104 could inform the reader 112 to change how it is working through the list with a prompting signal send via an LED control signal, or may do so through an interruption to the power supply of the reader 112. This ensures that the code generator 148 does not necessarily have to go through a finite list of valid rolling codes in the same order until a new list of codes is provided to the code generator 148. Rather, the same list may be used for a relatively longer amount of time and a higher level of security can be maintained.

[0046] In an alternative embodiment, data received from the credential 116 may dictate what sequence the rolling code should follow. For example, when a first type of credential 116 is read, the reader 112 may use a first rolling code selection algorithm or select a rolling code from a first list of rolling codes. When a second type of credential 116 is read by the reader 112, the reader may change to a different rolling code selection algorithm and/or list of rolling codes. When the reader 112 switches from one rolling code selection algorithm to another, it should indicate to the upstream device that such a switch has been made. Alternatively, the upstream device may recognize that a second type of credential 116 has been read and automatically knows to switch to a different rolling code selection algorithm.

[0047] Of course different algorithms may be used in a similar fashion. The code generator 148 may use a first algorithm to generate valid codes, then upon receiving a prompting signal from an upstream device, like a control panel 104, a different algorithm is used by the code generator 148. Furthermore, data used by the algorithm to compute a valid rolling code may be changed in an analogous way.

[0048] Once the rolling code data and credential data have been determined, the reader 112 generates a message containing both the credential data and rolling code data (step 316). In step 320, it is determined if the signal containing the message is to be encrypted. If the signal is not to be encrypted, then the reader 112 transmits the message (step 332). However, if the message is to be encrypted, then an encryption key is determined (step 324). Thereafter, the message is encrypted using the encryption key (step 328). By encrypting the message, the communications between the reader 112 and the control panel 104 becomes more secure. Even if someone is harvesting signals sent from the reader 112 to the control panel 104, they must know the encryption/decryption key and decrypt the message before any substantive information about the message can be determined. Essentially, the encryption of the message makes it more difficult for an attacker to steal a valid rolling code and valid credential data.

[0049] In step 332, the message, whether encrypted or not, is transmitted. Then, if the rolling code is based upon the number of sent messages from a particular reader 112, the reader increments to the next rolling code in the valid rolling code sequence (step 336). A valid rolling code may depend on the time of day or the amount of time the reader 112 has been operational. In this case, the rolling code is not necessarily updated after a message is transmitted. In one embodiment, a list of valid rolling codes, for example rolling codes A, B, C, D, and E may be used. The reader 112 starts by appending rolling code A to the first message it generates and transmits to the control panel 104. The next rolling code the reader 112 transmits may be rolling code B, then rolling code C and so on. Once the reader 112 has went through the entire list of rolling codes, it may start over by appending rolling code A to the next message it generates. Alternatively, the reader may append rolling code D after it has appended rolling code E and work through the list of rolling codes that way. As long as the reader 112 follows the predetermined rolling code selection protocol, it will continue to generate valid rolling codes. Using a list of a select number of rolling codes provides for an inexpensive implementation of the present invention. However, a persistent attacker may eventually discover the finite

WAVELYNX EX. 1003, Pg. 1199
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

list of rolling codes thus jeopardizing the secure access system 100. In order to create a more secure access system, valid rolling codes may be generated based on predetermined algorithms using previously agreed upon criteria.

[0050] As can be appreciated by one of skill in the art, the reader 112 is not the only device that may be used to generate a signal containing both rolling code data and credential data. If there are other devices present in an unsecured area, those devices may be required to generate rolling code data in order to guarantee their validity, and the validity of devices connected thereto to the control panel 104. These devices may include credentials 116, intermediate devices 120, and/or any other downstream device.

[0051] Referring now to Fig. 4, a method of receiving and processing a signal containing credential and/or rolling code data will be described in accordance with at least some embodiments of the present invention. The method begins when a message is received at an upstream device like a control panel 104 (step 404). The control panel 104 determines if the message has been encrypted, or should have been encrypted at step 408. If the message has been encrypted, then the encryption key is determined (step 412). Using the encryption key, the control panel 104 decrypts the message (step 416). Once the message has been decrypted, or never was encrypted, the reader 112 separates the credential data from the rolling code data (step 420). It is not necessary to separate the credential data from the rolling code data literally. As long as the control panel 104 knows where the credential data ends and the rolling code data starts.

[0052] Once the credential data has been separated from the rolling code data, the control panel 104 compares the received rolling code to the required code. The required code may be maintained at the control panel 104 or in the database 144 separate from the control panel 104. In step 428 it is determined if the received code matches the required rolling code. If the received code does not match the required code, then the control panel 104 determines that a valid reader did not generate the signal or a valid reader has been tampered with. In response to determining that there is a problem with the reader 112, the control panel 104 performs invalid reader logic (step 432). An invalid reader logic action may include, sounding an alarm, notifying security/maintenance personnel that a reader is defective, not opening a door, disabling a reader by discontinuing power supply thereto, and other appropriate actions associated with determining that a reader is not valid and as are dictated by the particular circumstances. However, if the reader 112 was valid and did generate a valid rolling code, the credential data is analyzed in step 436. If the credential data is determined to be invalid, then the control panel 104 performs invalid credential logic (step 440). An invalid credential logic action may include actions similar to invalid reader logic actions. Different actions may be taken by the control panel 104 in response to determining that a credential is invalid including, taking no action and/or controlling an LED on the reader notifying the holder of the credential that access has not been granted. However, if the control panel 104 can verify both the rolling code data and credential data, then the control panel 104 performs valid message logic (step 444). A valid message logic action may include opening/unlocking a door, unlocking a computer, disabling an alarm, *etc.* Then if valid rolling codes are based on a list of rolling codes, the control panel 104 increments to the next valid code in the rolling code sequence (step 448). If the validity of the reader 112 could not be determined in step 428 then the control panel 104 typically does not increment to the next valid code in the rolling code sequence. However, if the reader 112 was valid, but the credential could not be authenticated, then a valid reader 112 will expect to increment to the next code in the rolling code sequence. Because of this, the control panel 104 should also increment to the next code in the rolling code sequence so that the valid reader 112 and control panel 104 continue to agree upon a valid rolling code.

[0053] Referring now to Fig. 5, a method of continually sending an update message from a unidirectional communications protocol device to an upstream device will be described in accordance with at least some embodiments of the present invention. Initially, the downstream device, for example a reader 112, will determine an initial code in the rolling code sequence (step 504). Then the upstream device determines the periodicity with which it needs to receive a valid code from a downstream device, for example a reader 112. Most of these determinations may be made upon installation of the reader 112 or may be based upon other synchronization techniques known in the art. A valid reader 112 is informed of the required check in period and determines how often it needs to transmit a valid code to the upstream device (step 508). The downstream device waits until it is time to send an update signal in step 512. If the required amount of time has not passed since the last update message, the downstream device continues to wait at step 512. Once it becomes time to transmit the message, the downstream device generates and transmits a message to the upstream device (step 516). The transmitted message contains the valid code in the rolling code sequence. The valid code is sent to the upstream device to verify to the upstream device that the downstream device is still operational. Once the downstream device has sent the message containing the valid rolling code, the downstream device updates to the next code in the rolling code sequence (step 520).

[0054] A downstream device may be required to send in an update signal every second or fraction of a second for example. Having such a short period between update signals may preclude an attacker from cutting the connection between the upstream device and the downstream device as any interruption in communication may be discovered due to the high frequency of required updates. However, in order to conserve bandwidth, a lower

WAVELYNX EX. 1003, Pg. 1200
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

frequency of update may be required.

[0055] As noted above a reader 112, intermediate device 120, hub 108, or control panel 104 may be considered an upstream and/or downstream device depending on where it resides in relation to other devices in the system. A first control panel 104 may be connected to a master control panel. The first control panel 104 may be required to update its status to the master control panel in which case the first control panel 104 would be considered the downstream device and the master control panel would be considered the upstream device.

[0056] Referring now to Fig. 6 a method of ensuring that a downstream device is updated and valid will be described in accordance with at least some embodiments of the present invention. Initially, the period with which a downstream device is required to "check-in" is determined (step 604). Then, the number of acceptable missed messages or "check-ins" is determined (step 608). For a more secure system, the number of acceptable missed messages may be set to a very low number, i. e. zero, one, or two. In less secure systems the number of acceptable missed messages may be set higher, giving the system a higher tolerance to missed messages.

[0057] Once the required update rate and number of acceptable missed messages is determined, a variable representing elapsed time is set equal to zero (step 612). During this system initialization a variable representing the number of missed messages is set equal to zero (step 616). Then as time progresses the upstream device waits to receive a signal from a downstream device. When the predetermined amount of time between required updates has passed (step 620), the upstream device determines if it has received a valid rolling code (step 624). The upstream device may require the downstream device to "check-in" right on the required time. Alternatively, a downstream device may only be required to transmit a valid code once every period. In the latter configuration, if a downstream device sends a message in response to reading a credential and appends a valid rolling code with that message, the upstream device may not require another update message from the downstream device during that time span. However, if the upstream device does require the downstream device to transmit a valid rolling code on the required time, even if the downstream device already sent a message with a valid rolling code earlier in the time period, the downstream device will be required to transmit another valid rolling code at the predetermined time or in a predetermined time window.

[0058] If the upstream device does receive a valid rolling code at step 624 for that time period, then the method returns to step 612 and the variable representing elapsed time is set equal to zero. If the upstream device does not receive a valid rolling code (*e.g.* no check-in signal is received or the check-in signal included an invalid rolling code), then the variable representing the number of missed messages is incremented by one (step 628). In step 632, it is determined if the number of missed check-in messages is greater than the acceptable number of missed messages. If the threshold for missed check-in messages has not been realized, then the method returns to step 620 to wait for the next required check in time or time window. If the threshold for missed check-in messages has been exceeded then the upstream device determines that there is a problem with the downstream device, typically a reader, and performs the required steps to notify personnel that the subject downstream device is malfunctioning (step 636).

[0059] Referring now to Fig. 7, a data structure employed by both an upstream device and downstream device will be described in accordance with at least some of the embodiments of the present invention. The data structure may be in the form of a list of valid rolling codes or a rolling code sequence 700. The rolling code sequence 700 comprises a rolling code data field 704 and a required check in time field 708. One copy of the rolling code sequence 700 is maintained in the upstream device that will be determining the authenticity of a downstream device. The rolling code sequence 700 may alternatively be maintained in the database 144 and referenced by the upstream device when analyzing a message that includes a rolling code. In addition to maintaining the rolling code sequence 700 in the upstream device, the rolling code sequence 700 is maintained in the downstream device. This ensures that both the upstream and valid downstream device "agree" on a valid rolling code. The rolling code sequence 700 may be employed in a system 100 that utilizes a unidirectional protocol because substantive data typically cannot be sent from upstream device to the downstream device. Therefore, each device in the system 100 can utilize the rolling code sequence 700 to determine a valid rolling code without engaging in bilateral communications. In the event that a fraudulent reader not having the rolling code sequence 700 attempts to send a message to the upstream device, the upstream device will be able to determine that the downstream device is either fraudulent or malfunctioning.

[0060] The rolling code sequence 700 may comprise up to x rolling codes or rolling code generation variables that are required to be transmitted at a check in time up to k periods after the first check in time, where x and k are typically greater than one.

[0061] Each rolling code in the rolling code data field 704 may be a unique predetermined rolling code. Alternatively, an algorithm may use the data stored in the rolling code data field 704 in order to generate a valid rolling code. The upstream device will expect rolling code A from a downstream device at time T in order to determine the authenticity of the downstream device. Then at a time later than time T, the upstream device will expect rolling code B. Since a valid downstream device will have the rolling code sequence 700, it will know what rolling code to send and when to send it. A fraudulent reader on the other hand will not have access to the rolling code sequence 700 and thus will not be able to send a valid rolling code to the upstream device at the required time. This will result in the upstream device determining that the

WAVELYNX EX. 1003, Pg. 1201
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

downstream device is not valid or is not functioning properly. A valid rolling code generally includes the next rolling code to be sent in the rolling code sequence. As can be appreciated, a less noise sensitive system may be created that identifies more than one rolling code as a valid rolling code. For example, an upstream device may accept the next rolling code up to X more rolling codes in the rolling code sequence. This valid rolling code buffer can be implemented to provide some level of resistance to one or more rolling codes being missed due to noise or other factors.

[0062] In an alternative configuration, a prompt signal may be sent from the upstream device to the downstream device asking for the next valid rolling code in the rolling code sequence 700. The prompting signal may be sent via the LED control signal in the case of the Wiegand protocol. When the prompt signal is received at the downstream device, the next rolling code is chosen in the sequence of rolling codes 700. This particular configuration is beneficial in that a predetermined period of reply does not necessarily need to be employed. Rather, a prompt signal may be sent randomly from an upstream device to a downstream device. In order for the downstream device to prove its authenticity to the upstream device, it should generate a valid rolling code and transmit it back to the upstream device.

[0063] As can be appreciated by one of skill in the art, the relationship of an upstream device and a downstream device is generally defined by the flow of credential information. The downstream device transmits credential information to an upstream device, which may further forward the information to another upstream device or analyze the information to determine an authenticity af the downstream device. Downstream devices are not limited to a reader 112, but rather may include an intermediate device 120, a credential 116, and/or a control panel 104. Moreover, upstream devices are not limited to control panels 104, but also may include a reader 112, an intermediate device 120, and/or a credential 116.

[0064] The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g., for improving performance, achieving ease and\or reducing cost of implementation.

[0065] The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. In the foregoing Detailed Description for example, various features of the invention are grouped together in one or more embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment Thus, the following claims are hereby incorporated into this Detailed Description, with each claim standing on its own as a separate preferred embodiment of the invention.

[0066] Moreover though the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g., as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative embodiments to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

Claims

1. A method of maintaining a secure access system that uses a unidirectional communication protocol, the secure access system comprising at least one credential, at least one reader, and a device upstream of said reader, comprising:

   reading a credential with a reader;
   said reader generating a first message comprising credential data associated with said credential and a first code;
   transmitting said first message to an upstream device; and
   said upstream device, analyzing said credential data in order to determine the authenticity of said credential and further analyzing said first code in order to determine the authenticity of said reader.

2. The method of claim 1, further comprising:

   said reader generating a second message comprising a second code, wherein said second code is different from said first code;
   transmitting said second message to an upstream device; and
   said upstream device analyzing said second code in order to determine the authenticity of said reader.

WAVELYNX EX. 1003, Pg. 1202
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

3. The method of claim 2, wherein said second message is generated a predetermined amount of time after said first message is generated.

4. The method of claim 2, wherein said second message is generated in response to receiving a prompting signal from said upstream device.

5. The method of claim 1, wherein said first message is encrypted by said reader prior to transmitting said first message to said upstream device and decrypted by said upstream device prior to analyzing said first message.

6. The method of claim 1, wherein a code selection algorithm is used to generate said first code.

7. The method of claim 6, wherein said code selection algorithm generates said first code based upon at least one of time of day, total operation time of said reader, a reader unique ID, number of cards read, and a reader manufacturer ID.

8. The method of claim 6, wherein said code selection algorithm generates said first code based upon a number of messages previously transmitted from said reader to said upstream device.

9. The method of claim 1, wherein said first code is a unique code chosen from a rolling code list.

10. The method of claim 9, further comprising:

said upstream device accessing a second list that corresponds to said rolling code list;
said upstream device comparing said first code to one or more valid codes from said second list;
determining that said first code matches a valid code; and
in response to said upstream device determining that said first code matches said valid code, said upstream device determining that the authenticity of said reader is valid.

11. The method of claim 1, wherein said transmitting utilizes a Wiegand protocol.

12. The method of claim 1, wherein said credential is machine readable and comprises at least one of an RFID device, a contact smart card, a contactless smart card, a proximity card, a magnetic stripe card, a barium ferrite card, a bar code, a Wiegand card, a PDA, and a cellular phone.

13. The method of claim 1, wherein credential data is at least one of a user name, a social security number, a title, access permissions, a key, a password, a manufacturer ID, site code, customer code, and a unique ID.

14. The method of claim 1, wherein said upstream device is at least one of a control panel, a host computer, a processor, a database, and an intermediate device.

15. The method of claim 1, wherein said reader comprises a second device that generates the codes.

16. The method of claim 15, wherein said second device is integral with a housing of said reader.

17. A method of maintaining a secure access system that uses a unidirectional communication protocol, comprising:

providing a downstream device associated with at least one interrogator device that is operable to transmit a rolling code as a part of a message;
providing an upstream device that is operable to receive said message and analyze said rolling code;
requiring said downstream device to transmit a first message comprising a first valid rolling code at a first time; and
requiring said downstream device to transmit a second message comprising a second valid rolling code at a second time.

18. The method of claim 17, wherein at least one of said first and second is a window of time in which said downstream device is required to transmit said message.

19. The method of claim 17, wherein at least one of said first and second message is time stamped in order to verify to said upstream device that said at least one of said first and second message was transmitted at their respective required time.

20. The method of claim 17, further comprising, determining a required first and second time of check in.

21. The method of claim 20, wherein at least one of said first and second time is before at least one of said required first and second time of check in.

22. The method of claim 20, wherein at least one of said first and second time related is after at least one of said required first and second time of check in.

23. The method of claim 17, wherein in response to said downstream device not transmitting at least one of said first and second valid rolling codes, determining that said downstream device is at least one of fraudulent and malfunctioning.

WAVELYNX EX. 1003, Pg. 1203
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

24. The method of claim 17, wherein in response to said downstream device not transmitting said first rolling code, determining that said downstream device is at least one of fraudulent and malfunctioning.

25. The method of claim 24, wherein in response to determining that said downstream device is at least one of fraudulent and malfunctioning, performing an invalid reader logic action.

26. The method of claim 25, wherein said invalid reader logic action is at least one of sounding an alarm, notifying security/maintenance personnel that said downstream device is defective, not opening a door, and disabling said downstream device.

27. A secure access system utilizing a unidirectional communication protocol, comprising:

a credential;
a reader that is operable to read credential data from said credential upon presentation of said credential to said reader, generate a message comprising some or all of said credential data and code data, and to transmit said message;
an upstream device that is operable to receive said message and upon receiving said message is operable to analyze said credential data in order to determine the authenticity of said credential and to analyze said code data in order to determine the authenticity of said reader.

28. The system of claim 27, wherein said message is encrypted by said reader prior to transmitting said message to said upstream device and decrypted by said upstream device prior to analyzing said message.

29. The system of claim 28, wherein a key is used to encrypt and decrypt said message.

30. The system of claim 27, wherein the code is a rolling code.

31. The system of claim 30, wherein a code selection algorithm is used to generate said rolling code.

32. The system of claim 31, wherein said code selection algorithm generates said rolling code based upon at least one of time of day, total operation time of said reader, a reader unique ID, and a reader manufacturer ID.

33. The system of claim 31, wherein said code selection algorithm generates said first code based upon the number of messages previously transmitted from said reader to said upstream device.

34. The system of claim 30, wherein said rolling code is a unique code chosen from a rolling code list.

35. The system of claim 34, wherein said upstream device is further operable to access a list corresponding to said rolling code list, compare said rolling code to a valid code from said list, determine that said first code matches said valid code, and in response to determining that said first code matches said valid code, determine that the authenticity of said reader is valid.

36. The system of claim 27, wherein said message is transmitted by said reader utilizing a Wiegand protocol.

37. The system of claim 27, wherein said credential is at least one of an RFID device, magnetic stripe card, bar code, barium ferrite card, and smart card.

38. The system of claim 27, wherein said upstream device is an intermediate device.

39. The system of claim 27, wherein said upstream device is a control panel.

40. A device adapted for use in a secure access system utilizing a unidirectional communication protocol, comprising:

an input adapted to receive messages from a reader, wherein at least a portion of said messages comprise a code;
an authentication member operable to determine the authenticity of said reader based upon an analysis of said code; and
an output operable to transmit said message to an upstream device, wherein said message is transmitted to said upstream device in response to said authentication member determining the authenticity of said reader is valid.

41. The device of claim 40, wherein at least a portion of said messages are encrypted prior to being received at said input, and wherein said authentication member is operable to decrypt said message prior to said analysis of said code.

42. The device of claim 40, wherein said authentication member is further operable to encrypt said message after said analysis of said code and prior to being transmitted at said output.

43. The device of claim 40, wherein said authentication member comprises a valid rolling code sequence and wherein said valid rolling code sequence is used by said authentication member to analyze said code.

WAVELYNX EX. 1003, Pg. 1204
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

44. The device of claim 40, wherein said authentication member transmits a prompting signal to said reader that prompts said reader to generate a message comprising a code.

45. The device of claim 40, wherein said message further comprises credential data that is related to a credential and wherein said authentication member is further operable to determine the authenticity of said credential based on said credential data.

46. A device for use in a secure access system that uses a unidirectional communication protocol, wherein said device is operable to read credential data from a credential, comprising:

a code generator that is operable to generate a first message comprising credential data associated with a credential that is used to determine the authenticity of said credential and a first code that is used to determine the authenticity of said device; and
an output for transmitting said first message to an upstream device.

47. The device of claim 46, wherein said code generator is further operable to generate a second message comprising a second code, wherein said second code is different from said first code.

48. The device of claim 47, wherein said second message is generated a predetermined amount of time after said first message is generated.

49. The device of claim 47, wherein said second message is generated in response to receiving a prompting signal from said upstream device.

50. The device of claim 46, wherein said first message is encrypted by said code generator prior to transmitting said first message to said upstream device.

51. The device of claim 46, wherein said code generator comprises a code selection algorithm.

52. The device of claim 51, wherein said code selection algorithm generates said first code based upon at least one of time of day, total time of operation, a reader unique ID, and a reader manufacturer ID.

53. The device of claim 51, wherein said code selection algorithm generates said first code based upon a number of messages previously transmitted from said device to said upstream device.

54. The device of claim 51, wherein said code selection algorithm changes in response to receiving a prompting signal from said upstream device.

55. The device of claim 46, wherein said code generator comprises a rolling code list.

56. The device of claim 55, wherein said code generator changes how the rolling code list is used in response to receiving a prompting signal from said upstream device.

57. The device of claim 56, wherein said prompting signal is transmitted randomly from said upstream device.

58. The device of claim 46, wherein said upstream device comprises a reader and wherein a credential comprises said code generator.

WAVELYNX EX. 1003, Pg. 1205
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

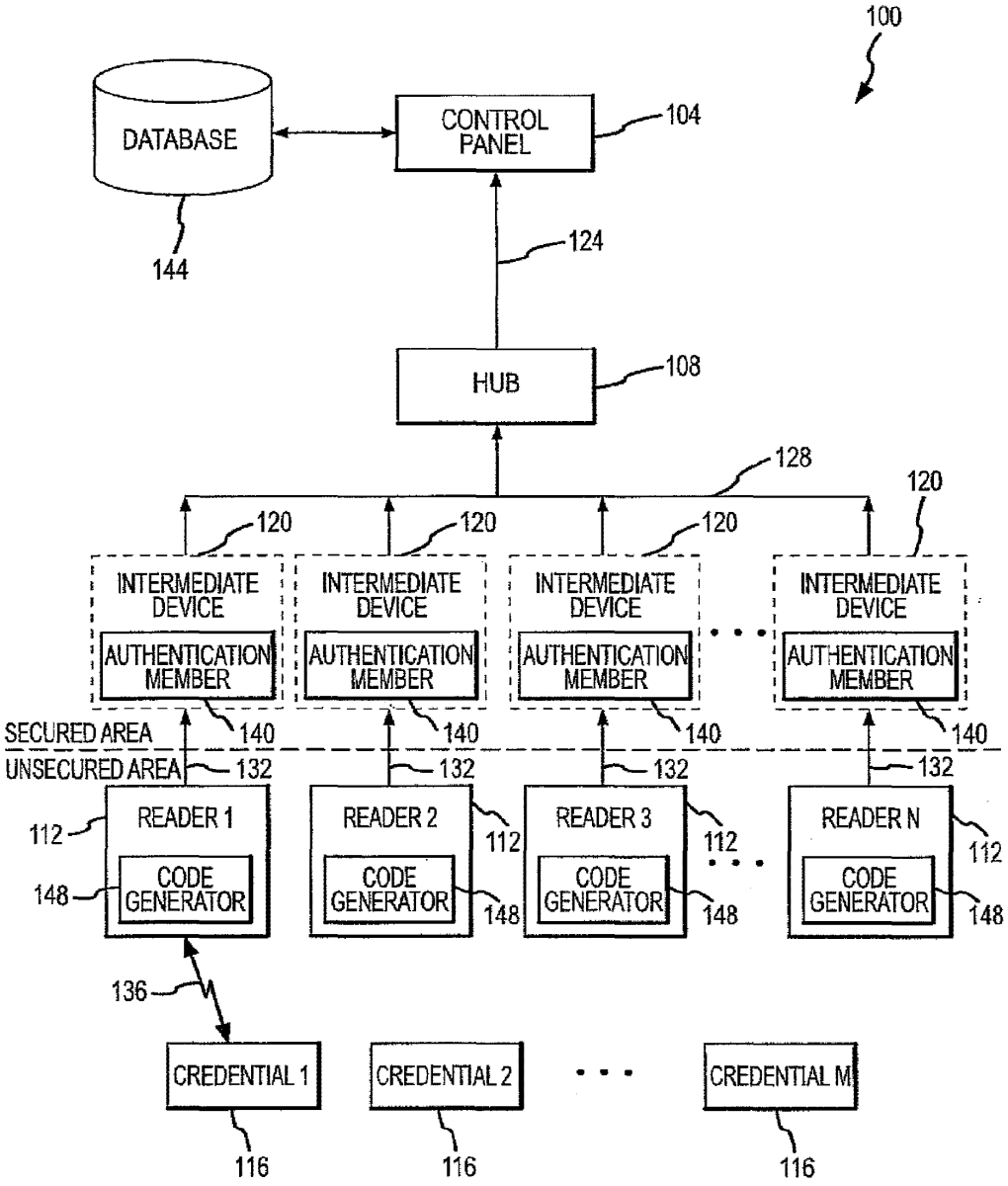


FIG.1

WAVELYNX EX. 1003, Pg. 1206
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

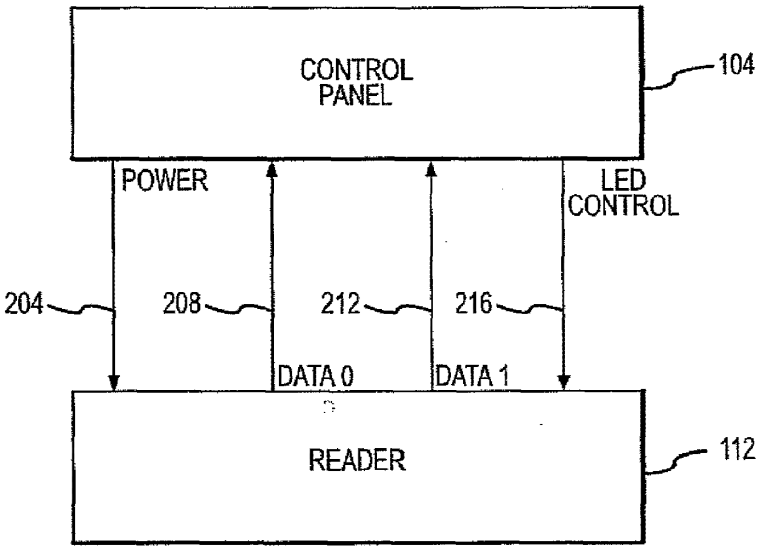


FIG.2
PRIOR ART

WAVELYNX EX. 1003, Pg. 1207
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

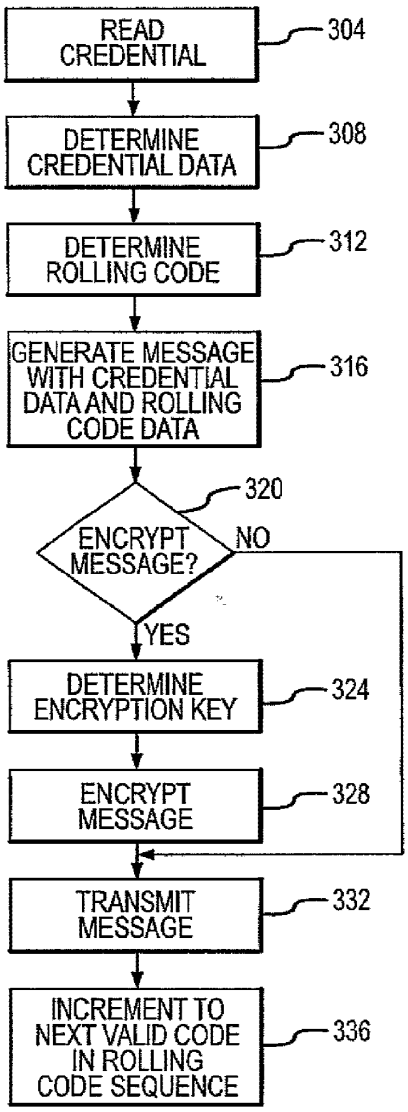


FIG.3

WAVELYNX EX. 1003, Pg. 1208
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

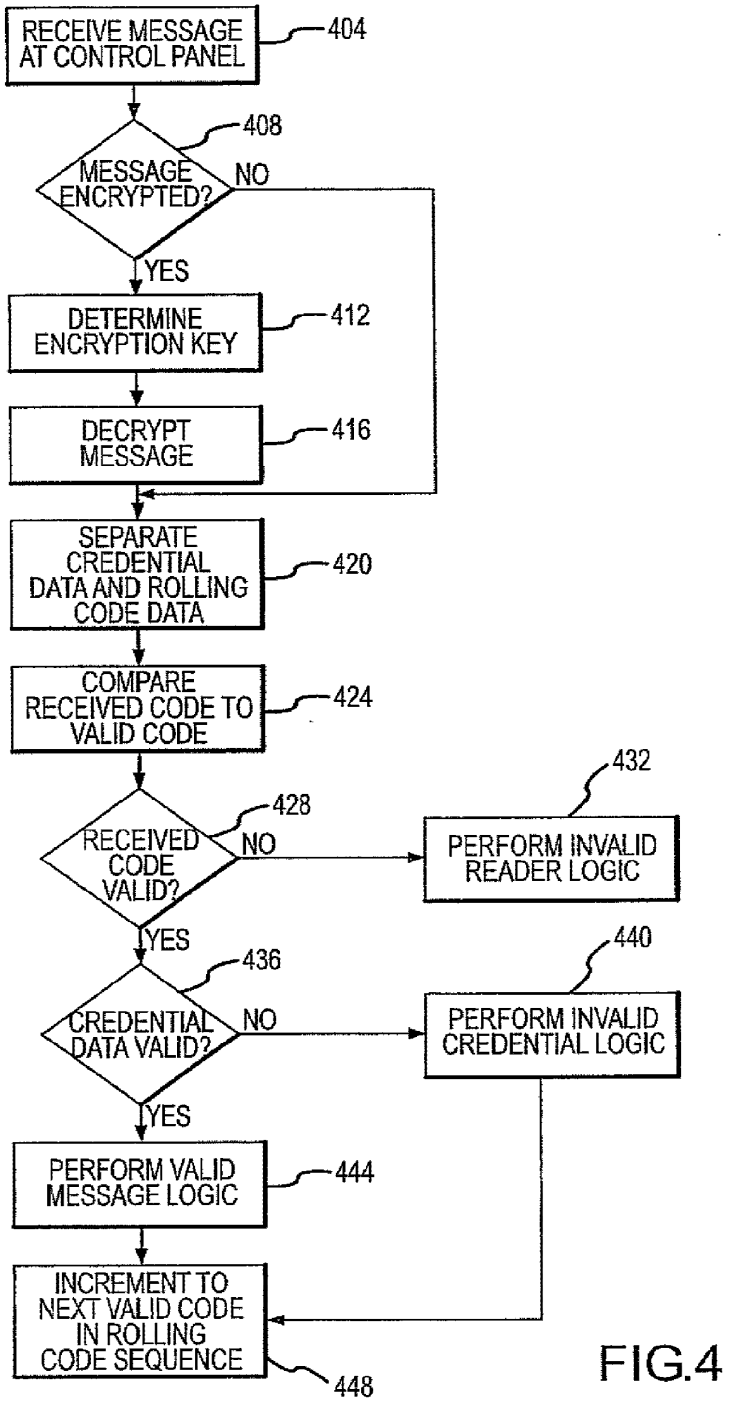


FIG.4

WAVELYNX EX. 1003, Pg. 1209
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

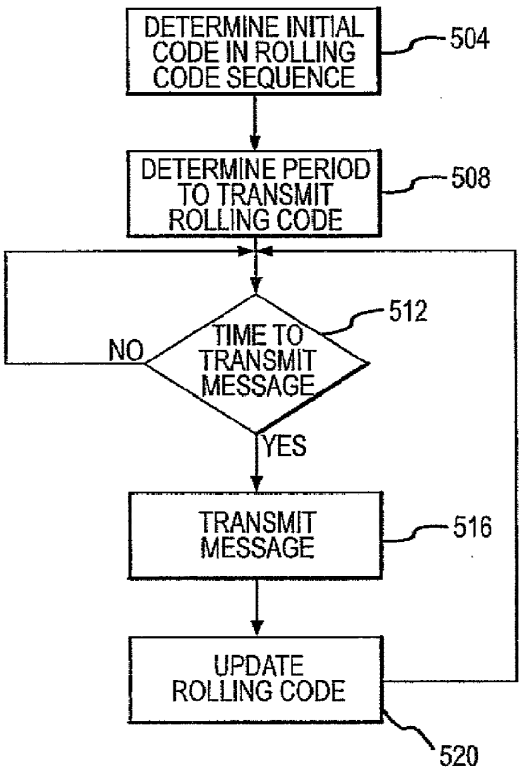


FIG.5

WAVELYNX EX. 1003, Pg. 1210
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

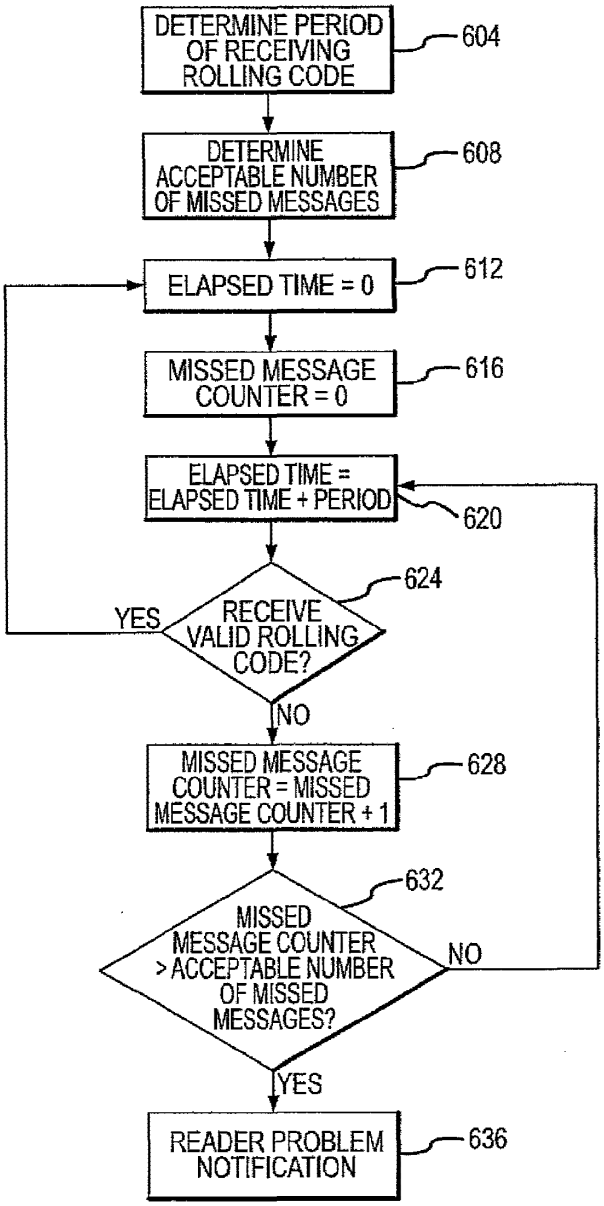
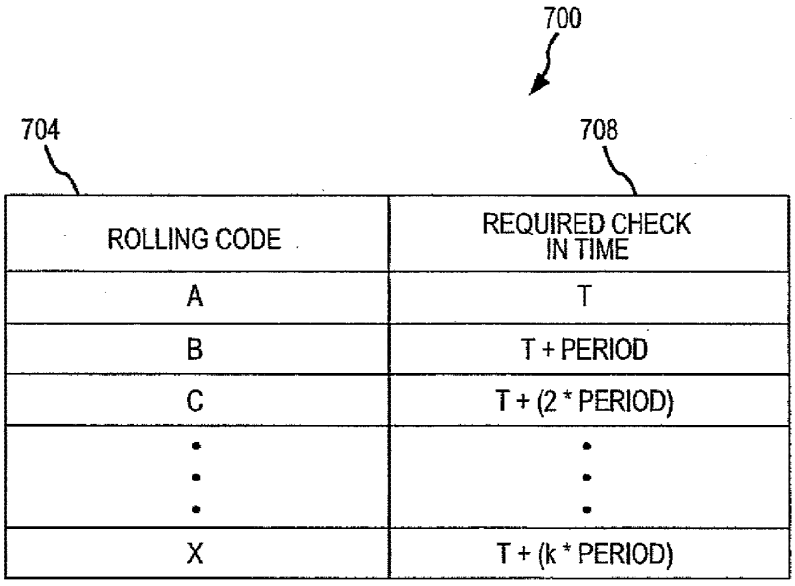


FIG.6

WAVELYNX EX. 1003, Pg. 1211
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



ROLLING CODE	REQUIRED CHECK IN TIME
A	T
B	T + PERIOD
C	T + (2 * PERIOD)
• • •	• • •
X	T + (k * PERIOD)

FIG.7

WAVELYNX EX. 1003, Pg. 1212
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 71352805 P **[0001]**
- US 6988203 B, Davis **[0013]**
- WO 2005038729 A, Merkert **[0014]**

WAVELYNX EX. 1003, Pg. 1213
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Method and circuit for generating a pseudo-random sequence and its use.

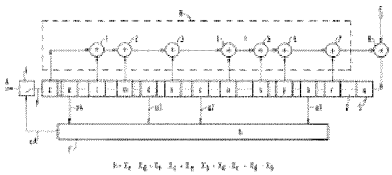
Publication number: EP0616429 (A1)
Publication date: 1994-09-21
Inventor(s): HESS ERWIN DR RER NAT [DE]; SCHRENK HARTMUT DR RER NAT [DE]; EBERHARD GUENTHER DIPL-PHYS [DE]; RUEPPEL RAINER DR [CH] +
Applicant(s): SIEMENS AG [DE] +
Classification:
- international: ***G01R31/3183; G06F7/58; G06F11/27; H03K3/84; H04L9/26;*** **G01R31/28; G06F7/58; G06F11/27; H03K3/00; H04L9/18;** (IPC1-7): H03K3/84; G06F7/58; H04L9/22
- European: G01R31/3183R; G06F11/27; H03K3/84; H04L9/26
Application number: EP19940100237 19940110
Priority number(s): DE19934301279 19930119

Also published as:
EP0616429 (B1)
JP6244684 (A)

Cited documents:
US4202051 (A)
EP0147716 (A2)
US5060265 (A)

Abstract of **EP 0616429 (A1)**

The invention proposes a method and a circuit arrangement for carrying out the method in order to generate a pseudo random sequence of bit data, using a feedback-type shift register device, at least one switching state of the shift register device determining whether the bit data are output. Such a method and a circuit arrangement for carrying out the method are preferably used for encrypting data, particularly for detecting the authenticity of a data carrying arrangement, for example a chip card.



Data supplied from the ***espacenet*** database — Worldwide

WAVELYNX EX. 1003, Pg. 1214
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 616 429 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **94100237.0**

(22) Anmeldetag: **10.01.94**

(51) Int. Cl.[5]: **H03K 3/84**, G06F 7/58, H04L 9/22

(30) Priorität: **19.01.93 DE 4301279**

(43) Veröffentlichungstag der Anmeldung: **21.09.94 Patentblatt 94/38**

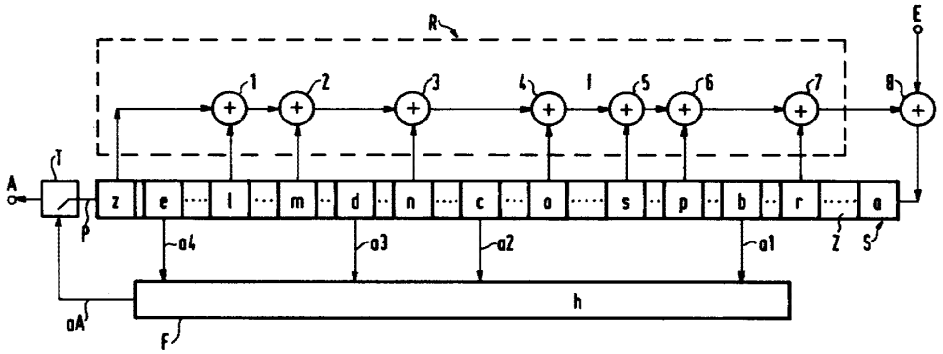
(84) Benannte Vertragsstaaten: **DE FR GB GR IT**

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
D-80333 München (DE)

(72) Erfinder: **Hess, Erwin, Dr. rer. nat.**
Meisenstrasse 18
D-85521 Ottobrunn (DE)
Erfinder: **Schrenk, Hartmut, Dr. rer. nat.**
Fasanenweg 22
D-85540 Haar (DE)
Erfinder: **Eberhard, Günther, Dipl.-Phys.**
Herbststrasse 45
D-82223 Eichenau (DE)
Erfinder: **Rueppel, Rainer, Dr.**
Bahnhofstrasse 242
CH-8623 Wetzikon (CH)

(54) Verfahren und Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge sowie deren Verwendung.

(57) Die Erfindung schlägt ein Verfahren und eine Schaltungsanordnung zur Durchführung des Verfahrens vor, um eine Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung zu erzeugen, wobei mindestens ein Schaltzustand der Schieberegistereinrichtung festlegt, ob eine Ausgabe der Bitdaten erfolgt. Ein solches Verfahren bzw. eine Schaltungsanordnung zur Durchführung des Verfahrens wird bevorzugt zur Verschlüsselung von Daten, insbesondere zur Echtheitserkennung einer Datenträgeranordnung, beispielsweise einer Chipkarte, verwendet.



$$h = X_e \cdot X_d + X_e \cdot X_c + X_e \cdot X_b + X_d \cdot X_c + X_d \cdot X_b$$

EP 0 616 429 A1

WAVELYNX EX. 1003, Pg. 1215
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Die Erfindung betrifft ein Verfahren und eine Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung.

Pseudozufallsfolgen bzw. pseudozufällige Binärfolgen werden vielfach zur Untersuchung von analogen und digitalen Systemen eingesetzt. Darüber hinaus spielen Pseudozufallsfolgen eine bedeutende Rolle bei der Verschlüsselung von Daten.

Es sind zahlreiche Schaltungsanordnungen bekannt, solche Pseudozufallsfolgen von Bitdaten zu erzeugen. In dem Buch Tietze, Schenk "Halbeiter-Schaltungstechnik", 5. Auflage sind auf den Seiten 509 bis 512 Schaltungsanordnungen beschrieben, um solche Pseudozufallsfolgen zu erzeugen. Zur Erzeugung von Pseudozufallsfolgen verwendet man üblicherweise Schieberegister, die in bestimmter Weise rückgekoppelt sind. Die Rückkopplung wird dabei aus Exklusiv-ODER-Schaltungen zusammengesetzt. Die größte nicht periodische Bitfolge, die ein Schieberegister mit n Stufen erzeugen kann, ist $N = 2^n-1$ Bit lang. So kann mit einem vierstufigen Schieberegister beispielsweise eine Pseudozufallsfolge mit einer maximalen Periodenlänge von 15 Bit erzeugt werden. Eine dafür geeignete Schaltung ist in Abbildung 20.23 der genannten Literaturstelle zu sehen.

Beim Verschlüsseln von Daten wird dagegen die rückgekoppelte Schieberegistereinrichtung mit einer Schlüsselinformation, d.h. ein geheimes Datenwort, beaufschlagt. Mit diesem Datenwort wird festgelegt, an welcher Stelle der Pseudozufallsfolge am Ausgang der rückgekoppelten Schieberegistereinrichtung der Datenstrom der Pseudozufallsfolge beginnt.

Befindet sich beispielsweise in einer tragbaren Datenträgeranordnung, wie z.B. einer Chipkarte, und in einer mit dieser zusammenarbeitenden Datenein-/ausgabeeinrichtung jeweils ein gleiches rückgekoppeltes Schieberegister, und ist der gleiche Schlüssel auf beiden Seiten bekannt, so können die von der einen Datenträgeranordnung zur Datenein/ausgabeeinrichtung verschlüsselt gesendeten Daten wieder entschlüsselt bzw. ein zwischen beiden Seiten ausgetauschter Datenstrom gleichermaßen verschlüsselt und die verschlüsselten Daten verglichen werden. Damit ist unter anderem ein Echheitsnachweis der Chipkarte möglich und ein gewisser Schutz vor Fälschungen bzw. Mißbrauch sichergestellt.

Bisherige Verfahren und Konzepte zur Sicherung solcher Datenträgeranordnung verwenden anstelle einer strengen Echtheitsprüfung zur Ausschaltung von Fälschungen und Mißbrauch die Überprüfung eines durch Nachbauten oder Emulationen nur sehr schwer realisierbaren charakteristischen Merkmals. Bekannt ist darüber hinaus auch die Überprüfung der Gültigkeit der gespeicherten Daten über den Zusatz eines mit dem oben bereits erwähnten geheimen Schlüssel in einer Datenträgeranordnung erzeugten Codes für einen Echtheitsnachweis des Dateninhalts.

Problematisch ist bei diesem bekannten Verfahren, daß die Kontrollsignale abgehört bzw. am Ein/Ausgang der Datenträgeranordnung, beispielsweise der Chipkarte, abgegriffen werden können, wodurch ein Wiedereinspielen der Kontrollinformation zur Fälschungszwecken möglich ist.

Bei elektronischen Schaltungen mit Mikroprozessorarchitektur wird dieser Nachteil durch Einsatz eines kryptografischen Authentifikations- oder Identifikationsvorganges nach dem Prinzip der herausfordernden Frage und dazu passenden Antwort (Challenge und Response-Prinzip) bzw. mit Zero-Knowledge-Protokoll ausgeschaltet.

Dieses Challenge-Response-Prinzip sieht beispielsweise bei einer Chipkarte und einer Datenein-/ausgabeeinrichtung zum Lesen dieser Chipkarte vor, daß zunächst die Datenein-/ausgabeeinrichtung Daten "Challenge" generiert und diese zur Chipkarte sendet. Dort dient diese "Challenge" zur Berechnung einer sogenannten "Response". Diese "Response" wird mittels eines Algorithmusses zum Echtheitsnachweis berechnet und hängt zweckmäßigerweise von weiteren Daten, dem geheimen Kartenschlüssel und z.B. einer weiteren Größe, wie einem internen Zählerstand, ab. Die von der Chipkarte zur Datenein-/ausgabeeinrichtung gesendete "Response" wird in der Datenein-/ausgabeeinrichtung mit dort vorliegenden Daten verglichen. Diese dort vorliegenden Daten werden mit dem gleichen Algorithmus, dem gleichen geheimen Kartenschlüssel, der Challenge und der Zusatzinformation berechnet. Stimmt die Response mit dieser Berechnung überein, so ist die Chipkarte als gültig erkannt. Andernfalls erfolgt ein Abbruch der Datenverbindung zwischen Chipkarte und Datenein-/ausgabeinrichtung.

Die eingangs erwähnte rückgekoppelte Schieberegistereinrichtung wird bei diesen bekannten Systemen dazu verwendet, den geheimzuhaltenden Kartenschlüssel in eine längere Pseudozufallsfolge, eine sogenannte Schlüsselstromfolge, zu transformieren. Bei Vorgabe beliebiger Teile der Schlüsselstromfolge muß es einem Angreifer, der den Kartenschlüssel unbefugter Weise berechnen will, unmöglich sein, weitere Teile der Schlüsselstromfolge vorherzusagen. Dies impliziert, daß es ebenfalls unmöglich sein muß, auf den Schlüssel zurückzurechnen. Die bisher bekannten rückgekoppelten Schieberegistereinrichtungen gewähren hierfür bereits einen guten Schutz, sofern die Schieberegistereinrichtung hinreichend lang ist, z.B. 50 hintereinander geschaltete Schieberegisterzellen aufweist. Es besteht jedoch ein Bestreben dahin, diese bekannten Verfahren mit geringstmöglichen Auf-

WAVELYNX EX. 1003, Pg. 1216
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

wand noch besser zu sichern. Hier setzt die Erfindung an.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung sowie eine Schaltungsanordnung zur Durchführung des Verfahrens anzugeben, das gegenüber dem bisher bekannten Verfahren und Schaltungsanordnungen eine höhere Sicherheit aufweist. Darüber hinaus soll eine geeignete Verwendung für dieses Verfahren und diese Schaltungsanordnung aufgezeigt werden.

Diese Aufgabe wird für ein Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung dadurch gelöst, daß mindestens ein Schaltzustand der Schieberegistereinrichtung festlegt, ob eine Ausgabe der Bitdaten erfolgt.

In eine Weiterbildung des erfindungsgemäßen Verfahrens ist es vorgesehen, daß Ausgangssignale einzelner Schieberegisterzellen der Schieberegistereinrichtung einer nichtlinearen logischen Funktion als Eingangsvariable zugeführt werden und ein logisches Ausgangssignal der nichtlinearen logischen Funktion die Ausgabe der Bitdaten steuert.

Die Aufgabe wird für eine Schaltungsanordnung zur Durchführung des Verfahrens dadurch gelöst, daß eine ausgangsseitig eine Schalteinrichtung aufweisende rückgekoppelte Schieberegistereinrichtung mit einer Vielzahl hintereinander geschalteter Schieberegisterzellen vorgesehen ist, und daß eine vorgegebene Anzahl von Schieberegisterzellen ausgangsseitig mit einer eine nichtlineare logische Funktion realisierenden Schaltung verbunden ist, welche ausgangsseitig mit der Schalteinrichtung zu deren Steuerung in Verbindung steht.

In einer vorteilhaften Weiterbildung der erfindungsgemäßen Schaltungsanordnung ist vorgesehen, daß die eine nichtlineare logische Funktion realisierende Schaltung logische UND- und logische ODER-Gatter aufweist. Darüber hinaus kann die Schalteinrichtung selbst ein logisches Gatter, beispielsweise ein UND-Gatter sein, das an einer ersten Eingangsklemme mit einem Ausgang der Schieberegistereinrichtung und mit einer Eingangsklemme mit einer Ausgangsklemme der die nichtlineare logische Funktion realisierenden Schaltung verbunden ist. Am Ausgang dieses UND-Gatters ist dann die Pseudozufallsfolge abgreifbar. Je nachdem, ob die Schalteinrichtung ein- oder ausgeschaltet ist, gelangen demnach die von der rückgekoppelten Schieberegistereinrichtung erzeugten Bitdaten an den Ausgang der erfindungsgemäßen Schaltungsanordnung. So lange die Schalteinrichtung ausgeschaltet ist, gelangen dagegen keine Daten an die Ausgangsklemme der erfindungsgemäßen Schaltungsanordnung. Um eine solche Datenlücke zu vermeiden, kann vorgesehen werden, daß ausgangsseitig an die erfindungsgemäße Schaltungsanordnung ein Zwischenspeicher geschaltet wird, welches mit fortlaufendem Takt ausgelesen wird.

Gemäß der Erfindung wird das Verfahren oder die Schaltungsanordnung zur Verschlüsselung bzw. Entschlüsselung von Daten und/oder in einer Datenträgeranordnung, insbesondere Chipkarten mit integrierten Schaltungsanordnungen, zu deren Echtheitserkennung eingesetzt.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispieles in Zusammenhang mit einer Figur näher erläutert.

Die erfindungsgemäße Schaltungsanordnung sieht eine rückgekoppelte Schieberegistereinrichtung vor, welche eine Vielzahl von hintereinander geschaltete Schieberegisterzellen a...z aufweist. Die eingangsseitige Schieberegisterzelle ist mit dem Bezugszeichen a und die ausgangsseitige Schieberegisterzelle mit dem Bezugszeichen z bezeichnet. Diese hintereinander geschalteten Schieberegisterzellen a...z sind über eine EXOR-Gatter 1 bis 7 enthaltene Rückkopplungsschaltung R rückgekoppelt. Hierfür sind in dem in der Figur 1 gezeigten Ausführungsbeispiel sieben EXOR-Gatter 1 bis 7 in der Rückkopplungseinrichtung R vorgesehen. Diese EXOR-Gatter 1 bis 7 weisen jeweils zwei Eingangsklemmen und eine Ausgangsklemme auf, wobei ein erstes EXOR-Gatter 1 mit einem Ausgangssignal der letzten Schieberegisterzelle z und mit einem Ausgangssignal der Schieberegisterzelle 1 beaufschlagt ist. Die Ausgangsklemme des EXOR-Gatters 1 ist mit einer Eingangsklemme des zweiten EXOR-Gatters 2 in Verbindung, deren andere Eingangsklemme an den Ausgang einer mit m bezeichneten Schieberegisterzelle verbunden ist. In dem in der Figur dargestellten Ausführungsbeispiel sind die weiteren EXOR-Gatter 3, 4, 5, 6 und 7 derart verschaltet, daß dem EXOR-Gatter 3 das Ausgangssignal des EXOR-Gatters 2 und das Ausgangssignal einer Schieberegisterzelle n, dem EXOR-Gatter 4 das Ausgangssignal des EXOR-Gatters 3 und ein Ausgangssignal einer Schieberegisterzelle o, das Ausgangssignal des EXOR-Gatters 4 und ein Ausgangssignal der Schieberegisterzelle s dem EXOR-Gatter 5 zugeführt wird, daß das Ausgangssignal des EXOR-Gatters 5 und ein Ausgangssignal der mit p bezeichneten Schieberegisterzelle dem EXOR-Gatter 6 zugeleitet wird, und dessen Ausgangssignal und ein Ausgangssignal einer Schieberegisterzelle r dem EXOR-Gatter 7 zugeführt wird. Das mit dem Bezugszeichen 8 bezeichnete EXOR-Gatter erhält einerseits das Ausgangssignal des EXOR-Gatter 7 und andererseits ein Eingangssignal E, das unter anderem den geheimzuhaltenden Schlüssel repräsentiert. Ausgangsseitig ist dieses EXOR-Gatter 8 mit einem

WAVELYNX EX. 1003, Pg. 1217
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Eingang der ersten Schieberegisterzelle a der Schieberegistereinrichtung verbunden.

Dieses Eingangssignal E kann beispielsweise aus einer Geheiminformation, einer Zufallszahl als Challenge und gegebenenfalls einer Zusatzinformation (z.B. ein Datenspeicherinhalt) gewonnen werden. Die erfindungsgemäße Schaltungsanordnung ist nicht auf das in der Figur dargestellte EXOR-Gatter 8 beschränkt. Vielmehr kann dieses EXOR-Gatter 8 durch eine beliebige Verknüpfungslogik ersetzt sein.

Erfindungsgemäß ist an den Ausgang der rückgekoppelten Schieberegistereinrichtung eine Schalteinrichtung T geschaltet, die abhängig von einem Steuersignal aA die am Ausgang der letzten Schieberegisterzelle z anstehende Pseudozufallsfolge P von Bitdaten an eine Ausgangsklemme A durchschaltet oder nicht. Das Steuersignal aA wird erfindungsgemäß durch eine eine nichtlineare logische Funktion h realisierende Schaltung F erzeugt, welche in Abhängigkeit eines oder mehrerer Schaltzustände der Schieberegistereinrichtung S festlegt, ob die Schalteinrichtung T die an ihrem Eingang anstehende Pseudozufallsfolge P an die Ausgangsklemme A schaltet oder nicht. Hierfür ist die Schaltung F eingangsseitig mit Ausgängen von vorgegebenen Schieberegisterzellen verbunden. In diesem Ausführungsbeispiel ist angenommen, daß Ausgänge von vier Schieberegisterzellen nämlich der Schieberegisterzellen b, c, d und e über Verbindungsleitungen a1, a2, a3, a4 mit der Schaltung F in Verbindung stehen. Die nichtlineare logische Funktion h besteht beispielsweise aus einer Kombination von UND- und ODER-Gattern folgender Art:

$$h = X_e \cdot X_d + X_e \cdot X_c + X_e \cdot X_b + X_d \cdot X_c + X_d \cdot X_b.$$

Vorzugsweise werden die Abgriffe der die nichtlineare logische Funktion darstellenden Schaltung F an der Schieberegistereinrichtung nicht als nebeneinander liegende Blöcke gewählt. Es empfiehlt sich, diese Abgriffe zufällig und nicht übereinanderliegend zu wählen. Das gleiche gilt für die Rückkopplungsabgriffe zu den EXOR-Gattern 1 bis 7.

Die Arbeitsweise dieser erfindungsgemäßen Schaltungsanordnung ist folgende. Nach einer definierten Voreinstellung des Schieberegisterzustandes wird das Eingangssignal E, welches wie bereits erwähnt aus einer Geheiminformation, einer Zufallszahl und gegebenenfalls einer Zufallsinformation bestehen kann, in die rückgekoppelte Schieberegistereinrichtung S eingegeben. Diese Eingabe wird über eine Verknüpfungslogik, hier das EXOR-Gatter 8 mit der Rückkopplungsinformation am Ausgang des letzten EXOR-Gatters 7 verknüpft. Die Ausgabe eines Datenwortes zur Echtheitserkennung an der Ausgangsklemme A der erfindungsgemäßen Schaltungsanordnung wird durch die nichtlineare logische Funktion h der Schaltung F gesteuert. Diese wird aus der laufenden Pseudozufallsfolge P am Ausgang der letzten Schieberegisterzelle z ausgeblendet. Eine überprüfende Stelle kann dann in Kenntnis der Information E, d.h. also der Geheiminformation, der Zufallszahl und der gegebenenfalls vorhanden Zusatzinformation den gleichen Vorgang nachvollziehen. Bei Gleichheit ist die Echtheit festgestellt.

Die definierte Voreinstellung der Schieberegistereinrichtung S kann beispielsweise mit Unterbrechung der Rückkopplung über die Eingabe des Eingangssignales E, vorzugsweise der Geheiminformation erfolgen. Die Reihenfolge der Eingabe nach einer Voreinstellung kann beliebig erfolgen. Die Sperrung der Ausgabe ist erfindungsgemäß zweckmäßigerweise so gewählt, daß eine für die Sicherheit ausreichende Nichtkorrelation zur Eingabe, insbesondere der Geheimzahl, gewährleistet wird. Vor der Eingabe und/oder zwischen den Eingaben des Eingangssignales E, können mehrere Taktzyklen dazwischengeschaltet werden. Eine längere Taktzyklusphase kann darüber hinaus der eigentlichen an der Ausgangsklemme A anstehenden Pseudozufallsfolge vorgeschaltet werden.

Es hat sich als zweckmäßig erwiesen, die Ausgabe aus dem Schieberegister entsprechend der nichtlinearen Ausgabefunktion in ein Zwischenregister zu schreiben, welches mit fortlaufendem Takt ausgelesen wird. Damit ist der Vorteil ereicht, daß eine kontinuierliche Datenfolge am Ausgang der erfindungsgemäßen Schaltungsanordnung abgreifbar ist, ohne daß die sonst bei der erfindungsgemäßen Schaltungsanordnung zwangsweise sich ergebenden Datenlücken auftreten. Darüber hinaus kann die Echtheitsprüfung nach jeder Änderung des Zustandes der zu überprüfenden Schaltung wiederholt werden. Im übrigen kann die Echtheitsprüfung zwischen zwei Schaltungen gegenseitig durch Austausch entsprechender Pseudozufallsfolgen vorgesehen werden.

Mit der erfindungsgemäßen Schaltungsanordnung und dem erfindungsgemäßen Verfahren ist es also möglich, mit Hilfe der rückgekoppelten Schieberegistereinrichtung und der nichtlinearen Verknüpfungsfunktion h eine Datenfolge zu erzeugen, die aus der Pseudozufallsfolge P am Ausgang der letzten Schieberegisterzelle z der Schieberegistereinrichtung S mit Hilfe der nichtlinearen Verknüpfungsfunktion h eine weitere Zahlenfolge durch Auswahl abgeleitet wird. Für die so erzeugte Folge muß über die Wahl der Rückkopplungsfunktion und der nichtlinearen Verknüpfungsfunktion erfindungsgemäß sichergestellt sein, daß eine Voraussagbarkeit des Signales an der Ausgangsklemme A nach praktischem Ermessen unmöglich wird.

WAVELYNX EX. 1003, Pg. 1218
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Patentansprüche

1. Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung (R, S),
dadurch gekennzeichnet, daß mindestens ein Schaltzustand der Schieberegistereinrichtung (S, R) festlegt, ob eine Ausgabe der Bitdaten erfolgt.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß Ausgangssignale (a1, a2, a3, a4) einzelner Schieberegisterzellen (b, c, d, e) der Schieberegistereinrichtung (S, R) einer nichtlinearen logischen Funktion (h) als Eingangsvariable zugeführt werden und ein logisches Ausgangssignal (aA) der nichtlinearen Funktion (h) die Ausgabe der Bitdaten steuert.

3. Schaltungsanordnung zur Durchführung des Verfahrens nach Anspruch 1 oder 2,
dadurch gekennzeichnet, daß eine ausgangsseitig eine Schalteinrichtung (T) aufweisende rückgekoppelte Schieberegistereinrichtung (S, R) eine Vielzahl hintereinander geschalteter Schieberegisterzellen (a...z) enthält, und daß vorgegebene Schieberegisterzellen (b, c, d, e) ausgangsseitig mit einer eine nichtlineare logische Funktion (h) realisierende Schaltung (F) verbunden ist, welche ausgangsseitig mit der Schalteinrichtung (T) zu deren Steuerung in Verbindung steht.

4. Schaltungsanordnung nach Anspruch 3,
dadurch gekennzeichnet, daß die eine nichtlineare logische Funktion (h) realisierende Schaltung logische UND- und logische ODER-Gatter aufweist.

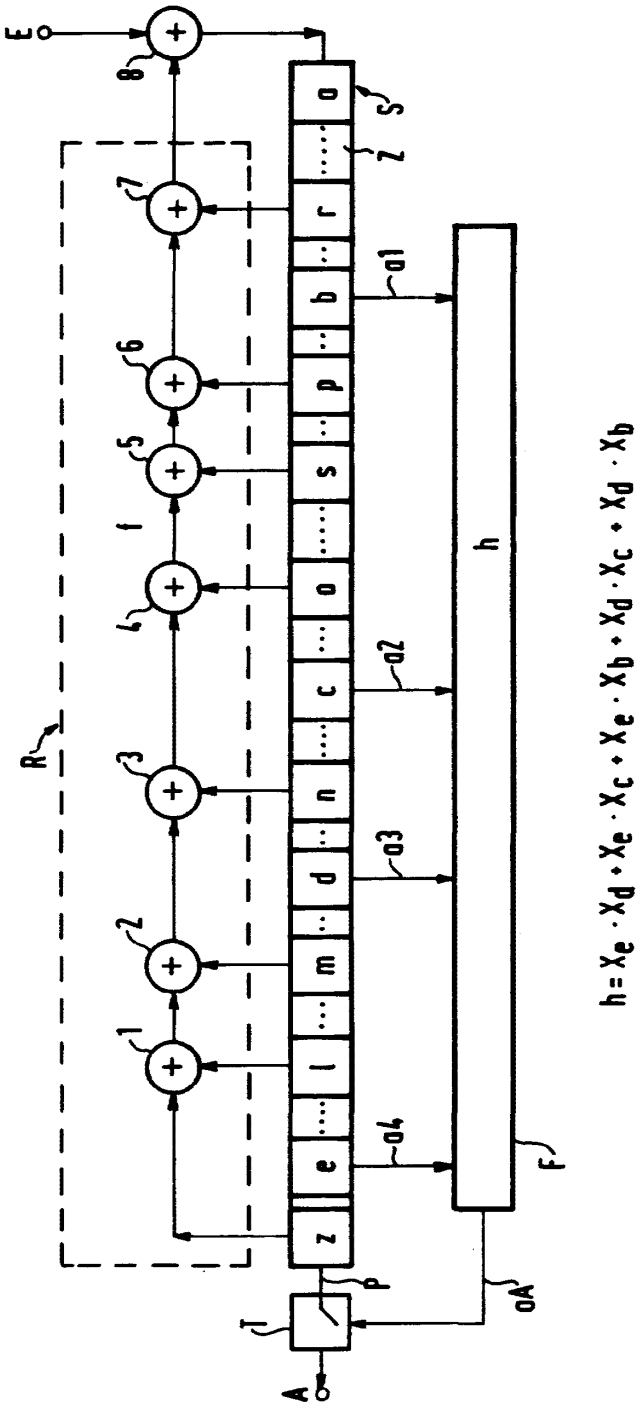
5. Schaltungsanordnung nach Anspruch 3 oder 4,
dadurch gekennzeichnet, daß die Schalteinrichtung (T) ein Logikgatter ist.

6. Schaltungsanordnung nach einem der Ansprüche 3 bis 5,
dadurch gekennzeichnet, daß an die Schalteinrichtung (T) ausgangsseitig eine Puffereinrichtung zum kontinuierlichen Ausgeben der Pseudozufallsfolge mit Daten vorgesehen ist.

7. Verwendung des Verfahrens nach Anspruch 1 oder 2 oder der Schaltungsanordnung nach einem der Ansprüche 3 bis 6 in einer Datenträgeranordnung, insbesondere einer Chipkarte mit einer integrierten Schaltungsanordnung, zur Echheitserkennung.

8. Verwendung des Verfahrens nach Anspruch 1 oder 2 oder der Schaltungsanordnung nach einem der Ansprüche 3 bis 6 zum Verschlüsseln und/oder von Daten.

WAVELYNX EX. 1003, Pg. 1219
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



WAVELYNX EX. 1003, Pg. 1220
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 94 10 0237

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.5)
A	US-A-4 202 051 (G. I. DAVIDA ET AL.) * das ganze Dokument * ---	1,3,8	H03K3/84 G06F7/58 H04L9/22
A	ADVANCES IN CRYPTOLOGY - AUSCRYPT '90, INTERNATIONAL CONFERENCE ON CRYPTOLOGY. PROCEEDINGS, SYDNEY, NSW, AU, 8-11 JAN. 1990 Seite 32-36 GONG GUANG: 'Nonlinear generators of binary sequences with controllable complexity and double key' * Abbildung 1 * ---	1,3	
A	EP-A-0 147 716 (ANT NACHRICHTENTECHNIK GMBH) * das ganze Dokument * -----	1,3,8	

RECHERCHIERTE SACHGEBIETE (Int.Cl.5)

H03K
H04L
G06F
G06K
G07F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
BERLIN	5. Mai 1994	Arendt, M

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 843 438 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.05.1998 Bulletin 1998/21

(51) Int Cl.[6]: **H04L 9/32**, H04N 7/167

(21) Application number: **97402542.1**

(22) Date of filing: **27.10.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **13.11.1996 FR 9613822**

(71) Applicant: **THOMSON multimedia**
92648 Boulogne Cédex (FR)

(72) Inventors:
- **Campinos, Arnaldo**
  92648 Boulogne Cedex (FR)
- **Fischer, Jean-Bernard**
  92648 Boulogne Cedex (FR)

(74) Representative: **Ruellan-Lemonnier, Brigitte et al**
THOMSON multimedia,
46 quai A. Le Gallo
92648 Boulogne Cédex (FR)

(54) Process for protecting an information item transmitted from a security element to a decoder and protection system using such a process

(57) The invention relates to a process for protecting an information item transmitted from a security element to a decoder and a protection system using such a process.

The information item is protected by encrypting within the security element the information item to be transmitted to the decoder and by decrypting this information item within the decoder.

The invention applies to conditional-access systems.

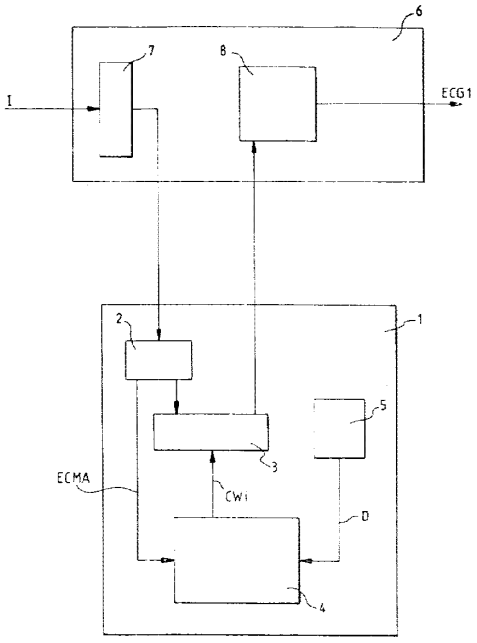


FIG.1

Printed by Jouve, 75001 PARIS (FR)

EP 0 843 438 A2

WAVELYNX EX. 1003, Pg. 1222
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

The invention relates to a process for protecting an information item transmitted from a security element such as, for example, a user-card of a conditional-access system, to a decoder.

The invention applies more particularly to conditional-access systems for which the descrambling operation is performed in the security element which is then, for example, a PCMCIA type card complying with the interface standard known by those skilled in the art as "CENELEC/DVB- Common Interface" or a chip card complying with the American NRSS standard (standing for "National Renewable Security System").

The invention applies to any type of conditional-access system, whether this system be of the on-line type or the standalone type.

In an on-line conditional-access system, the scrambled information item is an information item consisting of a signal distributed simultaneously to various users.

In a standalone conditional-access system, the scrambled information item is contained on standalone information media such as, for example, compact discs or digital video discs.

The information item making up the various programmes originating from the issuing source, such as, for example, a service provider, is transmitted to the security element. The security element descrambles the programme selected by the user (provided that the user's entitlements are present in the security element) and sends this programme, as well as the other programmes which have remained unchanged, to the decoder.

Such a process has the drawback that the programme selected by the user is transmitted unenciphered.

Such a transmission can readily be exploited by a pirate who can use it to distribute the pirated programme illegally.

Figure 1 represents the schematic of a security element/decoder assembly according to the prior art.

The system of Figure 1 comprises an information source I, a decoder 6 and a security element 1.

The decoder comprises a demodulation device 7 and a demultiplexing and decoding device 8.

The security element 1 contains a filtering device 2, a descrambling device 3, an access control device 4 and a user entitlement storage device 5.

The information item I issued by the issuing source contains one or more multiplexed programmes, for example, according to the MPEG-2 transport standard (standing for "Moving Picture Expert Group").

As is known to those skilled in the art, the programmes output by the issuing source are scrambled programmes. The information item I contains, in messages which will hereafter be denoted ECM, the encrypted control words allowing, after decryption, the descrambling of the scrambled programmes.

After the decoder receives the information item I, the latter is demodulated by the device 7 and then transmitted in full to the security element 1. The latter filters, with the aid of the device 2, the ECMs (denoted ECMA in Figure 1) corresponding to the programme selected by the user and transmits them to the device 4 for processing. The non-filtered part of the information item is transmitted without modification to the descrambler 3. The device 4 carries out the conventional functions for processing the ECMs, and, in particular, decrypts the control words CWi which they contain, provided that the entitlements D necessary for descrambling the selected programme and output by the device 5 are applied to the device 4.

The control words CWi are subsequently transmitted to the descrambling device 3 which uses them to descramble the programme selected by the user. The information item output by the descrambler 3 is transmitted to the demultiplexing and decoding device 8 so as to generate the usable, i.e., for example, displayable in the case of a film, information item ECG1.

The invention does not have this drawback.

The invention relates to a process making it possible to transfer from a security element to a decoder a stream of data arising from a descrambler included within the security element. The process comprises a first step making it possible to encrypt, in the security element, the information item arising from the descrambler under the action of a first encryption key and a second step making it possible to decrypt, in the decoder, the encrypted information item arising from the first step, under the action of a second encryption key.

The invention also relates to a security element containing a descrambler making it possible to descramble the information item which it receives under the action of control words. The security element comprises a device for encrypting the descrambled information item arising from the descrambler under the action of a first encryption key.

The invention also relates to a decoder making it possible to decode data arising from a security element, the said data representing at least one programme selected by a conditional-access system user. The decoder comprises a decryption device making it possible to decrypt, under the action of a second key, the data arising from the security element, the said data being data which are descrambled and encrypted under the action of a first key.

The invention further relates to an assembly made up of a security element and of a decoder. The security element is a security element according to the invention such as that mentioned above and the decoder is a decoder according to the invention such as that mentioned above.

As has been mentioned earlier, an advantage of the invention consists in protecting the transmission of the programme selected by the user from the security element to the decoder.

WAVELYNX EX. 1003, Pg. 1223
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Other characteristics and advantages of the invention will emerge on reading embodiments of the invention given with reference to the appended figures in which:

- Figure 1 represents the schematic of a security element/decoder assembly according to the prior art;
- Figure 2 represents the schematic of a security element/decoder assembly according to a first embodiment of the invention;
- Figure 3 represents the schematic of a security element/decoder assembly according to a second embodiment of the invention;
- Figure 4 represents the schematic of a security element/decoder assembly according to a third embodiment of the invention.

In all the figures, the same labels denote the same elements.

Figure 2 represents the schematic of a security element/decoder assembly according to a first embodiment of the invention.

In addition to the elements described in Figure 1, the decoder 6 comprises a decryption device 9 and the security element 1 comprises an encryption device 10. The programme selected by the user is encrypted by the device 10 using an encryption key K. Conversely, the device 9 decrypts the programme with the help of the same key K. Advantageously, this avoids having transmission of the programme unenciphered between the security element and the decoder.

According to the invention, the encryption and decryption key K can be common to all the security element/decoder pairs, but can also be specific to each pair or group of security element/decoder pairs. Advantageously, the production of pirate clones of security elements is thereby impaired.

Thus, this technique forces pirates to customize each of their clones on the basis of the decoder to which they are connected. This has the consequence of complicating their task and hence of reducing the rewards which they may derive from piracy.

According to a particular implementation of the embodiment of Figure 2, a public key algorithm can be used for the devices 9 and 10. In this case, the encryption key is different from the decryption key and, in a preferred manner, the secret key is used for encryption in the security element while the public key is used for decryption in the decoder.

According to this first embodiment of the invention, the key K is a key stored permanently both in the security element and in the decoder.

Figure 3 represents the schematic of a security element/decoder assembly according to a second embodiment of the invention.

In addition to the elements described in Figure 2, the decoder comprises a device 11 for generating a random number or random words AL and a device 12 for generating decryption keys and the security element comprises a device for generating encryption keys 13.

Instead of using a fixed key K, as in Figure 2, the encryption and decryption keys are here generated dynamically. To do this, the decoder 6 generates a random number AL by way of the device 11 and transmits it to the device 13 of the security element. Moreover, the device 11 transmits the random number to the device 12. The latter encrypts the random number AL under the action of a key K1 so as to give the decryption key K. In the same way, the device 13 of the security element encrypts the random number under the action of a key K1 and produces the encryption key K.

According to a particular embodiment of the invention, described in Figure 3, the encryption algorithm used by the devices 12 and 13 can be replaced by a "one-way" function with key K1. Such a function is for example described in the European patent application filed under number 96401336.1-2209.

Advantageously, the devices 12 and 13 prevent any pirate from discovering the encryption/decryption key K solely through the data item AL which travels between the decoder and the security element.

According to another particular embodiment of the invention, the key K1 used by the devices 13 and 12 can be specific to the security element/decoder pair, thus exhibiting the advantages mentioned earlier.

According to another particular advantageous embodiment of the invention, the procedure for generating the encryption and decryption key K can be renewed each session or else several times per session. Session should be understood to be an uninterrupted sequence of reception of one and the same programme by a user.

These renewals of the keys K exhibit, among other things, the following benefits:

- on the one hand, they make it possible to increase the soundness of the encryption/decryption algorithm of the devices 9 and 10. Soundness of the algorithm should be understood to be the resistance of the algorithm to piracy by cryptanalysis.

The frequency of renewal of the keys directly influences the amount of data encrypted with the same key made available to a pirate so as to cryptanalyse the algorithm. Since limiting this amount increases the resistance of the algorithm to attacks, frequent renewals of the key K increase the soundness of the encryption/decryption algorithm of the devices 9 and 10.

- on the other hand, it makes it possible to avoid replaying previously selected programmes.

Thus, if an ill-intentioned user or a pirate records the information output by the device 10, and therefore records, at the instant t, the selected programme in a form encrypted with a key denoted K_t, he will not be able to use the said programme subsequently since the de-

WAVELYNX EX. 1003, Pg. 1224
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

cryption key at the instant $t+\Delta t$, denoted $K_{t+\Delta t}$, will be different from the encryption key K_t.

Figure 4 represents the schematic of a security element/decoder assembly according to a third embodiment of the invention.

In addition to the elements described in Figure 2, Figure 4 includes, in respect of the decoder, a random number generator 11 and an encryption device 14 and, in respect of the security element, a decryption device 15.

The generator 11 generates a random number AL which is used directly as decryption key K by the device 9. Moreover, the random number AL is transmitted to the device 14 which encrypts it and transmits it to the device 15 of the security element. The encryption performed by the device 14 is performed under the action of a key K2. On the security element side, the encrypted random number E(AL) is decrypted by the device 15 under the action of a key K2 and the result AL is transmitted to the device 10 so that it serves as encryption key K.

According to another embodiment of the invention, a public key algorithm can be used for the devices 14 and 15. In this case, the encryption key is different from the decryption key and, in a preferred manner, the secret key is used for decryption in the device 15 whilst the public key is used for encryption in the device 14.

Advantageously, the devices 14 and 15, whether they use a symmetric algorithm or a public key algorithm, prevent any pirate from discovering the encryption/decryption key K merely by knowing E(AL).

According to the particular embodiments of the invention which were mentioned earlier:

- the random number AL can be generated once per session or indeed several times during the same session;
- the encryption/decryption key K2 used by the devices 14 and 15 can be made specific to the security element/decoder pair, thus exhibiting the abovementioned advantages.

In the context of the invention, for all the embodiments described in Figures 2, 3 and 4, the choice of the encryption/decryption algorithm of the devices 9 and 10 results from a compromise between the desired level of protection of the programmes and the complexity of the algorithm implemented in the decoder and in the security element.

Thus, a symmetric algorithm which is simple to implement via a dedicated circuit is preferred. Such an arrangement makes it possible, advantageously, to reduce the cost of implementation and to ensure high encryption/decryption rates, for example of the order of about ten Megabits per second. Renewal of the encryption keys then advantageously allows the use of a simple algorithm while decreasing the risks of piracy by cryptanalysis.

Furthermore the systematic decryption performed by the device 9 of the decoder exhibits a particular benefit, viz. that the user can display, via the decoder, only the programmes originating from the security element. This implies, for example, that unenciphered pirate programmes may not be played on the decoder alone.

In the case in which the keys K1, K2 are specific to each security element/decoder pair, the abovementioned property of systematic decryption has an additional advantage, viz. of preventing any pirate from supplying the same programme to decoders which are different from the decoder which he has pirated.

Moreover, for all the embodiments of the invention described in Figures 2, 3 and 4, the implementation consisting in integrating the devices 8 and 9 into the same electronic circuit will be preferred. This is so as to preclude the contents of the selected programme from appearing unenciphered between the two devices.

Claims

1. Process making it possible to transfer from a security element (1) to a decoder (6) a stream of data arising from a descrambler (3) contained in the security element (1), the said stream of data representing at least one programme selected by a conditional-access system user, characterized in that it comprises a first step making it possible to encrypt in the security element (1) the data arising from the descrambler (3) under the action of a first key (K) and a second step making it possible to decrypt in the decoder (6) the encrypted information item arising from the first step, under the action of a second key (K).

2. Process according to Claim 1, characterized in that the first step comprises a step making it possible to generate random words (AL) in the decoder and a step making it possible to encrypt the random words generated (AL) under the action of a third key (K1) in such a way as to generate the first key and in that the second step comprises a step making it possible to encrypt the random words (AL) in such a way as to generate the second key (K).

3. Process according to Claim 1, characterized in that the first step comprises a step making it possible to generate at least one random word (AL) in such a way that this random word constitutes the first key (K) during the whole of the descrambler (3) descrambling session and in that the second step comprises a step of encryption of the random word (AL) under the action of a fourth key (K2) in such a way as to make up an information item made up of an encrypted random word (E(AL)), and a step consisting of the decrypting of the encrypted random word (E(AL)) in such a way that the decrypted random word constitutes the second key (K).

WAVELYNX EX. 1003, Pg. 1225
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

4. Process according to Claim 1, characterized in that the first key (K) is stored permanently in the usercard (1) and in that the second key (K) is stored permanently in the decoder (6).

5. Security element (1) containing a descrambler (3) making it possible to descramble the data which it receives under the action of control words (Cw_i), the said data representing at least one programme selected by a conditional-access system user, characterized in that it comprises a device (10) for encrypting the descrambled information item arising from the descrambler (3) under the action of a first encryption key (K).

6. Security element (1) according to Claim 5, characterized in that it comprises a device for generating encryption keys (13) making it possible to generate the first key (K) under the action of a random word (AL).

7. Security element (1) according to Claim 5, characterized in that it comprises a decryption device (15) making it possible to generate, under the action of a decryption key (K2), the first key (K).

8. Decoder (6) making it possible to decode data arising from a security element (1), the said data representing at least one programme selected by a conditional-access system user, characterized in that it comprises a decryption device (9) making it possible to decrypt, under the action of a second key (K), the data arising from the security element (I), the said data being data which are descrambled and encrypted under the action of a first key (K).

9. Decoder (6) according to Claim 8, characterized in that it comprises a generator (11) of random words generating at least one random word (AL) and a device for generating decryption keys (12) from the random word thus generated, in such a way that the decryption key arising from the said generating device (12) is the second key (K).

10. Decoder (6) according to Claim 8, characterized in that it comprises a generator (11) of random words making it possible to generate at least one random word making up the second key (K) and an encryption device (14) making it possible to encrypt the random word making up the second key under the action of an encryption key (K2).

11. Assembly made up of a security element (1) and of a decoder (6) associated with this security element, characterized in that the security element is a security element (1) according to Claim 6 and in that the decoder (6) is a decoder according to Claim 9.

12. Assembly made up of a security element (1) and of a decoder (6) associated with this security element, characterized in that the security element is a security element (1) according to Claim 7 and in that the decoder (6) is a decoder according to Claim 10.

13. Assembly according to Claim 11 or 12, characterized in that the first key and the second key are keys specific to the said assembly.

WAVELYNX EX. 1003, Pg. 1226
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

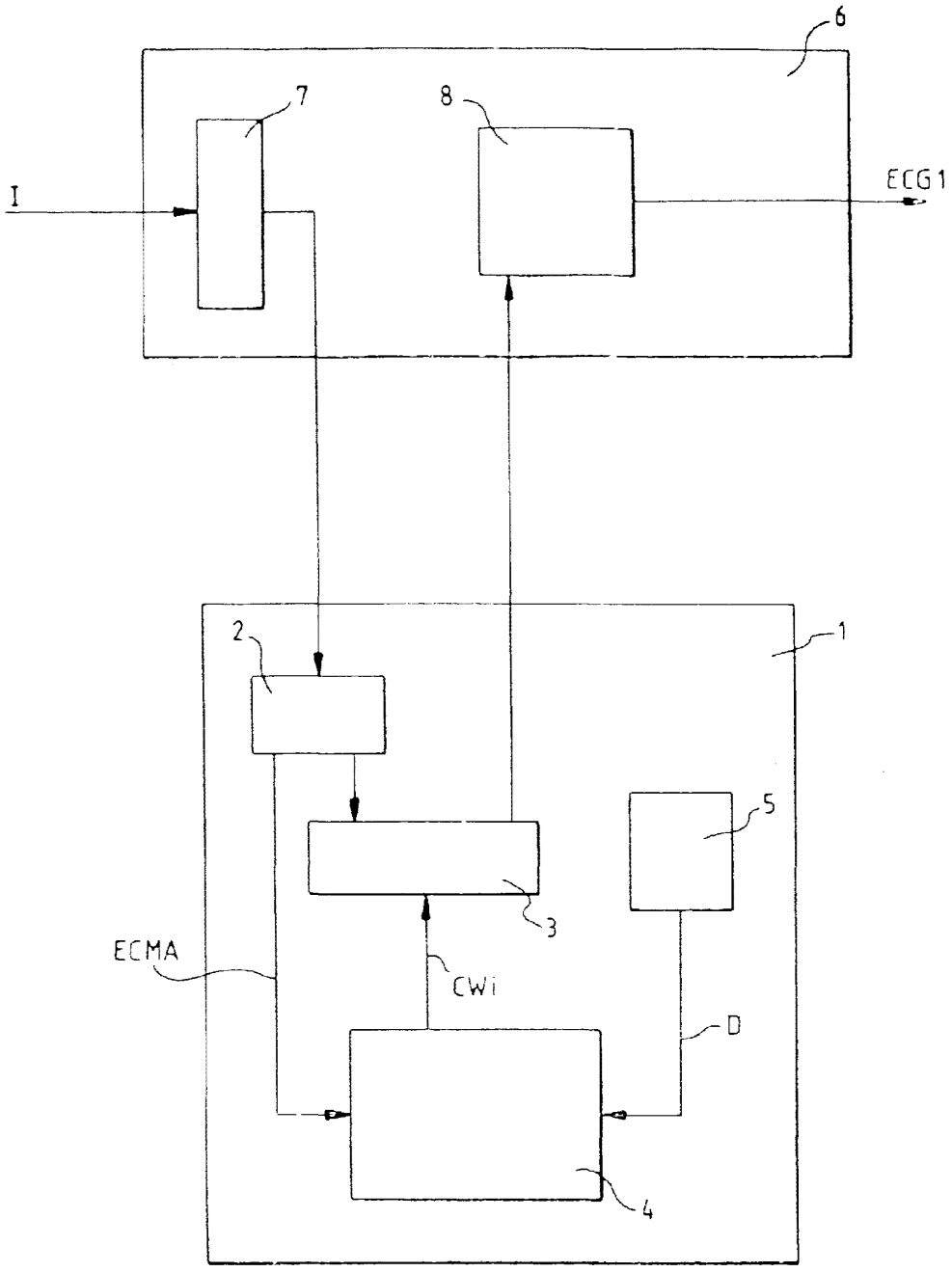


FIG.1

WAVELYNX EX. 1003, Pg. 1227
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

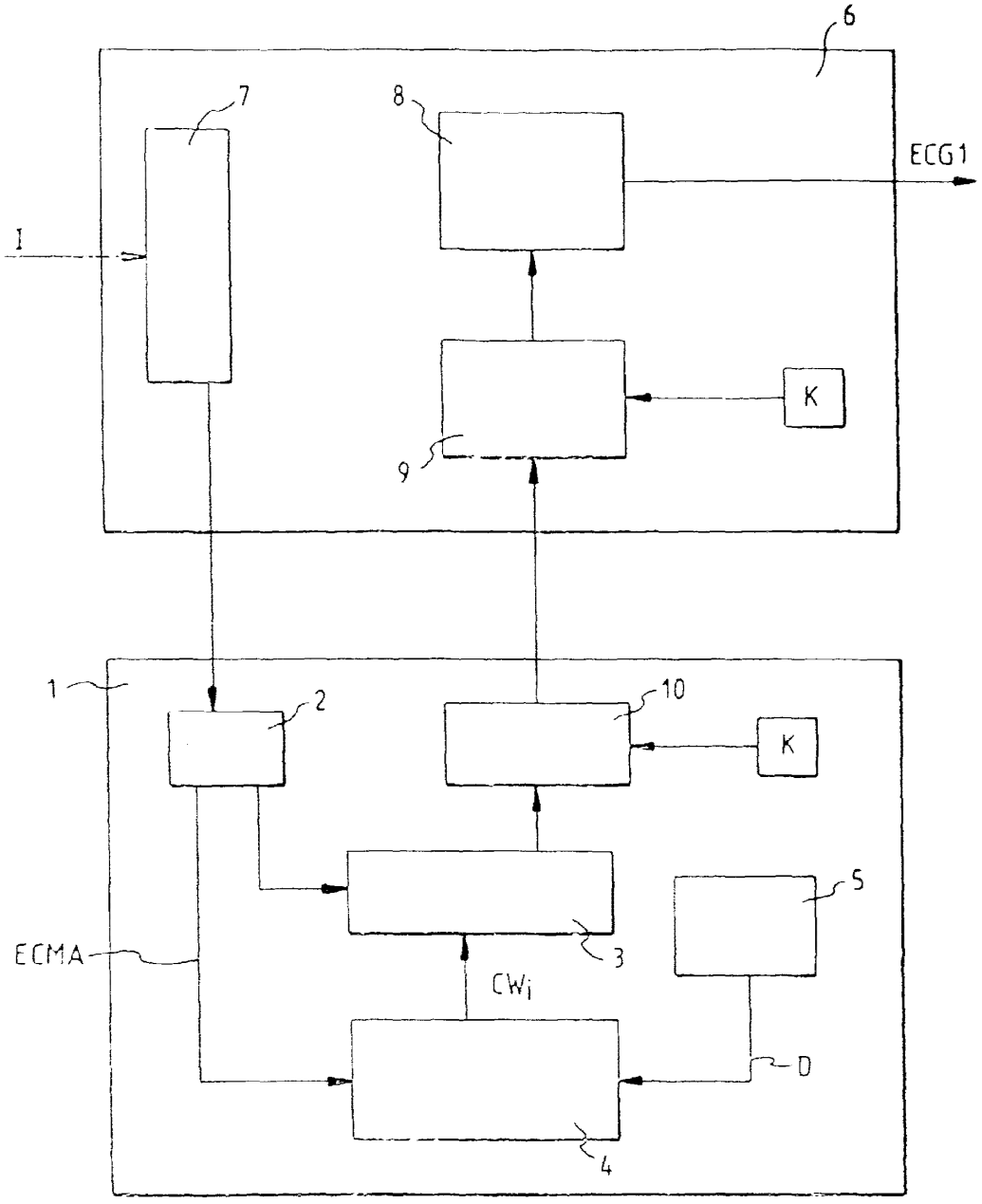


FIG. 2

WAVELYNX EX. 1003, Pg. 1228
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

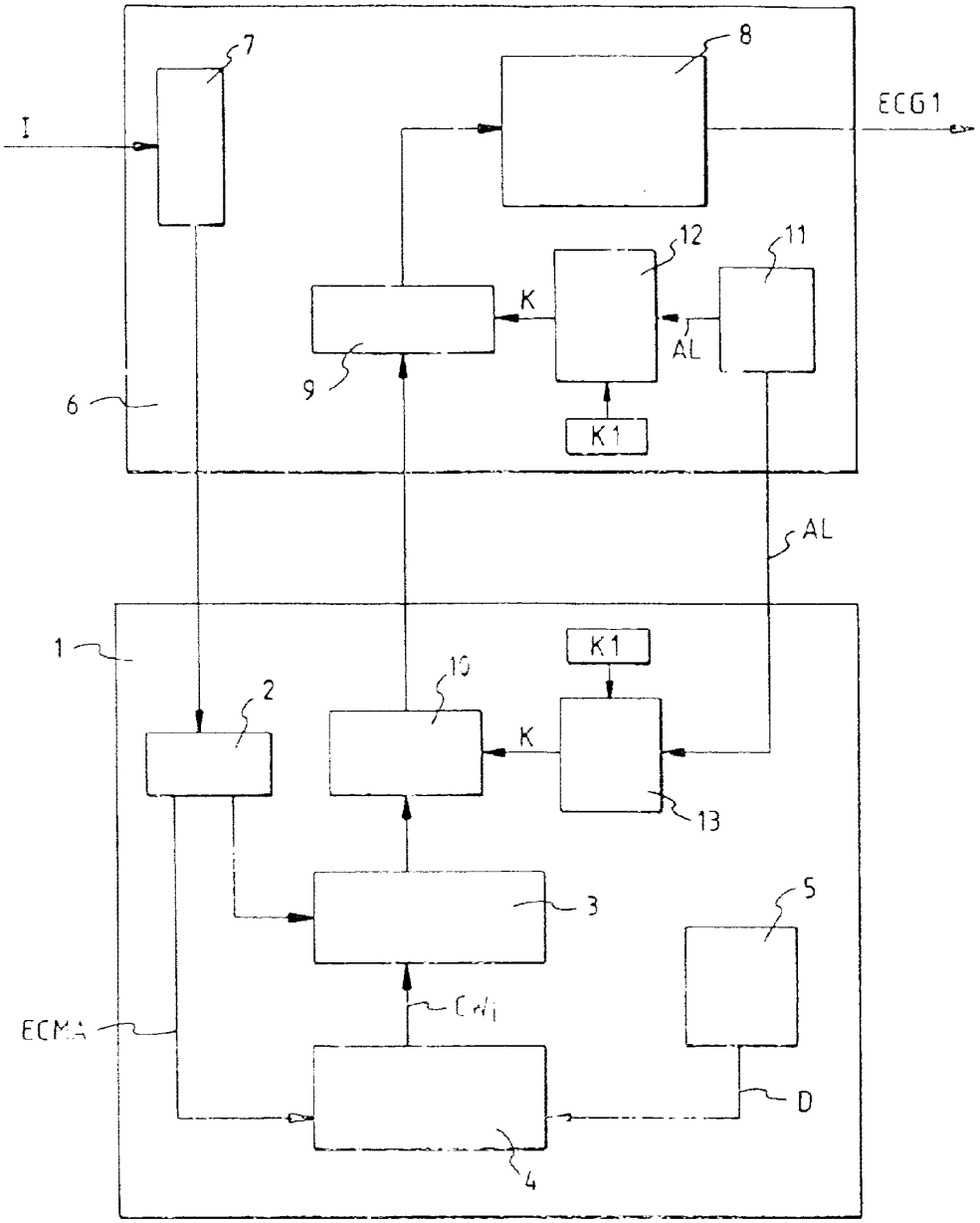


FIG.3

WAVELYNX EX. 1003, Pg. 1229
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

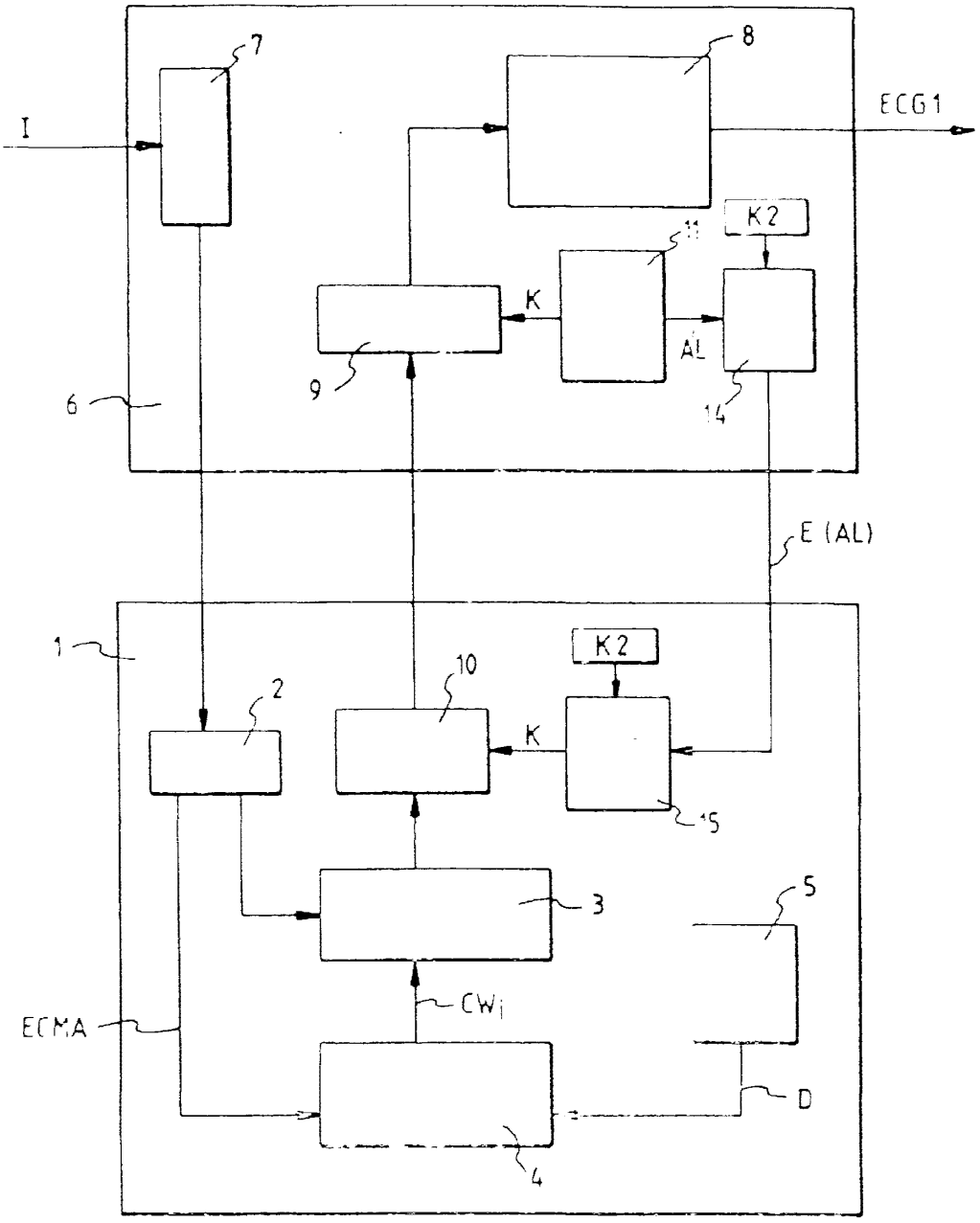


FIG.4

WAVELYNX EX. 1003, Pg. 1230
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 872 976 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.10.1998 Bulletin 1998/43

(51) Int. Cl.[6]: **H04L 9/22**, H04L 9/12, G06F 7/58

(21) Application number: **98201725.3**

(22) Date of filing: **29.06.1994**

(84) Designated Contracting States:
DE ES FR GB IT SE

(30) Priority: **30.06.1993 US 86080**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
94923275.5 / 0 706 735

(71) Applicant:
UNITED TECHNOLOGIES AUTOMOTIVE, Inc.
Dearborn, MI 48126-9982 (US)

(72) Inventors:
- **Koopman, Philip J., Jr.**
Hebron, Connecticut 06248 (US)
- **Finn, Alan M.**
Amston, Connecticut 06231 (US)

(74) Representative:
Gilding, Martin John et al
Eric Potter Clarkson,
Park View House,
58 The Ropewalk
Nottingham NG1 5DD (GB)

Remarks:
This application was filed on 22 - 05 - 1998 as a divisional application to the application mentioned under INID code 62.

(54) Method for quickly generating successive pseudorandom numbers

(57) A method of quickly generating successive pseudo random numbers, comprises providing a starting number, providing an iteration control signal which changes in a pseudo random manner in response to the generation of each successive pseudo random number and performing a variable number of iterations of an iterative pseudo random number generation operation on said starting number, said variable number determined by said iteration control signal.

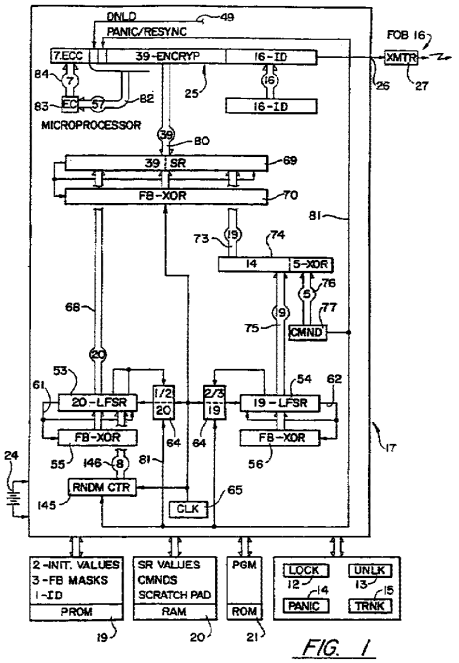


FIG. 1

EP 0 872 976 A1

Printed by Xerox (UK) Business Services
2.16.3/3.4

WAVELYNX EX. 1003, Pg. 1231
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

This patent application is a divisional application of European Patent Application number 94923275.5, which claims a method of cryptographic authentication of transmissions from a transmitting unit to a receiving module, a method of cryptographically authenticating transmissions from any of a plurality of remote command transmitting units to a command performing receiving module, a method of synchronized cryptographic authentication of transmissions from a remote command transmitting unit to a command performing receiving module selectively responsive thereto and a cryptographically authenticated remote control system in which a command transmitting unit may selectively cause a physical effect in a command receiving module rendered responsive thereto, as described herein.

Technical Field

This invention relates to pseudo random numbers and cryptographically encoded transmissions, such as the type involved with an automobile key chain fob transmitter which opens the automobile door locks or trunk in response to transmissions from the fob.

Background Art

The art of encoding transmissions so that the transmissions may be authenticated at a receiving module must meet criteria for technical viability (security) as well as low cost and convenience. The cost and convenience criteria result in an inability to use any encoding with, polynomials of excessive degree (such as binary numbers of hundreds of bits). Furthermore, cryptographic processing must require less than one second for acceptability by the user. Cost and weight constraints can limit the size and sophistication of a microprocessor or other signal processing equipment used in the system.

An example of such a system is disclosed in commonly owned U.S. Patent 5,191,610 to Hill and Finn. That system utilizes linear feedback shift register pseudo random number generation having the same seed number and the same, fixed feedback mask in the receiver as in the transmitter. The number of iterations of linear feedback shift register pseudo random number generation are counted in both the receiver and the transmitter, there being one additional iteration each time that a command is sent. Should the receiver not recognize one of the transmissions (because the transmitter was inadvertently activated at a great distance from the receiver, or otherwise), the receiver is allowed a moderate number of catch-up iterations in which it attempts to match the received transmission. Should that fail, the transmitter tells the receiver how many iterations from the seed it should perform in order to recreate a new current pseudo random number in order to resynchronize the receiver to the transmitter pseudo random number.

The aforementioned system requires that a receiver and a transmitter be wired or loaded with a binary feedback mask at the factory and sold as a pair. It also precludes matching a replacement transmitter with an existing receiver without the involvement of dealership personnel, which could compromise security. The pseudo random number generators of the Hill and Finn patent use one iteration per encrypted message. This saves time but results in a certain level of correlation between successive samples, so that the samples are less random-like. In other pseudo random number applications, the speed advantage of the aforementioned system could be useful but for the inherent correlation.

Any such system, except one that uses a truly random number of infinite degree, can be compromised either by analysis of a succession of intercepted signals, or by a brute force, exhaustive numerical trial approach which simply tries every number possible as the authentication word (the code or key).

Coded keypads used for unlocking vehicles have inherent security features. The generation of the code word by pressing keys can be shielded from view, and is certainly not capable of being determined beyond a line of sight. Furthermore, there would be great risk for an intruder entering every possible number into a keypad in an attempt to replicate the code (unless, of course, the automobile were parked in an unobservable area, such as a private or otherwise vacant garage). Thus, the keypad cannot be breached by analysis, and is not likely to be breached by numerical trial.

In contrast, lock systems which employ remote transmissions are enormously subject to security tampering because the surveillance of the transmissions may be carried out in another vehicle, without attracting any attention whatsoever. Therefore, it is possible to record many transmissions to a given vehicle, such as in a reserved workplace parking space (which commonly contains expensive cars), as well as providing an unobservable opportunity to attempt the breach of a security system (or even several systems at one time) by broadcasting huge volumes of random numbers, in parking lots where vehicles remain for long periods of time, such as at airports.

Whenever a transmitter is newly assigned to be used with an existing receiver, it is not sufficient to allow the new fob to identify itself and become authorized, without limiting that activity to a time when there is authorized access to the receiver through other than the transmitter itself (that is, within the vehicle itself). Thus, access to the vehicle by means of a traditional key or the like assures the safety of matching a newly assigned transmitter to an existing receiver. In the case of loss of synchronization between the transmitter and the receiver, simply allowing the receiver to synchronize to a particular pseudo random number provided thereto by the transmitter makes it too easy for a surreptitious

WAVELYNX EX. 1003, Pg. 1232
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

breach of security based on the analysis of a few transmissions, and synchronizing thereafter to one of the previous transmissions, utilizing numbers expected to be successful based upon analysis. Mere obfuscation of the resynchronizing code could be compromised by analysis of successful resynchronizations, and determination of the obfuscation function. The danger is not just that a single car might be broken into, but that a sophisticated capability might be developed and thereafter utilized extensively to breach the security of a large number of automobiles of a similar type.

Disclosure of Invention

Objects of the invention include rapid pseudo random number generation with minimal correlation.

This invention is predicated on our observation that introducing non-linearities into the Galois field operation of linear feedback shift register pseudo random numbers can render a code very difficult to breach by or with aid from numerical analysis. The invention is further predicated on the fact that time constraints on authentication can render the numerical trial approach essentially useless. The invention is predicated in part on the reversibility characteristic of the well-known exclusive OR operation, and on the reversibility of encryption such as encryption involving linear feedback shift register operations.

The invention provides a method of quickly generating successive pseudo random numbers according to claim 1 of the appended claims.

According to the invention, as claimed in the corresponding parent application, an encryption, such as a linear feedback shift register pseudo random number generation operation, is performed on a word comprising a pair of concatenated, independently generated numbers, which may themselves be encrypted (such as pseudo random numbers) and the result transmitted to a receiving module where a decryption, such as a reverse pseudo random number generation operation, recovers the concatenated numbers for cryptographic authentication. In accordance further with the invention, the encryption and decryption are performed with a secret mask essentially unique to the transmitter. According further to the invention, an encrypted number, such as a pseudo random number, used for cryptographic authentication contains command bits exclusive ORed into at least a portion thereof.

According to the invention, a number, which may be utilized in authentication of command transmissions, is generated by an iterative encryption process, such as a linear feedback shift register pseudo random number generation operation, which has a variable number of iterations per authentication, the number varying in response to a pseudo random event. According further to the invention, a pair of pseudo numbers are iteratively encrypted, such as by linear feedback shift register pseudo random number generation operations, using a different number of iterations in each successive encryption, the sequence of the number of iterations of one of them being different from the sequence of the number of iterations of the other of them, said number of iterations being based upon respectively different pseudo random events related to the respective words.

According to the invention of the parent application a plurality of transmitters are usable with a single receiver by means of secret numbers (such as initial values and feedback masks for feedback shift register encryption) essentially unique to each transmitter which are replicated in any receiver with which a transmitter is to be used, the receiver being capable of determining if each received transmission can be authenticated utilizing the initial values and masks of any of its assigned transmitters.

In accordance with the invention of the parent application the initial secret values and feedback masks of transmitters to be associated with a given receiver are stored (such as in an erasable read-only memory) by downloading the secret numbers of a transmitter into a receiver, thereby permitting the addition of a transmitter to the family of transmitters to which a receiver can respond. Although this may be performed at a dealership, it does not require, nor need it permit, human knowledge of the precise numbers; therefore, the possibility of surreptitious access is nearly eliminated. In further accord with the invention, identification numbers are associated with the secret numbers of each transmitter, which pre-screen transmissions before authorization attempts, thereby reducing nuisance operations from similar, unauthorized transmitters, and reducing the time required for multiple authentication attempts

According to the invention of the parent application the reception of each word causes the receiver of a remote operating system to become unresponsive to further transmissions for a period of about one-half second or more, thereby significantly inhibiting the capability to breach the security thereof through exhaustive numerical trials.

According to the invention of the parent application cryptographic authentication of transmissions from a remote transmitter to a receiver module involves encryption, such as by linear feedback shift register pseudo random number generation operations, utilizing secret feedback masks which are essentially unique to each transmitter, and replicated only in a receiver which is to respond to the related transmitter.

Random iterations reduce correlation between successively generated pseudo random numbers. Cooperative use of all of the aforementioned features in a remote operating system renders the system extremely difficult to breach by analysis; and use of a half-second delay, for example, causes a 50% statistical probability of a 39 bit encrypted key word being breached by exhaustive numerical trials to require more than one month.

The invention may be used in remote systems other

WAVELYNX EX. 1003, Pg. 1233
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

than automobile lock systems.

Other objects, features and advantages of the present invention will become more apparent in the light of the following detailed description of exemplary embodiments thereof, as illustrated in the accompanying drawing.

Brief Description of the Drawings

Fig. 1 is a stylized, simplified schematic block diagram of a transmitter according to the invention of the parent application in which the method of the present invention may be used.

Fig. 2 is a stylized, simplified schematic block diagram of a receiver according to the invention of the parent application.

Fig. 3 is a logic flow diagram of a transmitter encryption routine.

Fig. 4 is a logic flow diagram of a switch interrupt subroutine.

Fig. 5 is a logic flow diagram of a first portion of a receiver decryption routine according to the invention of the parent application.

Fig. 6 is a logic flow diagram of a panic command or resynch command portion of a decryption routine according to the invention of the parent application.

Fig. 7 is a logic flow diagram of a normal command authentication portion of a decryption routine according to the invention of the parent application

Figs. 8 and 9 are logic flow diagrams of alternative routines for pseudo random iterations.

Best Mode for Carrying Out the Invention

One example of the present invention may be used in a remote, encrypted automobile door and trunk locking and unlocking mechanism. The command to perform a certain task, such as a lock-related command (lock or unlock the doors, release the trunk), or to operate the lights and the horn or other alarm on the automobile in the event of a panic situation, or to cause cryptographic synchronization or resynchronization between the transmitter and the receiver module in the automobile, are under control of a plurality of buttons 12-15 disposed on a keychain fob or other hand-held transmitter unit shown in Fig. 1. The switches 12-15 may be tactile or touch-type and feed a microprocessor 17 which is associated with a PROM 19, a RAM 20 and a ROM 21. The PROM 19 is programmable only once, capable of having one set of output/input relationships burned therein, as is well known in the art. Typically, upon manufacture, each fob 16 will have its PROM burned in so as to establish a 16 bit identification number, which is not protected as secret information, as is described more fully hereinafter; two secret initial (seed) values from which encrypted messages are originated; and three secret feedback masks defining suitable polynomials for feedback exclusive ORing in the encryption process, for the life of the fob, all as is described hereinafter. The RAM 20 is used as a scratch pad memory, in the usual way, and will contain changing values of the shift registers and commands, as described hereinafter. The program for the microprocessor 17 is contained in the ROM 21.

It is assumed that the microprocessor 17 is the type which has a stop mode in which the clock does not run, and the only function that the microprocessor can perform is to respond to an external interrupt, which in this case would be the closure of one of the switches 12-15. This keeps power consumption extremely low, and a suitable battery 24 could last about five years. The microprocessor 17 assembles a 64 bit command request word 25 which is applied serially over a line 26 to a suitable transmitter 27 (e.g., RF or infrared), which serially transmits the command request, as digital bits or otherwise, a suitable distance, such as not more than 10 meters. The fob 16 will, before beginning its useful life, be associated with a particular automobile along with up to three more fobs (in the example herein) so as to form a set of up to four fobs, any one of which can operate the locks or the panic alarm of a related receiver module 30 in an automobile or other secured enclosure. The receiver module 30 in the automobile includes a receiver 31 which receives the serial bits and applies them over a line 32 to a microprocessor 33, where the 64 bit word 25 is replicated in a 64 bit word 38. The microprocessor 33 is powered from the automobile battery system 39. The microprocessor 33 has an electrically erasable PROM 40, a RAM 41 and a ROM 42 associated therewith. Each fob 16 is associated with a module 30 at a dealership, so that lost fobs may be replaced and matched to the module 30 anytime. A 64 bit word 25 (Fig. 1) is formulated with each fobs' ID, secret initial values and masks, and a download signal is provided, in some fashion, by factory personnel on a line 49. This may be achieved by a jumper, or in any other suitable way, since it does not pose a security threat unless the receiver 30 is tampered with simultaneously, which can be avoided as described below. The 64 bit word 25 sent to the receiver module 30 during a download includes one bit indicating the download operation. The presence of the download bit in the 64 bit word 38 (Fig. 2) can result in a download signal on a line 50 provided that the auto receiver 30 has been put into a download condition, such as by the installation of a download jumper 51 or other security measure. When download is suitably indicated, the fob ID and two initial values from the PROM 19 will be stored in the electrically erasable PROM 40. Then two secret feedback masks, of the same bit length as the initial values, will be sent with the ID in a similar fashion; and finally, a feedback mask which is as long as the concatenation of the two initial values is sent from the PROM 19 to the EE PROM 40 in the auto receiver 30. In a similar fashion, the initial values, feedback masks and ID's of three other fobs (in this example) will be loaded

WAVELYNX EX. 1003, Pg. 1234
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

into the auto receiver 30 during valid download operations.

The word 25 appears in Fig. 1 to be within a special 64 bit register. However, the word 25 actually appears in various parts of the RAM 20, in addresses designated to be used for holding the parts of the outgoing, serially transmitted word. Similarly, all of the apparent hardware within the microprocessor 17 is merely illustrative of processes and relationships, which may indeed be performed by hardware which resembles that illustrated in Fig. 1, or may be implemented, as is preferred, by processing of bits utilizing the RAM 20 as a scratch pad memory, by means of software which is well within the skill of the art in the light of the teachings which follow hereinafter.

The microprocessor 33 has functions and processes illustrated therein which may either be hardware or software, as described with respect to Fig. 1 hereinbefore.

The narrative with respect to Fig. 1 is of a form describing hardware: software implementation is described with respect to Figs. 3-7, hereinafter.

The receiver module 30 is connected to the locks 43 of the automobile, as well as to the automobile horn and lights 44, or other suitable alarm arrangements on the automobile.

Before a fob can be utilized to operate the locks or alarms on an automobile, synchronization must occur. Herein, this is also referred to as resynchronization since it is utilized at different times during the life of the system, as described hereinafter. This resynchronization process is described hereinafter; suffice it at this point to say that the process will begin with the two secret initial (seed) values for the fob 16 located in a 20 bit linear feedback shift register (LFSR) 53, and a 19 bit LFSR 54, and suitable feedback masks for each of the LFSRs 53, 54 available at the input of corresponding feedback exclusive ORs 55, 56. The initial synchronization (an initial resynchronization command) includes 20 iterations of the shift register 53 and at least 19 iterations of the shift register 54, so as to provide a complete bit-wise convolution. For ease in programming, both shift registers may be provided with 20 iterations during initialization (which is assumed herein). In each cycle, the high order bit is transferred by a line 61, 62 to the low order bit and is also exclusively ORed with those bits of the shift registers 53, 54 identified by bits in the feedback masks, to form the next higher order bits within the shift registers 53, 54. This is the very well known function of linear feedback shift registers, in the process of generating maximal length pseudo random numbers, as described in Numerical Recipes, Press, Flannery, Teukolsky, and Vetterling; Cambridge University Press, Cambridge, MA (1986). The feedback mask has to represent a suitable polynomial so as to provide a maximal length code, having degree N, which repeats only after 2^N-1 iterations. This is more fully set forth at pages 108-109 of Error Correcting Techniques for Digital Communication, Michelson and Levesque, John Wiley & Sons, New York, NY (1985), and in Appendix C of Error Correcting Codes, Pederson and Weldon, MIT Press, Cambridge, MA (1972).

One embodiment herein uses linear feedback shift registers, in some cases modified to be non-linear feedback shift register systems by shifting a pseudo random number of iterations as described hereinafter. However, other well-known pseudo random number generation techniques may be used such as linear congruential pseudo random number generators or non-linear congruential pseudo random number generators as more fully set forth in Chapter 3 of The Art of Computer Programming, Volume 2/Seminumerical Algorithms, ed. 2, Knuth, Addison Wesley, Reading, MA (1981); or inverse congruential pseudo random number generators or generalized feedback shift register pseudo random number generators as more fully set forth in Chapters 7, 8 and 9 of Random Number Generation and Quasi-Monte Carlo Methods, Niederreiter, SIAM, Capitol City Press, Montpelier, VT (1992); or multiplicative, I/P, power, discrete exponential, kneading map, shift register, or cellular automatic pseudo random number generators as more fully set forth in "Pseudo random Number Generators in Cryptography and Number Theory", J. C. Lagarias, pages 115-143 of Cryptology and Computational Number Theory, Pomerance, ed., Volume 42, Proc. SIAM (1990).

In general the pseudo random number generator need not be reversible. A reversible generator is one where, given the current pseudo random number and complete knowledge of the generation process, the previous pseudo random number may be determined. For example, a linear feedback shift register pseudo random number generator is reversible.

The manner in which the system is originally synchronized and the registers are made ready to operate is described hereinafter, because the general operation should be first understood.

In the usual case, when everything has been established and the system is operating normally, assume that a lock, unlock or trunk release command has been provided by pressing one of the buttons 12-15. This will cause the microprocessor 17 to wake up and perform one cycle of operation. In the cycle of operation, the RAM 20 provides the values which were previously left in the shift registers 53, 54 and the PROM 19 provides the masks for the shift registers 55, 56. Then, depending upon some pseudo-random event, such as the status of one or more bits of the shifts registers 53, 54, each of the shift registers will be provided one or two iterations or two or three iterations of linear feedback shifting due to the effect of clock gates 64 on the output of a clock 65. This is a first aspect of the present invention: instead of being shifted a number of times equal to the number of bits (which takes too many cycles to permit 256 attempts at decryption), the shift registers are only put through a few iterations after the initialization.

WAVELYNX EX. 1003, Pg. 1235
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Because this provides less scrambling of the feedback bits, the difficulty of mathematically ascertaining what the code might be is increased by causing the LFSRs to each undergo a different, variable number of iterations, in successive cycles, in a pseudo-random fashion. The pseudo random number provided by the iterations of the shift register 53 is supplied over a trunk of 20 lines 68 to a 39 bit shift register 69. The shift register 69 is associated with feedback 70 in the same fashion as the LFSRs 53, 54, with the exception that the shift register 69 is loaded with new numbers before each cycle of shifting feedback iterations. In this sense, then, the shift register 69 and feedback operate more as a cyclic redundancy code generator. The other input to the 39 bit shift register 69 is a trunk of 19 lines 73 from a gate 74 that causes the low order 5 bits of the 19 bit LFSR 54 on a trunk of lines 75 to be exclusive ORed with 5 bits on a trunk of 5 lines 76 from a command register 77. The command register 77 simply registers up to 32 commands encoded from the operation of any of the switches 12-15 (or fewer commands if some bits are used in a discrete fashion). Thus, in each cycle, there is presented to the 39 bit shift register 69 the outputs of the LFSRs with a command exclusive ORed in the low order bits of one of them. Then, the shift register 69 undergoes 39 iterations of LFSR-type feedback through an exclusive OR process 70, which utilizes a secret feedback mask provided by the PROM 19. This provides a full bit-wise convolution of the two words from the shift registers 53, 54, which is a cryptographic necessity. Use of the shift register 69 may be employed in prior art systems, such as the two-generator embodiment of the Hill and Finn patent. When the 39 iterations are complete, the result is an encrypted, key word provided on a trunk of 39 lines 80 to the 64 bit word 25, along with 16 fob ID bits from the PROM 19, a download bit 49 if appropriate, and a command flag such as a panic/resynch bit provided from the command register 77 on a line 81, when appropriate. In the usual case of authentication, both of the download and panic/resynch bits will be 0's. Then, all of these bits are monitored on a trunk of 57 lines 82 by an error correcting code circuit 83 to create a 7 bit error correcting code component on a trunk of 7 lines 84 for the 64 bit word 25; typically, a single error correcting, multi-error detecting code (such as a Hamming code) will be used. The illustrated embodiment uses a linear feedback shift register as a cyclic redundancy code generator for encrypting the input into a key word. However, any of several well-known reversible encryption techniques may be used. For instance, the McEliece error correcting code encryption; the RSA cryptosystem; discrete exponentiation cryptosystem; linear or non-linear, full length or truncated congruential cryptosystems; or the DES cryptosystem, as more fully set forth in chapter 10 of Contemporary Cryptology: The Science of Information Integrity, Simmons, ed., IEEE Press New York, NY (1992).

When the 64 bit word is fully assembled, it is transmitted serially (bit-by-bit) or otherwise, by any well-known technique, through the transmitter 27 to the receiver 31 of the receiver module 30 to become the 64 bit word 38 therein. All of the bits of the word 38 are applied over trunks of 57 lines 90 and 7 lines 91 to an error correcting and detecting process 92. If a single bit error has occurred, a signal on a line 93 (as appropriate) will correct the bit that is in error. If a multiple bit error is detected, the process is totally void, and the receiver module 30 simply goes into a half second wait state, which simply slows down any attempts to crack the code which is being used, as is described more fully hereinafter. If a multiple bit error has occurred but is not detected, the cryptographic authentication process will almost certainly fail. On the other hand, if the error correcting code shows that the 64 bit word 38 has no errors, then a first OK signal is provided on a signal line 94.

When it is believed that there are no errors in the 64 bit word 38, it is proper to determine whether the 16 bit, non-secret identification word matches any of the fobs that have been loaded into the receiver module 30. The ID of the fob reduces the probability that a command from a wrong fob will be cryptographically acceptable; it also reduces the amount of time it takes to iterate the code words in the receiver module to reach authentication (a match). However, in this embodiment, there is no restriction on which fobs are assigned as a group to an automobile, and it is assumed that there is approximately one chance in 11,000 that two fobs assigned to a particular automobile will have the same ID number. A feature of the invention is that if one fob with matching ID does not become authenticated, the receiver module 30 will see if there is another assigned fob with that same ID number, and if so, attempt authentication.

The 16 bit ID in the 64 bit word 38 is provided over a trunk of 16 lines 97 to a 16 bit compare circuit 98, the other inputs of which, on a trunk of 16 lines 99, are provided by the ID register 100, which really represents four different locations in the EE PROM 40, one for each associated fob. If, indeed, the message has come from one of the four associated fobs, a second OK signal appears on a line 101, and the identification number of the fob which has sent the message is provided on a trunk of 4 lines 102 to the PROM 40 and to the RAM 41 so as to utilize in the ensuing decryption process the secret mask for the selected fob and the two LFSR values which have previously been created for that fob. The previous LFSR values are utilized, rather than the initial secret values, because, according to the invention, the LFSR values are built upon, with only one, two or three iterations for each command received by the receiver module 30.

At this stage, the normal decryption process can begin. The 39 bit encrypted key word is provided over a trunk of 39 lines 107 to a 39 bit shift register 108 which can be identical in either structure or function to the 39

WAVELYNX EX. 1003, Pg. 1236
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

bit shift register 69 in the fob, except that it is iterated in a reversing process. The reversing process is easily understood, one bit at a time, by considering how the received 39 bits got to be what they were. In the last iteration between the shift register 69 and the exclusive OR circuit 70 (Fig. 1) if the high order bit (leftmost bit in Fig. 1) was a 1, then exclusive ORing in accordance with the secret mask is provided against each bit of given order in the 39 bit shift register in order to determine what the next bit in order would be at the end of the iteration. That is to say, the ninth bit becomes the tenth bit (0 or 1 as the case may be) unless it is inverted by the exclusive OR. In order to be inverted by the exclusive OR, the ninth bit of the secret mask would have to be 1, and the most significant bit at the start of the iteration would also have to have been 1; and the most significant bit advances to the least significant stage, in a wrap-around. If either the most significant bit is a 0 or the corresponding bit in the secret mask is a 0, the ninth bit would simply advance into the tenth stage Since what was the most significant bit becomes the least significant bit, inspection of the least significant bit determines whether or not exclusive ORing occurred. If the least significant bit in the shift register 108 is a 1, it is applied to exclusive OR the bits of each order with the same secret mask which was downloaded for this fob originally. For any bit (such as the ninth bit) for which there is a corresponding bit in the secret mask, whenever the lowest ordered bit at the start of the iteration is a 1, that bit will be inverted from 1 to 0 or from 0 to 1. But if there is no corresponding bit in the secret mask, then the bit in question is simply advanced to the next lower order stage (in the example here, bit 10 becomes bit 9) without being inverted. Or, if the least significant bit (the rightmost bit in Fig. 2) is a 0, then none of the bits are inverted as they are advanced from one stage to the next lower stage in the shift register 108. By doing this the same number of times (39 iterations in the example herein), the original word in the 39 bit shift register 69 is reconstructed. The operation of the 39 bit shift register is very much like cyclic redundancy code (CRC) generators, used for error detection and correction. The process in the 39 bit shift registers herein is the same as in the LFSRs with the exception of the fact that the shift registers herein receive a whole new starting word before the iterations of each cycle. More on CRCs, Galois field arithmetic, and the generation and utilization of pseudo random binary numbers, may be found in Theory and Practice of Error Control Codes, Blahut, Addisson Wesley Pub. Company, Reading, MA (1984); An Introduction to Error-Correcting Codes, Shu Lin, Prentice Hall, Englewood Cliffs, NJ (1970); and Error-Control Techniques for Digital Communication, Michaelson and Levesque, John Wiley & Sons, New York, NY (1985).

In decryption, part of the process is reversed, and part of it is matched. Thus, the 39 bit encrypted code word is reversed by 39 reversing iterations, and the results thereof are compared to what should be identical results from the LFSRs.

Once a fob is identified in the 16 bit compare circuit 98, its two secret feedback masks are loaded (from RAM 41) for use in corresponding exclusive ORs 113, 114, and its previously achieved 20 bit LFSR value is loaded into a 20 bit LFSR 115, while its previously achieved 19 bit LFSR value is loaded into the 19 bit LFSR 116. Dependent upon a given bit of each of the LFSRs, the LFSR is shifted (with or without exclusive ORing as described hereinbefore) either once or twice, in the case of the LFSR 115 or two or three times in the case of the LFSR 116 in dependence upon a pair of corresponding gates 117 which control the application of a clock 118 thereto, in the same fashion as described with respect to Fig. 1 hereinbefore. The 20 bits of the 20 bit LFSR 115 so generated are applied over a trunk of 20 lines 123 to a compare circuit 124, to be compared with 20 bits provided from the 39 bit shift register 108 over a trunk of 20 lines 125. Similarly, the high order 14 bits which are generated in the 19 bit LFSR 116 are provided by a trunk of 14 lines 127 to the compare circuit 124 for comparison with 14 bits of the 39 bit shift register 108 provided on a trunk of 14 lines 128. Assuming that both the 20 bit and 14 bit words compare properly, this signals a successful authentication on a line 129 and the receiver module 30 is allowed to receive and respond to the command made by the fob.

Recalling that the five bit command is exclusively ORed to the low order five bit positions provided from the 19 bit LFSR 54, the only way to recover those bits is to exclusive OR the low order 5 bit positions from the 19 bit LFSR 116 with the low order 5 bit positions of the reconstituted word in the 39 bit shift register 108. Therefore, the low order 5 bit positions produced by the 19 bit LFSR 116 are provided over a trunk of five lines 130 to a five bit exclusive OR circuit 131, the opposite inputs of which consist of the lowest order 5 bit positions from the 39 bit shift register 108 on a trunk of 5 lines 132. The result of the exclusive OR on a trunk of 5 lines 137 comprise the command which is stored in a command register 138. The typical commands provided on a trunk of lines 139 to the locks 43 comprise door unlock, door lock, and trunk release. Another command indicated by a signal on a line 140 may comprise a panic command which will cause the horn and lights 44 (or other alarms) on the car to scare away a loiterer as the driver approaches the car with the fob (as described more fully hereinafter).

If the first attempt to match the outputs of the LFSRs 115, 116 with corresponding 34 bits of the 39 bit shift register 108 fails, then the LFSRs 115, 116 are cycled again. In each cycle, the LFSR 115 will be shifted once or twice depending upon the random bit utilized as a control over its gate 117, and the LFSR 116 will be shifted two or three times in dependence on the random bit utilized to control its clock gate 117. This is to allow the receiver module 30 to catch up, in cycles, and there-

WAVELYNX EX. 1003, Pg. 1237
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

fore in iterations, to the status of the LFSRs 53, 54 in the fob 16.

Anytime that one of the buttons 12-15 on the fob is depressed, the fob will undergo one cycle, and the shift registers 53, 54 will undergo one or two, or two or three iterations, respectively. The pressings of the buttons 12-15 may occur simply by being crushed in a purse, children playing with the fob, or otherwise. Since each fob keeps its own LFSR generated numbers, and the receiver module 30 likewise maintains separate LFSR generated numbers for each fob, each fob will generally be able to track with the receiver module except for the inadvertent pressings of the switches 12-15. Whenever the switches 12-15 have caused a cycle that is not responded to by the receiver module 30, the first time the switches are pressed and the receiver module does respond, the content of the LFSRs 115, 116 will not compare with the corresponding bits of the 39 bit shift register 108. However, provision is made in accordance with the invention to allow the receiver module 30 to initiate additional cycles, and the additional one or two iterations for the LFSR 115 and two or three iterations for the LFSR 116, so as to catch up to the fob. To this end, an 8 bit counter 143 allows the receiver module 30 to try to catch up to the fob in question by repeating as many as 256 cycles, automatically. In a normal case, the receiver module 30 will catch up to the fob in only a few cycles. But if the receiver module is more than 256 cycles behind, as may occur by repetitive pressings of one of the switches 12-15 in a suitcase or handbag, then the LFSRs 115, 116 will not match up with the 39 bit shift register 108. The receiver module 30 is non-responsive to incoming signals while it is attempting authentication of a previous signal; the 256 attempts to catch up will transpire in only a half second or less; thus, authentication will not be hampered by repetitive pressing of the unlock button 13 due to impatience. Eventually, the operator will understand that the receiver module is out of synchronization (cryptographic synchronization), and will press two buttons at one time (such as lock and unlock), or some other combination that will be recognized in the fob as a command to effect cryptographic resynchronization between the receiver module 30 and the fob 16, as well as to reinitialize following a loss of battery power (dead or changed), which allows the RAM data to disintegrate.

A recognized command to synchronize ("resynch command", hereinafter) in the command generator 77 (Fig. 1) will produce the panic/resynch bit on the line 81. The resynchronization process in accordance with the present invention includes returning to the beginning; that is, returning to the use of the secret initial values and starting all over again. As described hereinbefore, the resynch command is used to initialize the units in the first place, and when they become out-of-synch, they are in a sense reinitialized just as when they are new. To that end, the panic/resynch bit on the line 81 will cause the two initial secret values to be loaded from the PROM 19 to the LFSRs 53, 54 and the two initial secret feedback masks to be made available to the exclusive ORs 55, 56, and the 39 bit secret feedback mask to be made available to the exclusive OR 70. The panic/resynch command on the line 145 causes the clocking gates 64 to cause 20 iterations, respectively, of the LFSRs 53, 54. The purpose is that, utilizing as many iterations as there are bits in the word, causes the maximal mix of the feedback, regardless of what the mask is, to assure complete bit-wise convolution. In this case, however, two additional changes from normal occur: the eight low order bit positions of the shift register 53 are provided with a truly random number on a trunk of 8 lines 146 from an 8 bit counter 145 which is allowed to respond to the clock 65 in a manner related to pressing of the buttons 12-15, as described with respect to Fig. 3 hereinafter. Since it is impossible for persons to depress buttons carefully enough to achieve other than a random number at computer clocking frequencies (500 KHz or more), the likelihood of this number being exactly the same in successive resynch processes is extremely small. After twenty iterations of feedback shifting, with the low order 8 bit positions of the LFSR 53 comprising those from the counter 145, outputs of the 20 bit LFSR 53 and the 19 bit LFSR 54 are provided to the 39 bit shift register 69. The shift register 69 thereafter undergoes 39 feedback shifting iterations, of the type described hereinbefore, to produce the 39 bit encrypted word in the 64 bit word 25. As before, the 16 bit ID for the fob is provided to the word 25, along with a panic/resynch bit (described hereinbefore) to indicate that this is a panic or resynch request, and the error correction code is computed and the code bits added to the word 25 as described hereinbefore. The 20 bit LFSR and 19 bit LFSR results, after 20 iterations, form the pseudo random starting words to be used in authenticating future transmissions.

In the receiver module 30, the first two steps are the same as in a normal command. Error correction is provided if possible, and if the word is correct, the first OK signal appears on the line 94. Then, the four possible IDs are compared with the incoming ID in the word 38, and if there is a match, the second OK signal appears on the line 101 and the signals on the trunk of four lines 102 tell the EE PROM 40 which fob is being worked with and therefore which of the sets of two secret initial values and three secret feedback masks should be utilized. The appropriate secret initial values and three feedback masks are loaded into the LFSRs 115, 116, and the exclusive ORs 113, 114 and 109. The content of the 39 bit shift register 108 is reconstructed by 39 reverse iterations, as described hereinbefore, so as to recover the word in the 39 bit shift register 69. However, since the output of the 20 bit LFSR 53 does not reflect 20 shift iterations of only the secret initial value that was placed therein, but rather represents 20 iterations of 12 high ordered bits of the secret initial value and 8 random low ordered bits, comparisons with the high order bits of the

WAVELYNX EX. 1003, Pg. 1238
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

39 bit shift register 108 cannot be made in the receiver module 30. Instead, the 20 bit LFSR value must be recovered in the same way that the 39 bit shift register value is recovered. That is, a reverse linear feedback shift register operation, utilizing the exclusive OR mask with the least significant bit, is achieved in a 20 bit LFSR 151 (Fig. 2) in association with a 20 bit exclusive OR 152. This restores the unscrambled number in which the 12 high order bit positions of the LFSR 151 should be the same as the 12 high order bit positions of the secret initial value in the 20 bit LFSR 115, and the low order 8 bit positions of the 20 bit LFSR 151 are some random number (produced by the counter 145).

The next step in the resynch process is to compare the high order 12 bit positions of the reconstituted word in the LFSR 151 with the 12 bits of the secret initial value of the 20 bit LFSR 115. Thus, the 12 bits on the trunk of 12 lines 160 are compared with the 12 bits on the trunk of 12 lines 161, which are created solely in response to the initial secret value. And, the 14 bits on the trunk of lines 127 are compared with the 14 bits on the trunk of lines 128; these should also compare because the 19 bit LFSR 116 has been passed through 20 iterations in response to its secret initial value so it should match the result in the 19 bit LFSR 54, the 14 high order bit positions of which have been reconstituted in the 14 bits of the 39 bit shift register 108 to which the trunk of lines 128 respond.

If both the 12 bit and 14 bit comparisons are successful, a determination is made whether the panic/resynch bit, provided on a line 150 from the 64 bit word 38, had been caused by a panic command or by a resynch command. If a resynch or panic command was sent, the resynch or panic command would have been exclusively ORed into the five low order bits of the 19 bit shift register 54, as described with respect to other commands hereinbefore. Therefore, the command will be extracted by the five bit exclusive OR 131 and provided over the trunk of lines 137 to the command register 138. Since performing the panic command cannot breach vehicle security, it is used as the default command; if the resynch command is not present on the line 140, then the panic/resynch command on the line 150 may be deemed to be a panic command, if desired, even if not decoded. Up to this point, the panic command and the resynch command are identical.

The next step in the resynch process is to compare the 8 bit random number in the low ordered bit positions of the 20 bit shift register 151 with the last four prior low order 8 bit random numbers received during resynchronizing. In the present invention, the random number is compared with the last four such random numbers previously received by providing the 8 low order bit positions of the 20 bit LFSR 151 on a trunk of 8 lines 153 to 8 bits of the compare circuit 124 which are also responsive to a trunk of 8 lines 154 from a first in, first out stack 155 (actually embodied in the EE PROM 40), which keeps track of the last four 8 bit random numbers received during resynchronization operations. If, during resynchronization, the 8 central bits of the compare circuit 124 compare with any of the four 8 bit words in the first in, first out stack (FIFO) 155, the operation is a failure, and the receiver module 30 reverts to a half second wait period before it will react to the next command (as described hereinafter) and the matched word goes to the head of the stack and remaining words in the FIFO are adjusted accordingly. On the other hand, if the 8 bit word on the trunk of lines 153 does not compare with any of the bits in the stack 155, the comparison is a success and the operation can proceed; additionally, the 8 bit word on the trunk of 8 lines 153 is applied over the trunk of lines 154 to the FIFO stack 155, for comparison with subsequent random 8 bit words during subsequent resynchronization operations. In such a case, the new word goes in the FIFO and the oldest word is dropped out of the FIFO.

Assuming that there is no match of the 8 bit random word, the resynchronization operation is complete. When the resynchronization is commanded, after successful comparisons of the 12 high order bits and the 14 bits as described hereinbefore and no comparison with the FIFO, the values established in the shift registers 53, 54, 115 and 116 are left as they are, for use in authenticating the next normal command cycle.

The panic command is the same as has been described with respect to the resynch command, except that, if the command register 138 produces the panic command signal on the line 140, the lights and the horn 44 (or other alarm) are operated, and, all of the LFSRs 53, 54, 115, 116 are then restored to whatever setting they had immediately before sending and receiving the panic command. The panic command operates differently from lock, unlock and trunk release commands, so that there will be response, even with total missynchronization between the fob and the receiver module. In the case of the panic command, starting over with the secret initial values ensures that authentication (to avoid nuisance responses) will be successful on the first try. Therefore, the panic command in the fob (Fig. 1) causes the LFSRs to be loaded with the initial values in the PROM 19, rather than the shift register values which had been achieved to date through iterations in the RAM 20, and the panic/resynch process just described is performed to ensure that there will be authentication to execute the panic command.

The foregoing description is given as if it were hardware, and indeed the invention may be implemented in hardware along the lines described hereinbefore. However, the invention has been implemented in suitably programmed microprocessors, which are deemed most suitable. In the flowcharts described hereinafter, exemplary software routines are illustrative of the processing of the invention, but not necessarily of the individual steps of the program in any given embodiment of the invention.

The process of encryption in the fob is illustrated in

WAVELYNX EX. 1003, Pg. 1239
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Fig. 3. It is assumed that the fob comprises a microprocessor, such as a 68HC11, which has a stop mode in which the clock is stopped, the power consumption is negligible, and the only thing the processor can do is to respond to an external interrupt to get started again. In such a processor, application of battery power would cause the program to be reached through a power up entry point 170 and the processor would immediately stop at a step 171 where the only function is to perform a test 172 to determine whether any of the buttons 12-15 have been pressed, or not. So long as no button is pressed, the processor waits in a low power stop mode, in the loop 171, 172. As soon as a key is pressed, an affirmative result of test 172 reaches steps 173 in which a switch word in RAM 20 is ORed with the one of the switches which was pressed. Generally, two switches cannot be pressed within a few computer clocks of each other, so the first one will be sensed. As described hereinafter, if a second one is pressed within about 1/2 to one second, it will be treated as paired-up with the first; if the two are correct (e.g., lock and unlock) a resynch command is declared. A switch interrupt, selectively enabled during normal command cycles only, allows sensing the second switch of a resynch.

In Fig. 3, the steps 173 also enable the switch interrupt and start the random counter. Then, a decode command subroutine 179 is performed and a test 180 determines if the command is either panic or resynch. If so, an affirmative result of test 180 reaches a series of steps 181 in which the shift register contents are saved in buffers, the panic/resynch (P/R) bit on line 81 is set to 1; a working register, herein referred to as a "shift register" (SR), is set with the random counter in its low order 8 bit positions and with the higher order bit positions equal to a 12 bit secret initial value for the 20 bit LFSR, the mask associated with the SR is set equal to the 20 bit secret feedback mask from the PROM 19, and a cycle counter C is set to 20 iterations. Then a bitwise linear feedback shift register iteration subroutine 182 is performed in which each bit is shifted to the next higher order position, with or without inversion, dependent upon the secret mask and/or whether the low order bit position has a 1, as described hereinbefore. Then the C counter is decremented in a step 183 and a test 184 determines if a complete, 20 iteration LFSR cycle has yet occurred. If not, another iteration is performed by the subroutine 182 and the C counter is decremented again. After 20 iterations, an affirmative result of the test 184 reaches a step 185 where the 20 bit shift register storage location in RAM 20 is set equal to the content of the working shift register. The steps and test 182-185 comprise an LFSR cycle 186.

Then the 19 bit shift register 54 is prepared in a series of steps 190 in which the content of the shift register is set equal to the content of the 19 bit secret initial value in the PROM 19, the mask associated with the shift register set equal to the 19 bit secret feedback mask in the PROM 19, and the C counter is set equal to 19. Then an LFSR cycle subroutine 191 (similar to the subroutine 186) is performed. Then the 39 bit shift register 69 is prepared for its LFSR cycle in a series of steps 192. Specifically, the 5 low order bit positions are the exclusive OR of the command with the 5 low stages of the 19 bit shift register 54; the high 14 bits of the 19 bit shift register 54 are placed directly in the 39 bit shift register; and the highest order 20 bit positions are set equal to the 20 bit positions of the 20 bit shift register 53. The mask is set equal to the secret feedback mask for the 39 bit shift register, found in the PROM 19, and the C counter is set to 39. Then, an LFSR cycle subroutine 193 is performed, this time with 39 iterations, and the result restored in the 39 bit shift register embodied in the scratch pad memory 20. In a routine 194, the 16 bits of the fob ID from the PROM 19, the 39 encrypted bits now in the 39 bit shift register, the P/R bit, and the download bit are all transmitted serially while the calculation for error correcting code bits is performed. These are calculated and transmitted, to complete the process of a panic or resynch command transmission. Whether it be a panic or a resynch is determined by the status of the five command bits. If a resynch was performed, the new values of the 20 bit shift register and 19 bit shift register will be retained as the pseudo random starting words to be used for future authentication of transmissions to the receiving module. But if this is a panic command, the new values are only used to ensure synchronized response, one time, and a test 195 causes the previous values of the 20 bit and 19 bit shift registers to be restored from the buffers in a step 196.

Assuming that a normal command has been given, a negative result of the test 180 reaches a series of steps 199 in which the working shift register is set equal to the 20 bit shift register in the RAM 20 (not the secret initial value), so as to take advantage of the pseudo random number generated by all of the previous iterations. In accordance with invention, the mask for the shift register is set equal to the 20 bit shift register secret feedback mask from the PROM 19, and a set of random bits (which determines how many iterations are to be performed, similar to the gates 64 of Fig. 1) is set equal to whatever random bits have been selected to be used to control the iterations for the 20 bit shift register. This might, for instance, be the third and the ninth bit of the 20 bit shift register, or in a general case, can be anything else that is deterministically computable but difficult to predict. Then a pair of tests 200 determines what the random bits are: if both are a 1, a step 201 sets the C counter to 1; if both are a 0, a test 202 sets the C counter to 2. But if they are different, a step 201a sets the C counter to 3. Then, either a 1 iteration, 2 iteration or 3 iteration LFSR cycle subroutine 203 is performed. The method of the invention may be used in prior art systems, such as in the Hill et al patent. Next, the same sort of operation is accomplished with the 19 bit shift register; a series of steps 204 set the working shift register equal to the content of the 19 bit shift register in the

WAVELYNX EX. 1003, Pg. 1240
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ram 20, the mask for the working shift register is set equal to the secret feedback mask for the 19 bit shift register in the PROM 19, and the random bit is set equal to whatever bit has been chosen to be random for the 19 bit shift register. Then a test 205 determines if the random bit is 1, or not. If it is, a step 206 sets the C counter to 3, and otherwise a step 207 sets the C counter to 2. This provides four iterations (201, 206; 202, 207) whether the random bit is 1 or 0; but it may be set in other ways, if desired. Then a 2 or 3 iteration LFSR cycle subroutine 191 is performed. Then the series of steps 192 set things up so as to form the 39 bit encrypted word, a 39 iteration LFSR cycle subroutine 193 is performed so as to produce the 39 bit encrypted word, and the subroutine 194 transmits all the bits together with a calculated error correction code. Thus, the differences between encrypting and transmitting normal commands and the panic/resynch command are the setting of the P/R bit, the use of the random counter 145, the use of the secret initial values and the particular code which is exclusive ORed into the 19 bit shift register 54.

When a command word has been transmitted by the subroutine 194, and if a panic command, the shift registers have been restored from the buffer, the program advances to a one-half second wait in a step 208. This is to ensure that successive button pressings which are independent of each other will occur no closer than one-half second apart. During the time from when the computer was awakened by a command interrupt (at test 172 until the end of the one-half second waiting period at step 208), a switch interrupt might have occurred as a result of a second pressing of one of the switches 12-15. As described hereinbefore, this is most likely the case of an attempt to press two switches at once (such as lock and unlock) to thereby cause a resynch. Whenever the switch interrupt is enabled, closing of one of the switches 12-15 will reach the interrupt subroutine of Fig. 4 through an entry point 209. In a series of steps 210, the particular switch which caused the present interrupt is remembered by being ORed into the switch word within the RAM 20; and since this may be a request for resynchronization, an internal resynch flag is set. The random counter is stopped, to provide the random number which is used in resynchronization, and then whatever part of the program of Fig. 3 was in process when the interrupt was sensed is returned to; this return may be to any of the functional steps ahead of the waiting step 208, or may be within the waiting step 208. Of course, if the waiting step 208 is interrupted, it will in fact turn out to be more than one-half second when the counting therefor is completed; this is irrelevant.

In Fig. 3, after the waiting period is over, a test 211 determines if the resynch flag has been set. If it has, an affirmative result of test 211 reaches a step 212 which resets the resynch flag, and then the program advances to the decode command subroutine 179. If the first switch which was pressed, turning on the computer, was either lock or unlock, and the second switch which was pressed, causing the switch interrupt, was either unlock or lock, respectively, then the decode command subroutine will in fact decode a resynch command, to cause a resynch operation of the type described hereinbefore. If not, any other two-key series may be decoded into a lock command for security, or into a panic command since the panic command will not affect security, or it could cause reversion to the one-half second waiting period, at step 208, or otherwise as suits any particular implementation of the invention. Of course, if two switches which can cause a resynch command are pressed essentially simultaneously, the decode command subroutine will decode a resynch command without the aid of Fig. 4 and the resynch flag. If switches are repetitively pressed at less than half-second intervals, the switch word will either contain gibberish or will simply repeat the resynch command.

After waiting one-half second at the step 208, if the resynch flag has not been set, a negative result of test 211 will cause a pair of steps 213 to return the switch word to all zeros and to disable the switch interrupt, so that all future operation of the switches can only turn on the computer from its stop condition, at test 172. It should be noted that the command interrupt and the switch interrupt respond to the same thing: the operation of any of the switches; the difference is the microprocessor's response to them, as is well known in the art.

It is assumed that the decryption of Fig. 5 is carried out in a microprocessor of the same general type as is used in the fob. When connected to a battery, the routine is entered through a power up transfer point 214 and the processor immediately goes into a stop mode at a step 215, where the clock is off and the only function is to respond to a receiver interrupt at a test 216. In between usages, the processor in the automobile will remain in the stop mode, in the loop 215, 216. When an incoming message is sensed, an affirmative result of the test 216 will reach a subroutine 217 which handles receiving all 64 bits of the word transmitted from a fob, calculating the error correcting code, and fixing any single error which can be fixed. Then a test 218 determines if the error correction code indicates correct data. If it does not, a negative result of test 218 reaches a transfer point 219 and then a step 220 where the program just waits for half of a second. The purpose of this is to severely hamper any attempts to break the code through repetitive application of numbers, with or without calculated likely candidates. After waiting one-half second, the processor returns to the stop mode in the loop 215, 216.

If the incoming word is OK, an affirmative result of test 218 reaches a step 221 where a working number, n, is set equal to 4 (or to such other number as the number of fobs which can be associated with the automobile). Then, a subroutine 223 compares all the bits of the

WAVELYNX EX. 1003, Pg. 1241
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

incoming ID number to all the bits of the ID number for fob 4. If they are not equal, a negative result of a test 224 will reach a step 225 where n is decremented and a test 226 determines if all of the fobs have been checked or not. If they have, that means a signal has been received from a fob of another automobile by accident, or from some other unauthorized source. Therefore, an affirmative result of test 226 is taken to be a failure, and the wait step 220 is reached through the wait transfer point 219. Otherwise, the ID of another fob is checked in the subroutine 223. Assuming that the ID number matches for one of the fobs, another working number, N, is set equal to n so as to identify the words in the PROM and RAM needed for decryption, in a step 227. Since the received word may relate to a fob other than fob N, but having the same ID number, the shift register values for fob N are saved in a buffer, in a pair of steps 228, so they may be restored if authentication fails. This is also necessary since if a panic operation has been commanded, the iterations of the shift registers continue in a normal fashion, after performing the panic command. Then a test 229 determines if the P/R bit was present in the incoming word, or not. If it is present in the incoming word, the panic/resynch decrypt routine of Fig. 6 is reached through a transfer point 230.

In Fig. 6, the first steps 232 set a main working shift register (SR) and its mask equal to the secret initial value and the secret feedback mask for the 19 bit LFSR, respectively, from the PROM 40 for the selected fob N, and a C counter is set equal to 20 so as to cause 20 iterations. Then, a 20 iteration LFSR cycle subroutine 233 is performed on the 19 bit shift register. It is assumed that the 39 bit encrypted word portion of the 64 bit received word 38 is stored immediately in a 39 bit shift register location within the RAM 41, which is where it now can be found. Then the 39 bit encrypted word, in the 64 bit word 38, and the 39 bit secret mask for the fob N are provided to the shift register and the C counter is set for 39 iterations, in step 234. Then, a bitwise reverse LFSR iteration subroutine 235 is performed which looks at the low order bit to determine whether the bits corresponding to the mask should be flipped before they are shifted to the next lower order position in the shift register to reconstitute the original word prior to encryption. After each iteration, the C counter is decremented in a step 236 and when all 39 iterations have been performed, an affirmative result of a test 237 will reach a step 238 wherein the content of the working shift register is stored in the 39 bit shift register in RAM 41. The steps and tests 235-238 comprise a reverse cycle subroutine 239, which recovers the initial unencrypted value of the concatenation in the 39 bit shift register 69 in the fob.

Bits 19-38 of the decrypted 39 bit shift register are now loaded-into the working shift register in steps 242, the mask for the shift register is set equal to the 20 bit secret feedback mask for fob N from the EE PROM 40, and C is set equal to 20, and a 20 iteration, reverse LFSR cycle subroutine 243 is performed to recover the combined word (initial value plus random). In a subroutine 244, there is a bitwise comparison of the 39 bit shift register bits 27-38 with the twelve bits of the 20 bit secret initial value for fob N, from EE PROM 40, and of bits 5-18 of the 39 bit shift register with bits 5-18 of the 19 bit shift register for fob N, which are found in the RAM 41. This is equivalent to the comparison of the 12 high order bits on the trunk of lines 160 with those on the lines 161 and of the 14 bits on the line 128 with the 14 bits on the lines 129, in Fig. 2. If these are not equal, the decryption is unsuccessful, the attempted access is a failure, and a negative result of a test 246 will reach a test 247 to see if another fob could match the ID; if it might, Fig. 5 is reverted to through a transfer point 248, the shift registers for fob N are restored from the buffers in steps 249 (Fig. 5), and the process is repeated for another fob. If all fobs have had their ID's checked, the routine reaches a pair of steps 250 where the shift registers for fob N are returned to their former values, and the program enters the half second wait at step 220 through the transfer point 219.

If the comparison is successful, indicating partial authentication, an affirmative result of test 246 reaches a subroutine 252 where the value in the command register 138 is set equal to the exclusive OR of the low order bits of the 39 bit shift register and the low order bits of the 19 bit shift register, both taken from the RAM 41. Then, a test 253 determines if the panic/resynch bit was established in response to a resynch command. If not, the panic command is performed by turning on the lights, horn, or other alarm of the automobile in a step 254. Then, the shift registers for fob N are restored in the steps 250 and the wait step 220 is reached through the transfer point 219.

If the command were a resynch, a positive result of test 253 reaches a subroutine 255 which compares bits 19-26 of the 39 bit shift register (the regenerated random number) to a queue of previously used random numbers in the first in, first out stack (FIFO) 155, in EEPROM 40. If the random word compares to any of the last four (or whatever size FIFO is chosen) random words in the queue which were used in resynchronization, the resynchronization is deemed to be unsuccessful, since it is assumed that there has been clandestine playback of a copied random word. In such a case, an affirmative result of a test 256 reaches a subroutine 257 that rearranges the FIFO stack by moving the random word from its position in the queue in the FIFO stack to the first position thereof, and adjusting the position of the other words in the queue, without losing any. And, since this is deemed to be an unsuccessful attempt to resynchronize the unit, the old values in the 19 bit and 20 bit shift registers for fob N are restored in the steps 250. Then, the wait step 220 is reached through the transfer point 219.

If the random word did not compare with any word in the FIFO, a complete authentication exists, and a

WAVELYNX EX. 1003, Pg. 1242
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

negative result of test 256 reaches a subroutine 258 which rearranges the FIFO for fob N simply by adding bits 19-26 of the 39 bit shift register to the first location in the queue and shifting all the other words downward therein, causing the oldest word to fall out. In this case, the resynch operation is successful, so the steps 250 are bypassed and the setting of the 19 bit shift register for fob N in RAM 20 is left as it was established by the resynchronization operation, at subroutine 233. The 20 bit LFSR word created in the subroutine 243 is placed in the RAM for fob N (step 259), for use en futuro.

Resynchronization occurs only after: 20 iterations of the 19 and 20 bit shift registers from their secret initial values and the random number; performing 39 iterations in the 39 bit shift register with those values, and the exclusive OR of the command; reverse iterations of the 39 bit encrypted word in the receiver module; reverse iteration of the 20 bits which include the secret initial value of the 20 bit shift register and the random counter; generation and successful comparison of the high order bits of the 19 bit shift register; and a failure of comparison of the random word with any of the last four random words used to resynchronize the system. This is quite secure.

Assuming that there is no P/R bit 81 in the 64 bit word which is received, a negative result of test 229 in Fig. 5 will reach the normal command decryption routine of Fig. 7 through a transfer point 261. In the normal command decryption process, the iterated 19 bit and 20 bit words in the RAM 20 are given 1-3 additional iterations and compared with the reverse-processed bits of the 39 bit encrypted word. As described hereinbefore, since the fob may have its buttons pressed when the automobile cannot respond to it, they can become unsynchronized. Each time that a command is received in the receiver module 30, it is allowed 256 cycles to try to iterate to a correct pair of words that will match those which were transmitted to it. If it does so, then the command is responded to, and the iterated values are saved for authenticating the next command. If not, resynchronization is required, as described hereinbefore. In order to keep track of how many tries are made, the try counter 143 is set to its maximum count in a first one of a series of steps 262. Then, the working shift register (SR) is set equal to the 39 bit shift register in the RAM 20, which contains the 39 bit encrypted word. The mask for the shift register is set equal to the 39 bit secret feedback mask in the EE PROM 40, the C counter is set equal to 39, and a reverse LFSR cycle subroutine 267 is performed. Then a series of steps 271 cause the contents of the 20 bit shift register for fob N to be loaded from the RAM 41 into the working shift register (SR), the mask for the shift register is set equal to the secret feedback mask for fob N in the EE PROM 40 and a random bit is set equal to whatever bit or bits have been chosen for the 20 bit shift register (as described with respect to steps 199 in Fig. 3). Then the random bits are tested in a pair of steps 272, and if both are a 1, the C counter is set equal to 1 (step 273), if both are a 0, the C counter is set equal to 2 (step 274), and otherwise the C counter is set equal to 3 (step 274a). Then, an LFSR cycle subroutine 275 is performed. Then a series of steps and tests 276-279 prepare to run an LFSR cycle subroutine 280 for the 19 bit shift register in a similar fashion. Then a subroutine 284 does bit-by-bit comparisons of the 39 bit shift register to the 20 bit shift register and to the high order bit positions of the 19 bit shift register, for fob N. If all the bits are equal, an affirmative result of a test 285 causes the particular command to be found by exclusive ORing the 5 low order bits in a subroutine 286 and the command is performed in a step 287, such as locking or unlocking the door, or releasing the trunk lid. But if the bits do not compare, a negative result of test 285 reaches a step 288 where the try counter is decremented and a test 289 to determine if 256 tries have been made yet. If not, another pair of iterations 275, 280 are performed and compared. This goes on until the receiver module 30 catches up with the fob 16 (if it can). If after 256 tries, a comparison has not been reached, an affirmative result of test 289 will reach a test 290 to see if all the fobs have been given consideration. If not, the restoration steps 249 (Fig. 5) are reached through the transfer point 248. Otherwise, the shift registers for fob N are restored to their starting values in steps 292 and the program reverts to the wait step 220 (Fig. 5) through the transfer point 219.

In Fig. 8, an alternative random iteration utilizes a pair of bits from the random counter to determine the number of iterations of the 20 bit shift register operation and one bit thereof to determine the number of iterations in the 19 bit shift register operation. In a set of steps 199a (in place of steps and tests 199-202a, Fig. 3), the cycle counter, C, has its two low ordered bit positions (0, 1) set equal to the selected hits (3 and 6 in this example) of the random counter, and it is incremented to ensure that a zero-valued pair of bits will not result in no iteration. Similarly, steps 204a replace steps and test 204-207 to provide one or two iterations in the 19 bit operation. In Fig. 9, the random number is found at the head of the queue in the FIFO memory (40) for fob N. Steps 271a replaces steps and tests 271-274a and steps 276a replace steps and tests 276-279. In this embodiment, the number of iterations in each case is one higher (1-4; 1 or 2) than the value of the bit or bits (taken together as low ordered bits) selected from the random counter. However, fewer choices of the number of iterations may be used in response to random counter bits, as in tests 200 and 272, or by means of any other decode. Of course, more bits and higher numbers may be used.

In a system which uses only one or two fobs, or in which speed of response is not important, the system may be utilized without the use of ID numbers, simply by trying all of the sets of stored shift register words and masks; this would make the system subject to more nuisance iterations since the ID number would no longer

WAVELYNX EX. 1003, Pg. 1243
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

screen out many transmissions from similar, unauthorized systems. And there must be some sort of a tag to correlate the generated pseudo random words with the correct feedback mask for subsequent iterations, as well as with the correct initial value. This may be achieved by arbitrary numbering of the various sets of initial values and masks and corresponding registers for storing the iterated words.

The various number of iterations used during synchronization may be the same (e.g., 20, or more) for both random words generated from initial values, or they may be different (e.g., 20 and 19, or more).

As used herein, the term "encryption" inherently defines a process capable of decryption. Thus, if the process of encryption employs a pseudo random number generation operation of any type, that generation operation must be capable of being practiced in reverse, such as the reverse LFSR operation utilized herein. The encryption processes and operations used herein may be any of those described hereinbefore by way of example, and others. However, the LFSR pseudo random number generation operation is one of the easier ones to understand, and probably the simplest to implement in dedicated or quasi-dedicated hardware. That is, if the signal processing means of the invention includes dedicated shift registers and the like as may be implied in Figs. 1 and 2, the LFSR form of encryption may be preferred. Similarly, if the signal processing means of the present invention is implemented with microprocessors having suitable program routines as disclosed in Figs. 3-7 herein, the advantage of LFSR operations over other forms of encryption may be less distinct. The term "encryption" is, therefore, used herein in its broadest sense, so long as the word which becomes encrypted can be recovered through decryption.

In the foregoing embodiments, secret initial values and secret feedback masks for generating maximal length sequences of pseudo random numbers are essentially unique to each transmitter, but not necessarily totally unique. By this it is meant that the sets of two secret initial values and three secret feedback masks, taken together, are capable of distinguishing more vehicles than are made in a lifetime; however, the method of assignment, or human error or design, could result in some few with the same set of numbers. Within this definition, however, it is quite possible that several transmitters will have the same 19 bit secret initial value and/or the same 20 bit secret mask, or other similar combinations. In contrast, the use of a 16 bit identification number means that there will be several fobs each year possibly having the same identification number (but not the same secret values) so that over a course of time, there could be many fobs (such as about 5,000 fobs in the USA over a 10-year period for each possible identification number). Within statistical probability, it is possible that as many as one out of 10,000 automobiles having four fobs each may have two fobs with the same identification number. It is an important aspect of the present invention, that even if one fob having a correct identification number is not authenticated within 256 tries (or whatever is used), it will nonetheless try any other fob that may have the same ID number. If trying three or four fobs results in too much delay, the last tried fob is likely to be reported as faulty, and a new fob issued, with very minuscule likelihood that the new fob would have the same identification number as the remaining fobs in the set.

In the present embodiment, each encryption (such as the 19 bit, the 20 bit and the 39 bit shift register encryptions) are the same (linear feedback shift register pseudo random number generation). However, they need not all be the same, and in fact can be different algorithms to further confuse any attempted analysis. Similarly, the number of bits in the shift registers can be whatever is desired. In all cases, the greater number of bits, the harder to break the code by analysis. The numbers used herein provide a safe system, but greater or fewer numbers of bits may be chosen in practicing the invention if desired. Similarly, the words may be considered to be single words, or double words in the sense that the 19 bit shift register produces one portion of 14 bits which is used for cryptographic authentication, and another portion which carries the command but is not used in cryptographic comparison for authentication. These portions can be considered to be two different words except for the fact that in the embodiment herein they are generated in the same process. Of course, separate processes could be used, or two processes of a different split of numbers of bits could be used to encrypt and iterate the encryption of the word in which the command bits are found. For instance, in place of a single 19 bit shift register operation, a 10 bit shift register operation and a 9 bit shift register operation could be utilized, the results thereof concatenated, and five command bits exclusive ORed into a portion of one of them, before being used in the final encryption.

In the disclosed embodiments, the 20 bit shift register operation may employ one through five iterations, dependent upon the random occurrence of a pair of bits within the register, or a pair of random bits. Similarly, the 19 bit shift register operation may employ one through three iterations, depending upon one of its bits or a random bit. In the general case, these numbers may as well be reversed, they may be the same, they may depend on each other or on any pseudo random events that can be duplicated in the receiver, and/or either of them may be greater, provided that time constraints do not prohibit a greater number of iterations, and that every possible condition results in at least one iteration. It is to be noted that the small number of iterations would not be important but for the fact that in any given transmission, the receiver is allowed up to 256 attempts to catch up, iteratively, to the encryption process for the given transmitter (or for several transmitters). There is even more flexibility when the variable iterations are used in a

WAVELYNX EX. 1003, Pg. 1244
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

pseudo random number generator in other than transmitter/receiver environments (such as in computer processes).

Thus, although the invention has been shown and described with respect to exemplary embodiments thereof, it should be understood by those skilled in the art that the foregoing and various other changes, omissions and additions may be made therein and thereto, without departing from the scope of the invention as claimed in the appended claims.

Claims

1. A method of quickly generating successive pseudo random numbers, comprising:

   providing a starting number;
   providing an iteration control signal which changes in a pseudo random manner in response to the generation of each successive pseudo random number; and
   performing a variable number of iterations of an iterative pseudo random number generation operation on said starting number, said variable number determined by said iteration control signal.

2. A method according to claim 1 wherein said step of performing an iterative pseudo random number generation operation comprises performing a linear iterative pseudo random number generation operation.

3. A method according to claim 1 wherein said step of performing an iterative pseudo random number generation operation comprises performing a feedback shift register operation.

4. A method according to claim 1 wherein said step of performing an iterative pseudo random number generation operation comprises performing a linear feedback shift register operation.

5. A method according to claim 1 wherein said variable number of iterations is a small fraction of the degree of said starting number.

6. A method according to claim 1 wherein said starting number is an initial value.

7. A method according to claim 1 wherein said starting number is the pseudo random number generated in the prior iteration of said pseudo random number generation operation.

8. A method according to claim 1 wherein said iteration control signal changes in response to the value of a bit position of a changing number.

9. A method according to claim 8 wherein said iteration control signal changes in response to the value of a plurality of bit positions of a changing number.

10. A method according to claim 8 wherein said iteration control signal changes in response to the value of a bit position of said starting number.

11. A method according to claim 8 wherein said iteration control signal changes in response to the value of a plurality of bit positions of a random number.

WAVELYNX EX. 1003, Pg. 1245
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

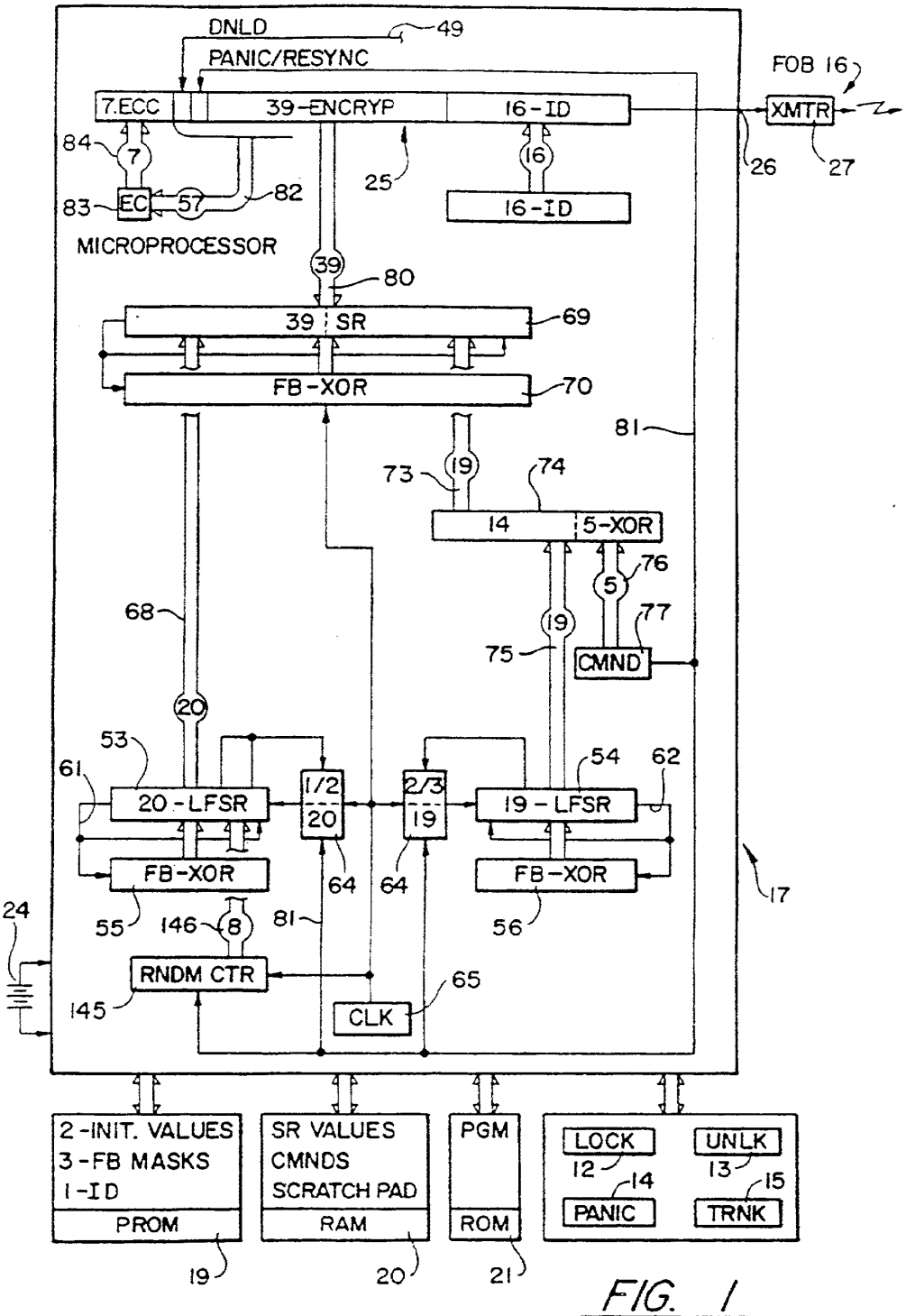


FIG. 1

WAVELYNX EX. 1003, Pg. 1246
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

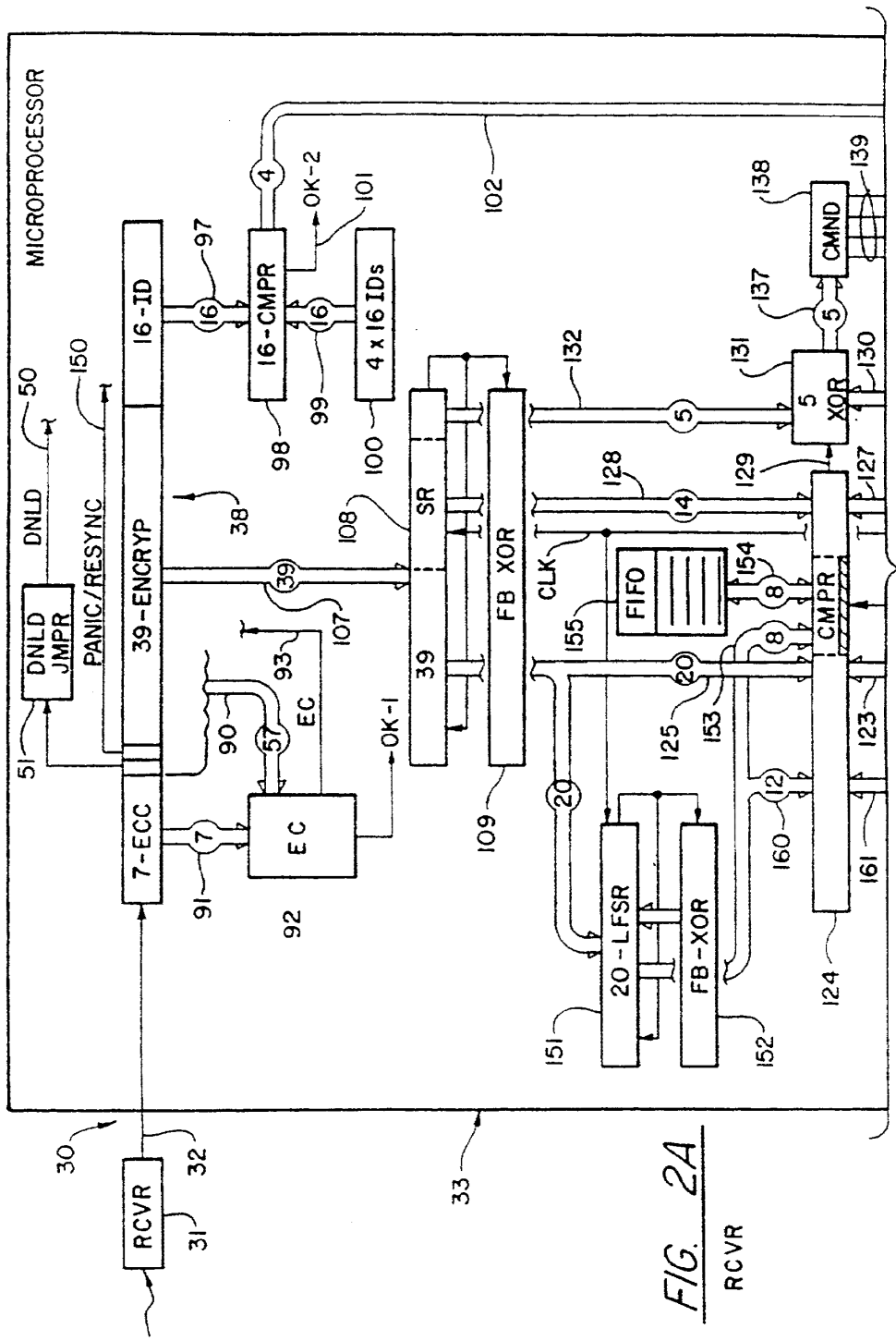


FIG. 2A

FIG. 2B

WAVELYNX EX. 1003, Pg. 1247
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

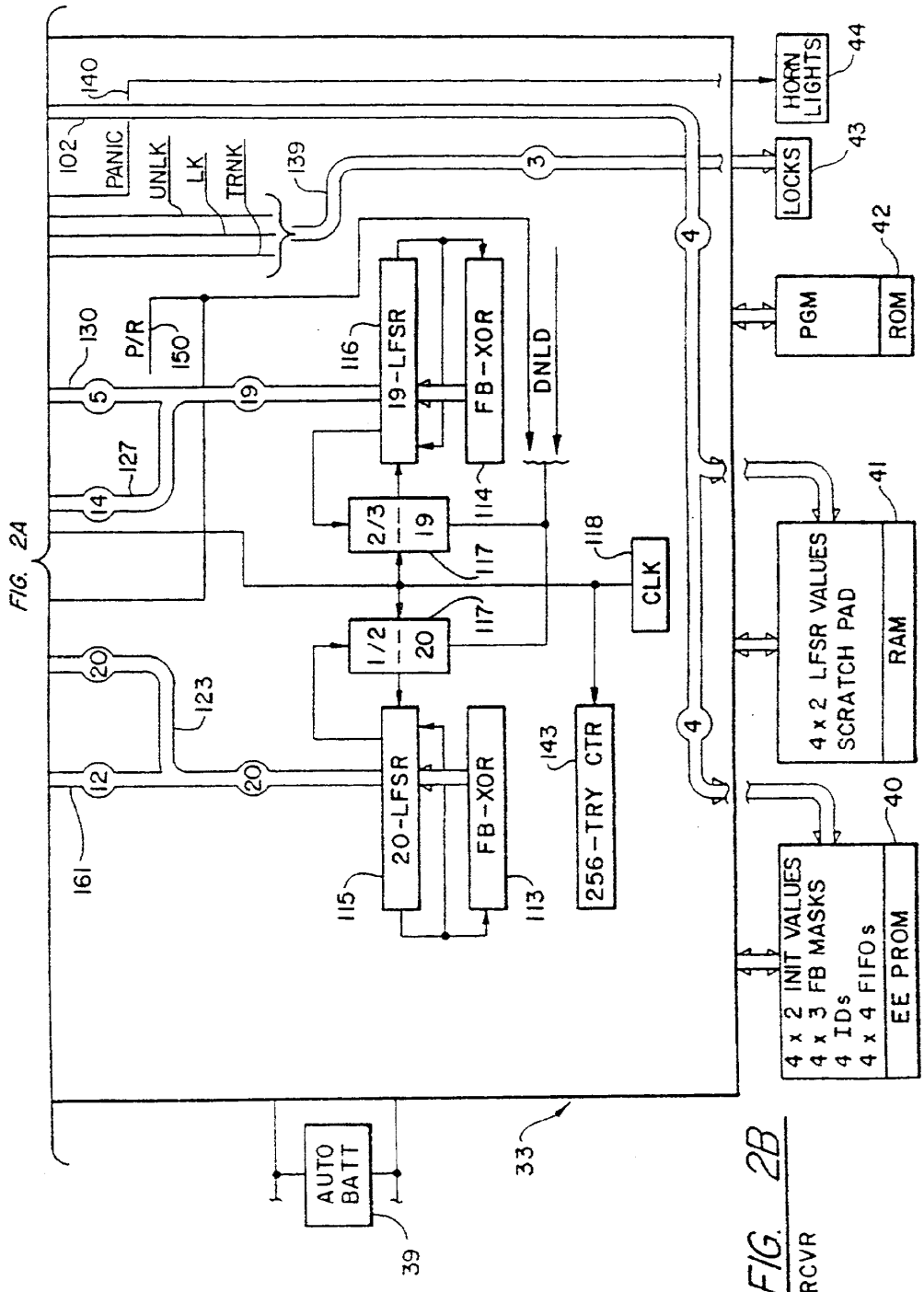


FIG. 2B
RCVR

WAVELYNX EX. 1003, Pg. 1248
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

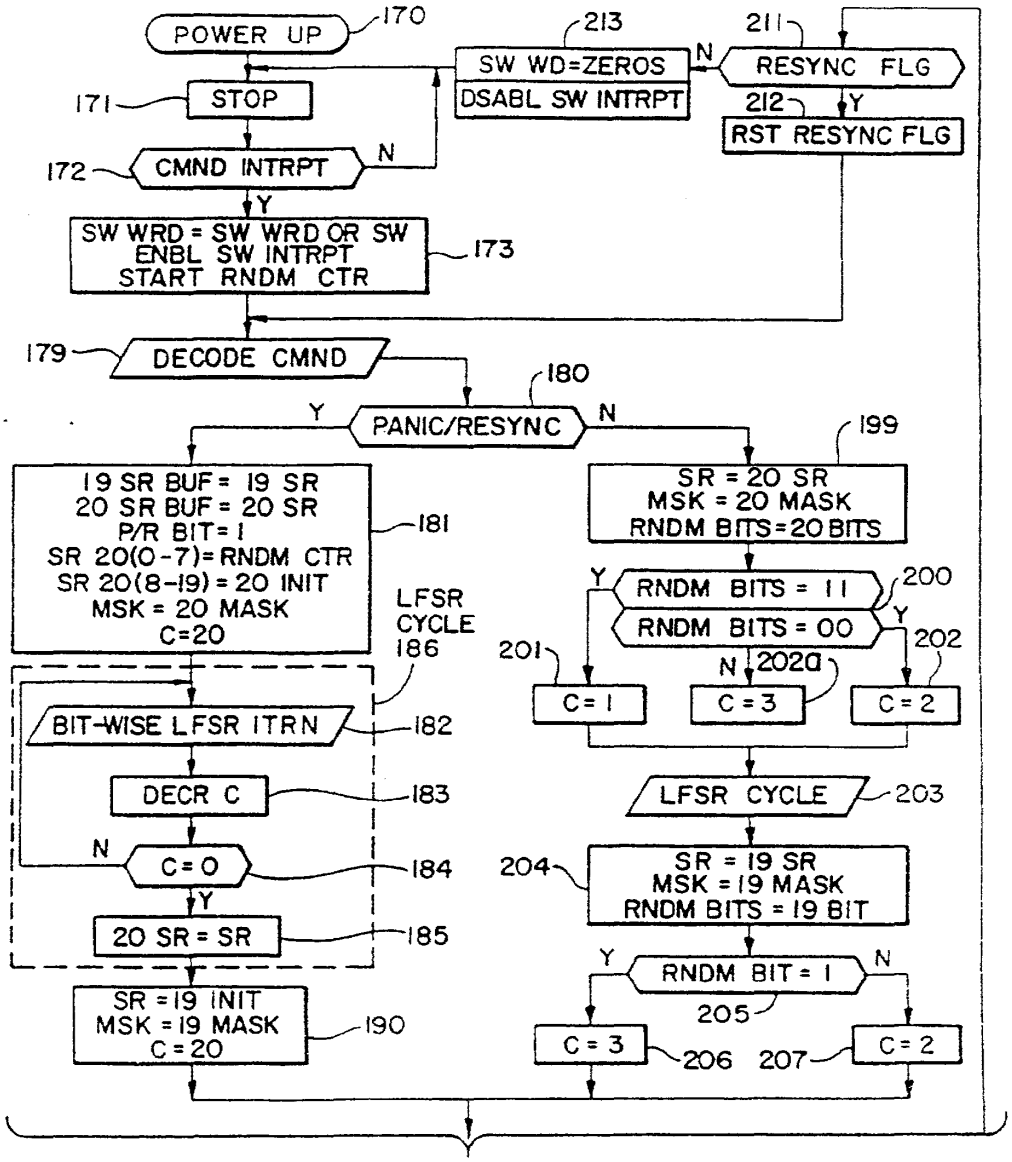


FIG. 3B

FIG. 3A

FOB - ENCRYP

WAVELYNX EX. 1003, Pg. 1249
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 3A

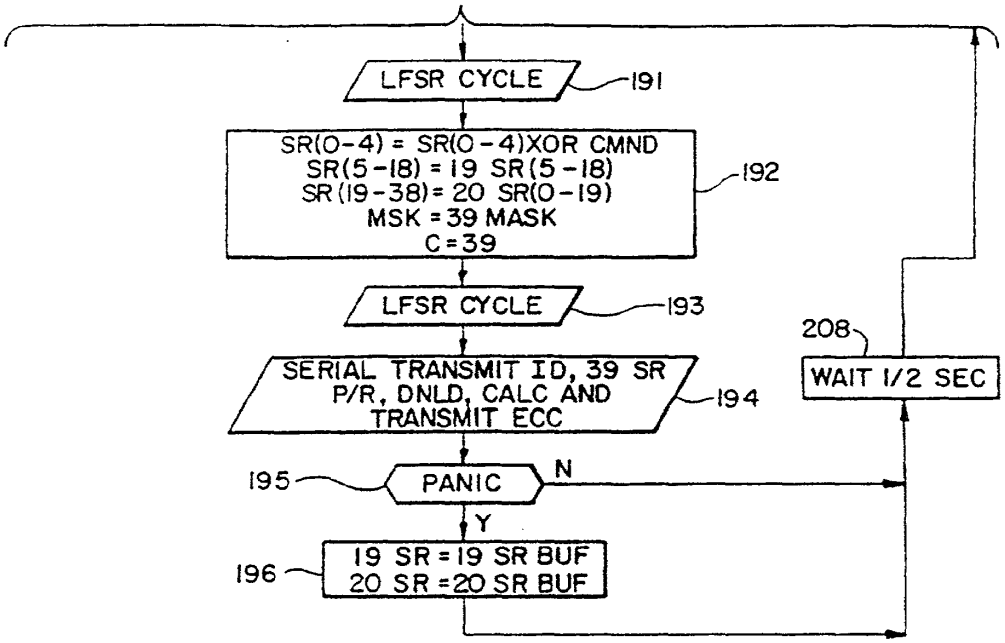


FIG. 3B

FOB - ENCRYP

WAVELYNX EX. 1003, Pg. 1250
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 4

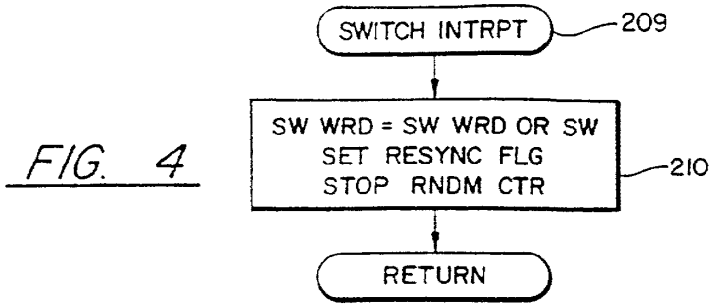


FIG. 5

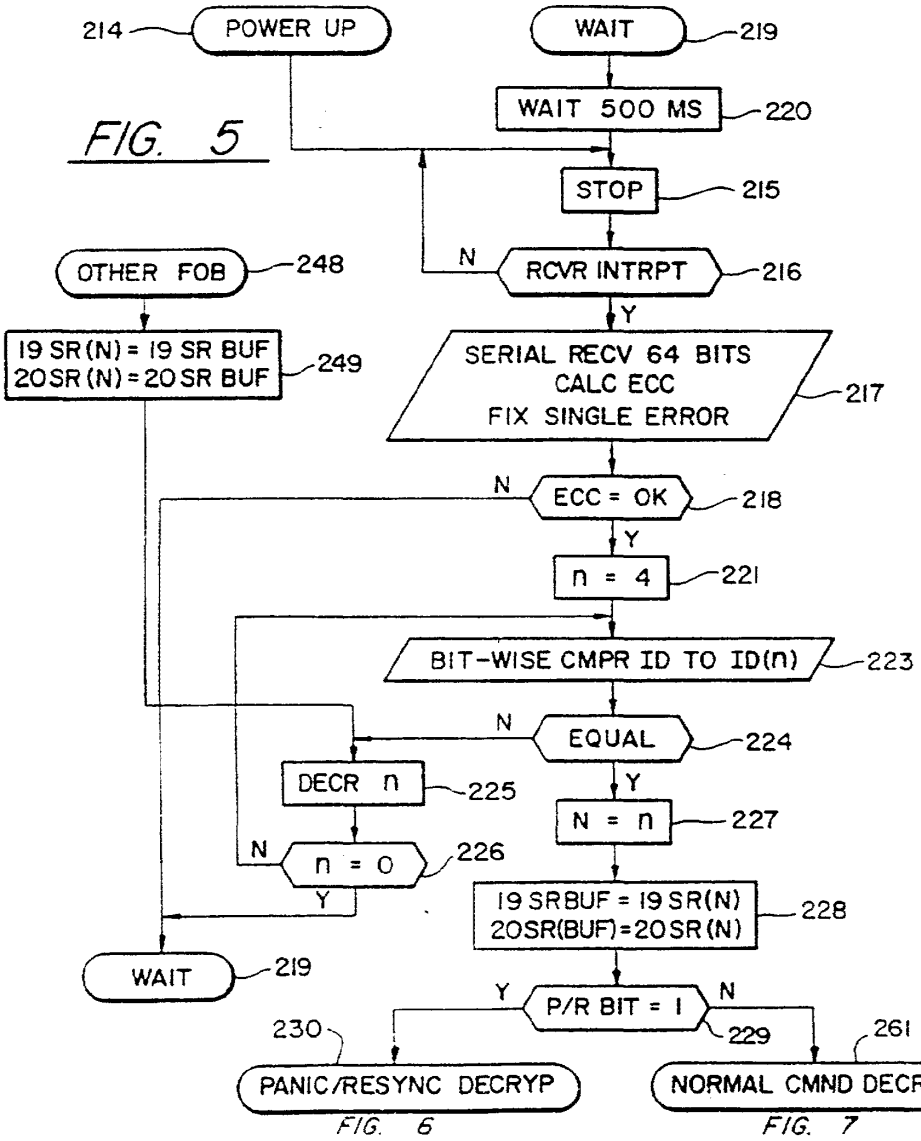
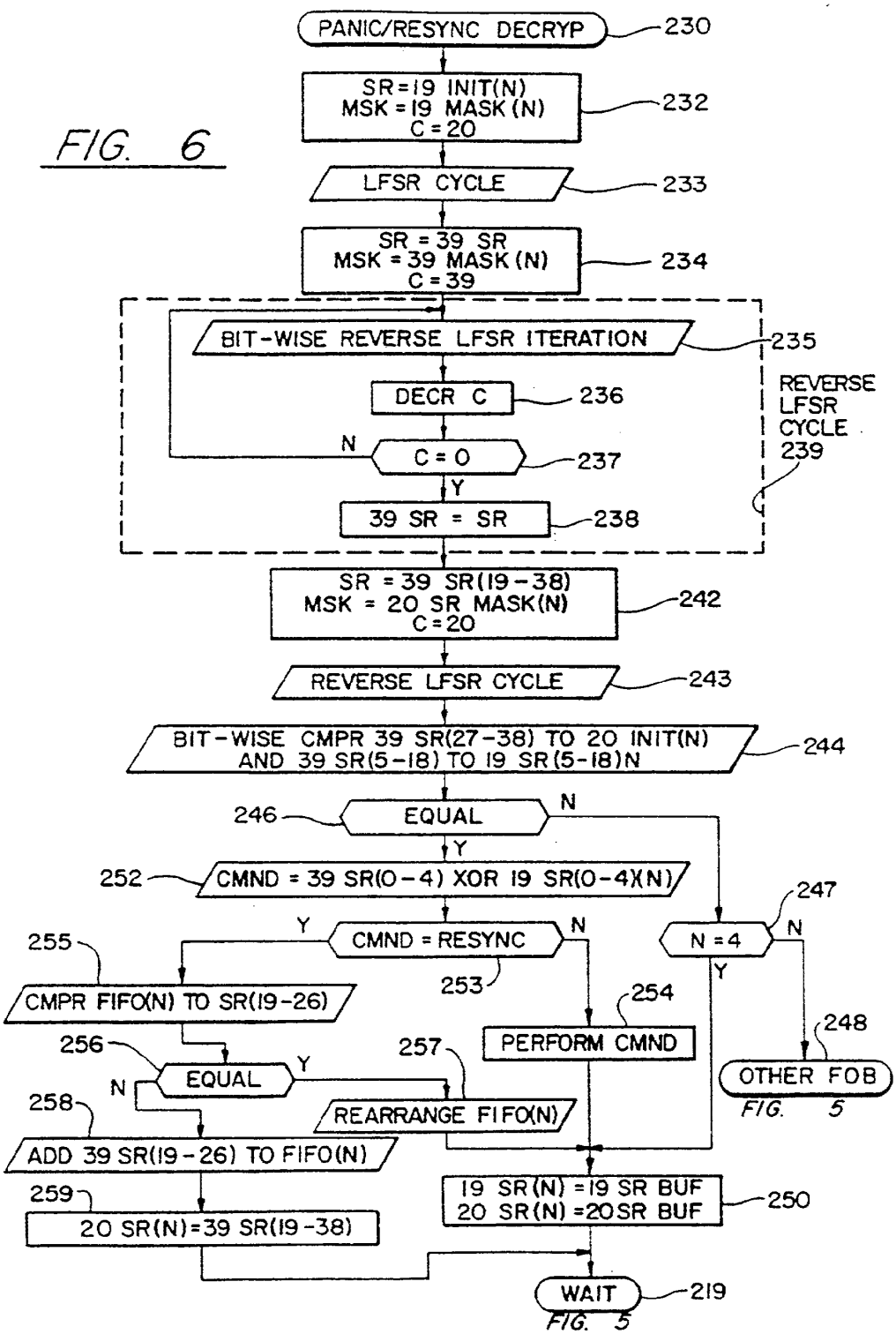


FIG. 6

FIG. 7

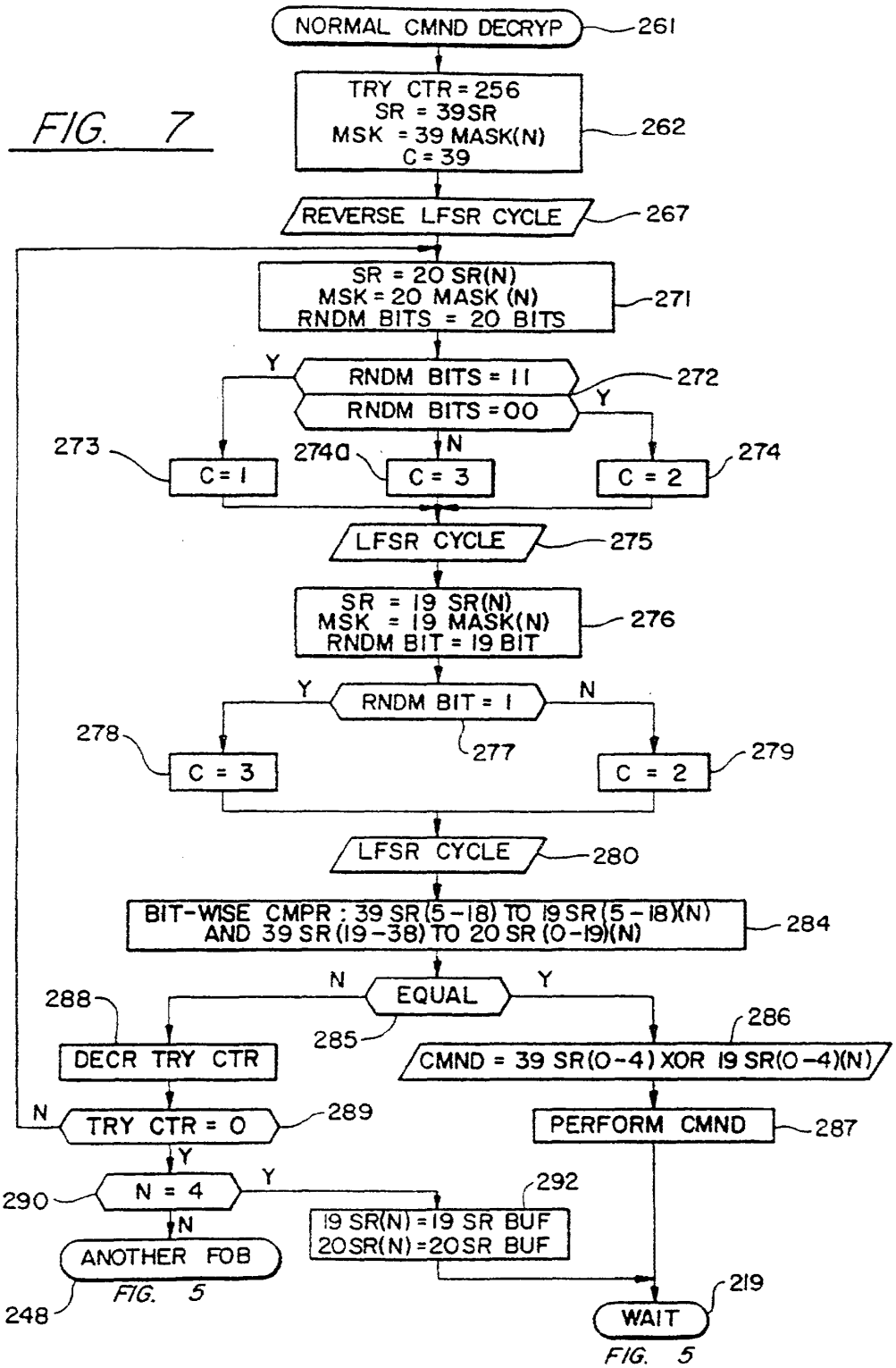
WAVELYNX EX. 1003, Pg. 1251
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 6



WAVELYNX EX. 1003, Pg. 1252
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 7



WAVELYNX EX. 1003, Pg. 1253
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

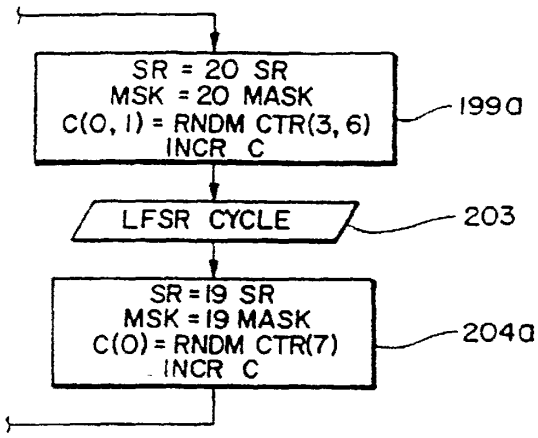


FIG. 8

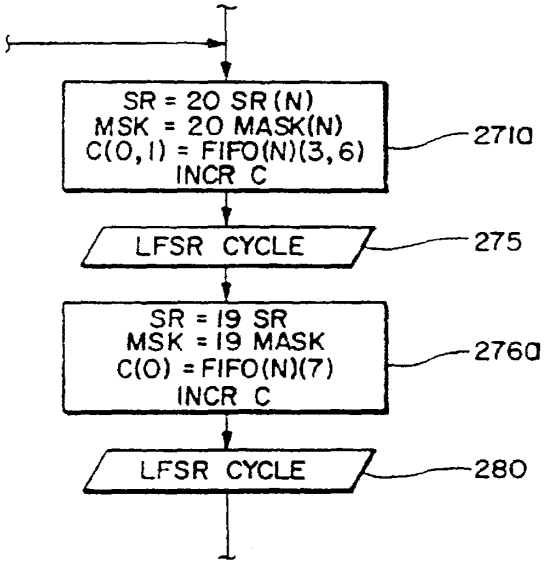


FIG. 9

WAVELYNX EX. 1003, Pg. 1254
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 20 1725

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 283 758 A (CRYPTO AG) 28 September 1988 * page 2, line 35 - line 51 *	1-4,7,8, 10	H04L9/22 H04L9/12 G06F7/58
A	* page 3, line 55 - page 4, line 13 *	9,11	
A	EP 0 220 437 A (BBC) 6 May 1987 * page 5, line 24 - page 7, line 28 * * abstract *	1-4	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

H04L
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 August 1998	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1255
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Method for generating pseudo-random data words to be used for encryption

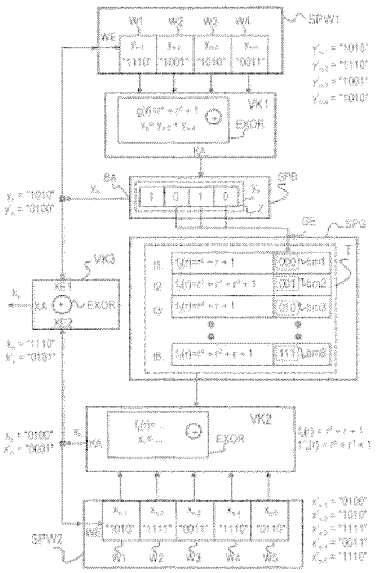
Publication number: EP0924894 (A2)
Publication date: 1999-06-23
Inventor(s): HEEKE HELMUT [DE] +
Applicant(s): SIEMENS AG [DE] +
Classification:
- international: ***H04L9/22; H04L9/24;*** **H04L9/18;** (IPC1-7): H04L9/22
- European: H04L9/22
Application number: EP19980123376 19981208
Priority number(s): DE19971057370 19971222

Also published as:
EP0924894 (A3)
DE19757370 (A1)
DE19757370 (C2)

Cited documents:
US4860353 (A)
US5432853 (A)
US5079733 (A)
US4817145 (A)

Abstract of **EP 0924894 (A2)**

The method involves forming first and second pseudo-random data words (yn,xn) using first and second methods, respectively, for generating pseudo-random data words. The second data words are generated dependent on at least one actual generated first data word. Pseudo-random data words (kn) are generated using first and second generated data words. Preferably, a further pseudo-random data word is generated using a further method. The further data word and the first and second data words are used to generated the pseudo-random data words.



Data supplied from the ***espacenet*** database — Worldwide

WAVELYNX EX. 1003, Pg. 1256
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 924 894 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
23.06.1999 Patentblatt 1999/25

(51) Int. Cl.[6]: **H04L 9/22**

(21) Anmeldenummer: **98123376.0**

(22) Anmeldetag: **08.12.1998**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

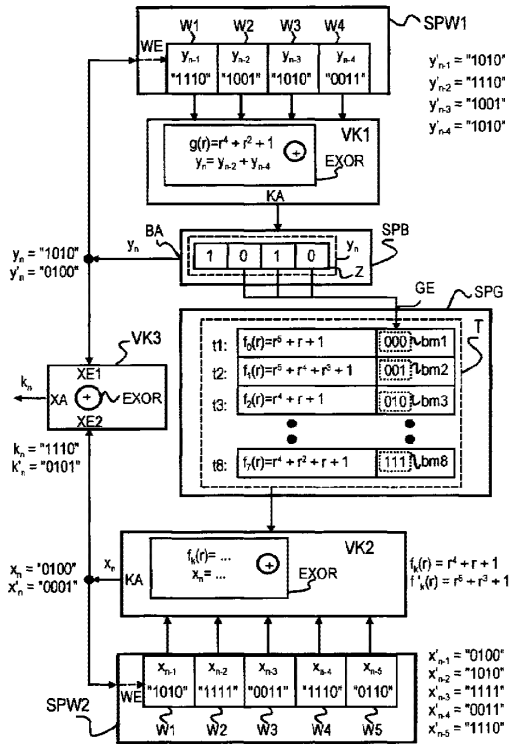
(30) Priorität: **22.12.1997 DE 19757370**

(71) Anmelder:
SIEMENS AKTIENGESELLSCHAFT
80333 München (DE)

(72) Erfinder: **Heeke, Helmut**
81245 München (DE)

(54) Verfahren zur Erzeugung pseudo-zufälliger Datenworte zur Verschlüsselung

(57) Mit Hilfe eines ersten Verfahrens werden erste pseudozufällige Datenworte (y_n) gebildet und in Abhängigkeit von diesen aus mehreren Verknüpfungsvorschriften ($f_{0...7}(r)$) eine aktuelle Verknüpfungsvorschrift ($f_k(r)$) ausgewählt. Mit Hilfe eines zweiten Verfahrens werden zweite pseudo-zufällige Datenworte (x_n) durch Verknüpfung von Datenworten ($x_{n-1}...x_{n-5}$) einer Folge von Datenworten gemäß der aktuell ausgewählten Verknüpfungsvorschrift ($f_k(r)$) gebildet. Aus den zweiten pseudo-zufälligen Datenworten (x_n) werden pseudo-zufällige Datenworte (k_n) gebildet, wobei diese vorteilhaft zur zuverlässigen Verschlüsselung hochbitratiger Nutzinformationen vorgesehen sind.



EP 0 924 894 A2

WAVELYNX EX. 1003, Pg. 1257
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Beschreibung

[0001] In der aktuellen Kommunikationstechnik werden für die Sicherung und die Authentifizierung vertraulicher, über drahtgebundene oder drahtlose Kommunikationsnetze zu übermittelnder Nutzdaten unterschiedliche Verschlüsselungsverfahren eingesetzt. Aktuelle Verschlüsselungsverfahren sind entweder dem Blockchiffrierungs- oder den Stromchiffrierungsverfahren zuzuordnen.

[0002] Beim Blockchiffrierungsverfahren werden Nutzinformationen repräsentierende Datenbits oder aus mehreren Datenbits bestehende Datenworte zu einer Gruppe von Datenbits oder Datenworte zusammengefaßt und gemeinsam verschlüsselt. Einfache Blockchiffrierungsverfahren basieren beispielsweise auf einfachen Zeichensubstitutionen und verarbeiten 8 zu einer Gruppe oder zu einem Datenblock zusammengefaßte Datenbits. Polyalphabetische Verfahren - auch als Vigenere-Chiffrierung bezeichnet - verarbeiten beispielsweise Datenblöcke von 8 Byte oder 256 Byte, wobei die Datenbits eines Datenblockes auf komplizierte Weise verknüpft werden. Beispiele für implementierte Blockchiffrierungsverfahren sind: DES - Digital Encryption Standard -, IDEA, RC5.

[0003] Stromchiffrierungsverfahren werden beispielsweise zur OnlineChiffrierung von Nachrichtenkanälen oder zur Verschlüsselung von auf Patenträger zu speichernden Nutzinformationen eingesetzt. In Abhängigkeit von einem Schlüssel wird eine pseudozufällige, aus Datenbits oder Datenworte bestehende Datenwortfolge erzeugt, mit welcher die zu verschlüsselnden Nutzinformationen Exklusiv-ODER verknüpft werden. Die Sicherheit eines Chiffrierverfahrens, insbesondere der Stromchiffrierungsverfahren, ist von der Qualität der erzeugten pseudo-zufälligen Folge von Datenbits oder Datenworten abhängig. Pseudo-zufällige Datenworte müssen ein statistisch eindeutiges Verhalten aufweisen, wobei aus einer Teilfolge der erzeugten, pseudozufällige Datenworte nicht die gesamte Datenwortfolge oder der Schlüssel zur Erzeugung der pseudozufälligen Datenworte rekonstruierbar sein darf. Bekannte Stromchiffrierungsverfahren sind beispielsweise: RC4, SEAL, oder A5.

[0004] In der Druckschrift "Abenteuer Kryptologie: Methoden, Risiken und Nutzen der Datenverschlüsselung, Reinhard Wobst, Bonn, Reading, Massachusetts [u.a.], Addison-Wesley-Longman, 1997" ist beispielsweise die Verschlüsselung von GSM-Funkkanälen in drahtlosen Kommunikationsnetzen mit Hilfe des Stromchiffrierungsverfahrens "A5" beschrieben. Bei dem beschriebenen Algorithmus werden für die Erzeugung von pseudo-zufälligen Datenbits Schieberegister mit linearer Rückkopplung - auch als LFSR bzw. Linear Feedback Shift Register bezeichnet - eingesetzt. Ein Schieberegister stellt eine Speicherzelle dar, in welcher eine beliebige Anzahl z von Datenbits speicherbar sind. Schieberegister sind vorteilhaft durch eine hohe Verarbeitungsgeschwindigkeit aufweisende Schaltkreise realisierbar. Durch im Schieberegister realisierte, lineare Funktionen werden bestimmte, in den Speicherzellen des Schieberegisters gespeicherte Datenbits ausgewählt und Exklusiv-ODER verknüpft. Bei einer anschließenden, durch Taktsignale gesteuerten Links- bzw. Rechts-Verschiebung der im Schieberegister angeordneten Datenbits wird durch die Rückkopplung das im vorhergehenden Taktintervall gebildete Verknüpfungsergebnis in der frei gewordenen höchst- oder niederwertigsten Speicherzelle des Schieberegisters gespeichert, wobei das vorhergehende nieder- oder höchstwertigste Datenbit über einen Ausgang weitergeleitet wird - vgl. Seite 209, Abb. 5.18. Zur Verschlüsselung von Nutzinformationen wird entweder das bei jedem Taktintervall erzeugte, aktuelle Verknüpfungsergebnis der Exklusiv-ODER Verknüpfung oder das bei jeder Verschiebung des Schieberegisters an den Ausgang geleitete Datenbit als pseudo-zufällige Datenbit-Folge zur Verschlüsselung von Nutzinformationen genutzt. Bei einer Initialisierung des Schieberegisters zu Beginn eines Verschlüsselungsvorgangs werden gemäß eines vorher definierten Schlüssels in den einzelnen Speicherzellen des Schieberegisters bestimmte Initialisierungs-Datenbits gespeichert. Mit Hilfe des beschriebenen LFSR-Schieberegisters kann eine pseudo-zufällige Folge von Datenbits mit einer Periodenlänge von max. 2^{z-1} erzeugt werden, wobei z der Anzahl der im LFSR-Schieberegister gespeicherten Datenbits entspricht. Den ständig steigenden sicherheitstechnischen Anforderungen in der Kommunikationstechnik, insbesondere bei der übermittlung von vertraulichen Informationen, können die bekannten Verschlüsselungsverfahren nicht immer gerecht werden.

[0005] Der Erfindung liegt daher die Aufgabe zu Grunde, die Verschlüsselung bzw. die Chiffrierung von in Kommunikationsnetzen, insbesondere in Teilnehmeranschlußnetzen zu übermittelnden oder in diesen zu speichernden Nutzinformationen zu verbessern. Die Aufgabe wird durch die Merkmale des Patentanspruchs 1 gelöst.

[0006] Beim erfindungsgemäßen Verfahren zur taktilen Erzeugung pseudo-zufälliger Datenworte werden erste pseudo-zufällige Datenworte mit Hilfe eines ersten Verfahrens zur Erzeugung pseudo-zufälliger Datenworte und zweite pseudo-zufällige Datenworte mit Hilfe eines zweiten Verfahrens zur Erzeugung pseudo-zufälliger Datenworte gebildet. Der wesentliche Aspekt des erfindungsgemäßen Verfahrens besteht darin, daß in Abhängigkeit von den gebildeten ersten pseudo-zufälligen Datenworten aus mehreren Verknüpfungsvorschriften eine aktuelle Verknüpfungsvorschrift ausgewählt wird, und daß die zweiten pseudo-zufälligen Datenworte durch Verknüpfung von Datenworten einer Folge von Datenworten gemaß der aktuell ausgewählten Verknüpfungsvorschrift gebildet werden. Aus den zweiten pseudo-zufälligen Datenworten werden die pseudo-zufälligen Datenworte gebildet.

WAVELYNX EX. 1003, Pg. 1258
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0007] Der wesentliche Vorteil des erfindungsgemäßen Verfahrens besteht darin, daß einer Folge von Datenworten mehrere Rückkopplungsfunktionen zugeordnet sind, wobei abhängig vom Verarbeitstakt, bzw. für die Dauer eines Verarbeitungstaktes jeweils eine Rückkopplungsfunktion zufällig ausgewählt wird. Durch die erfindungsgemäße schnelle Variation der aktuell ausgewählten Rückkopplungsfunktionen, werden lineare Zusammenhänge zerstört. Ein weiterer Vorteil des erfindungsgemäßen Verfahrens besteht darin, daß durch die Verwendung bzw. Verknüpfung von Datenworten die gebildeten pseudo-zufälligen Datenworte mit einer hohen Datenrate bereitgestellt werden. Durch die dadurch ermöglichte Verarbeitung der zu übermittelnden Informationen mit vielen unterschiedlichen Rückkopplungsfunktionen wird die Sicherung von hochbitratigen, über ein Kommunikationsnetz zu übermittelnden und/oder in diesen zu speichernden Nutzinformationen gegen den Zugriff unbefugter Dritter erheblich verbessert.

[0008] Vorteilhaft werden beim ersten Verfahren zur Erzeugung pseudo-zufälliger Datenworte die ersten pseudo-zufälligen Datenworte durch Verknüpfung von Datenworten einer ersten Folge von Datenworten gemäß einer ersten Verknüpfungsvorschrift gebildet - Anspruch 3. Durch diese vorteilhafte Ausgestaltung ist das erfindungsgemäße Verfahren ohne großen technischen Aufwand mit Hilfe von Rechner-gesteuerten Prozessen realisierbar, wobei die pseudo-zufälligen Datenworte mit einer hohen Datenrate bereitgestellt werden.

[0009] Gemäß einer vorteilhaften Ausgestaltung werden weitere pseudo-zufällige Datenworte durch Verknüpfung von Datenworten einer weiteren Folge von Datenworten gemäß einer weiteren Verknüpfungsvorschrift gebildet, wobei die aktuelle weitere Verknüpfungsvorschrift in Abhängigkeit von den gebildeten ersten und/oder zweiten pseudo-zufälligen Datenworten aus den mehreren Verknüpfungsvorschriften und/oder aus mehreren weiteren Verknüpfungsvorschriften ausgewählt wird. Mit Hilfe der gebildeten ersten und/oder zweiten und/oder weiteren pseudozufälligen Datenworte werden die pseudo-zufälligen Datenworte gebildet - Anspruch 4. Durch diese vorteilhafte Ausgestaltung wird eine beliebige Skalierbarkeit des erfindungsgemäßen Verfahrens ermöglicht, wobei die Rekonstruierbarkeit der erzeugten, pseudo-zufälligen Datenworte bzw. die Rekonstruierbarkeit des dem Verschlüsselungsverfahren zu Grunde liegenden Schlüssels weiter erschwert wird.

[0010] Gemäß einer weiteren vorteilhaften Ausgestaltung wird die Erzeugung der ersten pseudo-zufälligen Datenworte mit einer 1 bis m vorgegebene Datenworte aufweisenden ersten Datenwort-Startfolge und die Erzeugung der zweiten pseudo-zufälligen Datenworte mit einer 1 bis l vorgegebene Datenworte aufweisenden zweiten Datenwort-Startfolge gestartet. Während des Ablaufs des erfindungsgemäßen Verfahrens wird bei jedem Verarbeitungstakt aus den aktuell vorliegenden Folgen von Datenworten gemäß der ersten und der ausgewählten Verknüpfungsvorschrift das erste und das zweite pseudo-zufällige Datenwort gebildet und das vorhergehend erste bis (m-1)-te Datenwort der ersten Folge von Datenworten zum aktuellen zweiten bis mten Datenwort der ersten Folge von Datenworten. Das vorhergehend erste bis (l-1)-te Datenwort der zweiten Folge von Datenworten wird zum aktuellen zweiten bis l-ten Datenwort der zweiten Folge von Datenworten und das gebildete erste und zweite pseudo-zufällige Datenwort wird zum aktuellen ersten Datenwort der ersten und zweiten Folge von Datenworten. Die Datenworte und die gebildeten ersten und zweiten pseudozufälligen Datenworte und die gebildeten pseudozufälligen Datenworte repräsentieren vorteilhaft binäre Informationen - Anspruch 5 und 6. Durch diese vorteilhafte Ausgestaltung ist das erfindungsgemäße Verfahren mit Hilfe von Hardware-Implementierungen - beispielsweise durch Schieberegister mit linearer Rückkopplung - realisierbar, wobei durch den Einsatz schaltungstechnischer Komponenten eine hohe Verarbeitungsgeschwindigkeit erreicht wird und vorteilhaft eine eine hohe Datenrate aufweisende Folge von pseudo-zufälligen Datenworte zur Verschlüsselung hochbitratiger Datenströme erzeugt wird.

[0011] Vorteilhaft erfolgt die Bildung der ersten pseudo-zufälligen Datenworte mit einem ersten Verarbeitungstakt und die Bildung der zweiten pseudo-zufälligen Datenworte mit einem zweiten Verarbeitungstakt - Anspruch 11. Durch die Verwendung unterschiedlicher Verarbeitungstakte wird die Qualität der Verschlüsselung weiter verbessert.

[0012] Weitere vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind den weiteren Ansprüchen zu entnehmen.

[0013] Im folgenden wird das erfindungsgemäße Verfahren anhand eines den erfindungsgemäßen Ablauf zur Bildung pseudo-zufälliger Datenworte k_n darstellenden Blockschaltbildes näher erläutert.

[0014] Das Blockschaltbild zeigt einen ersten Datenwortspeicher SPW1, in welchem gemäß diesem Ausführungsbeispiel - m = 4 - vier Datenwort-Speicherzellen W1...4 angeordnet sind. In jeder Datenwort-Speicherzelle W1...4 ist ein Datenwort $y_{n-1}...y_{n-4}$ speicherbar, wobei die gespeicherten Datenworte $y_{n-1}...y_{n-4}$ jeweils eine binäre Information mit der Wortbreite b repräsentieren. Die Wortbreite b ist beliebig wählbar - $b \geq 1$ -; in diesem Ausführungsbeispiel weisen die Datenworte $y_{n-1}...y_{n-4}$ jeweils eine Wortbreite von b = 4 Bit auf. Die im ersten Datenwortspeicher SPW1 gespeicherten Datenworte $y_{n1}...y_{n-4}$ werden über Verbindungsleitungen einer ersten dem ersten Datenwortspeicher SPW1 zugeordneten Verknüpfungseinheit VK1 zugeführt - durch Pfeile angedeutet. Durch in der ersten Verknüpfungseinheit VK1 angeordnete Verknüpfungsmittel EXOR wird aus den herangeführten Datenworten $y_{n-1}...y_{n-4}$ gemäß einer vorgegebenen, ersten

WAVELYNX EX. 1003, Pg. 1259
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Verknüpfungsvorschrift g ein erstes Verknüpfungsergebnis y_n gebildet. In diesem Ausführungsbeispiel ist die erste Verknüpfungsvorschrift g durch ein erstes Generatorpolynom $g(r) = r^4 + r^2 + 1$ beschrieben, nach welchem das zweite, an die erste Verknüpfungseinheit VK1 herangeführte Datenwort y_{n-2} und das vierte, an die erste Verknüpfungseinheit VK1 herangeführte Datenwort y_{n-4} zu dem aktuellen ersten Verknüpfungsergebnis y_n Exklusiv-ODER verknüpft, und das gebildete erste Verknüpfungsergebnis y_n an einen Ausgang KA der ersten Verknüpfungseinheit VK1 weitergeleitet wird. Das am Ausgang KA anliegende, erste Verknüpfungsergebnis y_n wird in einer Speicherzelle Z eines Bitmuster-Speichers SPB gespeichert - durch einen Pfeil angedeutet. Durch im Bitmuster-Speicher SPB angeordnete Maskierungs-Mittel - nicht dargestellt - werden die drei niederwertigsten Datenbits des in der Speicherzelle Z gespeicherten Datenwortes y_n erfaßt und aus diesen ein aktuelles Bitmuster bm_n gebildet, wobei das gebildete, aktuelle Bitmuster bm_n an einen Eingang GE eines Speichers SPG herangeführt ist. Des Weiteren ist das in der Speicherzelle Z gespeicherte erste Verknüpfungsergebnis Y_n über einen Ausgang BA des Bitmuster-Speichers SPB und über Verbindungsleitungen an einen Eingang WE des ersten Datenwortspeichers SPW1 und an einen ersten Eingang XE1 eines dritten Verknüpfungsmittels VK3 geführt. Der Eingang WE des ersten Datenwortspeichers SPW1 ist mit der ersten im ersten Datenwortspeicher SPW1 angeordneten Speicherzelle W1 verbunden - durch einen strichlierten Pfeil angedeutet.

[0015] Im Speicher SPG ist eine acht Tabelleneinträge t1...8 aufweisende Tabelle T angeordnet. In jedem Tabelleneintrag t1...8 ist ein, jeweils eine zweite Verknüpfungsvorschrift $f_{0...7}$ repräsentierendes, zweites Generatorpolynom $f_{0...7}(r)$ gespeichert, wobei jeder gespeicherten zweiten Verknüpfungsvorschrift $f_{0...7}$, bzw. jedem gespeichertem zweiten Generatorpolynom $f_{0...7}(r)$ eine durch eine binäre Information der Wortbreite von beispielsweise n = 3 repräsentierte Bitmusterkombination bm1...8 zugeordnet ist. Beispielsweise ist die erste zweite Verknüpfungsvorschrift f_0 durch das erste zweite Generatorpolynom $f_0(r) = r^5 + r + 1$ dargestellt, wobei dem ersten zweiten Generatorpolynom $f_0(r)$ die erste Bitmusterkombination bm0 = „000" zugeordnet ist. Des Weiteren ist die zweite zweite Verknüpfungsvorschrift f_1 durch das zweite zweite Generatorpolynom $f_1(r) = r^5 + r^4 + r^3 + 1$ dargestellt, welcher die zweite Bitmusterkombination bm2 = „001" zugeordnet ist. Dem im dritten Tabelleneintrag t3 gespeicherten dritten zweiten Generatorpolynom $f_2(r) = r^4 + r + 1$ ist die dritte Bitmusterkombination bm3 = „010" und beispielsweise dem im achten Tabelleneintrag t8 gespeicherten, achten zweiten Generatorpolynom $f_7(r) = r^4 + r^2 + r + 1$ ist die achte Bitmusterkombination bm8 = „111" zugeordnet.

[0016] Durch im Speicher SPG angeordnete Vergleicher-Mittel - nicht dargestellt - wird das am Eingang GE des Speichers SPG anliegende, aktuelle Bitmuster bm_n mit den in den einzelnen Tabelleneinträgen t0...7 gespeicherten Bitmusterkombinationen bm1...8 verglichen und diejenige Bitmusterkombination bm1...8 ermittelt, welche mit dem am Eingang GE anliegenden aktuellen Bitmuster bm_n identisch ist. Nach Bestimmung der mit dem aktuellen Bitmuster bm_n übereinstimmenden Bitmusterkombination bm1...8 wird die entsprechende, der identischen Bitmusterkombination bm1...8 zugeordnete Verknüpfungsvorschrift $f_{0...7}$ bzw. das diese darstellende Generatorpolynom $f_{0...7}(r)$ ausgewählt und das ausgewählte Generatorpolynom $f_{0...7}(r)$ über einen Ausgang GA des Speichers SPG an eine dem Speicher SPG zugeordnete zweite Verknüpfungseinheit VK2 übermittelt - durch einen Pfeil angedeutet.

[0017] Die zweite Verknüpfungseinheit VK2 weist Verknüpfungsmittel EXOR auf, in welcher die vom Speicher SPG an die zweite Verknüpfungseinheit VK2 herangeführte Verknüpfungsvorschrift $f_{0...7}$ als aktuell ausgewählte Verknüpfungsvorschrift f_k bzw. als aktuell ausgewähltes Generatorpolynom $f_k(r)$ gespeichert ist. Die zweite Verknüpfungseinheit VK2 ist über Verbindungsleitungen - nicht dargestellt - mit einem zweiten Datenwortspeicher SPW2 verbunden. Gemäß dem Ausführungsbeispiel sind im zweiten Datenwortspeicher SPW2 fünf Datenwort-Speicherzellen W1...5 angeordnet - 1 = 5 -, in welche jeweils ein eine binäre Information mit der Wortbreite c darstellendes Datenwort $x_{n-1}...x_{n-5}$ speicherbar ist. Die Wortbreite c ist beliebig wählbar - $c \geq 1$ -; vorteilhaft ist im Ausführungsbeispiel die Wortbreite c der im zweiten Datenwortspeicher SPW2 gespeicherten Datenworte $x_{n-1}...x_{n-5}$ an die Wortbreite b der im ersten Datenwortspeicher SPW1 gespeicherten Datenworte $y_{n-1}...y_{n-4}$ angepaßt - c = b = 4 Bit. Jedes der im zweiten Datenwortspeicher SPW2 gespeicherten Datenworte $y_{n-1}...y_{n-5}$ wird der zweiten Verknüpfungseinheit VK2 zugeführt - durch Pfeile angedeutet. Durch die in der zweiten Verknüpfungseinheit VK2 angeordneten Verknüpfungsmittel EXOR werden die herangeführten Datenworte $x_{n-1}...x_{n-5}$ gemäß der ausgewählten, vom Speicher SPG an die zweite Verknüpfungseinheit VK2 herangeführten und in dieser gespeicherten Verknüpfungsvorschrift f_k bzw. gemäß dem die ausgewählte Verknüpfungsvorschrift f_k repräsentierenden Generatorpolynom $f_k(r)$ zu einem aktuellen zweiten Verknüpfungsergebnis x_n verknüpft, und anschließend das gebildete zweite Verknüpfungsergebnis x_n an einen Ausgang KA der zweiten Verknüpfungseinheit VK2 geführt.

[0018] Das am Ausgang KA der zweiten Verknüpfungseinheit VK2 anliegende zweite Verknüpfungsergebnis x_n wird über Verbindungsleitungen an einen zweiten Eingang XE2 der dritten Verknüpfungseinheit VK3 und an einen Eingang WE des zweiten Datenwortspeichers SPW2 weitergeleitet. Der Eingang WE des zweiten Datenwortspeichers SPW2 ist an die erste im zweiten Datenwortspeicher SPW2 angeordneten Spei-

WAVELYNX EX. 1003, Pg. 1260
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

cherzelle W1 herangeführt - durch einen strichlierten Pfeil angedeutet. Durch in der dritten Verknüpfungseinheit VK3 angeordnete Verknüpfungsmittel EXOR wird das am ersten Eingang XE1 anliegende erste Verknüpfungsergebnis y_n mit dem am zweiten Eingang XE2 anliegenden zweiten Verknüpfungsergebnis x_n zu einem das pseudo-zufällige Datenwort k_n repräsentierenden, dritten Verknüpfungsergebnis Exklusiv-ODER verknüpft und an einen Ausgang XA der dritten Verknüpfungseinheit VK3 weitergeleitet.

[0019] Alle im Blockschaltbild dargestellten Einheiten SPW1, SPW2, VK1, VK2, SPB, SPG, VK3 sind mit nicht dargestellten Taktmitteln zur Bereitstellung von Taktintervalle definierenden Taktimpulsen verbunden.

[0020] Im folgenden wird das erfindungsgemäße Verfahren zur taktilen Erzeugung der pseudo-zufälligen Datenworte k_n näher erläutert:

[0021] Während des den Beginn des Verfahrens repräsentierenden ersten Taktintervalls t sind in den vier im ersten Datenwortspeicher SPW1 angeordneten Datenwort-Speicherzellen W1...4 eine erste Datenwort-Startfolge repräsentierende InitialisierungsDatenworte $Y_{n-1}...y_{n-4}$ und in den fünf im zweiten Datenwortspeicher SP2 angeordneten Datenwort-Speicherzellen W1...5 eine zweite Datenwort-Startfolge repräsentierende Initialisierungs-Datenworte $x_{n-1}...x_{n-5}$ gespeichert. Gemäß dem Blockschaltbild ist in der ersten im ersten Datenwortspeicher SPW1 angeordneten Speicherzelle W1 die binäre Information "1110" als erstes Datenwort Y_{n-1} gespeichert. Des Weiteren ist in der zweiten Datenwort-Speicherzelle W2 die binäre Information "1001" als zweites Datenwort Y_{n-2}, in der dritten Datenwort-Speicherzelle W3 die binäre Information "1010" als drittes Datenwort y_{n-3} und in der vierten Datenwort-Speicherzelle W4 die binäre Information "0011" als viertes Datenwort y_{n-4} gespeichert. Im zweiten Datenwortspeicher SPW2 ist in der ersten Datenwort-Speicherzelle W1 die binäre Information "1010" als erstes Datenwort x_{n-1}, in der zweiten Datenwort-Speicherzelle W2 die binäre Information "1111" als zweites Datenwort x_{n-2}, in der dritten Datenwort-Speicherzelle W3 die binäre Information "0011" als drittes Datenwort X_{n-3}, in der vierten Datenwort-Speicherzelle W4 die binäre Information "1110" als viertes Datenwort x_{n-4} und in der fünften Datenwort-Speicherzelle W5 die binäre Information "0110" als fünftes Datenwort x_{n-5} gespeichert.

[0022] Gemäß dem in der ersten Verknüpfungseinheit VK1 gespeicherten Generatorpolynom $g(r) = r^4 + r^2 + 1$, bzw. gemäß der durch dieses Generatorpolynom g(r) dargestellten ersten Verknüpfungsvorschrift $y_n = y_{n-2} + y_{n-4}$ wird das zweite und das vierte an die erste Verknüpfungseinheit VK1 herangeführte Datenwort Y_{n-2}, y_{n-4} zu dem ersten Verknüpfungsergebnis Y_n Exklusiv- ODER verknüpft und das Verknüpfungsergebnis y_n = "1010" in der Speicherzelle Z des Bitmuster-Speichers SPB gespeichert. Durch die im Bitmuster-Speicher SPB angeordneten Maskierungsmittel werden die drei niederwertigsten Datenbits des ersten Verknupfungsergebnisses y_n ermittelt und als aktuelles Bitmuster bm_n = "010" an den Eingang SE des Speichers SPG weitergeleitet. Durch die im Speicher SPG angeordneten Vergleichsmittel wird das am Eingang GE anliegende, aktuelle Bitmuster bm_n mit den in den einzelnen Tabelleneinträgen t1...8 gespeicherten Bitmusterkombinationen bm1...8 auf Übereinstimmung überprüft. Gemäß dem Ausführungsbeispiel wird eine Übereinstimmung mit der im dritten Tabelleneintrag t3 gespeicherten dritten Bitmusterkombination bm3 = "010" festgestellt, und die der dritten Bitmusterkombination bm3 zugeordnete dritte Verknüpfungsvorschrift f_2 bzw. das diese darstellende dritte Generatorpolynom $f_2(r) = r^4 + r + 1$ als aktuelle zweite Verknüpfungsvorschrift f_k ausgewählt, an die zweite Verknüpfungseinheit VK2 übermittelt und in dieser gespeichert.

[0023] Gemäß dem übermittelten und als aktuelle zweite Verknüpfungsvorschrift f_k gespeicherten Generatorpolynom $f_2(r) = r^4 + r + 1$ wird das an die zweiten Verknüpfungseinheit VK2 herangeführte erste Datenwort x_{n-1} = "1010" mit dem herangeführten vierten Datenwort x_{n-4} = "1110" durch die Verknüpfungsmittel EXOR zu dem zweiten Verknüpfungsergebnis x_n Exklusiv-ODER verknüpft und das gebildete zweite Verknüpfungsergebnis x_n = "0100" an den Ausgang KA der zweiten Verknüpfungseinheit VK2 geleitet. Durch die in der dritten Verknüpfungseinheit VK3 angeordneten Verknüpfungsmittel EXOR wird das an den ersten Eingang XE1 herangeführte erste Verknüpfungsergebnis y_n = "1010" mit dem an den zweiten Eingang XE2 herangeführte zweiten Verknüpfungsergebnis x_n = "0100" zu dem dritten Verknüpfungsergebnis k_n = "1110" Exklusiv-ODER verknüpft und das dritte Verknüpfungsergebnis k_n = "1110" als erstes erzeugtes pseudo-zufälliges Datenwort k_n an den Ausgang XA der dritten Verknüpfungseinheit VK3 geleitet. Das am Ausgang XA anliegende pseudo-zufällige Datenwort k_n kann für die Verschlüsselung bzw. Chiffrierung von Nutzdaten insbesondere zur Verschlüsselung von Nutzdaten übermittelnden Datenstromen eingesetzt werden.

[0024] Zu Beginn des folgenden Taktintervalls t+1 wird das in der Speicherzelle Z des Bitmusterspeichers SPB gespeicherte und am Eingang WE des ersten Datenwortspeichers SPW1 anliegende erste Verknüpfungsergebnis y_n = "1010" als aktuelles erstes Datenwort Y'_{n-1} in der ersten Datenwort-Speicherzelle W1 des ersten Datenwortspeichers SPW1 gespeichert. Entsprechend wird das im vorherigen Taktintervall t in der ersten Speicherzelle W1 gespeicherte, vorhergehende erste Datenwort y_{n-1} als aktuelles zweites Datenwort y'_{n-2} = "1110" in der zweiten Datenwort-Speicherzelle W2, das im vorhergehenden Taktintervall t in der zweiten Datenwort-Speicherzelle W2 gespeicherte, vorhergehende zweite Datenwort y_{n-2} als aktuelles drittes Datenwort y'_{n-3} = "1001" in der dritten Datenwort-Speicherzelle W3, und das im vorhergehenden Taktintervall t in der dritten Datenwort-Speicherzelle W3 gespeicherte, vor-

WAVELYNX EX. 1003, Pg. 1261
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

hergehende dritte Datenwort y_{n-3} als aktuelles viertes Datenwort y'_{n-4} = "1010" in der vierten Datenwort-Speicherzelle W4 gespeichert. Das im vorhergehenden Taktintervall t in der vierten Datenwort-Speicherzelle gespeicherte, vorhergehende vierte Datenwort y_{n-4} wird verworfen.

[0025] Des Weiteren wird während des aktuellen Taktintervalls t+1 das am Eingang WE des zweiten Datenwortspeichers SPW2 anliegende, aktuelle zweite Verknüpfungsergebnis X_n = "0100" als aktuelles erstes Datenwort x'_{n-1} = "0100" in der ersten Datenwort-Speicherzelle W1 des zweiten Datenwortspeichers SPW2 gespeichert. Entsprechend wird das im vorhergehenden Taktintervall t in der ersten Datenwort-Speicherzelle W1 gespeicherte vorhergehende erste Datenwort x_{n-1} als aktuelles zweites Datenwort X'_{n-2} = "1010" in der zweiten Datenwort-Speicherzelle W2 gespeichert; das im vorhergehenden Taktintervall t in der zweiten Datenwort-Speicherzelle W2 gespeicherte, vorhergehende zweite Datenwort x_{n-2} wird als aktuelles drittes Datenwort x'_{n-3} = "1111" in der dritten Datenwort-Speicherzelle W3 gespeichert; das im vorhergehenden Taktintervall t in der dritten Datenwort-Speicherzelle W3 gespeicherte, vorhergehende dritte Datenwort x_{n-3} wird als aktuelles viertes Datenwort x'_{n-4} = "0011" in der vierten Datenwort-Speicherzelle W4 gespeichert; das im vorhergehenden Taktintervall t in der vierten Datenwort-Speicherzelle W4 gespeicherte, vorhergehende vierte Datenwort x_{n-4} wird als aktuelles fünftes Datenwort y'_{n-5} = "1110" in der fünften Datenwort-Speicherzelle W5 gespeichert; das im vorhergehenden Taktintervall t in der fünften Datenwort-Speicherzelle W5 gespeicherte vorhergehende fünfte Datenwort x_{n-5} wird verworfen.

[0026] Wie bereits für das vorhergehende Taktintervall t beschrieben, wird durch die in der ersten Verknüpfungseinheit VK1 angeordneten Verknüpfungsmittel EXOR im folgenden Taktintervall t+1 das anliegende aktuelle zweite Datenwort Y'_{n-2} = "1110" mit dem anliegenden, aktuellen vierten Datenwort y'_{n-4} = "1010" gemäß dem die Verknüpfungsvorschrift g repräsentierenden Generatorpolynom $g(r) = r^4 + r^2 + 1$ Exklusiv-ODER verknüpft und das gebildete, aktuelle erste Verknüpfungsergebnis y'_n = "0100" in der Speicherzelle Z des Bitmuster-Speichers SPB gespeichert. Wie bereits erläutert werden durch die im Bitmuster-Speicher SPB angeordneten Maskierungs-Mittel die drei niederwertigsten Datenbits des gespeicherten, aktuellen ersten Verknüpfungsergebnisses y'_n ermittelt und als aktuelles Bitmuster bm'_n = "100" an den Eingang SE des Speichers SPG weitergeleitet. Durch die im Speicher SPG angeordneten Vergleicher-Mittel wird die mit dem am Eingang SE anliegenden, aktuellen Bitmuster bm_n übereinstimmende Bitmusterkombination bm1...8 ermittelt; in diesem Ausführungsbeispiel wird für das aktuelle Taktintervall t+1 die im nicht dargestellten vierten Tabelleneintrag t4 gespeicherte vierte Bitmusterkombination bm4 = "100" ermittelt und entsprechend das zugeordnete vierte Generatorpolynom - beispielsweise $f_3(r) = r^5 + r^3 + 1$ -als aktuelle zweite Verknüpfungsvorschrift f'_k an die zweite Verknüpfungseinheit VK2 übermittelt und in dieser gespeichert. Durch die in der zweiten Verknüpfungseinheit VK2 angeordneten Verknüpfungsmittel EXOR wird das an der zweiten Verknüpfungseinheit VK2 anliegende, aktuelle fünfte Datenwort x'_{n-5} = "1110" mit dem anliegenden, aktuellen dritten Datenwort x'_{n-3} = "1111" zu dem aktuellen zweiten Verknüpfungsergebnis x'_n = "0001" gemäß der für das aktuelle Taktintervall t+1 aktuell wirksamen zweiten Verknüpfungsvorschrift $x_n = x_{n-5} + x_{n-1}$ Exklusiv-ODER verknüpft und anschließend das gebildete, aktuelle zweite Verknüpfungsergebnis x'_n = "0001" und das aktuelle erste Verknüpfungsergebnis y'_n = "0100" in beschriebener Art und Weise durch die in der dritten Verknüpfungseinheit VK3 angeordneten Verknüpfungsmittel EXOR zu dem aktuellen, pseudo-zufällige Datenwort k'_n = "0101" Exklusiv-ODER verknüpft.

[0027] Für die nachfolgenden Taktintervalle t+i - i>1 - läuft das erfindungsgemäße Verfahren zur Erzeugung pseudo-zufälliger Datenworte k_n in beschriebener Art und Weise ab.

[0028] Vorteilhaft können der erste Datenwortspeicher SPW1 und die diesem zugeordnete erste Verknüpfungseinheit VK1 sowie der zweite Datenwortspeicher SPW2 und die diesem zugeordnete zweite Verknüpfungseinheit VK2 mit unterschiedlichen Taktimpulsen zur Realisierung unterschiedlicher Taktintervalle t angesteuert werden, wodurch die Qualität der erzeugten pseudo-zufälligen Datenworte k_n und somit die Qualität der Verschlüsselung von Nutzinformationen mit Hilfe der erzeugten pseudo-zufälligen Datenworte k_n weiter verbessert wird.

[0029] Bei dem erfindungsgemäßen Verfahren stellen die die erste und zweite Datenwort-Startfolge repräsentierenden Initialisierungs-Datenworte $Y_{n-1}...y_{n-4}$, $x_{n-1}...x_{n-5}$, die in der ersten Verknüpfungseinheit VK1 gespeicherte Verknüpfungsvorschrift g, die im Speicher SPG gespeicherten Verknüpfungsvorschriften $f_{0...7}$ und deren zugeordnete Bitmusterkombinationen bm1...8 sowie die Informationen über die eingesetzten Taktintervalle t Schlüsselinformationen dar, welche zum Entschlüsseln der mit Hilfe des erfindungsgemäßen Verfahrens verschlüsselten Nutzinformationen bekannt sein müssen.

[0030] Gemäß einer nicht dargestellten weiteren vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens werden in beschriebener Art und Weise weitere Verknüpfungsergebnisse bzw. pseudo-zufällige Datenworte mit Hilfe weiterer Datenwortspeicher und weiterer Verknüpfungseinheiten gebildet und die gebildeten weiteren Verknüpfungsergebnisse zusammen mit den ersten und zweiten Verknüpfungsergebnissen y_n, x_n zu dem pseudo-zufälligen Datenwort k_n beispielsweise Exklusiv-ODER verknüpft. Durch diese Ausgestaltungsvariante wird das Entschlüsseln der Nutzinformationen und die Rekonstruierbarkeit der Schlüsselinformationen weiter erschwert.

WAVELYNX EX. 1003, Pg. 1262
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Patentansprüche

1. Verfahren zur taktilen Erzeugung pseudo-zufälliger Datenworte (k_n),

   - bei dem erste pseudo-zufällige Datenworte (y_n) mit Hilfe eines ersten Verfahrens zur Erzeugung pseudo-zufälliger Datenworte gebildet werden, und
   - bei dem zweite pseudo-zufällige Datenworte (x_n) mit Hilfe eines zweiten Verfahrens zur Erzeugung pseudo-zufälliger Datenworte gebildet werden,

   dadurch gekennzeichnet,

   - daß in Abhängigkeit von den gebildeten ersten pseudo-zufälligen Datenworten (y_n) aus mehreren Verknüpfungsvorschriften ($f_{0...7}(r)$) eine aktuelle Verknüpfungsvorschrift ($f_k(r)$) ausgewählt wird,
   - daß die zweiten pseudo-zufälligen Datenworte (x_n) durch Verknüpfung von Datenworten ($x_{n-1}...x_{n-5}$) einer Folge von Datenworten gemaß der aktuell ausgewählten Verknüpfungsvorschrift ($f_k(r)$) gebildet werden, und
   - daß aus den zweiten pseudo-zufälligen Datenworten (x_n) die pseudo-zufälligen Datenworte (k_n) gebildet werden.

2. Verfahren nach Anspruch 1,
   dadurch gekennzeichnet,
   daß zusätzlich mit Hilfe der gebildeten ersten pseudo-zufälligen Datenworte (y_n) die pseudo-zufälligen Datenworte (k_n) gebildet werden.

3. Verfahren nach Anspruch 1 oder 2,
   dadurch gekennzeichnet,
   daß beim ersten Verfahren zur Erzeugung pseudo-zufälliger Datenworte die ersten pseudo-zufälligen Datenworte (y_n) durch Verknüpfung von Datenworten ($y_{n-1}...y_{n-4}$) einer ersten Folge von Datenworten gemäß einer ersten Verknüpfungsvorschrift (g(r)) gebildet werden.

4. Verfahren nach einem der vorherigen Ansprüche,
   dadurch gekennzeichnet,

   - daß weitere pseudo-zufällige Datenworte durch Verknüpfung von Datenworten einer weiteren Folge von Datenworten gemäß einer weiteren Verknüpfungsvorschrift gebildet werden, wobei die aktuelle weitere Verknüpfungsvorschrift in Abhängigkeit von den gebildeten ersten und/oder zweiten pseudo-zufälligen Datenworten aus den mehreren Verknüpfungsvorschriften ($f_{0...7}(r)$) und/oder aus mehreren weiteren Verknüpfungsvorschriften ausgewählt wird, und
   - daß mit Hilfe der gebildeten ersten und/oder zweiten und/oder weiteren pseudo-zufälligen Datenworte (y_n, x_n) die pseudo-zufälligen Datenworte (k_n) gebildet werden.

5. Verfahren nach Anspruch 3 oder 4,
   dadurch gekennzeichnet,

   - daß die Erzeugung der ersten pseudo-zufälligen Datenworte (y_n) mit einer 1 bis m vorgegebene Datenworte ($y_{n-1}...y_{n-4}$) aufweisenden ersten Datenwort-Startfolge und die Erzeugung der zweiten pseudo-zufälligen Datenworte (x_n) mit einer 1 bis 1 vorgegebene Datenworte ($x_{n-1}...x_{n-5}$) aufweisenden zweiten Datenwort-Startfolge gestartet wird, und
   - daß bei jedem Verarbeitungstakt (t, t+1)

     -- aus den aktuell vorliegenden Folgen von Datenworten ($y_{n-1}...y_{n-4}$,$x_{n-1}...x_{n-5}$) gemäß der ersten und der ausgewählten Verknüpfungsvorschrift (g(r), $f_k(r)$) das erste und das zweite pseudo-zufällige Datenwort (y_n, x_n) gebildet wird, und
     -- das vorhergehend erste bis (m-1)-te Datenwort ($y_{n-1}...y_{n-3}$) der ersten Folge von Datenworten zum aktuellen zweiten bis m-ten Datenwort ($y'_{n-2}...y'_{n-4}$) der ersten Folge von Datenworten wird,
     -- das vorhergehend erste bis (l-1)-te Datenwort ($x_{n-1}...x_{n-4}$) der zweiten Folge von Datenworten zum aktuellen zweiten bis l-ten Datenwort ($x'_{n-2}...x'_{n-5}$) der zweiten Folge von Datenworten wird,
     -- das aktuell gebildete erste und zweite pseudo-zufällige Datenwort (y_n, x_n) zum aktuellen ersten Datenwort (y'_{n-1},x'_{n-1}) der ersten und zweiten Folge von Datenworten wird.

6. Verfahren nach einem der vorherigen Ansprüche,
   dadurch gekennzeichnet,
   daß die Datenworte ($y_{n-1}...y_{n-4}$, $x_{n-1}...x_{n-5}$) und die gebildeten ersten und zweiten pseudo-zufälligen Datenworte (y_n, x_n) und die gebildeten pseudo-zufälligen Datenworte (k_n) binäre Informationen repräsentieren.

7. Verfahren nach einem vorherigen Ansprüche,
   dadurch gekennzeichnet,
   daß die Verknüpfungsvorschriften (g(r), $f_{0...7}(r)$) jeweils durch Generatorpolynome realisiert sind.

8. Verfahren nach einem der vorherigen Ansprüche,
   dadurch gekennzeichnet,
   daß die Datenworte ($y_{n-1}...Y_{n-4}$, $x_{n-1}...x_{n-5}$) und die gebildeten ersten und zweiten pseudo-zufälligen

WAVELYNX EX. 1003, Pg. 1263
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Datenworte (y_n, x_n) und die gebildeten pseudo-zufälligen Datenworte (k_n) jeweils eine Wortbreite b,c ≥ 1 umfassen.

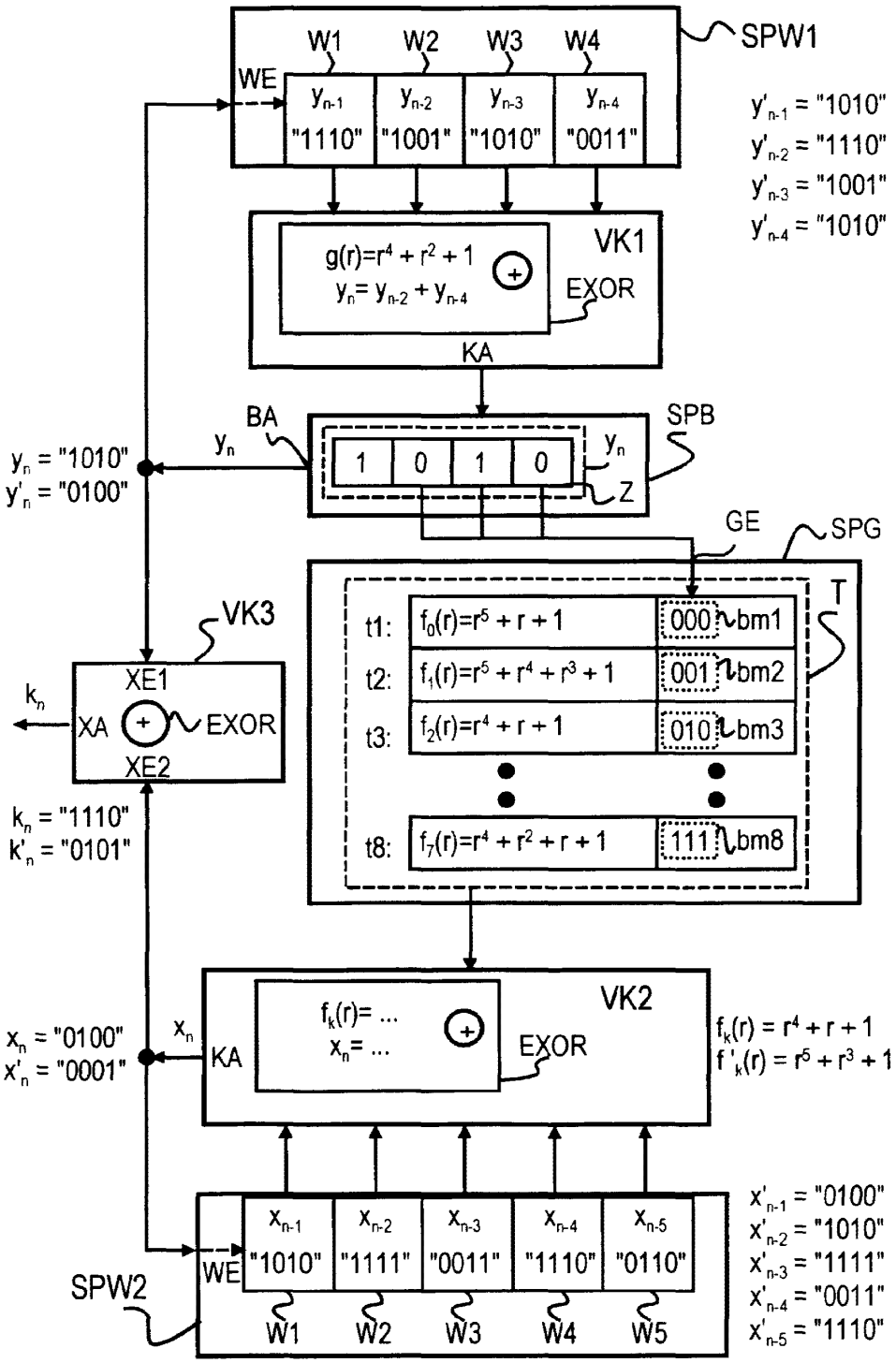
9. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet,** daß die pseudo-zufälligen Datenworte (k_n) jeweils durch eine Exklusiv-ODER Verknüpfung der gebildeten ersten und zweiten pseudo-zufälligen Datenworte (y_n, x_n) gebildet werden.

10. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet,** daß die aktuelle Verknüpfungsvorschrift ($f_k(r)$) mit Hilfe einer Bit-Maske in Abhängigkeit von dem zumindest einen gebildeten, ersten pseudo-zufälligen Datenwort ($y_n...y_{n-4}$) aus den mehreren Verknüpfungsvorschriften ($f_{0...7}(r)$) ausgewählt wird.

11. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet,** daß die Bildung der ersten pseudo-zufällige Datenworte (y_n) mit einem ersten Verarbeitungstakt und die Bildung der zweiten pseudo-zufällige Datenworte (x_n) mit einem zweiten Verarbeitungstakt erfolgt.

12. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet,** daß mit Hilfe der gebildeten pseudo-zufälligen Datenworte (k_n) Nutzinformationen codiert/verschlüsselt oder decodiert/entschlüsselt werden.

WAVELYNX EX. 1003, Pg. 1264
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



WAVELYNX EX. 1003, Pg. 1265
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 949 563 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.10.1999 Bulletin 1999/41

(51) Int Cl.[6]: **G06F 7/58**

(21) Application number: **99301314.3**

(22) Date of filing: **23.02.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **04.03.1998 US 34829**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

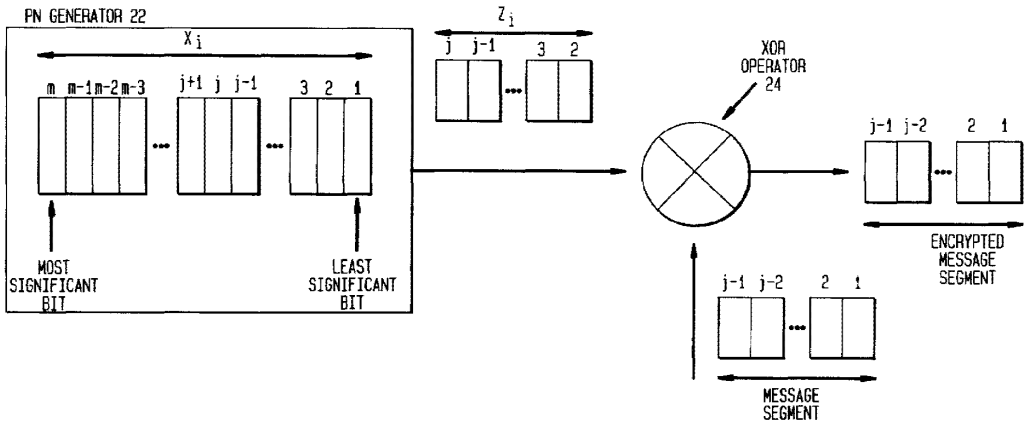
(72) Inventors:
- **Patel, Sarvar**
  Montville, New Jersey 07045 (US)
- **Sundaram, Ganapathy Subramanian**
  Scotch Plains, New Jersey 07076 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) A method for generating pseudo-random numbers

(57) The present invention is a method for outputting larger bit size pseudo-random number z_j that is cryptographically secure. Since larger bit size pseudo-random numbers are being outputted, larger bit size segments of messages may be encrypted resulting in a speedier encryption process than encryption processes of the prior art. In one embodiment, the present invention is a pseudo-random number generator defined by a modular exponential function $x_j = g^{x_{j-1}} \bmod p$. The output of the pseudo-random number generator being a pseudo-random number z_j comprising a j-1 bit size segment of x_j. The value of j being less than or equal to m-2c (i.e., $j \leq m$-2c). In an embodiment of the present invention, the pseudo-random number z_j includes the j least significant bits of x_j excluding the least significant bit of x_j.

FIG. 3



EP 0 949 563 A2

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1266
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

Field of the Invention

[0001] The present invention relates generally to cryptography and, in particular, to pseudo-random number generators.

Background of the Related Art

[0002] Pseudo-random generators are used in some forms of cryptography to provide secured communication means for the transmission of messages between a transmitter and a receiver. Security is provided such that only an intended receiver can understand a message (e.g., voice or data) transmitted by an authorized transmitter, and only the authorized transmitter can send the message to the intended receiver. The challenge of cryptography is to change a message into a form that only the intended receiver can comprehend. This must be done in a way that is both economical for the transmitter and for the intended receiver. At the same time, it must be very difficult (in terms of time and/or processing capabilities) for an unauthorized receiver (i.e., not the intended receiver) to comprehend the message. As unauthorized receivers and unauthorized transmitters become more sophisticated, the need for secured communications become greater.

[0003] FIG. 1 depicts a functional block diagram of a transmitter 10 in the prior art having a cryptographic device for encrypting messages. The cryptographic device comprising pseudo-random number (PN) generator 12 and XOR operator 14. PN generator 12 is defined by the following modular exponential function:

$$x_i = g^{x_{i-1}} \bmod p \qquad \text{(equation 1)}$$

wherein x_i is a value comprising m bits, p is a prime number comprising k bits, g is a generator of integer mod p, and $1<i\leq n$. Since equation 1 is a modular exponential function, the value of m should be less than or equal to k (i.e., $m\leq k$). Value x_i is generated initially by providing PN generator 12 with seed value x_0, which is a secret value comprising m bits and known only to the authorized transmitter and the intended receiver. Thus, value x_1 is equal to $g^{x0} \bmod p$. Value x_1 is used to generate x_2 (i.e., $x_2 = g^{x1} \bmod p$), which is then used to generate x_3, and so on.

[0004] PN generator 12 outputs a pseudo-random number z_i comprising a d bit size segment of x_i. The pseudo-random number z_i is then used to encrypt a d bit size segment of a message to be transmitted. Specifically, XOR operator 14 receives as inputs the message segment and the pseudo-random number z_i. The message segment is XOR with the pseudo-random number z_i to produce a d bit size encrypted message segment. The values of d, m, and k depend, in part, on the degree of cryptographic security (or difficulty) sought to be attained, as will be described herein.

[0005] Cryptographic security depends on two factors: (I) the degree of difficulty in solving a discrete logarithm problem for x_i, and (2) the degree of difficulty in breaking the pseudo-random number generator given one or more pseudo-random numbers z_i (comprising d bits). Assuming all m bits of x_i are available, solving a discrete logarithm problem for x_i involves the determination of x_{i-1} such that $x_i = g^{x_{i-1}} \bmod p$. A discrete logarithm problem is considered computationally hard, and therefore cryptographically secure, if 2^c number of operations are required to solve it, wherein c represents a cryptographic security threshold level. The standard belief is that a discrete logarithm problem is hard if it takes at least 2^{64} number of operations to solve it (i.e., $c\geq 64$).

[0006] A discrete logarithm problem can be solved by a variety of techniques. The two most efficient techniques being the well-known index calculus technique and square root technique. To solve the discrete logarithm problem for x_i using the index calculus technique, it would require

$$\text{operations}_{\text{index}} = O(2^{\alpha\sqrt{\log_2 p \times \log_2 \log_2 p}}) \qquad \text{(equation 2)}$$

number of operations, wherein α is a constant. If c=64, the hard threshold (of 2^{64} number of operations) is met when p comprises at least 512 bits (i.e., $k\geq 512$). Thus, the value selected for k is dependent upon the value of c. By contrast, to solve the discrete logarithm problem for x_i using the square root technique, it would require

$$\text{operations}_{\text{sq-rt}} = \sqrt{2^m} \qquad \text{(equation 3)}$$

number of operations. If c=64, the hard threshold is met when x_i comprises at least 128 bits (i.e., $m\geq 128$). Thus, the

WAVELYNX EX. 1003, Pg. 1267
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

value of m is also dependent upon the value of c.

[0007] As mentioned earlier, solving the discrete logarithm problem for x_i assumes all m bits of x_i are available. If only d bit size segments of x_i (i.e., pseudo-random number z_i) are available, then the predecessor step to solving the discrete logarithm problem for x_i is to somehow determine all m bits of x_i. This is the aforementioned second factor of cryptographic security, which involves breaking the pseudo-random number generator given one or more pseudo-random number z_i. A pseudo-random number generator is considered cryptographically secure if, given one or more pseudo-random numbers z_i, all m bits of x_i would be difficult to predict or determine. It is believed that if the PN generator outputs smaller bit size pseudo-random numbers z_i (i.e., small segments of x_i), less data would be available to a cryptanalyst to use to predict any other bits of x_i. The exact size of pseudo-random number z_i being outputted would depend on the degree of cryptographic security sought to be attained - that is, the value of d is dependent upon the value ofc.

[0008] Blum-Micali presented a PN generator which outputted pseudo-random numbers z_i comprising only the most significant bit of x_i, i.e., d=1. Blum-Micali showed that the degree of difficulty in breaking this PN generator is equivalent to the degree of difficulty in solving a discrete logarithm problem for the modular exponential function of x_i. Thus, if solving the discrete logarithm problem for x_i is hard, then breaking Blum-Micali's PN generator (outputting pseudo-random numbers z_i comprising only the most significant bit) is also hard.

[0009] By contrast, Peralta presented a successor PN generator which outputted pseudo-random numbers z_i comprising log2 m most significant bits, i.e., d=$\log_2 m$. For example, if x_i comprises 512 bits, then the PN generator would output pseudo-random numbers z_i comprising no more than the nine (i.e., log2 512) most significant bits of x_i. Or if x_i comprises 1024 bits, then the PN generator would output pseudo-random numbers z_i comprising no more than the ten (i.e., $\log_2$ 1024) most significant bits of x_i. Peralta showed that the degree of difficulty in breaking this PN generator is also equivalent to the degree of difficulty in solving the discrete logarithm problem for the modular exponential function of x_i. Thus, if solving the discrete logarithm problem for x_i is hard, then breaking Peralta's PN generator (outputting pseudo-random numbers z_i comprising only $\log_2 m$ most significant bits) is also hard.

[0010] Although encryption processes that use the PN generators presented by Blum-Micali and/or Peralta are cryptographically secure, these PN generators output pseudo-random numbers z_i comprising no more than $\log_2 m$ bits of x_i. Since $\log_2 m$ is a relatively small value, only small bit size segments of messages can be encrypted for every pseudo-random numbers z_i outputted by the PN generator. This results in a slower encryption process because more pseudo-random numbers z_i have to then be outputted to encrypt the entire message. Accordingly, there exists a need for a pseudo-random number generator that outputs lager bit size pseudo-random numbers z, and is cryptographically secure.

Summary of the Invention

[0011] The present invention is a method for outputting larger bit size pseudo-random number z_i that is cryptographically secure. Since larger bit size pseudo-random numbers are being outputted, larger bit size segments of messages may be encrypted resulting in a speedier encryption process than encryption processes of the prior art. In one embodiment, the present invention includes a pseudo-random number generator defined by a modular exponential function $x_i = g^{x_{i-1}} \bmod p$, wherein x_i is a value comprising m bits, p is a prime number comprising k bits, g is a generator of integer mod p, $m \leq k$, and $1 < i \leq n$. The values of m and k being selected to make solving the discrete logarithm for the modular exponential function of x_i hard. The output of the pseudo-random number generator is a pseudo-random number z_i comprising a j-1 bit size segment of x_i. The value of j being less than or equal to m-2c (i.e., $j \leq m$-2c). In an embodiment of the present invention, the pseudo-random number z_i includes the j least significant bits of x_i excluding the least significant bit of x_i. The output of the pseudo-random number generator is then used to encrypt an equal size segment of a message to be transmitted.

[0012] Advantageously, the present invention uses larger bit size pseudo-random numbers z_i to encrypt messages, thus resulting in an encryption process that is faster than encryption processes of the prior art that use smaller bit size pseudo-random numbers z_i (e.g., pseudo-random numbers comprising $\log_2 m$ bits). Although the use of larger bit size pseudo-random numbers is counter intuitive to prior art cryptographic security beliefs with respect to breaking the pseudo-random number generator, the present invention utilization of larger bit size pseudo-random numbers z_i is cryptographically secure. Specifically, the degree of difficulty in breaking the pseudo-number generator of the present invention is equivalent to the degree of difficulty in solving the discrete logarithm for a short exponential function $y = g^s \bmod p$, wherein y is a value comprising m bits, s is a short exponent comprising 2c bits, p is the prime number comprising k bits, g is the generator of integer mod p, c represents a cryptographic security (or difficulty) threshold level, and $2c << m \leq k$. The values of c and k being selected to make solving the discrete logarithm for the short exponential function of y hard.

WAVELYNX EX. 1003, Pg. 1268
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Brief Description of the Drawings

[0013] The features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG 1 depicts a functional block diagram of a transmitter in the prior art having a cryptographic device for encrypting messages;
FIG. 2 depicts a functional block diagram of a transmitter comprising a cryptographic device for encrypting messages used in accordance with the present invention; and
FIG. 3 depicts a diagram of the pseudo-random generator of FIG. 2 generating a value x_i and outputting thej least significant bits excluding the least significant bit.

Detailed Description

[0014] FIG. 2 depicts a functional block diagram of a transmitter 20 comprising a cryptographic device for encrypting messages used in accordance with the present invention. The cryptographic device comprising pseudo-random number (PN) generator 22 and XOR operator 24. PN generator 22 is a device for outputting pseudo-random numbers, such as an n stage maximal length shift register or an ASIC executing a pseudo-random number generator program. PN generator 22 is defined by the following modular exponential function:

$$x_i = g^{x_{i-1}} \bmod p \qquad \text{(equation 4)}$$

wherein x_i is a value comprising m bits, p is a prime number comprising k bits, g is a generator of integer mod p, and $1<i\leq n$. Since equation 4 is a modular exponential function, the value of m is less than or equal to k (i.e., $m\leq k$).

[0015] The values of m and k are chosen such that it would be difficult or hard to solve a discrete logarithm problem for the modular exponential function of x_i using any of the well-known techniques for solving discrete logarithm problems, such as the index calculus technique and the square root technique, wherein difficulty or hardness is expressed in terms of requiring 2^c number of operations to solve the discrete logarithm problem and c represents a cryptographic security threshold level. Specifically, the value *of k* should be chosen such that 2^c is approximately equal to or less than

$$O(2^{\alpha\sqrt{\log_2 p \log_2 \log_2 p}}),$$

and the value of m should be chosen such that 2^c is approximately equal to or less thank $\sqrt{2^m}$. For example, if the degree of difficulty sought to be attained is at least 2^{64} (i.e., $c\geq 64$), then $k\geq 512$ and $m\geq 128$.

[0016] Value x_i is generated initially by providing PN generator 22 with seed value x_0, which is a secret value comprising m bits and known only to the transmitter 20 and an intended receiver. Thus, x_1 is equal to $g^{x0} \bmod p$. Value x_1 is used to generate x_2 (i.e., $x_2 = g^{x1} \bmod p$), which is then used to generate x_3, and so on. Although PN generator 22 generates all m bits of x_i, it only outputs pseudo-random numbers z_i comprising a j-1 bit size segment of x_i. The value of j being some value less than or equal to m-2c. In one embodiment, the pseudo-random number z_i comprises the j least significant bits of x_i excluding the least significant bit of x_i (i.e., x_i segment includes the second least significant bit of x_i through the jth least significant bit of x_i). See FIG. 3, which depicts a diagram of the pseudo-random generator 22 (defined by equation 4) generating a value x_i and outputting the j least significant bits excluding the least significant bit. For illustrative purposes, the remainder of this application will be described herein with respect to a pseudo-random number generator that outputs pseudo-random numbers z_i comprising the second least significant bit of x_i through thejth least significant bit of x_i. This should not, however, be construed to limit the present invention in any manner.

[0017] As described in the section entitled "Proof" below, the degree of difficulty in breaking this PN generator (which outputs, for example, the second throughjth least significant bits of x_i) is equivalent to solving a discrete logarithm problem for a short exponential function

$$y = g^s \bmod p \qquad \text{(equation 5)}$$

wherein y is a value comprising m bits, s is a short exponent comprising 2c bits, p is the prime number comprising k bits, and g is the generator of integer mod p. Since equation 5 is a short exponential function, the value of $2c$ is typically much less than the values of m and k (i.e., $2c<<m\leq k$).

WAVELYNX EX. 1003, Pg. 1269
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0018] If the discrete logarithm problem for the short exponential function of y is difficult to solve, then the PN generator of the present invention is difficult to break. The values of c and k are chosen such that it would be difficult to solve the discrete logarithm problem for the short exponential function of y using any of the well-known techniques for solving discrete logarithm problems, such as the index calculus technique and the square root technique. For example, suppose the degree of cryptographic security sought to be attained is at least 2^{64} (number of operations) to solve the discrete logarithm problem for y. Then the value of k should be at least comprise 512 bits and m should at least comprise 128 bits - that is, if $k \geq 512$ and $m \geq 128$, then at least 2^{64} number of operations are required to break the pseudo-random number generator of equation 4 outputting thej least significant bits excluding the least significant bit. If at least 2^{64} number of operations are also required to solve the discrete logarithm problem of equation 4, then $2X2^{64}$ (i.e., 2^{65}) combined number of operations are required to solve both discrete logarithm problems (for x_i and y). Since PN generator 22 is defined by a modular exponential function (of equation 4), then the value of m could be as large as the value of k. If the value ofk is 512 (or 1024), then the value of m could be as large as 512 (or 1024). Accordingly, when k is 512 (or 1024) and c is 64, PN generator 22 can output pseudo-random numbers z_i as large as 383 (or 895) bits, which is substantially larger than the bit sizes of the pseudo-random numbers being outputted by prior art PN generators.

[0019] PN generator's 22 output (i.e., pseudo-random number z_i) is provided as input to XOR operator 24, which is a device for performing XOR operations, such as an XOR gate or an ASIC executing an XOR operation. XOR operator 24 receives PN generator 22's output and XORs it with an equal size segment of a message to produce an encrypted message segment comprising j-1 bits, as shown in FIG. 3. Note that XOR operator 24 may be replaced with any other device for combining the bits of the PN generator's output with the bits of the message.

[0020] The encrypted message is subsequently transmitted by the transmitter 20 to a receiver comprising a pseudo-random number generator defined by the same exponential function and an XOR operator. If the receiver is the intended receiver, the seed value x_0 would be known or determinable by the receiver. Thus, the intended receiver would be able to generate the same pseudo-random numbers z_i as those generated by the transmitter. The pseudo-random numbers z_i could then be used to decrypt the encrypted message segments, therefore allowing the intended receiver to comprehend the transmitted message.

Proof

Introduction

[0021] A function f is said to be one way if it is easy to compute but hard to invert. With appropriate selection of parameters, the discrete exponentiation function over a finite field, g^x mod p where g is a generator of the cyclic group of non zero elements in the finite field, is believed to be a one way function. The intractability of its inverse, the discrete logarithm problem, is the basis of various encryption, signature and key agreement schemes. Apart from finite fields, other finite groups have been considered in the context of discrete exponentiation. One such example is the group of points on an elliptic curve over a finite field. Koblitz and Miller (independently) [Ko], [Mil], considered the group law on an elliptic curve to define a public key encryption scheme suggesting that elliptic curve addition is also a one way function. Another number theoretic problem that is considered to be hard is the problem of factoring integers. Examples of functions relying on factoring which are believed to be one way are the RSA and Rabin functions. Closely related to factoring is the problem of deciding quadratic residuosity modulo a composite integer.

[0022] A concept which is intimately connected to one way functions is the notion of hard bits. Based on one way functions, Blum & Micali were the first to introduce the concept of hard bits. Informally, a hard bit B(.) for a one way function f(.) is a bit which is as hard to compute as it is to invert f. Blum and Micali showed that the most significant bit is a hard bit for the discrete logarithm problem over a finite field. To be precise, their notion of most significant bit corresponds to the Boolean predicate which is one if the index of the exponent is greater than (p-1)/2 and zero otherwise. They defined and proved this hard bit and successfully used it to show the importance of hard bits in secure pseudo random bit generation. Soon after, the hard bits of RSA & Rabin functions were also discovered by Ben-Or-et al [BCS] which led to a new secure pseudo random bit generator. In 1986, Blum, Blum and Shub [BBS] used the quadratic residue problem over a composite integer to design yet another secure pseudo random bit generator. Their work was based on the security of the quadratic residue problem which was investigated by Goldwasser and Micali [GM84]. Later Goldreich and Levin [GL] proved that all one way functions have a hard bit. More generally they were able to show that for any one way function a logarithmic number of one bit hard predicates exist. This in particular proves the existence of at least a logarithmic number of secure pseudo random bit generators attached to a given one way function. The use of pseudo random bits in cryptography relates to one time pad style encryption and bit commitment schemes, to name a few.

[0023] All the above generators based on one bit predicates suffer from the same problem, namely they are too slow. All of them output one bit per modular exponentiation. The concept of simultaneous hardness is the first step in speeding things up. Intuitively, the notion of simultaneous hardness applied to a group of bits associated to a one way function

WAVELYNX EX. 1003, Pg. 1270
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

f states that it is computationally as hard as the inverse of the one way function to succeed in computing any information whatsoever about the given group of bits given only f(x). Using this notion one can extract collections of bits per operation and hence the speed up. Long and Widgerson [LW] were the first to show that log log p bits of the discrete log modulo a prime number p are simultaneously hard. On the other hand the works of Vazirani and Vazirani [VV] and Alexi-et al [ACGS] address the notion of simultaneous hardness of RSA and Rabin bits. Later Kaliski showed individual hardness of bits (in the Blum Micali sense) of the elliptic curve group addition problem using a novel oracle proof technique applicable to any finite Abelian group. His methods extend to show simultaneous hardness (stated but not proved in the paper) of log n bits where n is the order of the group, [Ka]. More recently, Hastad, Schrift and Shamir [HSS], have designed a much more efficient generator which produces n/2 bits per iteration where n is the number of bits of the modulus. The one way function they have considered is the discrete exponentiation function modulo a composite integer (to be precise a Blum integer). Once again the method of generation relies on the proof that n/2 bits of every iteration are simultaneously hard. The use of a composite modulus allows them to relate individual and simultaneous hardness of bits to factoring the modulus. In all these works the common strings are the results of Yao contained in his seminal work [Y] which laid the foundations to a complexity theoretic approach to cryptography which paved the way for a quantification of security in terms of known hard problems.

[0024] In this paper we construct a very efficient cryptographic pseudo random bit generator attached to modular exponentiation in a finite field. We show that n-O(log n)$^+$ bits of every iteration are simultaneously secure where O(log n)$^+$ is equal to the smallest non polynomial quantity in log n. Hence each iteration produces more bits than any other method discovered so far. The novelty in this work is to relate the security of the random bit generation to the problem of solving the discrete logarithm with short exponents. The motivation for this technique is derived from the above mentioned work of Hastad-et al where although they are using a modular exponential function modulo a composite, the security of the system is related to factoring the underlying modulus. In a similar but not so obvious sense, we use exponential in a finite field for the generation but relate the security to the strength of the discrete log problem (over the same prime modulus) but with short exponents. In this paper an oracle for the i-th bit gives the value of i-th bit when the binary representation is used for the argument. This is a different representation of the i-th bit than that used by Blum-Micali and Long-Widgerson. Also, our representation is the same as the representation that Hastad-et al have considered. The paper is organized as follows: In section 2 we discuss the discrete log problem and in particular the short exponent discrete log problem. Details of the oracles and hardness of bits are formalized in this section. In section 3 we show that the trailing n-O(log n)$^+$ bits are individually hard with respect to the discrete logarithm problem with short exponents. In section 4 we prove simultaneous hardness of n-O(log n)$^+$ bits. Once again this is with respect to the discrete log with short exponents problem. In section 5 we discuss the design of the system and provide the proof of security and conclude in section 6. In the appendix, we discuss some extensions of this work to include other Abelian groups and possible ways to improve the efficiency of the pseudo random generator.

The Discrete Logarithm Problem

[0025] We first define the discrete logarithm problem. Let p be a prime and g a generator for $(Z/(p))^*$, the multiplicative cyclic group of nonzero elements in the finite field of order p. Then for $1 <= x <= (p-1)$ the function $g^x \bmod p$ defines a permutation.

Problem 1

[0026] The discrete logarithm problem is to find x given y in $(Z/(p))^*$ such that $g^x \bmod p = y$. Let n = log p be the length of p in binary, then $g^x \bmod p$ is computable in Poly (n) time. However, there is no known deterministic or randomized algorithm which can compute the discrete logarithm in Poly (n) number of steps. The best algorithm to compute the discrete logarithm in a finite field of order p, is the index calculus method. Even this is not feasible if p is appropriately large (e.g. 1024 bits) since the complexity is sub-exponential and not polynomial in n. On the other hand for primes such that (p-1) consists of only small factors, there are very fast algorithms whose complexity is equal to the complexity of the discrete log in a field whose cardinality is equal to its largest prime factor. This algorithm is due to Pohlig and Hellman [PH].

Discrete Logarithm with Short Exponents

[0027] For efficiency purposes the exponent x is sometimes restricted to c bits (c=128 or 160 bits) since this requires fewer multiplication. There are square root time algorithms to find x in square root of c steps, due to Shanks [Sh] and Pollar [Po]. Thus c should be at least 128 bits to provide 64 bits of security. By this we mean an attacker should perform at least 2^{64} number of operations in order to crack the discrete logarithm using these algorithms. At the moment, there is no faster way to discover the discrete logarithm even with x so restricted.

WAVELYNX EX. 1003, Pg. 1271
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0028] We will also restrict x, in particular, we will restrict it to be slightly greater than O(log n) bits, but not to save on multiplication. The exact size of the exponent will be denoted $O(\log n)^+$, where the superscript + indicates that it is greater than any polynomial in log n. Hence even with the square root attack one needs greater than $2^{O(\log n)}$ steps or greater than a polynomial in n number of steps.

[0029] The hard problem we consider in this paper is the inverse of this special case of the discrete exponentiation function. To be precise, we consider the case of modular exponentiation in a finite field of order p (a prime number) with short exponents. The inverse of this problem is the discrete logarithm with short exponents (DLSE). In other words:

Problem 2

[0030] Let p be a large bit prime which has at least one large prime factor. Let x be an integer which is significantly smaller compared to p. Let g be a generator of the cyclic group of nonzero elements in the finite field of integers modulo the chosen prime p. Given g and $g^x=y$, find x.

[0031] The DLSE problem has been scrutinized and a summary of the results are presented in [OW], where they study this problem in the context of the Diffie-Hellman key agreement scheme. The use of short exponents in the Diffie-Hellman protocol is to speed up the process of exponentiation. Typically the cost of computing g^x is linearly related to the bit length of x, hence real-time computing costs have motivated the use of low order exponents. Care is necessary to ensure that such optimizations do not lead to security weaknesses. The above mentioned paper [OW], presents a set of attacks and methods to rectify the situation. In particular their conclusions suggest the use of safe primes.

[0032] Another example of the use of shorter exponents is in the generation of digital signatures. The digital signature standard (DSS) published by the NIST [DSS] is based on the discrete logarithm problem. It is a modification of the ElGamal signature scheme [EG]. The ElGamal scheme usually leads to a signature having 2n bits, where n is the number of bits of p (the modulus). For potential applications a shorter signature is desirable. DSS modifies the ElGamal scheme so that a 160 bit message is signed using a 320 bit signature but computations are all done modulo a 512 bit prime. The methodology involves the restrictions of all computations to a subgroup of size 2^{160}. The assumed security of the scheme is based on two different but very related problems. First of these is the discrete log in the entire group which uses a 512 bit modulus, where the index calculus algorithm applies. The second is the discrete log problem in the subgroup of the cyclic group of nonzero elements in the finite field. Here Shanks's square root algorithm reduces the complexity to $O(2^{80})$ since the exponent is only 160 bits.

Hardness of Bits

[0033] As indicated in the introduction, the notion of hard bits is very characteristic of every one way function. In particular hardness of bits with respect to the discrete logarithm has been extensively studied. In this paper we define a mild variation of hard bits.

Definition 1

[0034] Let f and f' be one way functions, where R_f is the range off. Let B: R_f to {0,1} be a Boolean predicate. Given f(x) for some x, the predicate B(x) is said to be f'-hard if computing B(x) is as hard as inverting f'.

[0035] Normally when we discuss hard bits, f and f' are the same. For example, discovering the Blum-Micali bit is as hard as computing the discrete logarithm. But in this paper we allow f and f' to be different. An example of this new phenomenon, is discrete exponentiation modulo a composite modulus. Here the discrete logarithm in the ring of integers modulo a composite is a hard function, and so is factoring. Here given g^x for some fixed g and generic x, finding individual bits of this discrete logarithm is as hard as factoring. This was proved by Hastad-et al in [HSS]. In this paper we consider a similar situation. We consider the one way function of discrete exponentiation, but we prove that the n-$O(\log n)^+$ bits of the exponent are DLSE-simultaneously hard. The best previous result showed simultaneous hardness of n/2 of the bits [HSS], but our result shows simultaneous hardness for almost all the n bits. Our results are maximal as far as the discrete logarithm is concerned. In other words if in any iteration we drop only O(log n) bits, then any attacker can compute the seed of the generator by making a polynomial number of guesses. Hence one cannot improve on these results regarding number of bits produced per iteration any further.

Binary Representation

[0036] The number x can be represented in binary as $b_{n-1}2^{n-1} + b_{n-2}\,2^{n-2} + \ldots + b_1 2 + b_1$ where b_i is either 0 or 1. The i-th bit problem is to discover the value of b_i of x. The i-th bit is hard if computing it is as difficult as computing the entire logarithm. If we had an oracle, $O^i(g,p,y)$, which outputs the value of b_i then the bit is hard if there is a Poly(n) time algorithm which makes Poly(n) queries to the oracle $O^i(g,p,Y)$ for various values of Y and computes the entire value

WAVELYNX EX. 1003, Pg. 1272
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

of x. We know the least significant bit is not hard because there is a Poly (n) time algorithm to compute it, namely by computing the Legendre symbol.

[0037] An imperfect oracle, O_epsilon(p,g, Y), is usually defined as an oracle which outputs the correct bit value with probability greater than 1/2 + 1/Poly (n).

Blum-Micali Representation

[0038] In this paper, we will use the binary representation when we discuss the security of the i-th bit, however, we want to mention another interpretation of i-th bit. Blum-Micali introduced a particular bit predicate, B(x) and showed its hardness. B(x) is 0 if 0 <= x <= p-1/2 and B(x) is 1 if p-1/2 < x <= p-1. This is sometimes referred to as the most significant bit of x and it is clearly different from the most significant bit of x under the binary representation. Others [LW] have extended the definitions to define the k most significant bits. Often the Blum-Micali representation is used to refer to the most significant bits, while the binary representation is used for the least significant bits. In this paper we will use the binary representation when referring to the i-th bit, unless specified otherwise.

Individual Hardness of Bits

[0039] In this section, we discuss the security of the trailing n-O(log n)$^+$ bits, where O(log n)$^+$ is as defined earlier. To be precise we show that except the least significant bit, all the n-O(log n)$^+$ lower bits are individually hard with respect to the DLSE problem. Based on definition 1, this amounts to proving the bits of the discrete logarithm are DLSE-hard.

[0040] Let $O^i(g,y,p)$ be an oracle which gives the i-th bit (for any i in [2,n-O(log n)$^+$]. Note that i increases from right to left and i=1 for the least significant bit. Given this oracle we show that in polynomial number of steps we can compute the short exponent discrete logarithm. In addition, we prove hardness of individual bits by showing that given $O^i_{epsilon}$ (g,y,p) with epsilon advantage to predict the i-th bit (for any i in the prescribed range) which runs in polynomial time, we can turn this into an algorithm to compute the discrete logarithm of a short exponent by making polynomial number of queries to this oracle. For the rest of the paper we will refer to lower k bits to mean lower k bits excluding the least significant bit, for any k.

Theorem

[0041] The lower n-O(log n)$^+$ bits are DLSE - individually hard.

[0042] Proof: According to definition 1, it is enough to show that given $O^i(g,y,p)$ we can compute log y for all y such that x=log y is a short exponent. Without loss of generality, let us assume that p-1=2q, where q is an odd integer.

(a) Perfect Oracles - $O^i(g,y,p)$.We are given g^x and g and we know in advance that x is small (consisting of O(log n)$^+$ bits). Now, computing the least significant bit is always easy, via the Legendre symbol. Hence we compute it and set it to zero. Let i=2 and suppose we have an oracle for the 2nd bit. If this is a perfect oracle then we compute the second bit. Once this is computed then we set it to zero and we will continue to refer to the new number as g^x. Next we compute the square roots of g^x. The roots are $g^{x/2}$ and $g^{x/2+(p-1)/2}$ where we refer to the former as the principal square root. Since the two least significant bits of g^x are zero, we know that the principal square root has LSB equal to zero (or equivalently Legendre symbol one). This allows us to identify the principal square root. Now run the oracle on the principal square root and compute the second least significant bit. This bit is really the third least significant bit of x. Once again, set this bit to zero and repeat the process. Clearly, in poly(n) steps we would have computed x one bit at a time from right to left. Now, when i>2 we square g^x, (i-1) times. Then the 2nd LSB is at the i-th position, and we run the oracle to compute this bit. Zero this bit and once again compute square roots.

The principal square root corresponds to the root with LSB equal to zero. Now the (i+1)-th of x can be computed by running the oracle on the principal square root. Continue this process and in k steps where k=log x, we would know x.

(b) Imperfect Oracles - $O^i_{epsilon}(g,y,p)$. Suppose we have an imperfect oracle which succeeds in finding the i-th bit in only epsilon more than fifty percent of the x in $(Z/(p))^*$. Then we can concentrate the stochastic advantage and turn this oracle into an oracle which answers any specific instance correctly with arbitrarily high probability.

[0043] We divide the proof into two parts

(i) The lower 2 times O(log n) bits are individually hard.
(ii) The middle n-O(\log n)$^+$ to 2 times O(log n) bits are individually hard.

WAVELYNX EX. 1003, Pg. 1273
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0044] (i) Suppose we have an imperfect oracle whose advantage is epsilon, i.e., the oracle can give the correct answer on epsilon more than fifty percent of the possible inputs (and we do not know which ones). Then let r_j be a sequence of polynomial number of random numbers between 1 and p-1. We run the oracle on g^{x+r_j}, where the LSB of x is zero. Via the weak law of large numbers, a simple counting of the majority of 1's and 0's of the oracle output (after neutralizing the effect of the random number)for the second LSB yields this bit. Now compute the square roots and pick the principal square root as earlier. Once again repeat the process with a fresh set of random numbers to discover the next bit. Clearly in poly(n) steps we would have discovered x one bit at a time from right to left. The proofs are omitted, and we refer to [Pe] for details.

[0045] Suppose $i>2$. Then we square g^{x} $i-1$ times, and repeat the above process and conclude that any oracle which has an ϵ advantage will lead to a polynomial time algorithm to compute x. The only aspect that needs additional mention is the fact, when we randomize it is possible that for some r_j when we add them to the exponent we may exceed $p-1$. We refer to this as cycling. Assuming that we pick our random numbers uniformly, then we argue that the probability of this cycling is bounded above by $\frac{1}{poly(n)}$ and hence we need to increase the number of queries by a certain amount corresponding to the drop in cycling. Once again the details of the proofs are omitted and the reader is refereed to Blum-Micali [BH], for the techniques.

[0046] (ii) The proof of this step is also similar to the second part of the proof of (i) except that one has to set the initial t bits to zero by guessing, before we start the randomizing process. Here t is again a poly($\log n$) number and hence the probability of cycling is bounded above as earlier. Once again the details are omitted for brevity and will be included in an expanded version of this paper.

[0047] Suppose i>2. Then we square g^x i-1 times, and repeat the above process and conclude that any oracle which has an epsilon advantage will lead to a polynomial time algorithm to compute x. The only aspect that needs additional mention is the fact, when we randomize it is possible that for some r_j when we add them to the exponent we may exceed p-1. We refer to this as cycling. Assuming that we pick our random numbers uniformly, then we argue that the probability of this cycling is bounded above by 1/poly(n) and hence we need to increase the number of queries by a certain amount corresponding to the drop in cycling. Once again the details of the proofs are omitted and the reader is referred to Blum-Micali [BH], for the techniques.

[0048] (ii) The proof of this step is also similar to the second part of the proof of (i) except that one has to set the initial t bits to zero by guessing, before we start the randomizing process. Here t is again a poly(log n) number and hence the probability of cycling is bounded above as earlier. Once again the details are omitted for brevity and will be included in an expanded version of this paper.

Discrete Logarithm Hides Almost n bits

[0049] In this section we prove the simultaneous hardness of n-O(log n)$^+$ lower bits of the index in modular exponentiation. Intuitively, given a generator g of a finite field of order p, and g^x for some x then we show that gaining *any information* about the trailing n-O(log n)$^+$ bits is *hard*. Here hardness is with respect to the DLSE problem. In other words, for any prime p given a random generator g and a random element g^x of the finite field, any information on the relevant bits of x can be converted into an poly(n) algorithm to solve the DLSE problem. Now, the phrase gaining any information is rather vague, and this is clarified by the concept of simultaneous security which is defined below for any generic one way function.

Definition 2

[0050] Let f be a one way function. A collection of k bits, $B^{k(x)}$ is said to be simultaneously secure for f if $B^{k(x)}$ is easy to compute given x and for every Boolean predicate B an oracle which computes $B(B^{k(x)})$ correctly with probability greater than ½ given only f(x) can be used to invert fin Poly(n) time.

[0051] In this paper we will be employing a modified notion of simultaneous security relative to a possibly different one way function.

Definition 3

[0052] Let f and f be one way functions whose range is [0,N] A k-bit predicate B^k is said to be f-simultaneously hard if given f(x), for every non-trivial Boolean predicate B on k bits, an oracle which outputs $B(B^{k(x)})$ can be used to invert fin polynomial time. If B^k is a f' hard predicate then we say the bits of $B^{k(x)}$ are f-simultaneously hard.

[0053] The above definition, although precise, is not easy to apply when understanding simultaneous security. A more working definition is provided in definition 4, phrased in the language of the discrete logarithm problem over a prime modulus.

WAVELYNX EX. 1003, Pg. 1274
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Definition 4

[0054] The bits of the exponentiation function g^x mod p at location j <= i <= k are DLSE-simultaneously hard if the [j,k] bits of the discrete logarithm of g^x mod p are polynomially indistinguishable from a randomly selected [i,k] bit string for random chosen (g, p, g^x mod p). In addition any polynomial distinguishability will lead to an oracle which solves the DLSE problem in polynomial time.

[0055] Once again, proving polynomial indistinguishability of a group of bits as above is difficult. But the notion relative hardness helps alleviate this problem and in fact leads to a test of simultaneous security.

Definition 5

[0056] The ith bit, j <= i <= k, of the function g^x mod p is relatively hard to the right in the interval [i,k] if no polynomial time algorithm can, given a random admissible triplet (g, p, g^x mod p) and in addition given the k-i bits of the discrete logarithm of g^x to its right, computes the i the bit of the discrete logarithm of g^x with probability of success greater than ½ + 1/poly(n) for any polynomial poly(n) where n=log p.

[0057] Based on this definition, we have a test for simultaneous security. The statement of this test is the following theorem.

Theorem 1

[0058] Definitions 4 and 5 are equivalent.

[0059] The proof of this equivalence for non-biased bits is basically the well-known proof of the universality of the next bit test due to Yao [Y]. This proof technique is explained in [BH]. Now, using this theorem and the intractability of the DLSE problem we show that the trailing n - $O(\log n)^+$ bits are simultaneously hard.

Theorem 2

[0060] The n - $O(\log n)^+$ trailing bits of g^x mod p are simultaneously hard, with respect to the DLSE problem.

[0061] Proof: It is sufficient to show that every trailing bit of g^x is relatively hard to the right in the interval [2,n-$O(\log n)^+$]. Note that, individual hardness of bits does not imply the simultaneous hardness of all bits. Following the definitions and theorem above we know that, in order to show simultaneous security, we are allowed to use only a weak oracle: given g^x, to predict the ith bit of x , all the i-1 trailing bits of the unknown x should also be given to the oracle. This is a very hard task in general.

[0062] Assume the theorem is false. Then, for some i in [2,n-$O(\log n)^+$] there exists an oracle which when supplied with the trailing i-1 bits of a generic g^x succeeds in predicting the ith bit of x with advantage epsilon where epsilon is 1/poly(n). Now pick an element $S=g^s$ where s is a short exponent. We can shift s to the left by squaring S the appropriate number of times. Since 0 <= i < n-$O(\log n)^+$ we can shift s by i-$O(\log n)$ bits to the left without cycling. Recall, by cycling we mean the exponent exceeds p-1 and hence its remainder modulo p-1 replaces the exponent. Now the 2nd LSB of s rests on the ith bit and we can run the oracle repeatedly by multiplying by g^r mod p where r is a random number between 0 and p-1. In order to make sure that the probability of cycling is low we may have to set the t=poly(log n) leading bits of s to zero which we can exhaustively guess and run the algorithm for each guess. At the end of the algorithm we have a candidate and we can see if $g^{candidate}$ equals S. If it does then we stop or else repeat the algorithm with another guess. Since we will continue to have an epsilon' >= epsilon -1/t advantage we can deduce the bit from the oracle in poly(n) time. We know the 2nd LSB of s in this manner. We set that bit to zero, and take the square root of the number. Of the two roots we should pick the one which is the quadratic residue because all the lower bits are zero to begin with and hence the square root should have a zero in the LSB. Now the next bit of s is in the ith position and we can run the oracle repeatedly to discover this bit and so on to recover all the bits of s. Note the Oracle is very weak unlike the case for the individual bit oracle. The oracle here will tell you the ith bit with epsilon advantage provided you also supply all the i-1 bits to the right of i. However we are able to do this because all the bits to the right of the shifted s are known to be zero, since we started with a short exponent. Now we have shown that for every i such that 2 <= i < O(log n) we can use this weak oracle to discover s thus we have shown the trailing bits to be simultaneously hard provided the function g^s mod p with s of size $O(\log n)^+$ is hard to invert.

Pseudo Random Bit Generator

[0063] In this section we provide the details of the new pseudo random bit generator. In particular we extend the scheme used by Blum-Micali [BM] to extract more bits. This is the same scheme that Long-Widgerson [LW] used in their generator but their output consisted of log n bits per iteration. In our new scheme we produce n-$O(\log n)^+$ bits per

WAVELYNX EX. 1003, Pg. 1275
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

iteration. Recall from section 2 that the Blum-Micali scheme used a mildly different definition of "bits". We use the same definition of bits as Hastad-et al, but we do not encounter the difficulties they did in defining the generation scheme since our exponentiation induces a permutation on {Zp}*.

[0064] **NEW GENERATOR** : *Pick a seed* s_0 *from* $\{Z_p\}^*$. *Define* $s_{i+1}=g^{\{s_i\}} \bmod p$. *At the* i^{th} *step (i>0) output the lower n-O(log n)⁺ bits of* s_i, *except the least significant bit.*

Proof of Security

[0065] Suppose A is an epsilon-distinguisher of the 1(1 is poly in n) long output of our generator, then there is a (epsilon/1)-distinguisher for any output at the ith step. In particular there is a (epsilon/1)-distinguisher for n-O(log n) bits of s_0. According to our definitions in the previous section, due to Yao [Y], we can use a distinguisher to create a weak oracle which will tell us the ith bit of x provided we also give it the right most i-1 bits of x.

[0066] Now we note that we can use this to discover x given g^x mod p where x is slightly larger than O(log n). We repeatedly invoke the "oracle" by setting $s_0 = \{g^x\}\{g^r\}$. Thus we can discover the entire x. So if the output sequence of our generator is epsilon-distinguishable then in poly(n) time we can discover x of our exponentiation function. Assuming it is intractable to invert the function g^x mod p where x is slightly larger than O(log n) bits (i.e., short exponent) then the output sequence of our generator is polynomially indistinguishable.

[0067] Using techniques shown in theorem 3 we can discover the entire x. So if the output sequence of our generator is epsilon-distinguishable then in poly(n) time we can discover x of our exponentiation function. Assuming it is intractable to invert the function g^x mod p where x is slightly larger than O(log n) bits (i.e., short exponent) then the output sequence of our generator is polynomially indistinguishable.

Conclusion

[0068] We have shown that the discrete logarithm mod a prime p hides n-O(log n)⁺ bits by showing the simultaneous hardness of those bits. The hardness in this result is with respect to the discrete logarithm problem with short exponents, i.e., DLSE-simultaneously hard (as defined in section 2 of this paper).

[0069] This allows us to extract n - O(log n)⁺ bits at a time for pseudo random generation and other applications. As an example for n of size 1024 bits and s of size 128 bits this allows us to extract almost 900 bits per exponentiation. Spoken informally, we note that the security of this example is 2^{64} since it takes $O(2^{64})$ for the best known algorithm to crack a modular exponentiation with 128 bits. Also, if one desires more security at every step then we can decrease the number of bits extracted at every stage. This generator outputs the maximal number of bits from a single iteration. Extracting any more bits in any iteration leads to a prediction of bits - since we would then be dropping O(log n) bits and hence in polynomial number of guesses we would know the complete exponent in every iteration.

Bibliography

[0070]

[ACGS] W.\ Alexi, B.\ Chor, O.\ Goldreich and C.\ P.\ Schnorr,
RSA/Rabin bits are 1/2+1/poly(log N) secure,
Proceedings of 25th FOCS, 449--457, 1984.

[BCS] M.\ Ben-Or, B.\ Chor, A.\ Shamir,
On the cryptographic security of single RSA bits,
Proceedings of 15th STOC, 421--430, 1983.

[BBS] L.\ Blum, M.\ Blum, and M.\ Shub,
A simple secure pseudo-random number generator,
SIAM J. Computing, 15 No. 2:364--383, 1986.

[BM] M.\ Blum, and S.\ Micali,
How to generate cryptographically strong sequences of pseudo random bits,
SIAM J. Computing, 13 No. 4:850--864, 1984.

[BH] R.\ B.\ Boppana, and R.\ Hirschfeld,
Pseudorrandom generators and complexity classes,
Advances in Computing Research, 5 (S.\ Micali, Ed.), JAI Press, CT.

[DSS] U.\ S.\ Department of Commerce/N.I.S.T,
Digital Signature Standard, FIPS 186, May 1994.

[GL] O.\ Goldreich, and L.\ A.\ Levin,
A hard-core predicate for all one way functions,
Proceedings of 21st STOC, 25--32, 1989.

[GM] S.\ Goldwasser, and A.\ Micali,
Probabilistic encryption,

WAVELYNX EX. 1003, Pg. 1276
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Journal of Computer and Systems Science, 28: 270-299, 1984.
[HSS] J.\ Hastad, A.\ W.\ Schrift, and A.\Shamir,
The discrete logarithm modulo a composite modulus hides $O(n)$ bits,
Journal of Computer and System Sciences, 47: 376--404, 1993.
[ILL] R.\ Impagliazzo, L.\ A.\ Levin, and M.\ Luby,
Pseudo-random generation from one-way functions,
Proceedings of 20th STOC, 12--24, 1988.
[Ka] B.\ S.\ Kaliski,
A pseudo-random bit generator based on elliptic logarithms,
Advances in Cryptology - CRYPTO '86 (LNCS 263), 84--103, 1987.
[KMO] J.\ Kilian, S.\ Micali, and R.\ Ostrovsky,
Minimum resource zero-knowledge proofs,
Proceedings of 30th FOCS, 474--489, 1989.
[Kn] D.\ E.\ Knuth,
The Art of Computer Programming (vol 2): Seminumerical Algorithms,
Addison Wesley, 2nd edition, 1981.
[Ko] N.\ Koblitz,
Elliptic curve cryptosystems,
Mathematics of Computation, 48 :203--209, 1987.
[LW] D.\ L.\ Long, and A.\ Widgerson,
The discrete log hides $O(\log n)$ bits,
SIAM J. Computing, 17:363--372, 1988.
[Mi] V.\Miller,
Elliptic curves and cryptography,
Advances in Cryptology - CRYPTO '85 (LNCS 218), 417--426, 1986.
[Na] M.\ Naor,
Bit commitment using pseudo-randomness,
Advances in Cryptology - CRYPTO '89 (LNCS 435), 128--136, 1989.
[OW] P.\ van Oorschot, M.\ Wiener,
On Diffie-Hellman key agreement with short exponents,
Advances in Cryptology - EUROCRYPT '96 (LNCS 1070), 332--343, 1996.
[Pe] R.\ Peralta,
Simultaneous security of bits in the discrete log,
Advances in Cryptology - EUROCRYPT '85 (LNCS 219), 62--72, 1986.
[PH] S.\ C.\ Pohlig, and M.\ E.\ Hellman,
An improved algorithm for computing over $GF(p)$ and its cryptographic significance,
IEEE Trans. IT, 24: 106--110, 1978.
[Po] J.\ M.\ Pollard,
Monte Carlo methods for index Compton (mod p),
Mathematics of Computation, 32, No. 143:918--924, 1978.
[VV] U.\ V.\ Vazirani, and V.\ V.\ Vazirani,
Efficient and secure pseudo-random number generators,
Proceedings of 25th FOCS, 458--463, 1984.
[Y] A.\C.\Yao,
Theory and applications of trapdoor functions,
Proceedings of 23rd FOCS, 80--91, 1982.

Appendix

[0071] In this section we discuss some extensions of our results which will be addressed in an extended version of this paper.

Improving Efficiency of Computations

[0072] Let us focus on the mechanics of the generator. We start with a finite field, and a generator g of its multiplicative cyclic group. Let so be a secret seed. Then we define $s_{i+1} = g^{s_i}$ iteratively. The output of the generator are the trailing $n-O(\log n)^+$ bits of s_i for all $i>0$, where $n=\log p$.

[0073] Although the number of bits generated per iteration is large, each iteration involves a large exponent and this

WAVELYNX EX. 1003, Pg. 1277
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

could impact on the speed of the generator. Instead, we could start with p, g, and so as earlier but at each stage we define $s_{i+1} = g^{\{s_i,\}}$ where s_i, = leading $O(\log n)^+$ bits of s_i. This will ensure that at each stage we are using short exponents and hence guarantee a significant speed up. This raises some interesting questions.

Question

[0074] Will this speed impact the security of the generator?

[0075] Note that when we restrict our exponents we no longer have a permutation. Hence the simple construction used here is inapplicable. A possible method of settling this problem is outlined in Hastad et al in the context of discrete logarithms over composite moduli [HSS]. In particular, exploiting a certain hashing lemma proved in [ILL] they construct a *perfect extender* and the pseudo-random generation is achieved through repeated applications of the extender to a random seed.

Question

[0076] Is it possible to adapt techniques from [HSS] to short exponent exponentiation in a finite field and guarantee a speed up of computations and security?

Discrete Logarithms in Abelian Groups

[0077] Let G be a finite Abelian group. Let g in G and let $y = g^x$ (where x is unknown and we are using the multiplicative notation to denote the group operation). The discrete logarithm problem in the subgroup generated by g asks for the value of x given g and y. Clearly, the possible values x can take are from 0 to o(g), where o(g) denotes the order of g, and the subgroup generated by g is cyclic.

[0078] In this context, Kaliksi [Ka] has shown that under the intractability assumption of the discrete log in the subgroup generated by g the individual bits of x are hard. In this paper the Blum-Micali notion of bits is employed, and the proof of individual hardness is based on a novel and new oracle proof technique.

[0079] The main idea being, the identification of bits is based on a correlation function which automatically accommodates cycling and changes in bits due to randomization. In addition, he completely avoids the computation of square roots which is central to several of the other works on individual bit security. This paper also states that log n bits are simultaneously hard. Presumably, the techniques of Long-Widgerson once applied in the framework of generic Abelian groups yields this result.

[0080] Now, we note that assuming the discrete logarithm problem with short exponents is also hard in the chosen Abelian group our results on simultaneous hardness of the trailing bits are applicable. Here one could adapt the techniques outlined by Kaliski in order to deduce simultaneous hardness. Once this is shown then a pseudo random generation scheme can be outlined based on techniques developed by Hastad-et al. The main problem is to address the fact that the subgroup generated by g may be a proper subgroup and hence the group operation on g will not produce a permutation of the group to itself. The exact details of the simultaneous hardness and the subsequent scheme of pseudo random bit generation, will be deferred to an extended version of this paper. This result will be very useful when applied to elliptic curves over finite fields.

Bit Commitment Schemes

[0081] Several cryptographic schemes require the communicating individuals to commit to a certain message without revealing any information about the contents of the message. Several single bit and multi-bit commitment schemes have been presented in the past. Multi-bit schemes which improve the efficiency of existing protocols are outlined in [KMO]. An example of a multi-bit commitment scheme based on pseudo random bit generators is Naor's scheme [Na]. In [HSS], Hastad et al present a scheme which directly uses exponentiation modulo a composite integer. But all schemes based on pseudo-random generators depend on the efficiency of the generator. Hence the efficiency of the generator presented in this paper suggests that bit commitment schemes can be speeded up. This topic will also be explored later.

[0082] Although the present invention has been described in considerable detail with reference to cryptography and communication, other applications and versions are possible. For example, the pseudo-random number generator may be used for simulations and other cryptographic applications. Therefore, the spirit and scope of the present invention should not be limited to the description of the embodiments contained herein.

WAVELYNX EX. 1003, Pg. 1278
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Claims

1. A method of generating pseudo-random numbers using a pseudo-random generator defined by a modular exponential function $x_i = g^{x_{i-1}} \bmod p$, wherein x_i is a value comprising m bits, p is a prime number comprising k bits, g is a generator of integer mod p, and $1<i\leq n$, the method comprising the steps of:

   receiving a seed value x_0 comprising m bits; and

   CHARACTERIZED BY

   outputting a pseudo-random number z_i of the value x_i determined using the seed value x_0, the pseudo-random number z_i including a second least significant bit of the value x_i through a jth least significant bit of the value x_i, the valuej being no larger than m-2c, the value c representing a cryptographic security threshold level; and combining the pseudo-random number z_i with a message segment to produce an encrypted message segment.

2. The method of claim 1, wherein the cryptographic security threshold level c is at least 64.

3. The method of claim 1, wherein the value x_i comprises at least 512 bits.

4. The method of claim 1, wherein the value p comprises at least 512 bits.

5. The method of claim 1, wherein the value x_i comprises at least 1024 bits.

6. The method of claim 1, wherein the value p comprises at least 1024 bits.

7. The method of claim 1 comprising the additional step of:
   generating the value x_i.

8. The method of claim 1, wherein the message segment comprises j-1 bits.

9. The method of claim 1 wherein the message segment is combined with the pseudo-random number z_I using an XOR binary operation.

WAVELYNX EX. 1003, Pg. 1279
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 1

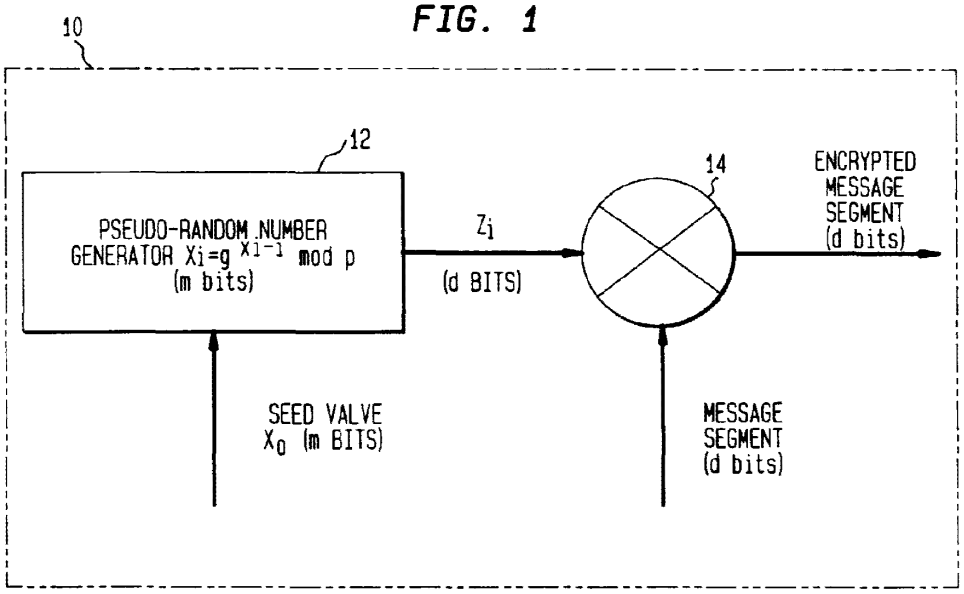
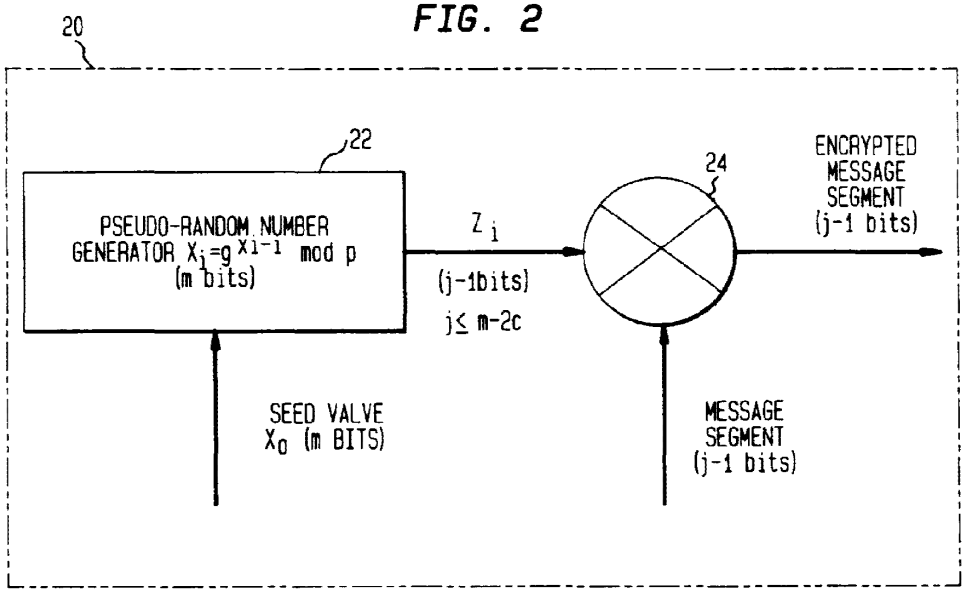


FIG. 2



WAVELYNX EX. 1003, Pg. 1280
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

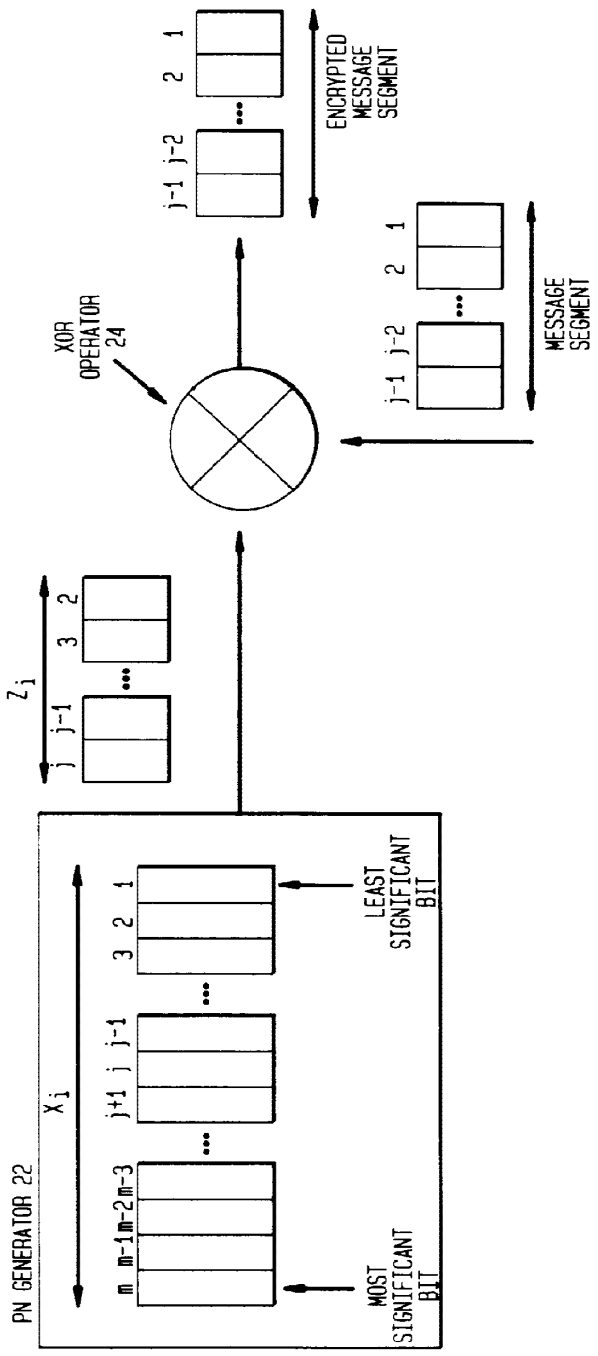


FIG. 3

WAVELYNX EX. 1003, Pg. 1281
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 996 928 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
02.06.2004 Bulletin 2004/23

(21) Application number: **98936946.7**

(22) Date of filing: **20.07.1998**

(51) Int Cl.[7]: **G06K 17/00**, G07D 7/00

(86) International application number:
PCT/US1998/015070

(87) International publication number:
WO 1999/004364 (28.01.1999 Gazette 1999/04)

(54) **VERIFICATION OF AUTHENTICITY OF GOODS BY USE OF RANDOM NUMBERS**

ÜBERPRÜFEN DER ECHTHEIT VON GÜTERN UNTER VERWENDUNG VON ZUFALLSZAHLEN

VERIFICATION DE L'AUTHENTICITE D'ARTICLES AU MOYEN DE NOMBRES ALEATOIRES

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.07.1997 US 897857**

(43) Date of publication of application:
03.05.2000 Bulletin 2000/18

(73) Proprietor: **Assure Systems Inc.**
Pleasanton, CA 94566 (US)

(72) Inventor: **DOLJACK, Frank, A.**
Pleasanton, CA 94566 (US)

(74) Representative: **Potter, Julian Mark et al**
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

(56) References cited:
WO-A-84/03019
WO-A-93/22745
US-A- 3 833 795
US-A- 4 463 250
US-A- 5 367 148

- **ANONYMOUS: "Point of Sale Transaction Logging Scheme. April 1980." IBM TECHNICAL DISCLOSURE BULLETIN, vol. 22, no. 11, April 1980, pages 5046-5049, XP002084211 New York, US**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 0 996 928 B1

Description

FIELD OF THE INVENTION

[0001] This invention relates to methods and systems for verifying the authenticity of items or goods using combination codes having random and non-random portions.

BACKGROUND OF THE INVENTION

[0002] Products which are mass produced are distributed to end users through sales and distribution channels. When the products have particular value associated with them, counterfeiters sometimes produce products which are copies of those produced by the original manufacturers. These counterfeit products are then introduced into the sales and distribution channels and end users become deceived regarding the source of the goods and/or their quality. Lost sales occur for the original manufacturer, and the end user may receive less value than what was expected. Name brand goods, certified products and copyrighted products are often the target of such counterfeiting activities.

[0003] To address the problem of counterfeiting, one prior art solution has been to attach a label containing an optical device which is difficult to reproduce, for example, a holographic image to the products to confirm their authenticity. The original manufacturer controls these labels and their content to prevent easy access to such labels by counterfeiters. Use of such an optical device is desirable in that the authentication procedure is relatively simple, for anyone may visually inspect the label and its presence indicates authenticity. Unfortunately, this approach suffers from the weakness that skilled counterfeiters, by extending substantial effort, can reproduce these labels. Once reproduction is achieved, the counterfeiter may easily introduce a multitude of counterfeit products within the sales and distribution channels. A second disadvantage to the optical device methodology is that the creation of the special labels is relatively expensive and therefore is only cost effective for certain classes of products.

[0004] In pre-paid service areas, the use of randomly generated numbers have been utilized to validate a user prior to accessing the pre-paid service. For example, pre-paid phone card access numbers generated by random numbers have been used for such purposes. The phone card number is input into a phone or other device to validate the user prior to registering a phone call. A second application involves the use of confirmation numbers as back-up identification for electronic ticketing air fares. The use of random numbers for access of such pre-paid services, however, is substantially different than the use of optical codes for authenticating mass produced goods. For example, in the pre-paid phone card application, each random number is held secret by the user of the service, therefore a theft of the phone card or its loss may allow someone to access the pre-paid service. In the electronic air fare ticketing application, neither secrecy nor duplication of the code is of great concern since the use of the random number is only for backup identification. Knowledge of the confirmation number by a third party is unlikely to cause any loss because a third party's attempt to board an airplane flight will conflict with the boarding by the valid party. Unlike the product authentication in which previously optical devices have been used, the pre-paid service using randomly generated numbers play no role in preventing or deterring large scale loss due to counterfeiting of mass-produced goods.

[0005] In another prior art method for authentication, an apparatus is used to measure a random characteristic of a card, tag or label. The random characteristic, or "fingerprint," is read by a special reading apparatus and converted to a code which is encrypted and printed on the tag or label. The encryption ties the label to the original manufacturer of the product and the code value in turn is tied to the particular label on which it is printed since that label has the "fingerprint." This method, although secure in authenticating single labels, introduces significant costs because the label must contain special technology for the development of the "fingerprint" and a special reader must be developed and used at the time of printing the label and when the label is subsequently field checked. These shortcomings introduce significant costs in attempting to authenticate mass produced goods. It is not necessary to prevent even single counterfeits, which this method does, since the manufacturer of mass produced goods is instead interested in deterring mass counterfeiting of his product.

[0006] U.S. Patent 5,367,148 discloses a method of verifying the authenticity of goods at retail outlets. Each product is provided with an identification number having random and non-random portions. The identification numbers are placed on registration cards which are read and compared to a database of identification numbers to see if the numbers are valid. The patent also uses a random number and a secret code as an identification number, wherein the secret code is calculated using an one-way hash function type algorithm.

[0007] U.S. Patent 3,833,795 discloses a method for verifying the authenticity of goods by providing each good with an identification number that has random and non-random portions. Authenticity of goods is determined by maintaining the identification numbers in a master list and comparing the random number on the analyzed good with the master list.

[0008] Therefore there is a need in the art for a low cost, secure way of verifying the authenticity of mass produced goods. There is also a similar need to track goods and/or detect a diversion of goods.

SUMMARY OF THE INVENTION

[0009] According to a first aspect of the invention,

WAVELYNX EX. 1003, Pg. 1283
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

there is provided a method of verifying the authenticity of items, comprising the steps of: generating combination codes, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes; encrypting the combination codes; associating the encrypted combination codes with one or more items; and examining the items to verify whether they are authentic; wherein the step of examining the items comprises the steps of: reading a code from one of the one or more items; decrypting the code; and determining whether the decrypted code contains the non-random portion of the combination code.

[0010] In a second aspect, the invention provides a method of verifying the authenticity of items, wherein combination codes have been generated, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes, the combination codes have been encrypted, and the combination codes have been associated with one or more items, the method comprising the step of: examining items to verify whether they are authentic; wherein the step of examining the items comprises the steps of: reading a code from one of the one or more items; decrypting the code; and determining whether the decrypted code contains the non-random portion of the combination code.

[0011] In a particular embodiment the non-random portion is not personalised to the item to which the code is applied.

[0012] The non-random portion may already be known and the step of determining whether the decrypted code contains the non-random portion may comprise inspecting the decrypted code and checking whether the already known non-random portion and the decrypted non-random portion match.

[0013] If the step of determining determines that the decrypted code contains the non-random portion, the method may further comprise determining whether the random portion of the decrypted code is unique, whereby non-uniqueness provides an indication that the product may be counterfeit.

[0014] In a particular embodiment the determining whether the random portion of the decrypted code is unique comprises comparing the decrypted random code to a local or master database.

[0015] The method may further comprise determining whether a tax has been paid properly using the decrypted combination code by evaluating whether the decrypted combination code contains a correct non-random portion. The method may further comprise destroying the codes after use. In one embodiment the method further comprises destroying or confiscating the items if a tax has not been paid properly.

[0016] The method may further include detecting a diversion of items with respect to which combination codes are associated from a desired channel of distribution, wherein a particular channel of distribution has an associated decryption key for decrypting codes and an associated non-random portion, the detecting comprising: inspecting items within the particular channel of distribution; decrypting the codes on the items with the decryption key; and comparing the non-random portions of the combination codes with the associated non-random portion for that channel of distribution; wherein a match indicates no diversion of the items from the desired channel of distribution.

[0017] In one embodiment the method further comprises the step of generating a pair of encryption keys, wherein one key is used to encrypt combination codes for the desired channel of distribution and the other key is used to decrypt the codes within the desired channel of distribution.

[0018] The step of reading the code may comprise scanning the code.

[0019] In a particular embodiment the non-random portion includes at least a secret portion that is encrypted, and wherein the secret portion is encrypted with a key and can be decrypted with a corresponding key.

[0020] The non-random portion of the combination code may include a secret encrypted portion containing tracking information, wherein examining the items includes: decrypting the combination code; and decrypting the secret portion of the decrypted combination code to determine the tracking information.

[0021] A third aspect of the invention provides a method of preparing combination codes for verifying the authenticity of items, comprising the steps of: generating combination codes, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes; and encrypting the combination codes.

[0022] The method may further comprise: associating the encrypted combination codes with one or more items.

[0023] Associating the encrypted codes with one or more items may comprise applying the encrypted combination codes to one or more items.

[0024] In a particular embodiment the method further comprises selecting the non-random portion as at least one of a trade name, a manufacturer's initials, a string, an alphanumeric or any type of recognizable message.

[0025] The method may further comprise storing in a master database the random portion of each combination code.

[0026] The method may further comprise applying the combination codes to items for use to determine whether a required tax or duty has been paid.

[0027] According to a fourth aspect of the invention, there is provided a system for preparing combination codes for verifying the authenticity of items, comprising: means for generating combination codes, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the

WAVELYNX EX. 1003, Pg. 1284
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

same for a plurality of the combination codes; and means for encrypting the combination codes.

[0028] The system may further comprise means for associating the combination codes with one or more items.

[0029] In a particular embodiment the system further comprises a code reader for reading a code on an item; and comparing means for comparing the random portion of a read code to unique random codes in a database, wherein the comparing means is operable to indicate whether the read code has been read on another item.

[0030] The system may be for detecting a diversion of items with respect to which combination codes are associated from a desired channel of distribution, wherein a particular channel of distribution has an associated decryption key for decrypting codes and an associated non-random portion, and the system may further comprise: means for inspecting items within the particular channel of distribution; means for decrypting the codes on the items with the decryption key; and means for comparing the non-random portions of the combination codes with the associated non-random portion for that channel of distribution; whereby a match indicates no diversion of the items from the desired channel of distribution.

[0031] The objects, advantages and novel features of the invention will become apparent from the following detailed description of the invention when considered in conjunction with the drawings. The following description is given by way of example only.

BRIEF DESCRIPTION OF THE DRAWINGS

[0032]

Figure. 1 is a system level diagram illustrating a system to generate and apply random codes to mass-produced goods and subsequently inspect the goods to verify their authenticity.

Figure 2 is a block diagram illustrating a process using a random code applied to goods to authenticate their authenticity.

Figure 3 is a block diagram illustrating an embodiment of the invention, using the system to generate encrypted codes for use in authenticating goods to thereby prevent counterfeiting.

Figure 4 is a chart illustrating the identification of a non-random portion of a decrypted combination code.

Figure 5 is a block diagram illustrating a process using the authentication system to prevent the diversion of goods.

Figure 6 is a perspective diagram illustrating goods having an encrypted combination code applied to an inside portion of a product wherein reading the code requires tampering with the product in an irreversible manner.

Figure 7 is a block diagram illustrating a process using a secret code included in a encrypted combination code.

Figure 8 is a block diagram illustrating another process using an encrypted combination code to determine information, such as proper payment of a tax on cigarettes or the like, regarding goods or the like.

DETAILED DESCRIPTION

[0033] The system and method of the following description provides for the verification of authenticity of goods by use of encrypted combination codes including a random code and a non-random code generated by a computer and subsequently produced on tags, labels or directly on products and ultimately placed within the stream of commerce. At a retail distribution outlet such as a retail store or alternatively, at any point earlier in the distribution chain, the encrypted combination codes are decrypted and read to identify its non-random portion. If the decrypted non-random portion matches the originally used non-random code, goods are authenticated while a mismatch indicates a counterfeit. The present system and method allows for a cost-effective verification of authenticity of goods and provides a substantial deterrent to those who wish to counterfeit mass produced items.

[0034] Figure 1 is a combined system and method diagram which illustrates the various components of the present invention and provides an environmental context in which the various components are utilized; Figure 1 therefore illustrates an authentication system 10. The authentication system 10 includes a host computer 12 having a processor 14 which contains the requisite hardware and software to provide a random number generator 16 and an encryptor 18. The processor 14 is coupled to an internal memory 20 for storage of generated random numbers or codes or alternatively for storage of various encryption algorithms to ensure that each code or encryption technique is unique. The processor 14 is also coupled to an I/O module 22 which provides input and output circuitry, drivers and interfaces to communicate with external components such as keyboards, printers and other peripherals or networks. Although the memory 20 has been illustrated as an internal memory, it should also be understood that the host computer 12 may alternatively utilize and access external memory. Upon generation of each random code, the processor 12 stores the random codes in a secure host database 24 for later access by field checkers to verify product authenticity.

[0035] The host computer 12 is coupled to a printer 26 via the I/O module 22. The printer 26 receives random codes generated by the processor 14 within the host computer 12 via the I/O module 22 and is operable to print out the random codes on various print media, for example, tags, labels or directly on various products. Depending upon the type of random code or combina-

WAVELYNX EX. 1003, Pg. 1285
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

tion code created by the random code generator 16, the printer 26 may generate a binary code 28 having a corresponding bar code for ease of reading or scanning, an alphanumeric code 30 having a corresponding bar code or alternatively a case sensitive alphanumeric code 32 with its corresponding bar code. Alternatively, other type codes may also be used. Depending upon the type of product being marked, the printer 26 generates the codes on a tag or label 34 (or alternatively directly on a product) which is then attached or affixed to the products 36, which are exemplary illustrated as the plurality of pants (clothing) which constitute a product inventory 38. Each product 36 is therefore marked with the label or tag 34, wherein each product 36 contains a unique random or combination code generated within the host computer 12. The products 36 are then distributed in commerce via various modes of transportation 40, for example, by air 42, by rail 44 or by standard freight shipping 46 to ultimately arrive at a retail distributor (or outlet) 48.

[0036] At the retail outlet 48 the label or tag 34 affixed to the product 36 is read by a tag reader (or scanner) 50 which is electrically coupled to the retail outlet's local computer 52. The local retail computer 52 is also in electrical communication with the secure host database 24 via a network-type connection 54. Various methods may be implemented utilizing the authentication system of Figure 1; for example, the system 10 may not only verify the authenticity of mass produced products, but may also be used to identify a diversion of such products into undesired channels of distribution.

[0037] Turning now to Figure 2, a method for verifying the authenticity of mass produced products via use of random codes utilizing the authentication system 10 of Figure 1 will be described. At step 60, the authentication system 10 generates one or more random codes. The one or more random codes are preferably generated within the host computer 12 via a user requesting such generation via an input device such as a keyboard which is coupled to the I/O module 22 which, in turn, is coupled to the processor 14. Upon such request, the processor 14 initiates generation of such a code via the random number (code) generator 16. Upon generation, the processor 14 checks whether the generated random code has been previously generated by comparing the generated random code to previously generated codes resident within the memory 20. If the generated random code has previously been generated, the processor 14 will erase the random code and generate another. The processor 14 may look within the memory 20 for all previous products made, or alternatively, or look within various subdirectories within the memory 20 to see whether the generated random code has been previously generated for the specified product now being addressed. Otherwise, the generated code is determined to be unique. The generation of random numbers in software is well known by those skilled in the art. For example, see "Suggestions for Random Number Generation in Software" by Tim Matthews, An RSA Data Security Engineering Report, Revised December 26, 1995.

[0038] Upon completion of the random code generation of step 60, the generated random codes are stored within the secure host database 24 at step 62. At this step, the host computer 12 has already verified that the random code is unique and sends the generated random code to the secure host database 24 via the I/O module 22. The secure host database 24 may be subsequently accessed to determine whether a valid random code read out in commerce has previously been used (which will be described in greater detail infra). After storage of the one or more random codes, each product is marked with one random code at step 64. The number of random codes required will be a function of the number of products 36 required to be marked. It is desirable that each product 36 has its own unique random code. Marking preferably is achieved by taking the generated random codes from the host computer 12 and printing them on a label 34 using the printer 26. As highlighted earlier, the random codes may be various types, for example, a binary 28, alphanumeric 30 or case sensitive alphanumeric code 32. Alternatively, other types of random codes may be utilized. Upon placing a random code to each of the various labels 34, the labels 34 are affixed to the desired products 36.

[0039] Upon the completion of product marking, the marked products are placed into the flow of commerce at step 66 via any of the modes of transportation 40 which are highlighted in Figure 1. Generally, such transportation constitutes standard freight shipping 46 such as by truck. The marked products 36 are then delivered to the retail outlet 48 where the marked products are read by a reading device or scanner 50 at step 68. Preferably, the label 34 on the product 36 is scanned by the scanner 50 upon the product's initial arrival at the retail outlet 48. Alternatively, the scanning may also be completed at a later time, for example, when the article is being purchased by a consumer. The scanner 50 scans the code on the tag 34, preferably by scanning the bar code which is a visual representation of the binary or alphanumeric random code being utilized. The scanner 50 takes the random code that has been scanned and downloads the scanned random code to the local computer 52.

[0040] The local computer 52 may be utilized for various accounting and inventory purposes in addition to the verification of authenticity of goods. In addition, the local computer 52 is in electrical communication with the secure host database 24 via either a wireless or wired network 54 or communication data link. The local computer 52, in accessing the secure host database 34, then compares the scanned random product code to those codes contained within the secure host database 24 at step 70 to verify whether the scanned random code is valid at step 72. If the scanned product code is not contained within the database 24 then the local computer 52 indicates to the individual performing the scan that

WAVELYNX EX. 1003, Pg. 1286
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the article is a counterfeit. Conversely, if the scanned product code is valid, that is, it has been found in the secure host database 24, the local computer 52 then checks the database 24 to see whether the scanned code has previously been used at step 74. If the database 24 indicates that the code has previously been used, the local computer 52 indicates to the user that the code is a duplicate. In this instance, one of two possibilities exist: either the present goods scanned are a counterfeit, or the product is authentic and the previously used code was attached to a counterfeit article. In either case, evidence of illegal counterfeiting activity has been uncovered. If the local computer 52, after analyzing the database 24, determines that the code has not previously been used, it indicates to the user that the goods are authentic and additionally indicates within the database 24 that a valid code has now been used at step 76. In this manner, the above method verifies the authenticity of mass produced products through use of random codes placed on the articles which are subsequently checked against a secure database whether the articles are at their retail outlet or perhaps at an intermediary wholesale location.

[0041] The effectiveness of the above-described method may be more fully appreciated through the following discussion of the method of Figure 2. Suppose, for example, the type of random code chosen is a 64 bit binary code. The number of possible 64 bit binary codes is 2^{64}, which is 1.8×10^{19} different numbers. Further suppose that a manufacturer wishes to mark 100 million similar products to verify their authenticity. 100 million unique 64 bit codes are then randomly chosen, stored in the secure database 24, and then each unique random code is applied to each respective product in a form which is preferably removal-resistant and perhaps even tamper-evident. Because this application of a product marking to the product itself is normally done, no significant incremental cost is associated with this operation. Further, since 100 million mass produced products have been marked and 1.8×10^{19} different codes are available, the probability of a counterfeiter guessing one of the used random codes is only 1 in 1.8×10^{11}. Therefore it is virtually impossible for a counterfeiter to come up with a significant number of valid codes without extending a considerable amount of effort and expense. For example, a counterfeiter must go to various retail outlets 48 and copy a number of valid random codes. This is an expensive and laborious process and further subjects the counterfeiter to potential discovery in the copying process. Additionally, whenever a counterfeiter applies a code which has been copied from products out in the field to his counterfeit products, the counterfeiter ends up labeling the product with a duplicate code. As already shown, all duplicates in the above method will be discovered which allows for subsequent investigation as to the source of the counterfeit product to identify the counterfeiter.

[0042] Even if the counterfeiter wishes to risk being identified by copying valid codes from the field, the counterfeiter must send someone into the retail outlets to copy valid codes from products already out in the stream of commerce. Suppose, for example, he extends considerable time and effort and gathers 1,000 valid codes. If he then produces one million counterfeit products he will use each of the 1,000 valid codes 1,000 times. He must then disguise his product by carefully mixing the marked items so that, once in the sales channel, field inspection is less likely to discover the duplicate at the same inspection site. This greatly complicates a counterfeiters logistics as well as his cost, thereby discouraging such counterfeiting activities. Furthermore, since multiple retail outlets will also access the database 24, even distributing the various codes to different outlets will still result in the duplicates being identified. Therefore, the care and effort taken by a counterfeiter to disguise his illegal acts only delays his discovery. Continued field checking will find the counterfeit products and will ultimately identify all the sales outlets which have or had the product. Therefore, it may be desirable for systematic field checking procedures to be put in place, for example, at the point of sale or at receipt of items at the retail outlet 48. In this manner, all counterfeit product will ultimately be intercepted and identified.

[0043] The randomly generated code may be, as in the previous example give, a 64 bit binary number. Alternatively, the random code may consist of, for example, an 8 bit alphanumeric code. These are the numbers 0 through 9 and the upper case and lower case alphabet A-Z and a-z, respectively. Since each bit of the 8 bit code can assume 62 different possibilities, there are 2.2×10^{14} different codes possible. As in the previous example, there will only be a one in 2,182,400 chance of guessing a valid code for 100 million products. If one disregards the case sensitivity in the alphanumeric character set, this can drop to one in 28,211 chances, which is still unguessable for practical purposes. Other variations may also be used in creating the random generated code.

[0044] In the process discussed with respect to Figure 2, the authentication system 10 utilizes field checking and subsequent validation and verification of codes between the local computer 52 and the secure host database 24 via the network data link 54. Therefore in that discussion, it is evident that the database 24 interacts with the local computer 52 to the extent that codes which have been read in previous field checking are labeled as such and identified with the sales outlet in which they are found. So, when accessed from the retail outlet 48, the database 24 updates this information in addition to determining that the valid code is present in the database and is not a duplicate. in this manner, verification of product authenticity is made at the time of database access. However, this is not the only solution. Alternatively, such verification may be accomplished locally at the retail outlet 48 field check location without access to a secure master database.

WAVELYNX EX. 1003, Pg. 1287
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0045] Proceeding onto Figure 3, a method of verifying the authenticity of products without accessing an offsite master database will be described in conjunction with the authentication system 10 of Figure 1. Figure 3 illustrates an embodiment of the invention. At step 80, the generation of random codes is established in a manner similar to that described earlier in step 60 of Figure 2; consequently, the details of such random code generation will not be repeated. At step 81, each random code is combined with a non-random code to thereby form a combination code. The non-random code may be, for example, the initials of the manufacturer, a tradename or other easily recognizable moniker or message, and combining may simply be accomplished by concatenating the initials to the end of each random code. Alternatively, the non-random code may be placed before or even interposed within the random code. Subsequent the generation of this combination code, the combination codes are encrypted at step 82 by the processor 14 within the host computer 12 which accomplishes the encryption via an internal encryptor 18. The encryptor 18, in a preferred embodiment, is a combination of processor hardware and software which allows for encryption of the generated combination codes which are developed from the random number generator 16 by concatenating each of its outputs with the non-random code. Preferably, the encryptor 18 uses an encryption key that is unique to each product manufacturer such that each manufacturer's products have their own unique encryption scheme. Preferably, the encryptor 18 uses an encryption scheme known as a public key cryptosystem. Such cryptosystems use two related keys, one for encryption and the other for decryption. One is kept private and the other is made public. After encryption, both the generated combination code (random number and its non-random portion) and its encrypted counterpart are both saved within the memory 20 for later comparison with subsequently generated random numbers to ensure that each generated random number and its encrypted counterpart are unique. After encryption, the encrypted combination code is generated via communication between the I/O module 22 and the printer 26. The printer 26 prints each encrypted combination code on a single tag so that each tag contains an encrypted combination code as well as its bar code representation. Therefore the code on each tag will consist of only an encrypted counterpart since the constant portion of the combination code is known. Again, as discussed earlier, these codes may be either a binary code 28, an alphanumeric code 30, a case sensitive alphanumeric code 32 as illustrated in Figure 1 or any other type code.

[0046] At step 84, the tags containing the encrypted combination codes are placed on products such that each product contains its own unique encrypted combination code and each product is then placed in the stream of commerce at step 86. Upon reaching the retail distributer or outlet 48 the encrypted combination code is read at step 88 before the various products 36 are accessible to the regular consumers. The scanner 50 scans the encrypted combination code at step 88 and downloads it to the local computer 52 which contains a decryption key which is unique and provided by the manufacturer (the public key). The local computer 52 then decrypts the read encrypted code at step 90 and compares the decrypted code to the already known non-random code portion at step 92.

[0047] At step 94 the local computer 52 checks to see whether the already known non-random code portion and the decrypted code that had been read by the scanner 50 match. If the decrypted code and the non-random code portion do not match, the local computer provides an indication to the checker by either an audible or visual indicator that the product 36 is a counterfeit. The manner in which one recognizes the non-random portion of the combination code may be more easily understood in conjunction with Figure 4. Figure 4 is a chart 99 in which eight different encrypted combination codes have each been decrypted using a public encryption key. Note that each decrypted combination code has the same non-random code portion "YOU" at the end. Consequently, a checker can easily verify the authenticity since they know what the non-random code portion should be although the checker will not know the intricacies of the public key decryption methodology. As stated earlier, the non-random portion of the combination code may be a tradename, the manufacturer's initials, or any type of recognizable message. Alternatively, the local computer 52, after decryption, may display the decrypted code on a display portion of the scanner 50 so that the user scanning the tags can visually view the non-random code portion and thereby verify authenticity.

[0048] If a match is found, the local computer 52 checks to see whether this code has previously been scanned by the scanner 50 at step 96 by analyzing the random portion of the code which is unique for each combination code. If this code has previously been used at that locality, then the local computer 52 provides an indication that the product 36 is a counterfeit at step 96. Alternatively, a master database containing used codes may also be maintained in which various local computers 52 at various retail outlets 48 are connected together to indicate the identification of various valid codes so that the verification of whether a code has been used in step 96 may be even more extensive. Finally, at step 98, if the identified valid code has not been used the local computer 52 provides an indication to the user that the code is valid and therefore the goods are authentic and further provides an indication either within its own memory or within the master database that the code has been used for any subsequent checking.

[0049] In the above-described method of Figure 3, a counterfeiter has few alternatives to try to defeat this method. The counterfeiter must create its own encryption method or encryption keys which will not match the encryption method or keys utilized to generate the en-

WAVELYNX EX. 1003, Pg. 1288
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

crypted combination codes in step 82 and therefore the decryption of the encrypted combination code will not match the already known non-random portion of the combination code in step 94 and a counterfeit will be detected. Further, if the counterfeiter chooses to copy codes after they become accessible to the public, these duplicate codes can be detected at step 96 since use of duplicate codes will be identified. Note also that a theft of the field checker's local computer 52 will not compromise the security provided by the host computer 12 since the local computer 52 contains a decryption key and a database listing of used codes. Recall that in a public key cryptosystem knowing the decryption key gives no knowledge of the encryption key. None of this information, therefore, is advantageous to the counterfeiter because it does not provide information regarding how to encrypt the codes nor does it indicate the existence of valid, presently unused codes.

[0050] The combination codes of Figures 3 and 4 provide an additional level of security by thwarting a counterfeiter who intercepts the field verifier (public key) and replaces them with his own verifier. If a counterfeiter steals the verifier and replaces it with one that includes the legitimate public key (obtained by analyzing the intercepted devices) and an additional bogus public key with control software, the counterfeiter will be able to inject counterfeit goods into the market that will appear valid via an analysis of the decrypted non-random code portion. However, as discussed earlier, the random code portions can be made virtually unguessable and the decrypted random code portions can be compared to a secure master database to see if the code is a valid random code that has not previously been used. Consequently, the combination provides another level of additional security, if desired.

[0051] Another method and system for identifying an undesired diversion of goods from a desired channel or channels of distribution is illustrated in Figure 5. The manner in which the method is performed will be discussed in conjunction with various components of the authentication system 10 of Figure 1. At step 100, a pair of encryption keys (wherein the first, the private key, encrypts a code and the second, the public key, decrypts the encrypted code) are generated by the host computer 12. The encryptor 18 within the processor 16 generates the encryption key pairs, one key pair for each distribution channel through which the manufacturer intends to ship his goods.

[0052] After a unique pair of encryption keys are generated by the computer 12 at step 100, and wherein this unique pair of keys is associated with a particular channel of distribution through which goods are to be tracked, the private key is provided to the manufacturer of the goods at step 102 and used by the manufacturer to generate encrypted combination codes (step 104) as discussed earlier for application to the goods at step 106. The encrypted combination codes may be generated by a printer such as the printer 26 of Figure 1 which is in electrical communication with a computer which dictates the combination code via the private encryption key. As discussed supra, the printer may apply the codes directly to the goods or alternatively may generate the codes on tags or labels for subsequent affixation to the goods. After the goods are properly marked, the goods are placed into commerce at step 108 into the particular channel of distribution via various modes of transportation (see, for example, Figure 1, reference numerals 42, 44 and/or 46).

[0053] To determine whether a diversion of the goods into an undesired channel of distribution has occurred, an inspection of the goods within the expected channel of distribution is undertaken by the manufacturer at step 110. Inspection of the goods involves scanning the encrypted combination codes with a scanner 50 which is in electrical communication with a local computer such as computer 52 of Figure 1 which contains the public encryption key which is associated with a particular distribution channel. At step 112, a determination is made whether or not the goods have been diverted by decrypting the encrypted combination code with the public encryption (decryption) key. If the decrypted code matches the already known non-random portion of the combination code no diversion has occurred, however, if no match is obtained, a diversion of goods from the desired channel of distribution has been discovered. Upon discovery, the manufacturer may then retrace the product shipments to identify the source of the diversion. To this end the manufacturer may use other public keys which are associated with other distribution channels to decrypt the encrypted combination code until he finds a match. In this way he can find the distribution channel into which the goods were first shipped.

[0054] The encrypted combination code may be on the product in a location that is hidden from view such that the reading of the code can only occur by tampering with the product in an irreversible manner such that the code is tamper evident. A simple example is illustrated in Figure 6, wherein a code 150 is affixed to an inside cover 151 of a sealed package 152. A seal 153 on the package 152 must be broken and the cover opened in order to read the code 160. Further, such reading may lower or destroy the value of the product whose code is being read. In this manner, a counterfeiter who attempts to gather valid codes from the goods within the distribution channel has an expensive task since great economic, expense is incurred when attempting to copy a meaningfully large number of valid codes. Further, a manufacturer's need to check codes on products within the distribution channel in order to statistically determine a lack of duplicity is dramatically reduced. A counterfeiter will gather fewer codes as a result of the above-described added expense and it follows that his goods will have a proportionately higher number of duplicates. More duplicates makes any sampling program operated by the manufacturer more likely to find duplicates. Therefore, the manufacturer may choose to reduce his

WAVELYNX EX. 1003, Pg. 1289
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

sampling program to save costs and still maintain high likelihood of discovering duplicates.

[0055] Summarizing a mode of practicing the process is to use public key encryption techniques. In this case the encryption is made with a secret, private key, and the verifying step is done by decrypting the code with the counterpart pubic key. It is well known in public key cryptography that anyone can have the public key and can inspect or verify the code because the public key gives no useful knowledge about the private key. Therefore, whoever has the public key cannot create the combination codes himself. Thus, the authenticity of the codes is assured. Only the private key holder can have created them.

[0056] It is noted that the combination codes and what they say are available to the verifier who performs the inspection. In general, the codes can be read by anyone with the public key and an exemplary utility of the system of the invention derives from the public nature of the inspection process.

[0057] However, the originator of the codes may wish to incorporate information in the combination codes which can provide the originator additional information for the purpose of tracking without generally revealing what this information is. One example of this process is a manufacturer might want to trace product from a distributor to its destination without the distributor or anyone with inspection/verification capability knowing that there is tracking information in the combination codes.

[0058] That information, such as tracking information, information as to (whether tax has been paid, as is described, or other information, can be hidden in the non-random constant portion of the combination code by a variety of useful techniques. The entire constant portion of the combination code can be a hidden message, or can be comprised of a normally readable portion with the remainder being a hidden message.

[0059] Two useful techniques to create the hidden message are secret key encryption and one way hash functions, In both cases the hidden message part of the non-random portion will appear as a meaningless string of characters. Only the originator will know that it has meaning and inspectors will know nothing of its meaning.

[0060] Referring to Figure 7, a flow chart 300 of the steps of this process is illustrated schematically. It will be appreciated that a person having ordinary skill in the art reviewing the block diagrams and flow charts as well as the description presented in this patent application would be able to write appropriate computer program code to carry out the processes and steps disclosed herein. In Figure 7 a secret key encryption implementation of hidden messages in the combination codes the originator simply decides (block 301) what the secret message is for combination codes which are planned for a given destination, encrypts the message with a secret key (block 302), then adds (block 303) this message to the non-random portion of the combination code. (Block 303 is shown in dotted outline signifying that this step may be omitted if the non-random code contains only secret information/code.) This composite non-random, constant portion is subsequently used in the creation of codes specified in the invention, e.g., by combining at block 304 with a random code obtained at block 305. When codes are later inspected and ultimately sent back to the originator, the originator can use the secret key to decrypt the hidden message and use the information to decide if fraudulent activity has occurred.

[0061] in a one way hash function Implementation of hidden messages the process is different as follows. One way hash functions are useful in that they can create a digest of a message which is shorter than the original message. The originator creates a message, creates the digest or hidden message from the original message by using the hash function, then saves the original message by adding it to a table of other messages that were previously used. The hidden message is used then in a combination code. When codes are sent back to the originator after inspection, the originator successively tries each original message from the table by hashing it and comparing the result to the hidden messages in the codes that are sent back. The one way hash function is not specifically illustrated in the drawings here in order to minimize the length of this patent application description; however, from the description that is presented and illustrated, it will be understood by a person who has ordinary skill in the art how to draw such a flow chart/block diagram.

[0062] The originator of the hidden message must cloak the hidden message so that those who have the ability to inspect and verify combination codes cannot begin to infer meaning to the hidden message part of the non-random code. If this part did not change from time to time and remained constant, soon this constant message would be hypothesized to have certain meanings. For example, a distributor who was being tracked by the originator by, say embedding his name in the hidden message, would soon realize that goods sent to him always had the same string of characters in a certain position within the combination code. For goods that were sent to other distributors, he would notice that this string of characters was different. He would then correctly infer that this character string corresponded to a code labeling goods sent to him alone. The originator's secret would no longer be secret at this point. Therefore, the process preferably does not simply encode messages in a relationship with, say, random character strings, and then maintain the relationship table secret. The random character strings are the hidden messages which are used in the combination codes.

[0063] A way to thwart this discovery is to regularly change the implementation of the hidden message but not necessarily change the tracking information in the original message. If, for example, on a daily basis the originator came up with a new secret relationship table in order that the hidden message implementation

WAVELYNX EX. 1003, Pg. 1290
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

changes daily, then the number of secret tables would grow to unmanageable portions in terms of storage and use. instead, the use of encryption or one way hash functions provides a way for the hidden message implementation to change continuously but the hidden information remains constant. And there are no significant storage requirements.

[0064] As was described above, the combination code has both a random and non-random portion. In Figure 7, for example, the non-random portion is comprised of a hidden message implementation and a readable portion which is usually constant, that is, the same from message to message. instead a part of the readable portion can be a changing value. For example, this part can comprise a field of sequentially changing numbers, or it may contain the current date. The originator may now combine this information with the information he wishes to hide, and then create the hidden message using either encryption or hashing as described above. The hidden message implementation will change as often as the readable field changes. Those who inspect (blocks 308, 307) can develop no meaning from observing the hidden message Implementation which is changing often. On the other hand, the originator can easily reconstruct the hidden message because he needs nothing other than either the secret (private) key (block 308) or the list of secret messages as described above, and using or noting the information obtained by the secret key decryption (block 304).

[0065] Reconstructing the hash message is straightforwardly done by using the readable field in combination with the messages from the secret list until a match is found.

[0066] To more clearly understand the usefulness of this embodiment consider the problem of cigarette tax stamps. Through the present date states of the United States and other taxing jurisdictions, such as other countries, territories and/or governmental bodies, have used the tax stamp as evidence that the tax has been paid for each pack of cigarettes bearing the stamp. These stamps have been in wide use for many years, and while they contain security features to thwart their counterfeiting, there still occurs a widespread problem of cigarette tax fraud through the counterfeiting of these stamps.

[0067] Refer to the flow chart/block diagram of Figure 8 for the following. Cigarettes or other goods are shipped to distributors who then have the responsibility to pay the state tax by buying stamps and affixing them to the packages which are then distributed in the state. instead of affixing a stamp to each package, application of this teaching will require that the distributors receive files of encrypted combination codes (block 401) from an origination source (block 402), which can be either the state or a contractor providing this service for the state. The distributor will then print the encrypted codes directly on the packages (block 403) using commercial printing equipment that has the capability to do so. Security procedures will assure that once printed the code files are destroyed (block 404) so they may not be used again.

[0068] State inspectors will be able to inspect (block 405) cigarette packages in the field using the public key (as described above) which is the counterpart to the private key which created the encrypted codes. The combination code in the original message contains a non-random portion which may be the name of the state and the value of the tax paid. Of course, if duplicates of codes are found, the inspectors have cause to immediately seize the cigarettes bearing these duplicates. Similarly, if the decryptions do not result in the message of state and tax value, the same action is warranted. This verification and checking is represented at block 406.

[0069] In addition to the state and tax value, it is useful to include the data the codes were originated for the following reasons. Suppose a counterfeiter spends resources collecting encrypted codes from cigarette packs that are out in distribution. This counterfeiter supposedly understands that he must avoid duplicate detection and therefore compiles over time as many different codes that he can possibly obtain. These codes will likely have many different dates and a good portion of the dates are likely to be old. Therefore, if an Inspector encounters a container of cigarette cartons and finds many different dates including old ones, he has proof that the tax has not been paid.

[0070] Let us now suppose that the state judges that the greater threat of fraud involves the distributor who may compile codes and re-use them. indeed, the state may wish to catch any such distributors and sets up this possibility by instead incorporating the date and distributor name within a hidden message such as described herein. The distributor's inventory, which turns over on nearly a daily basis, can be inspected by an inspector. When the inspected codes are sent to the originator, the hidden messages, can be read and they will reveal whether the dates are old. The distributor's name therein constitutes proof that the distributor re-used codes. Since the distributor could not discover that this dating was being done, he could not take any measures to hide his activity.

[0071] This is but one example where the invention described herein can be useful. It will be appreciated that the invention may be used with many other goods, items, etc., such as physical goods such as valuable products, tax stamps, documents, etc

[0072] The present invention is contemplated in the context of various types of mass produced goods. Although the above examples highlighted the invention in the context of consumer goods such as clothing apparel, etc. the invention is also applicable to other type goods. For example, the present invention may be incorporated with computer software in which the coding is placed on the packaging itself or alternatively may be placed on the storage media itself such as optical media in CD-ROMs or magnetic media such as diskettes, etc. in

WAVELYNX EX. 1003, Pg. 1291
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

this context the scanner is replaced by the magnetic or optical head that reads the information on the disk and performs the encryption, etc. as highlighted above.

[0073] Although the invention has been shown and described with respect to certain embodiments, other alterations and modifications will occur to others skilled in the art upon the reading and understanding of this specification and the annexed drawings.

Claims

1. A method of verifying the authenticity of items, comprising the steps of:

   generating (80, 81) combination codes, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes;
   encrypting (82) the combination codes;
   associating (84) the encrypted combination codes with one or more items; and
   examining the items to verify whether they are authentic;

   wherein the step of examining the items comprises the steps of:

   reading (88) a code from one of the one or more items;
   decrypting (90) the code and
   determining (92, 94) whether the decrypted code contains the non random portion of the combination code.

2. A method of verifying the authenticity of items, wherein combination codes have been generated (80, 81), each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes, the combination codes have been encrypted (82), and the combination codes have been associated with one or more items, the method comprising the step of:

   examining items to verify whether they are authentic;

   wherein the step of examining the items comprises the steps of:

   reading (88) a code from one of the one or more items;
   decrypting (90) the code; and
   determining (92, 94) whether the decrypted code contains the non-random portion of the combination code.

3. The method of claim 1 or claim 2, wherein the non-random portion is not personalised to the item to which the code is applied.

4. The method of any preceding claim, wherein the non-random portion is already known and the step of determining whether the decrypted code contains the non-random portion comprises inspecting the decrypted code and checking (94) whether the already known non-random portion and the decrypted non-random portion match.

5. The method of any preceding claim, wherein if the step of determining determines that the decrypted code contains the non-random portion, the method further comprises determining (96) whether the random portion of the decrypted code is unique, whereby non-uniqueness provides an indication that the product may be counterfeit.

6. The method of claim 5, wherein the determining whether the random portion of the decrypted code is unique comprises comparing the decrypted random code to a local or master database.

7. The method of any preceding claim, comprising:

   determining whether a tax has been paid properly using the decrypted combination code by evaluating whether the decrypted combination code contains a correct non-random portion.

8. The method of claim 7, further comprising destroying (404) the codes after use.

9. The method of claim 7 or 8, further comprising destroying or confiscating the items if a tax has not been paid properly.

10. A method of any one of claims 1 to 6, wherein the method further includes detecting a diversion of items with respect to which combination codes are associated from a desired channel of distribution, wherein a particular channel of distribution has an associated decryption key for decrypting codes and an associated non-random portion, the detecting comprising:

    inspecting items within the particular channel of distribution;
    decrypting the codes on the items with the decryption key; and
    comparing the non-random portions of the combination codes with the associated non-random portion for that channel of distribution;

    wherein a match indicates no diversion of the items from the desired channel of distribution.

WAVELYNX EX. 1003, Pg. 1292
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

11. The method of claim 10, further comprising the step of generating a pair of encryption keys, wherein one key is used to encrypt combination codes for the desired channel of distribution and the other key is used to decrypt the codes within the desired channel of distribution.

12. The method of any preceding claim, wherein the step of reading the code comprises scanning the code.

13. The method of any preceding claim, wherein the non-random portion includes at least a secret portion that is encrypted, and
wherein the secret portion is encrypted with a key and can be decrypted with a corresponding key.

14. The method of any preceding claim, wherein the non-random portion of the combination code includes a secret encrypted portion containing tracking information,
wherein examining the items includes:

decrypting the combination code; and
decrypting the secret portion of the decrypted combination code to determine the tracking information.

15. A method of preparing combination codes for verifying the authenticity of items, comprising the steps of:

generating (80, 81) combination codes, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes; and
encrypting (82) the combination codes.

16. The method of claim 15, further comprising:

associating (84) the encrypted combination codes with one or more items.

17. The method of claim 1 or claim 16, wherein associating the encrypted codes with one or more items comprises applying the encrypted combination codes to one or more items.

18. The method of any of claims 1 and 15 to 17, further comprising selecting the non-random portion as at least one of a trade name, a manufacturer's initials, a string, an alphanumeric or any type of recognizable message.

19. A method of any of claims 1 and 15 to 18, further comprising storing in a master database (24) the random portion of each combination code.

20. The method of any of claims 1 and 15 to 19, further comprising applying the combination codes to items for use to determine whether a required tax or duty has been paid.

21. A system for preparing combination codes for verifying the authenticity of items, comprising:

means (12) for generating combination codes, each combination code having a unique random portion and a non-random portion, wherein the non-random portion is the same for a plurality of the combination codes; and
means (18) for encrypting the combination codes.

22. The system of claim 21, further comprising means for associating the combination codes with one or more items.

23. The system of claim 21 or claim 22, further comprising:

a code reader (50) for reading a code on an item; and
comparing means for comparing the random portion of a read code to unique random codes in a database (24), wherein the comparing means is operable to indicate whether the read code has been read on another item.

24. The system of any one of claims 21, 22 or 23, for detecting a diversion of items with respect to which combination codes are associated from a desired channel of distribution, wherein a particular channel of distribution has an associated decryption key for decrypting codes and an associated non-random portion, the system further comprising:

means for inspecting items within the particular channel of distribution;
means for decrypting the codes on the items with the decryption key; and
means for comparing the non-random portions of the combination codes with the associated non-random portion for that channel of distribution;
whereby a match indicates no diversion of the items from the desired channel of distribution.

Patentansprüche

1. Verfahren zum Verifizieren der Authentizität von Gegenständen, das die Schritte aufweist:

Erzeugen (80, 81) von Kombinationscodes, wobei jeder Kombinationscode einen eindeuti-

WAVELYNX EX. 1003, Pg. 1293
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

gen Zufallsabschnitt und einen Nicht-Zufallsabschnitt hat, wobei der Nicht-Zufallsabschnitt derselbe für eine Mehrzahl der Kombinationscodes ist,
Chiffrieren (82) der Kombinationscodes,
Verknüpfen (84) der chiffrierten Kombinationscodes mit einem oder mehreren Gegenständen und
Untersuchen der Gegenstände, um zu überprüfen, ob sie authentisch sind,

wobei der Schritt des Untersuchens der Gegenstände die Schritte aufweist:

Lesen (88) eines Codes von einem des einen oder der mehreren Gegenstände,
Dechiffrieren (90) des Codes und
Bestimmen (92, 94), ob der dechiffrierte Code den nicht-zufälligen Abschnitt des Kombinationscodes enthält.

2. Verfahren zum Verifizieren der Authentizität von Gegenständen, wobei die Kombinationscodes erzeugt wurden (80, 81), wobei jeder Kombinationscode einen eindeutigen Zufallsabschnitt und einen Nicht-Zufallsabschnitt hat, wobei der Nicht-Zufallsabschnitt derselbe für eine Mehrzahl der Kombinationscodes ist, wobei die Kombinationscodes chiffriert wurden (82) und die Kombinationscodes einem oder mehreren Gegenständen beigeordnet wurden, wobei das Verfahren die Schritte aufweist:

Untersuchen der Gegenstände, um zu verifizieren, ob sie authentisch sind,

wobei der Schritt des Untersuchens der Gegenstände die Schritte aufweist:

Lesen (88) eines Codes von einem des einen oder der mehreren Gegenstände,
Dechiffrieren (90) des Codes und
Bestimmen (92, 94), ob der dechiffrierte Code den nicht-zufälligen Abschnitt des Kombinationscodes enthält.

3. Verfahren nach Anspruch 1 oder Anspruch 2, wobei der nicht-zufällige Abschnitt hinsichtlich des Gegenstandes, an den der Code angewendet wird, nicht individuell gestaltet ist.

4. Verfahren nach einem der vorherigen Ansprüche, wobei der nicht-zufällige Abschnitt bereits bekannt ist und der Schritt des Bestimmens, ob der dechiffrierte Code den nicht-zufälligen Abschnitt enthält, das Inspizieren des dechiffrierten Codes und das Überprüfen (94), ob der bereits bekannte, nicht-zufällige Abschnitt und der dechiffrierte, nicht-zufällige Abschnitt übereinstimmen, aufweist.

5. Verfahren nach einem der vorherigen Ansprüche, bei dem, wenn der Schritt des Bestimmens bestimmt, daß der dechiffrierte Code den nicht-zufälligen Abschnitt enthält, das Verfahren weiterhin aufweist das Bestimmen (96), ob der zufällige Abschnitt des dechiffrierten Codes einmalig ist, wobei die Nicht-Einmaligkeit einen Hinweis bereitstellt, daß das Produkt gefälscht sein kann.

6. Verfahren nach Anspruch 5, wobei das Bestimmen, ob der zufällige Abschnitt des dechiffrierten Codes einmalig ist, das Vergleichen des dechiffrierten zufälligen Codes mit einer lokalen Datenbank oder einer Hauptdatenbank aufweist.

7. Verfahren nach einem der vorherigen Ansprüche, das aufweist:

Bestimmen, ob eine Steuer richtig bezahlt wurde, unter Verwendung des dechiffrierten Kombinationscodes durch Bewerten, ob der dechiffrierte Kombinationscode einen korrekten nicht-zufälligen Abschnitt enthält.

8. Verfahren nach Anspruch 7, das weiterhin das Vernichten (404) der Codes nach der Verwendung aufweist.

9. Verfahren nach Anspruch 7 oder 8, das weiterhin das Vernichten oder Konfiszieren der Gegenstände aufweist, wenn eine Steuer nicht richtig bezahlt wurde.

10. Verfahren nach einem der Ansprüche 1 bis 6, wobei das Verfahren weiterhin beinhaltet das Erfassen einer Umleitung von Gegenständen unter Bezug darauf, welche Kombinationscodes von einem gewünschten Verteilungskanal beigeordnet werden, wobei ein bestimmter Verteilungskanal einen beigeordneten Dechiffrierungsschlüssel für das Dechiffrieren der Codes und einen beigeordneten, nicht-zufälligen Abschnitt hat, wobei das Erfassen aufweist:

Inspizieren der Gegenstände innerhalb des bestimmten Verteilungskanals,
Dechiffrieren der Codes auf den Gegenständen mit dem Dechiffrierungsschlüssel und
Vergleichen der nicht-zufälligen Abschnitte der Kombinationscodes mit dem beigeordneten, nicht-zufälligen Abschnitt für diesen Verteilungskanal,

wobei eine Übereinstimmung anzeigt, daß keine Umleitung der Gegenstände von dem gewünschten Verteilungskanal vorliegt.

11. Verfahren nach Anspruch 10, das weiterhin den

WAVELYNX EX. 1003, Pg. 1294
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Schritt aufweist des Erzeugens eines Paares von Chiffrierschlüsseln, wobei ein Schlüssel verwendet wird, um die Kombinationscodes für den gewünschten Verteilungskanal zu chiffrieren, und der andere Schlüssel verwendet wird, um die Codes innerhalb des gewünschten Verteilungskanals zu dechiffrieren.

12. Verfahren nach einem der vorherigen Ansprüche, wobei der Schritt des Lesens des Codes das Scannen des Codes aufweist.

13. Verfahren nach einem der vorherigen Ansprüche, wobei der nicht-zufällige Abschnitt zumindest einen geheimen Abschnitt beinhaltet, der chiffriert ist, und

wobei der geheime Abschnitt mit einem Schlüssel chiffriert worden ist und mit einem entsprechenden Schlüssel dechiffriert werden kann.

14. Verfahren nach einem der vorherigen Ansprüche, wobei der nicht-zufällige Abschnitt des Kombinationscodes einen geheimen chiffrierten Abschnitt beinhaltet, der eine Verfolgungsinformation enthält,

wobei das Untersuchen der Gegenstände beinhaltet:

Dechiffrieren des Kombinationscodes und
Dechiffrieren des geheimen Abschnitts des dechiffrierten Kombinationscodes, um die Verfolgungsinformation zu bestimmen.

15. Verfahren zum Anfertigung von Kombinationscodes für die Verifizierung der Authentizität von Gegenständen, das die Schritte aufweist:

Erzeugen (80, 81) von Kombinationscodes, wobei jeder Kombinationscode einen einmaligen zufälligen Abschnitt und einen nicht-zufälligen Abschnitt hat, wobei der nicht-zufällige Abschnitt derselbe für eine Mehrzahl der Kombinationscodes ist, und
Chiffrieren (82) der Kombinationscodes.

16. Verfahren nach Anspruch 15, das weiterhin aufweist:

Beiordnen (84) der chiffrierten Kombinationscodes zu einem oder mehreren Gegenständen.

17. Verfahren nach Anspruch 1 oder 16, wobei das Beiordnen der chiffrierten Codes zu einem oder mehreren Gegenständen das Anwenden der chiffrierten Kombinationscodes an einem oder mehreren Gegenständen aufweist.

18. Verfahren nach einem der Ansprüche 1 und 15 bis 17, das weiterhin aufweist das Auswählen des nicht-zufälligen Abschnitts als ein Warenzeichen bzw. eine Marke, als Initialen des Herstellers, als String, als alphanumerische Nachricht oder als irgendein Typ von wiedererkennbarer Nachricht oder als eine Kombination hiervon.

19. Verfahren nach einem der Ansprüche 1 und 15 bis 18, das weiterhin aufweist das Ablegen des Zufallsabschnitts von jedem Kombinationscode in einer Hauptdatenbank (24).

20. Verfahren nach einem der Ansprüche 1 und 15 bis 19, das weiterhin aufweist das Anwenden der Kombinationscodes an Gegenständen für die Verwendung, um zu bestimmen, ob eine erforderliche Steuer oder ein Zoll bezahlt wurde.

21. System für die Herstellung von Kombinationscodes für die Überprüfung der Authentizität von Gegenständen, das aufweist:

eine Einrichtung (12) für das Erzeugen von Kombinationscodes, wobei jeder Kombinationscode einen einmaligen zufälligen Abschnitt und einen nicht-zufälligen Abschnitt hat, wobei der nicht-zufällige Abschnitt für eine Mehrzahl von Kombinationscodes gleich ist, und
eine Einrichtung (18) für das Chiffrieren der Kombinationscodes.

22. System nach Anspruch 21, das weiterhin eine Einrichtung für das Beiordnen der Kombinationscodes zu einem oder mehreren Gegenständen aufweist.

23. System nach Anspruch 21 oder Anspruch 22, das weiterhin aufweist:

einen Codeleser (50) für das Lesen eines Codes auf einem Gegenstand, und
eine Vergleichseinrichtung für das Vergleichen des zufälligen Abschnitts eines gelesenen Codes mit einmaligen Zufallscodes in einer Datenbank (24), wobei die Vergleichseinrichtung derart betreibbar ist, daß sie anzeigt, ob der gelesene Code auf einem anderen Gegenstand gelesen wurde.

24. System nach einem der Ansprüche 21, 22 oder 23 für das Erfassen einer Umleitung von Gegenständen unter Bezug darauf, welche Kombinationscodes von einem gewünschten Verteilungskanal zugewiesen werden, wobei ein bestimmter Verteilungskanal einen beigeordneten Dechiffrierungsschlüssel hat für das Dechiffrieren von Codes und einen beigeordneten, nicht-zufälligen Abschnitt hat, wobei das System weiterhin aufweist:

eine Einrichtung für das Inspizieren der Gegenstände innerhalb des bestimmten Verteilungs-

WAVELYNX EX. 1003, Pg. 1295
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

kanals,
eine Einrichtung für das Dechiffrieren der Codes auf den Gegenständen mit dem Dechiffrierungsschlüssel und
eine Einrichtung für das Vergleichen der nichtzufälligen Abschnitte der Kombinationscodes mit dem beigeordneten, nicht-zufälligen Abschnitt für diesen Verteilungskanal,

wobei eine Übereinstimmung anzeigt, daß keine Umleitung der Gegenstände von dem gewünschten Verteilkanal auftritt.

Revendications

1. Procédé de vérification de l'authenticité d'articles, comprenant les étapes consistant à :

générer (80, 81) des codes de combinaison, chaque code de combinaison ayant une partie aléatoire unique et une partie non aléatoire, dans lequel la partie non aléatoire est la même pour une pluralité des codes de combinaison ;
crypter (82) les codes de combinaison ;
associer (84) les codes de combinaison cryptés à un ou plusieurs articles ; et
examiner les articles pour vérifier s'ils sont authentiques ;

dans lequel l'étape d'examen des articles comprend les étapes consistant à :

lire (88) un code provenant de l'un des un ou plusieurs articles ;
décrypter (90) le code ; et
déterminer (92, 94) si le code décrypté contient la partie non aléatoire du code de combinaison.

2. Procédé de vérification de l'authenticité d'articles, dans lequel des codes de combinaison ont été générés (80, 81), chaque code de combinaison ayant une partie aléatoire unique et une partie non aléatoire, dans lequel la partie non aléatoire est la même pour une pluralité des codes de combinaison, les codes de combinaison ont été cryptés (82), et les codes de combinaison ont été associés à un ou plusieurs articles, le procédé comprenant les étapes consistant à :

examiner des articles pour vérifier s'ils sont authentiques ;

dans lequel l'étape d'examen des articles comprend les étapes consistant à :

lire (88) un code provenant de l'un des un ou plusieurs articles ;
décrypter (90) le code ; et
déterminer (92, 94) si le code décrypté contient la partie non aléatoire du code de combinaison.

3. Procédé selon la revendication 1 ou 2, dans lequel la partie non aléatoire n'est pas personnalisée pour l'article auquel le code est appliqué.

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel la partie non aléatoire est déjà connue et l'étape consistant à déterminer si le code décrypté contient la partie non aléatoire consiste à inspecter le code décrypté et à vérifier (94) si la partie non aléatoire déjà connue et la partie non aléatoire décryptée concordent.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel, si l'étape de détermination détermine que le code décrypté contient la partie non aléatoire, le procédé consiste en outre à déterminer (96) si la partie aléatoire du code décrypté est unique, d'où il résulte que la non-unicité fournit une indication du fait que le produit peut être contrefait.

6. Procédé selon la revendication 5, dans lequel la détermination du fait de savoir si la partie aléatoire du code décrypté est unique consiste à comparer le code aléatoire décrypté à une base de données locale ou maîtresse.

7. Procédé selon l'une quelconque des revendications précédentes, consistant à :

déterminer si une taxe a été dûment payée par utilisation du code de combinaison décrypté en évaluant si le code de combinaison décrypté contient une partie non aléatoire correcte.

8. Procédé selon la revendication 7, consistant en outre à détruire (404) les codes après utilisation.

9. Procédé selon la revendication 7 ou 8, consistant en outre à détruire ou à confisquer les articles si une taxe n'a pas été dûment payée.

10. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel le procédé consiste en outre à détecter un détournement d'articles auquel des codes de combinaison sont associés, d'un canal de distribution souhaité, dans lequel un canal de distribution particulier a une clé de décryptage associée pour décrypter des codes et une partie non aléatoire associée, la détection consistant à :

inspecter des articles dans le canal de distribution particulier ;
décrypter les codes présents sur les articles

WAVELYNX EX. 1003, Pg. 1296
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

avec la clé de décryptage ; et
comparer les parties non aléatoires des codes de combinaison à la partie non aléatoire associée pour ce canal de distribution ;

dans lequel une concordance indique une absence de détournement des articles du canal de distribution souhaité.

11. Procédé selon la revendication 10, comprenant en outre l'étape consistant à générer une paire de clés de cryptage, dans lequel une clé est utilisée pour crypter des codes de combinaison pour le canal de distribution souhaité et l'autre clé est utilisée pour décrypter les codes dans le canal de distribution souhaité.

12. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de lecture du code, comprend le balayage du code.

13. Procédé selon l'une quelconque des revendications précédentes, dans lequel la partie non aléatoire contient au moins une partie secrète qui est cryptée, et
dans lequel la partie secrète est cryptée avec une clé et peut être décryptée avec une clé correspondante.

14. Procédé selon l'une quelconque des revendications précédentes, dans lequel la partie non aléatoire du code de combinaison comporte une partie cryptée secrète contenant des informations de suivi,
dans lequel l'examen des articles consiste à :

décrypter le code de combinaison ; et
décrypter la partie secrète du code de combinaison décrypté pour déterminer les informations de suivi.

15. Procédé de préparation de codes de combinaison pour vérifier l'authenticité d'articles, comprenant les étapes consistant à :

générer (80, 81) des codes de combinaison, chaque code de combinaison ayant une partie aléatoire unique et une partie non aléatoire, dans lequel la partie non aléatoire est la même pour une pluralité de codes de combinaison ; et
crypter (82) les codes de combinaison.

16. Procédé selon la revendication 15, consistant en outre à :

associer (84) les codes de combinaison cryptés à un ou plusieurs articles.

17. Procédé selon la revendication 1 ou 16, dans lequel l'association des codes cryptés à un ou plusieurs articles consiste à appliquer les codes de combinaison cryptés à un ou plusieurs articles.

18. Procédé selon l'une quelconque des revendications 1 et 15 à 17, consistant en outre à sélectionner la partie non aléatoire sous la forme d'au moins l'un d'une marque commerciale, d'initiales d'un fabricant, d'une chaîne, d'un caractère alphanumérique ou d'un type quelconque de message reconnaissable.

19. Procédé selon l'une quelconque des revendications 1 et 15 à 18, consistant en outre à stocker dans une base de données maîtresse (24) la partie aléatoire de chaque code de combinaison.

20. Procédé selon l'une quelconque des revendications 1 et 15 à 19, consistant en outre à appliquer les codes de combinaison à des articles pour une utilisation destinée à déterminer si une taxe ou une redevance exigée a été payée.

21. Système de préparation de codes de combinaison pour vérifier l'authenticité d'articles, comprenant :

un moyen (12) pour générer des codes de combinaison, chaque code de combinaison ayant une partie aléatoire unique et une partie non aléatoire, dans lequel la partie non aléatoire est la même pour une pluralité des codes de combinaison ; et
un moyen (18) pour crypter les codes de combinaison.

22. Système selon la revendication 21, comprenant en outre un moyen pour associer les codes de combinaison à un ou plusieurs articles.

23. Système selon la revendication 21 ou 22, comprenant en outre :

un lecteur de code (50) pour lire un code sur un article ; et
un moyen de comparaison pour comparer la partie aléatoire d'un code lu à des codes aléatoires uniques dans une base de données (24), dans lequel le moyen de comparaison a pour fonction d'indiquer si le code lu a été lu sur un autre article.

24. Système selon l'une quelconque des revendications 21, 22 ou 23, pour détecter un détournement d'articles auxquels des codes de combinaison sont associés, d'un canal de distribution souhaité, dans lequel un canal de distribution particulier a une clé de décryptage associée pour décrypter des codes et une partie non aléatoire associée, le système

WAVELYNX EX. 1003, Pg. 1297
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

comprenant en outre :

un moyen pour inspecter des articles dans le canal de distribution particulier ;
un moyen pour décrypter les codes présents sur les articles avec la clé de décryptage ; et
un moyen pour comparer les parties non aléatoires des codes de combinaison à la partie non aléatoire associée pour ce canal de distribution ;
d'où il résulte qu'une concordance indique une absence de détournement des articles du canal de distribution souhaité.

WAVELYNX EX. 1003, Pg. 1298
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

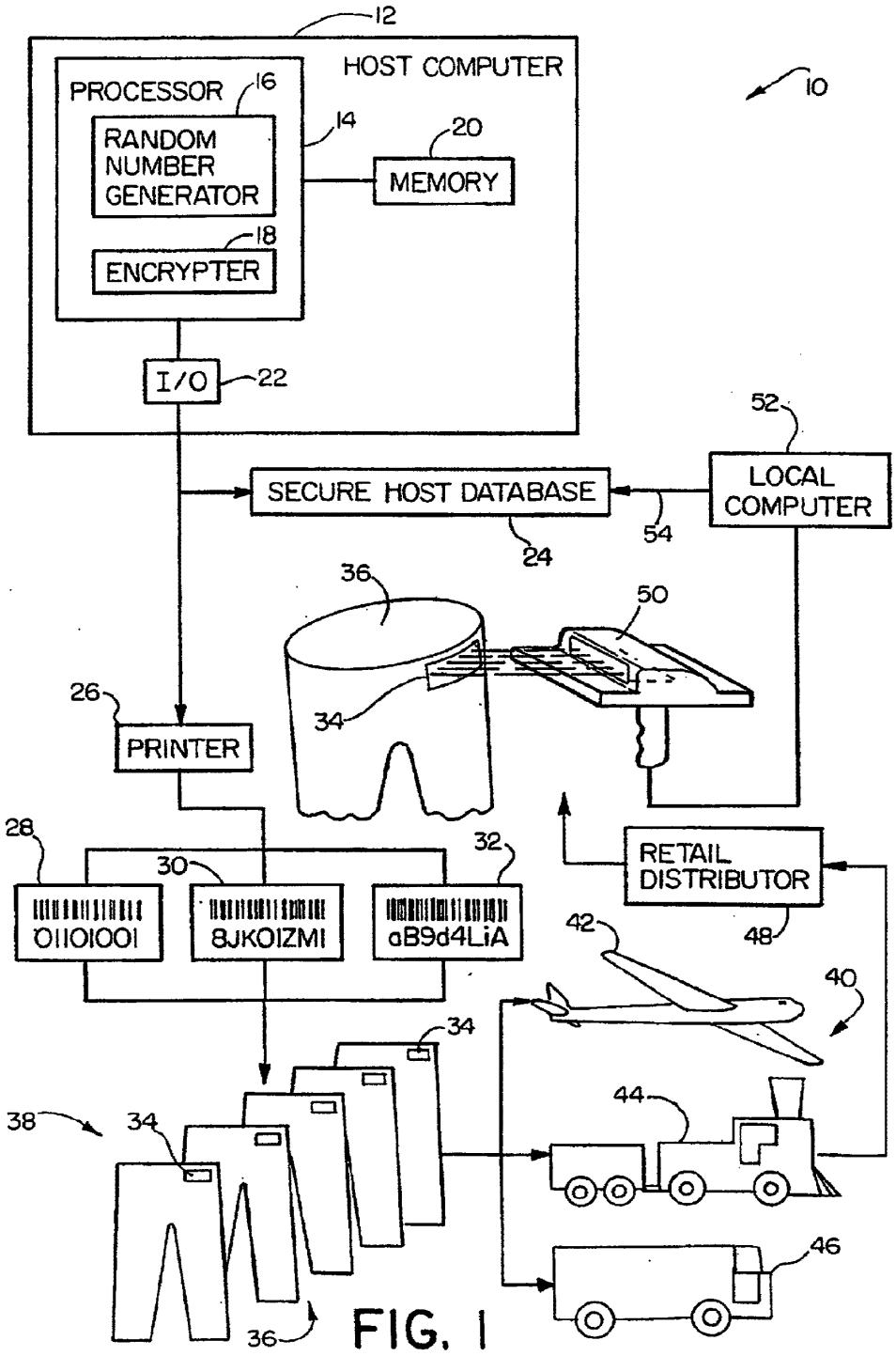


FIG. 1

WAVELYNX EX. 1003, Pg. 1299
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

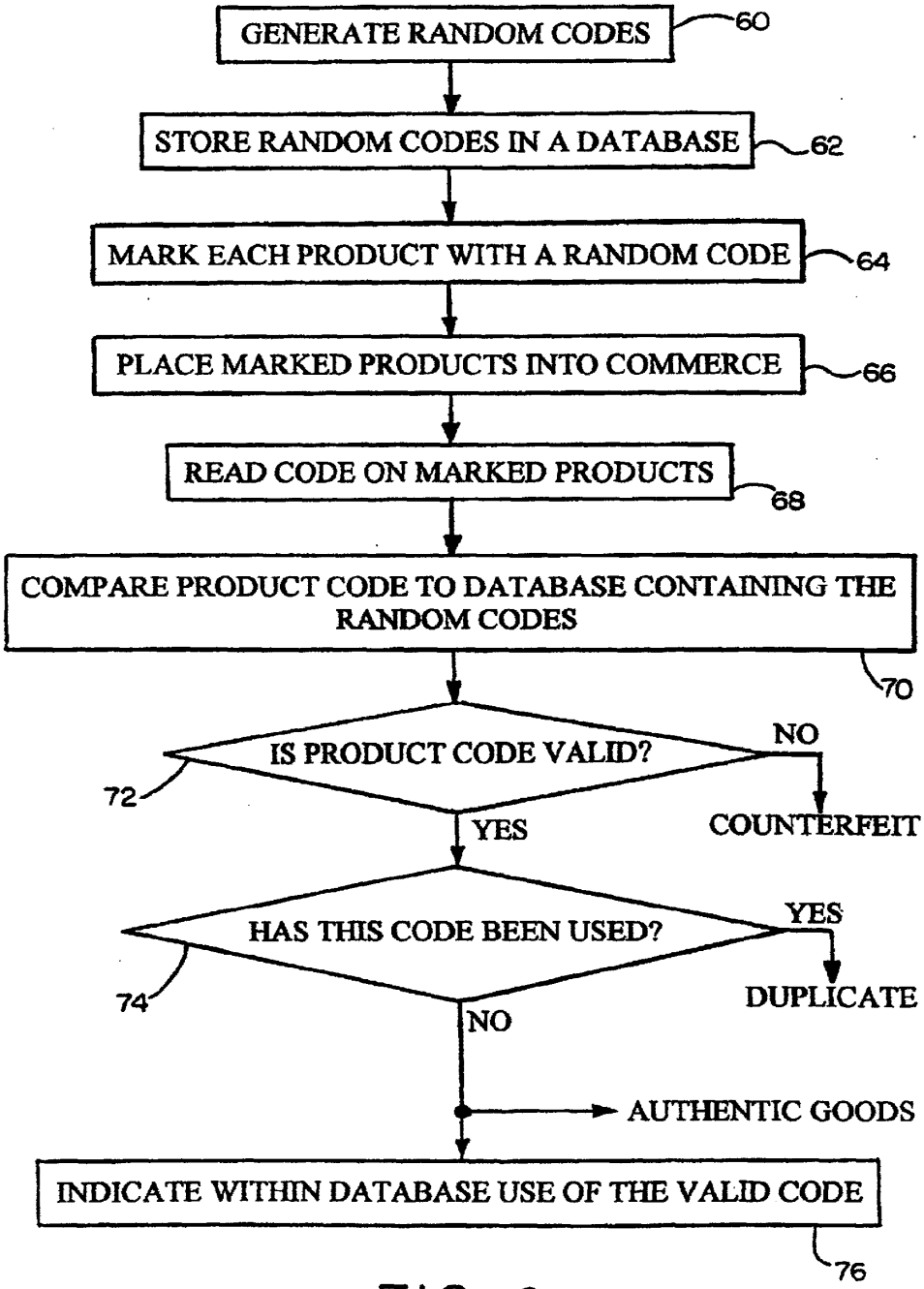


FIG. 2

WAVELYNX EX. 1003, Pg. 1300
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

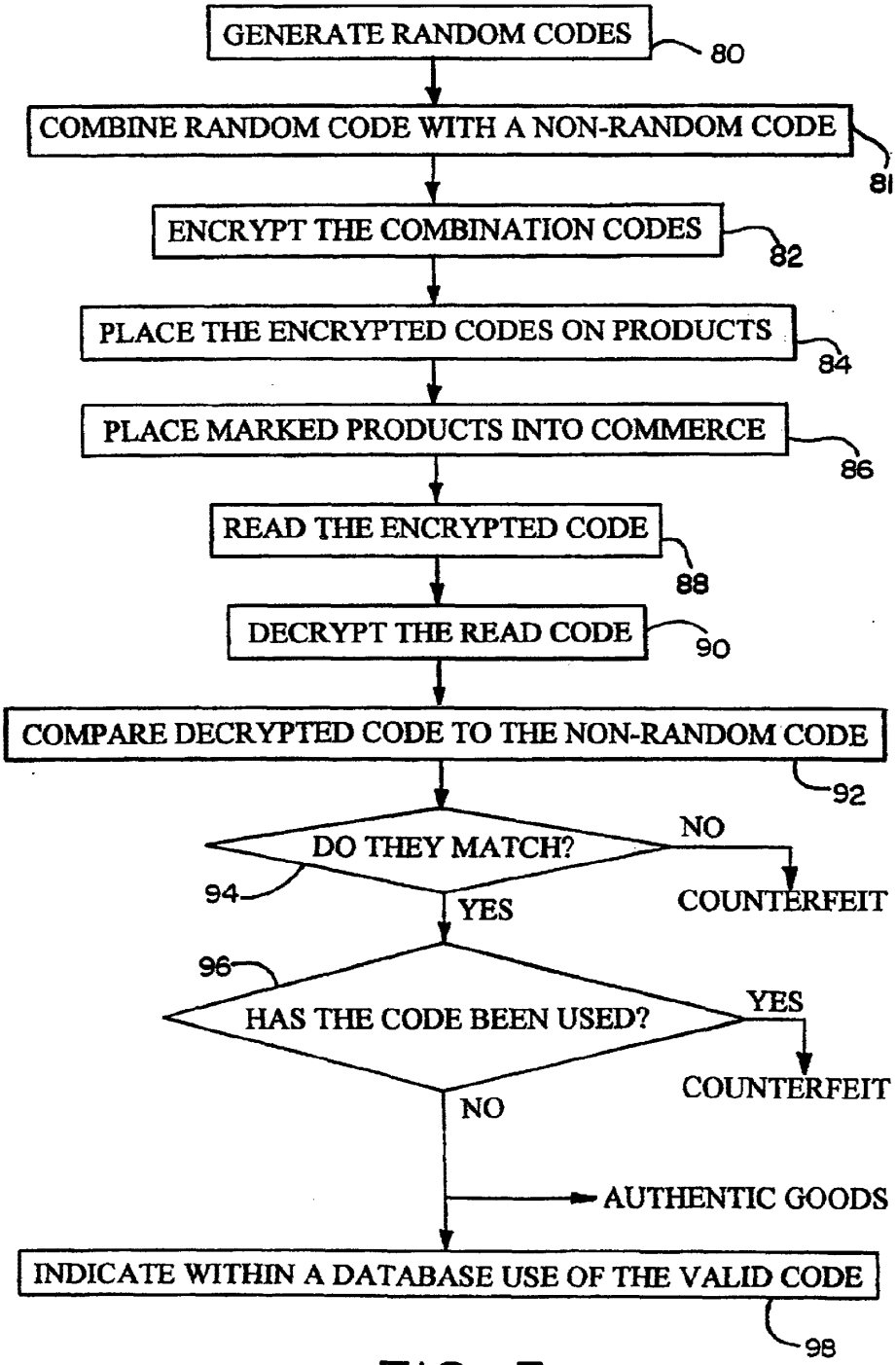


FIG. 3

WAVELYNX EX. 1003, Pg. 1301
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ENCRYPTED COMBINATION CODES	DECRYPTED CODE
O6JTWXQW855BD	OYEQUYOU
OGDQDX4WF3EVR	D1U56YOU
OH2FIW2EMK86Q	ONWPYYOU
1OF1TJVJBEMXZ	CI1D3YOU
1L3HDZ9EW36HZ	1HU3RYOU
O2WO8WDHJEJLX	4GP2MYOU
2HOM2YBBZ7VKE	AWDSEYOU
O88XIB8A3CXLX	BWKPTYOU

FIG. 4

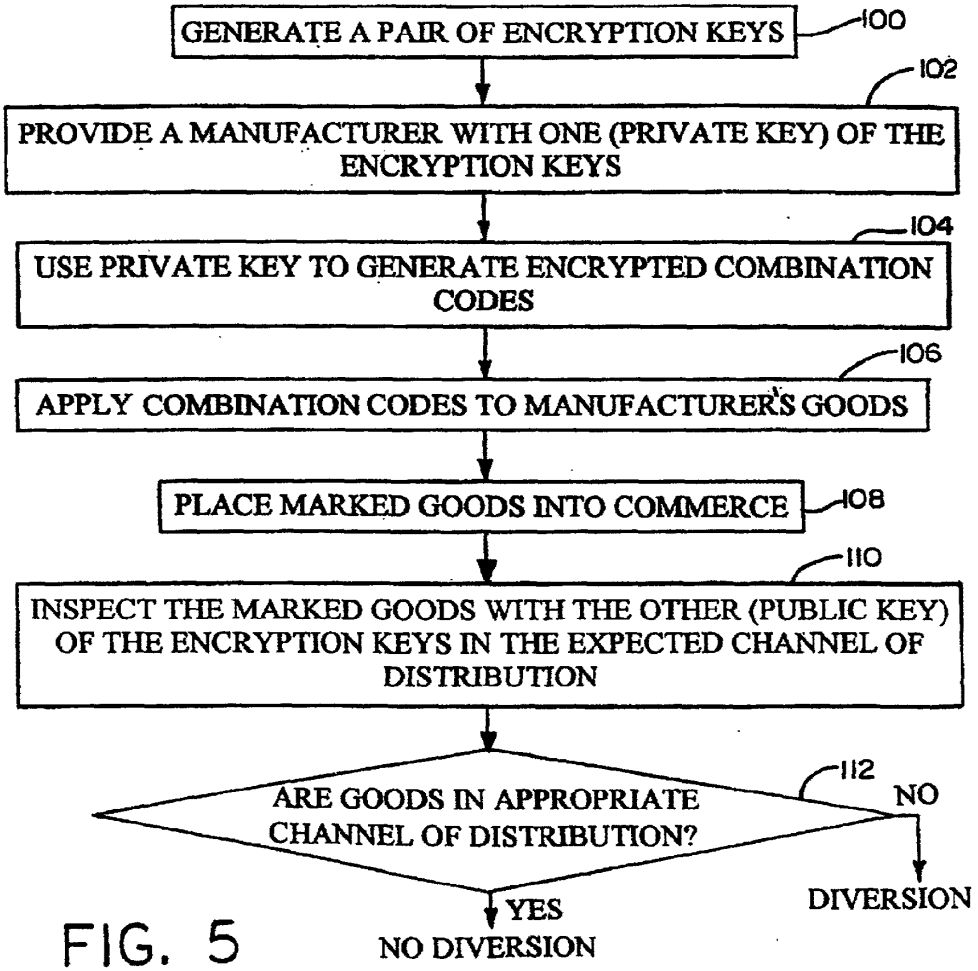


FIG. 5

WAVELYNX EX. 1003, Pg. 1302
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

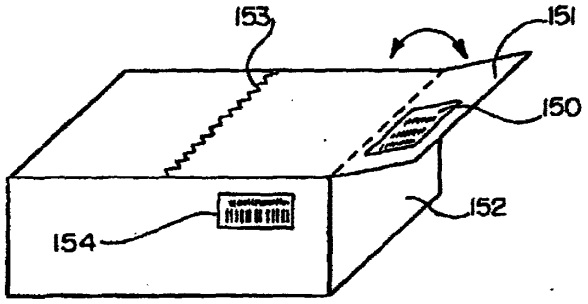


FIG. 6

WAVELYNX EX. 1003, Pg. 1303
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

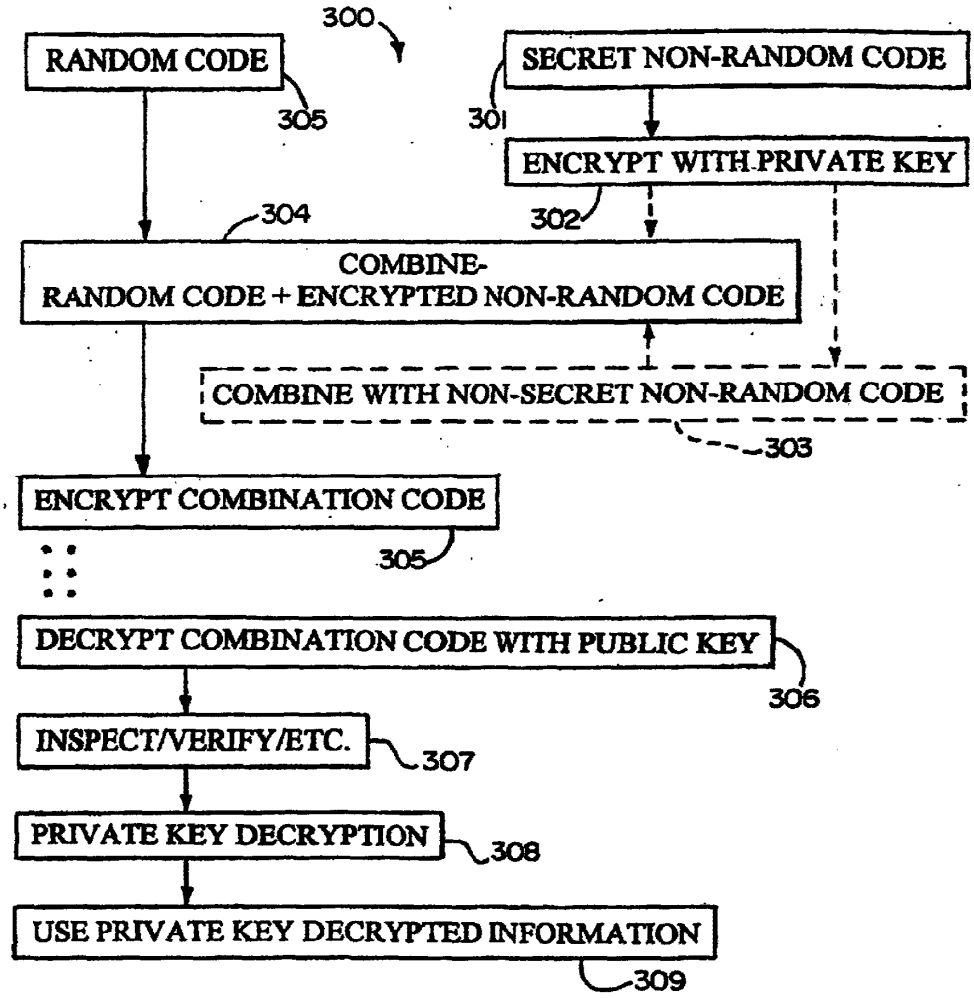


FIG. 7

WAVELYNX EX. 1003, Pg. 1304
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

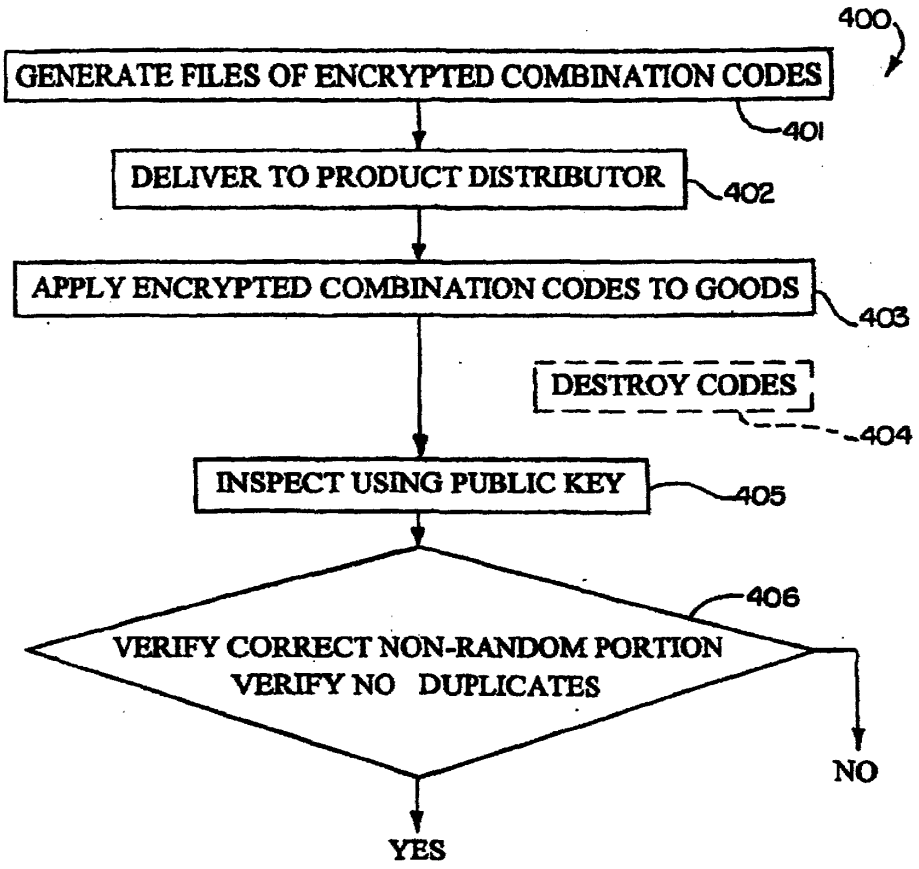


FIG. 8

WAVELYNX EX. 1003, Pg. 1305
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
TODD BLAKELY
SHERIDAN ROSS P.C.
SUITE 1200
1560 BROADWAY
DENVER, CO 80202

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	24 NOV 2009
Applicant's or agent's file reference 2943-178-PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2009/053430	11 August 2009	11 August 2008

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04K 1/02 (2009.01)
USPC - 380/252

Applicant ASSA ABLOY AB

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	17 November 2009	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2009/053430

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2009/053430

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the appicable time limit:

   ☐ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☒ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with

   ☒ not complied with for the following reasons:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-18, drawn to a communication method wherein first and second communication devices communication using a unidirectional protocol and obfuscation of the data is effected with a predetermined code.
Group II, claims 19-29, 37-40, drawn to a reader and method comprising obfuscating data using a rolling code/pseudorandom number generator.
Group III, claims 30-36, drawn to a communication method comprising transitioning a credential reader from a first mode of operation to a second mode of operation upon determining that a message has been received from an upstream device.

The inventions listed as Groups I, II and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: the unidirectional protocol and predetermined code as claimed therein is not present in the invention of Groups II and III. The special technical feature of the Group II invention: a rolling code/pseudorandom number generator as claimed therein is not present in the invention of Groups I or III. The special technical feature of the Group III invention: transitioning a credential reader from a first mode of operation to a second mode of operation upon determining that a message has been received from an upstream device as claimed therein is not present in the invention of Groups I or II.

Groups I, II and III lack unity of invention because even though the inventions of these groups require the technical feature of a credential reader which comprises a code generator, and a receiver which decodes the coded data, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2007/0046424 A1 (DAVIS et al) 01 March 2007, paragraphs [0043-0044].

Since none of the special technical features of the Group I, II or III inventions are found in more than one of the inventions, unity of invention is lacking.

4. Consequently, this opinion has been established in respect of the following parts of the international application:

   ☐ all parts

   ☒ the parts relating to claims Nos. 1-18

WAVELYNX EX. 1003, Pg. 1308
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2009/053430

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims	None	NO
Inventive step (IS)	Claims	9-13, 15	YES
	Claims	1-8, 14, 16-18	NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-4, 8, 16 and 18 lack an inventive step under PCT Article 33(3) as being obvious over DAVIS et al (US 2007/0121943 A1; hereinafter DAVIS) in view of TING (US 2008/0184349 A1).

Regarding claim 1, DAVIS discloses a communication method (Figure 3), comprising: data transmitted in a first message from a first communication device (figure 1; paragraph 0017: transmitting the first message to an upstream device) to a second communication device (Figure 1; paragraph 0017: the upstream device; paragraph 0019: downstream device to transmit a message; upstream device to receive the message), wherein the first and second communication devices communicate using a unidirectional communication protocol (paragraph 0016: Although well suited for use in an access system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol; paragraphs 0017, 0019: secure access system utilizing a unidirectional communication protocol) and wherein the data is effected with a predetermined code (paragraphs 0050, selecting a rolling code from a list of rolling codes; 0055: predetermined rolling code). DAVIS does not explicitly disclose obfuscating data, and the obfuscation of the data being affected with a predetermined code. DAVIS, however, teaches generating message with credential data and a predetermined rolling code data (Figures 3, step 316; paragraph 0054: the reader 112 generates a message containing both the credential data and rolling code data). TING, in disclosing a system and method for identity consolidation (Abstract), teaches the concept of obfuscating data (paragraph 0009: data-obfuscation techniques may also be used…) in a unidirectional communication protocol (paragraph 0056: Wiegand control signals to communicate signals from card readers to one or more control panels that determine whether to grant or deny access in accordance with various access policies; based on these policies, the system generates electrical pulses using the Wiegand protocol [a unidirectional communication protocol] that in turn control the door lock), the obfuscation of the data being affected with a predetermined code (paragraph 0026: obfuscated user-authentication credentials; paragraph 0054: using the hash and the account ID). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of TING to incorporate the above features into the invention of DAVIS in order to maintain the privacy of the credentials and to facilitate the building of cross-reference tables in a secure fashion (TING: paragraph 0009).

Regarding claim 2, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the predetermined code is agreed upon between the first and second communication devices prior to obfuscation of the data in the first message (paragraph 0051: the reader 112 and the control panel 104 may use a previously agreed upon sequence or list of valid rolling codes).

Regarding claim 3, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the predetermined code is one of a plurality of codes within a rolling code sequence (Figure 4: step 336, incrementing to the next valid code in rolling code sequence; paragraphs 0050, 0051; determining what the next valid code is in a rolling code sequence; paragraph 0055: predetermined rolling code selection), wherein the first and second communication devices each have a copy of the rolling code sequence (paragraphs 0050, 51; determining what the next valid code is in a rolling code sequence) and wherein data communicated between the first and second communication devices subsequent to the first message contains (is obfuscated with) a code from the rolling code sequence that is different from the predetermined code (paragraph 0065: database 144; paragraph 0067: unique predetermined rolling code; The upstream device will expect rolling code A from a downstream device at time T in order to determine the authenticity of the downstream device. Then at a time later than time T, the upstream device will expect rolling code B [that is different form the previously predetermined code]…since a valid downstream device will have the rolling code sequence 700, it will know what rolling code to send and when to send it), but is silent on obfuscating data with a code. However, TING teaches obfuscating data with a code as per discussion regarding claim 1. Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of TING to incorporate the above features into the invention of DAVIS in order to maintain the privacy of the credentials and to facilitate the building of cross-reference tables in a secure fashion (TING: paragraph 0009).

Regarding claim 4, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the unidirectional communication protocol comprises the Wiegand protocol (paragraph 0016: Although well suited for use in an access system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol; paragraph 0049).

WAVELYNX EX. 1003, Pg. 1309
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 8, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the predetermined code is employed to identify an authenticity of the first communication device and a timestamp (paragraph 0014: The reader stamps any signal sent therefrom with a time stamp indicating when the message was generated. Then the control panel reads the time stamp to ensure that the message is authentic. An attempt to harvest a signal and resubmit that signal again at a later time will result in the control panel determining the signal is invalid; paragraphs 0043, 0057, 0063; claim 19: at least one of said first and second message is time stamped in order to verify to said upstream device that said at least one of said first and second message was transmitted at their respective required time).

Regarding claim 16, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on wherein control signals are used to accommodate bi-directional communications in one of a half-duplex configuration and a full-duplex configuration. However, DAVIS teaches the need for bidirectional capabilities (paragraph 0010: Without bidirectional capabilities, it is very difficult to implement a modern protocol that provides for reader authentication), Furthermore, bidirectional communications in half-duplex or full-duplex configuration is well known in the art and the specifics would be a matter of design choice. Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to incorporate the above features into the invention of DAVIS in view of TING in order to implement a modern protocol that provides for reader authentication (DAVIS: paragraph 0010).

Regarding claim 18, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on wherein the first message maintains the same size before and after being obfuscated. However, choosing the size of a message before and after its modification is well known in the art and the specifics would be a matter of design choice. Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to incorporate the above features into the invention of DAVIS in view of TING in order to avoid the complexity in hardware and software by using the same size message for before and after modification.

Claims 5 and 6 lack an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of DAVIS et al (US 2006/0123466 A1; hereinafter DAVIS'466).

Regarding claim 5, DAVIS in view of TING discloses the method of claim 4, but is silent on wherein the first message comprises a Wiegand message. However, DAVIS'466 discloses a system and method of extending communications with the Wiegand protocol (Abstract) and teaches using a Wiegand message in a Wiegand protocol (paragraph 0011: the processing means is adapted to generate a data message for transmission onto the data bus via the data output means, wherein the data message has a Wiegand message field in accordance with the existing Wiegand protocol). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of DAVIS'466 to incorporate the above features into the invention of DAVIS in view of TING in order to allow improved functionality in the reader such that the user can provide different types of data inputs to the panel (DAVIS'466: paragraph 0007).

Regarding claim 6, DAVIS in view of TING discloses the method of claim 5, and DAVIS further teaches wherein the Wiegand message is encapsulated in one of a TCP and UDP packet and is transmitted over an IP network from the first communication device to the second communication device (paragraph 0036: protocols used to communicate between the control panel 104 and the readers 112 may include one or more of the TCP/IP protocol, RS 232, RS 485, Current Loop, Power of Ethernet (POE), Bluetooth, ZigBee, GSM, WiFi, and other communication methods and protocols known in the art).

Claims 7 lacks an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of DELLOW et al (US 2007/0121943 A1; hereinafter DELLOW).

Regarding claim 7, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on wherein obfuscation comprises computing an XOR of the predetermined code and the data. However, DELLOW discloses data obfuscation (Abstract) and teaches obfuscation comprising XORing the data and a code (Figure 1; paragraph 0017: the data portion may be obfuscated by performing a bitwise exclusive-or (XOR) function between the bits of the data portion and the mask... in hexadecimal format, an input of data portion 'B4675E56' when XORed with a corresponding mask '2DCA2DD8' would produce the output '99AD738E'). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of DELLOW to incorporate the above features into the invention of DAVIS in view of TING in order to provide for a fast and efficient means for modifying data so that unauthorized access to the data is prevented (DELLOW: paragraph 0005).

Claims 14 lacks an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of LEUNG (US 6,487,176 B1).

Regarding claim 14, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on further comprising: detecting a message collision on a communication path between the first and second communication devices; and initiating a cooperative transmission of messages over the communication path such that the first communication device transmits a message to the second communication device over the communication path at a different time than the second communication device transmits a message to the first communication device over the communication path. However, LEUNG discloses Methods for preventing and detecting message collisions in a half-duplex communication system (Abstract) and teaches transmission of a message at a later time if a message collision is detected (Abstract; col. 7, line 63 – col. 8, line 17: controller 104, upon receipt of the status signal indicating a high likelihood of a message collision, terminates transmission of the message, continuously monitors the status signal, and retransmits the message at a later time after it has been determined that communication channel 134 is clear). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of LEUNG to incorporate the above features into the invention of DAVIS in view of TING in order to detect message collisions regardless of the amount of channel delay and regardless of the source of the interfering signal (LEUNG: col. 4, lines 9-11).

WAVELYNX EX. 1003, Pg. 1310
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claims 17 lacks an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of ONG et al (US 2006/0083228 A1; hereinafter ONG).

Regarding claim 17, DAVIS in view of TING discloses the method of claim 1, but is silent on wherein the obfuscation is accomplished by the use of a stream cipher. However, ONG discloses a one time passcode system (Abstract) and teaches obfuscation (paragraphs 0092, 0100: the one time passcode is generated from CT... using a simple permutation function or an obfuscation function) by the use of a stream cipher (paragraphs 0091, 0098: PT is encrypted to produce ciphertext CT..., encryption can be done with any block cipher algorithm in any block or stream cipher mode). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of ONG to incorporate the above features into the invention of DAVIS in view of TING in order to protect against an attacker who could have captured the shared secrets (ONG: paragraph 0007).

Claims 9-13 and 15 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest:

Regarding claim 9, the feature of determining is performed by one or more of (i) analyzing an out-of-band communication received at the first communication device from the second communication device and (ii) analyzing a special code that identifies the second communication device is an advanced communication device in an advanced communication mode; and based on determining that the message was transmitted by the second communication device, transitioning the first communication device from a first mode of operation to a second mode of operation.

Regarding claims 10-13, each claim depends either directly or indirectly from claim 9.

Regarding claim 15, the feature of wherein out-of-band communications are transmitted from the second communication device to the first communication device at a timing different from message timing used in the unidirectional protocol.

Claims 1-18 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

WAVELYNX EX. 1003, Pg. 1311
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 2943-178-PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2009/053430	International filing date *(day/month/year)* 11 August 2009	(Earliest) Priority Date *(day/month/year)* 11 August 2008
Applicant ASSA ABLOY AB		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☒ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 3

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

WAVELYNX EX. 1003, Pg. 1312
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/053430

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-18

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

WAVELYNX EX. 1003, Pg. 1313
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/053430

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04K 1/02 (2009.01)
USPC - 380/252
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - H04K 1/00, 1/02; H04L 9/00 (2009.01)
USPC - 380/239, 252, 277

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent, Google Patents, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0046424 A1 (DAVIS et al) 01 March 2007 (01.03.2007) entire document	1-8, 14, 16-18
Y	US 2008/0184349 A1 (TING) 31 July 2008 (31.07.2008) entire document	1-8, 14, 16-18
Y	US 2006/0123466 A1 (DAVIS et al) 08 June 2006 (08.06.2006) entire document	5, 6
Y	US 2007/0121943 A1 (DELLOW et al) 31 May 2007 (31.05.2007) entire document	7
Y	US 6,487,176 B1 (LEUNG) 26 November 2002 (26.11.2002) entire document	14
Y	US 2006/0083228 A1 (ONG et al) 20 April 2006 (20.04.2006) entire document	17

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 November 2009	24 NOV 2009
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/053430

Continuation of Box III.

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-18, drawn to a communication method wherein first and second communication devices communication using a unidirectional protocol and obfuscation of the data is effected with a predetermined code.
Group II, claims 19-29, 37-40, drawn to a reader and method comprising obfuscating data using a rolling code/pseudorandom number generator.
Group III, claims 30-36, drawn to a communication method comprising transitioning a credential reader from a first mode of operation to a second mode of operation upon determining that a message has been received from an upstream device.

The inventions listed as Groups I, II and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: the unidirectional protocol and predetermined code as claimed therein is not present in the invention of Groups II and III. The special technical feature of the Group II invention: a rolling code/pseudorandom number generator as claimed therein is not present in the invention of Groups I or III. The special technical feature of the Group III invention: transitioning a credential reader from a first mode of operation to a second mode of operation upon determining that a message has been received from an upstream device as claimed therein is not present in the invention of Groups I or II.

Groups I, II and III lack unity of invention because even though the inventions of these groups require the technical feature of a credential reader which comprises a code generator, and a receiver which decodes the coded data, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2007/0046424 A1 (DAVIS et al) 01 March 2007, paragraphs [0043-0044].

Since none of the special technical features of the Group I, II or III inventions are found in more than one of the inventions, unity of invention is lacking.

WAVELYNX EX. 1003, Pg. 1315
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Electronic Acknowledgement Receipt

EFS ID:	7082150
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Amy Duarte
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	24-FEB-2010
Filing Date:	11-AUG-2009
Time Stamp:	18:38:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_01.pdf	1181545 8ead5cb1b88ef4baa0492894a4956239557bc85e	yes	11

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Filed (SB/08)		4	11	
Warnings:					
Information:					
2	Foreign Reference	AU_2006203768A1.pdf	1612054 4752c8c04197f9ff88b5e696209e1187218acffc	no	51
Warnings:					
Information:					
3	Foreign Reference	CA_2556843A1.pdf	1776869 72c1fdbf30ec47efcd5edfb3dcfc713f8ecc34ea	no	53
Warnings:					
Information:					
4	Foreign Reference	WO_01013218.pdf	900719 5e09d1f5576d05d0e69bf1864cb978d934bcf4a7	no	24
Warnings:					
Information:					
5	Foreign Reference	WO_0118331.pdf	1386802 5b9e493f3d9871b09d2188288346 8d39d126d530	no	31
Warnings:					
Information:					
6	Foreign Reference	WO_03027832.pdf	783673 7c29ee489300440aac89476fc48dc1a6d85e640e	no	28
Warnings:					
Information:					
7	Foreign Reference	WO_03042812.pdf	1659633 226e289ec6288ee617b924350be3e22dc53fa060	no	38
Warnings:					
Information:					
8	Foreign Reference	WO_04010373.pdf	1543899 e8d163f5bfb00ca554618de5a837f9d4b4222f1f	no	38
Warnings:					
Information:					

9	Foreign Reference	WO_05001777.pdf	454738 c2c0781d48cee2547775f52a29c7035979d0626f	no	12
Warnings:					
Information:					
10	Foreign Reference	WO_2004039119.pdf	605458 420ab1af9e365780e67e0c7f04cf384ffb3182637	no	17
Warnings:					
Information:					
11	Foreign Reference	WO_2005018137.pdf	2610998 543ce9b1a68d66351b990ebb114bf43ab337b3e8	no	70
Warnings:					
Information:					
12	Foreign Reference	WO_2005029315.pdf	583717 85f4f7dc5be92fea4bc7375ee08531d1af1f1c49	no	17
Warnings:					
Information:					
13	Foreign Reference	WO_2005038729A1.pdf	1309862 eb42c1d43fb0ef285f6e4a79f2e573bb059ced03	no	41
Warnings:					
Information:					
14	Foreign Reference	WO_2006015625.pdf	2959744 5b81d7fc0a52c7d003829c3ef498c32fc489a3f4	no	49
Warnings:					
Information:					
15	Foreign Reference	WO_2006032941.pdf	1432381 9779d50e09217f27bd018a2c401f1a9a0dca2cd4	no	31
Warnings:					
Information:					
16	Foreign Reference	WO_2006036521.pdf	1265691 43ff580497d49bdbe4b2ce17619d0bfb3a7752a2	no	29
Warnings:					
Information:					
17	Foreign Reference	WO_2006126668.pdf	3102558 da5261e7d262b355b61e32251950662c809ddd30	no	75
Warnings:					
Information:					

18	Foreign Reference	WO_2007103906.pdf	2691907 0660bb52a50c2730f539d45f72f092f266f3e0ba	no	56
Warnings:					
Information:					
19	Foreign Reference	WO_2007117315.pdf	591809 203451eef51e3a02487fe02ecceca32d0c7c17fd	no	14
Warnings:					
Information:					
20	Foreign Reference	WO_2007120215.pdf	5700883 23afb65e96ec828929d3684684050e5583bbb404	no	122
Warnings:					
Information:					
21	Foreign Reference	WO_2008001918A1.pdf	2340302 1d3ff4a5f18eda8eb9650e84a372643f5d2a53b6	no	58
Warnings:					
Information:					
22	Foreign Reference	WO_2008010441.pdf	1773955 acced1e2f30dc1952d2c6ec727f7f75081047446	no	45
Warnings:					
Information:					
23	Foreign Reference	EP1043687B1.pdf	3216759 a23f1fc99e5a93e49c9159befe7714c56973b9d3	no	54
Warnings:					
Information:					
24	Foreign Reference	EP1148644A3.pdf	196144 bd5a7ac1b7fe91618a22bb679ae333ed114c2e43	no	7
Warnings:					
Information:					
25	Foreign Reference	EP1292882B1.pdf	1729726 2deb511bb233f524da63f3b86fd61bf9108708f0	no	29
Warnings:					
Information:					
26	Foreign Reference	EP1398691A3.pdf	103164 e655fa61d9bc939483e2a38d54bdb704df153813	no	4
Warnings:					
Information:					

27	Foreign Reference	EP1420542A1.pdf	757981 0c30af6d4810e259a246fd00c1a56eb170ce c2e7	no	17
Warnings:					
Information:					
28	Foreign Reference	EP1460573A2.pdf	1236750 5d7c126bab6f2c1859551944b0212b7940d e4013	no	17
Warnings:					
Information:					
29	Foreign Reference	EP1643643A1_w_translation. pdf	2815274 dbc476f7c9f1ad26c8eb501cd735f0cb3516 8d94	no	52
Warnings:					
Information:					
30	Foreign Reference	EP1696360A1.pdf	976689 5fed5fa90c0729ffcf588fa1b3b02917bf9272 c7	no	18
Warnings:					
Information:					
31	Foreign Reference	EP1760985A2.pdf	1245045 1cd40d8c2d35c92a3034958f7bfddfc6be7b 8146	no	21
Warnings:					
Information:					
32	Foreign Reference	EP0616429A1_w_Abstract.pdf	542016 b8f90ec433321ccad88b4e70ee9490cca4a9 43e0	no	8
Warnings:					
Information:					
33	Foreign Reference	EP0843438A2.pdf	389836 81b3a2b576fcb64c19aa7fe6a66c51297475 a4e6	no	9
Warnings:					
Information:					
34	Foreign Reference	EP0872976A1.pdf	1647994 e1e3f7457d4fbf52d4290ce0d1e6a9d6b135 9038	no	25
Warnings:					
Information:					
35	Foreign Reference	EP0924894A2_w_Abstract.pdf	725582 962e50c164a2a72a37195b7daf39e2ba262f d45a	no	10
Warnings:					
Information:					

36	Foreign Reference	EP0949563A2.pdf	999952 f8c6d3c070c3854475525104d4c1ebc203b000df	no	16
Warnings:					
Information:					
37	Foreign Reference	EP0996928B1.pdf	1533885 a3b82a4a5bbfc2ed79fee18f9ce667e8321eabef	no	24
Warnings:					
Information:					
38	NPL Documents	EP06119388_EPO_Search_Report.pdf	17434703 a132a1ecb2802ed0aa55feab6dd20a45d3b14c5d	no	4
Warnings:					
Information:					
39	NPL Documents	PCTUS2009053430_Written_Opinion.pdf	771014 a096469368deabb19a47e6b81c6eeeb4fa46131c	no	6
Warnings:					
Information:					
40	NPL Documents	PCTUS2009053430_ISR.pdf	363140 10fa8e86c80676f4dc17584a86b49b06d191b3a4	no	4
Warnings:					
Information:					
41	NPL Documents	AU_2006203768_Examiner_Report_11-20-09.pdf	236370 cfed88f980bb5615748c0114c65193b86719da1b	no	2
Warnings:					
Information:					
42	NPL Documents	Access_Control_Standard_26_Bit_Wiegand_Reader.pdf	451056 5cda3c03b4ead3a9cad5f9bb622eb4796ef0510e	no	15
Warnings:					
Information:					
43	NPL Documents	Condoplex_The_World_Leader.pdf	70145 d2cc28f3fc677c0c2b43ce64dab719999bd3b407	no	1
Warnings:					
Information:					
44	NPL Documents	Contactless_Techn_for_Secure_Physical_Access.pdf	1798533 a12a26e3d6b4dd477066567d3d292254381a2b6d	no	36
Warnings:					
Information:					

45	NPL Documents	Information_Technology_Application_Profile.pdf	815406 319dac6ccae495fe7e77127c781d00792fb815db	no	16
Warnings:					
Information:					
46	NPL Documents	Technology_Basics_Understanding_Weigand.pdf	421891 c031a9e18916c551c8f18474c7c97f36a7948448	no	5
Warnings:					
Information:					
47	NPL Documents	Anashin_Uniformly_Distr_Seq_over_p-adic_Intergers.pdf	2061320 0b7dd79d4ed8a94543e0b913da1f11319e600f8c	no	23
Warnings:					
Information:					
48	NPL Documents	Anashin_Pseudorandom_Number_Generation-2004.pdf	740474 4ab73be2943e0bf84185a7b6ce744f09720c7689	no	55
Warnings:					
Information:					
49	NPL Documents	Anashin_Pseudorandom_Number_Generation_By_p-Adic_Addendum.pdf	205136 036ff6010e99b6947e54d573d8e10f2413c18528	no	9
Warnings:					
Information:					
50	NPL Documents	Anashin_Uniformly_Distr_Seq_In_Computer_Algebra.pdf	389177 7d1f255a70b3aed0c7a2adc16ea97d7268f4b0b2	no	36
Warnings:					
Information:					
51	NPL Documents	Anashin_Uniformly_Distr_Seq_of_p-Adic_Integers_II.pdf	519811 ae7af7e90c075deddce90b498a1f15d8cda5b505	no	53
Warnings:					
Information:					
52	NPL Documents	Anashin_Uniformly_Distr_Seq_of_p-Adic_Integers.pdf	2413523 30b86f84544d9a4d8ff3ea7b2972383341663641	no	25
Warnings:					
Information:					
53	NPL Documents	Brian_How_Remote_Entry_Works.pdf	424739 452dc47b94cdad00ed335711a19848b4c57559d3	no	8
Warnings:					
Information:					

54	NPL Documents	Damgard_On_the_Randomness_of_Legendre_and_Jacobi_Sequences.pdf	408815 6a0113998171527e6c657ceba251112de2534f3c	no	10
Warnings:					
Information:					
55	NPL Documents	Data_Sheet_26_Bit_Wiegand_Specifications.pdf	187628 4764fe010a589e5d53755518366d1412cb7d6df9d	no	1
Warnings:					
Information:					
56	NPL Documents	Data_Sheet_Micro_RWD_EM4001_Magswipe.pdf	860266 f3b7007d2d9c7bc3d07d33b00857f54f4322c869	no	8
Warnings:					
Information:					
57	NPL Documents	Davis_Reader_to_Panel.pdf	11949944 917a01a34c2be924ac1b08037dc406ed68389727	no	33
Warnings:					
Information:					
58	NPL Documents	Glass_DMCA_Used_Garage_Door_Battle.pdf	50851 d408326c0f65d91d33689efc872d94edd254cce4	no	1
Warnings:					
Information:					
59	NPL Documents	Knebelkamp_Latest_Generation_Technology.pdf	514582 4299c49a7e3c96973e36ab9240752982280 8f9f8	no	11
Warnings:					
Information:					
		Total Files Size (in bytes):	99474518		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2431
Scott B. Guthery	)	Confirmation No.: 9292
Serial No.: 12/539,431	)	Examiner: Not Yet Assigned
Filed: August 11, 2009	)	
Atty. File No.: 2943-178	)	INFORMATION DISCLOSURE STATEMENT
Entitled: "Secure Wiegand Communications"	)	
	)	Electronically Submitted

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references cited on attached Form PTO-1449 are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☒ To the best of applicants' belief, the pertinence of the foreign-language references are believed to be summarized in the attached English abstracts and in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☐ Examiner's attention is drawn to the following related applications:

Serial No. _____filed _____(Attorney's Ref. No. _____)

Serial No. _____filed _____(Attorney's Ref. No. _____)

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be

WAVELYNX EX. 1003, Pg. 1325
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

drawn as to the pertinence of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☒	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry into the national stage of an international application as set forth in 37 CFR 1.491 or ☒ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☐	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of one of the following conditions: (1) a final action under 37 C.F.R. 1.113 or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☐ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

WAVELYNX EX. 1003, Pg. 1326
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: February 24, 2016

WAVELYNX EX. 1003, Pg. 1327
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Electronic Acknowledgement Receipt

EFS ID:	7082234
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Amy Duarte
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	24-FEB-2010
Filing Date:	11-AUG-2009
Time Stamp:	18:48:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	NPL Documents	Levin_One_Way_Functions_and_Pseudorandom_Generators.pdf	652272 675e738b1524e79229c5a616eeb809b88e9c0c21	no	7

Warnings:	
Information:	

2	NPL Documents	Press_Release_RFID_based_immobilizer_systems.pdf	103526 a57c7c153bc79fdaa908f5797004048620b06f20	no	2
Warnings:					
Information:					
3	NPL Documents	Weinstein_DMCA_MaBell_Would_Be_Proud.pdf	1368681 9aa53c60d8d0b50da971c4bad8063bb91789b2e6	no	27
Warnings:					
Information:					
4	NPL Documents	Woodcock_p-adic_Chaos_and_Random_Number_Generation.pdf	199954 101f3b369607c178c36c803769531d565419159b	no	10
Warnings:					
Information:					
			Total Files Size (in bytes):	2324433	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	5600324	2/4/1997	Reed et al.	
	2	5844990	12/1/1998	Kokubu et al.	
	3	6078888	6/20/2000	Johnson, Jr.	
	4	6181252	1/30/2001	Nakano	
	5	6249866	6/19/2001	Brundrett et al.	
	6	6411199	6/25/2002	Geiszler et al.	
	7	6724296	4/20/2004	Hikita et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Acknowledgement Receipt	
EFS ID:	8320027
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Nancy Davis
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	30-AUG-2010
Filing Date:	11-AUG-2009
Time Stamp:	16:41:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_02.pdf	338411 d06ad0f2f288b3c9c17628c53319bf415194b7dc	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Filed (SB/08)	4	4
Warnings:			
Information:			
	Total Files Size (in bytes):	338411	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2416
Michael Davis	)	Confirmation No.: 9292
Serial No.: 12/539,431	)	Examiner: Not Yet Assigned
Filed: August 11, 2009	)	
Atty. File No.: 2943-178	)	SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Entitled: "Secure Wiegand Communications"	)	Electronically Submitted

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references cited on attached Form PTO-1449 are being called to the attention of the Examiner.

☐ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☐ To the best of applicants' belief, the pertinence of the foreign-language references are believed to be summarized in the attached English abstracts and in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☐ Examiner's attention is drawn to the following related applications:

Serial No. _____ filed _____ (Attorney Ref. No. _____)

Serial No. _____ filed _____ (Attorney Ref. No. _____)

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be

WAVELYNX EX. 1003, Pg. 1333
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

drawn as to the pertinence of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☒	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry into the national stage of an international application as set forth in 37 CFR 1.491 or ☒ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☐	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of one of the following conditions: (1) a final action under 37 C.F.R. 1.113 or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☐ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

WAVELYNX EX. 1003, Pg. 1334
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: August 30, 2010

WAVELYNX EX. 1003, Pg. 1335
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Gilberto Barron Jr.
Sheet	1	of	1	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	
	1	International Preliminary Report on Patentability for International (PCT) Patent Application No. PCT/US09/53430, mailed Feb. 24, 2011 (Attorney Ref. No. 2943-178-PCT)

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

SAC/TPD

PATENT COOPERATION TREATY

PCT/US2009/053430

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING TRANSMITTAL OF COPY OF INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER I OF THE PATENT COOPERATION TREATY)
(PCT Rule 44bis.1(c))

To:

BLAKELY, Todd P.
Sheridan Ross P.C.
1560 Broadway
Suite 1200
Denver, CO 80202
ETATS-UNIS D'AMERIQUE

MAR - 7 2011
SHERIDAN ROSS P.C.

Date of mailing *(day/month/year)*	
24 February 2011 (24.02.2011)	
Applicant's or agent's file reference	IMPORTANT NOTICE
2943-178-PCT	

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2009/053430	11 August 2009 (11.08.2009)	11 August 2008 (11.08.2008)

Applicant: ASSA ABLOY AB et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Yolaine Cussac

e-mail: pt05.pct@wipo.int

Form PCT/IB/326 (January 2004)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 2943-178-PCT	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2009/053430	International filing date *(day/month/year)* 11 August 2009 (11.08.2009)	Priority date *(day/month/year)* 11 August 2008 (11.08.2008)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant ASSA ABLOY AB		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☒	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 15 February 2011 (15.02.2011)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Yolaine Cussac
Facsimile No. +41 22 338 82 70	e-mail: pt05.pct@wipo.int

Form PCT/IB/373 (January 2004)

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
TODD BLAKELY
SHERIDAN ROSS P.C.
SUITE 1200
1560 BROADWAY
DENVER, CO 80202

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	24 NOV 2009
Applicant's or agent's file reference 2943-178-PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2009/053430	11 August 2009	11 August 2008

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04K 1/02 (2009.01)
USPC - 380/252

Applicant ASSA ABLOY AB

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	17 November 2009	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2009/053430

Box No. I **Basis of this opinion**

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US2009/053430

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the appicable time limit:

   ☐ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☒ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with

   ☒ not complied with for the following reasons:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-18, drawn to a communication method wherein first and second communication devices communication using a unidirectional protocol and obfuscation of the data is effected with a predetermined code.
Group II, claims 19-29, 37-40, drawn to a reader and method comprising obfuscating data using a rolling code/pseudorandom number generator.
Group III, claims 30-36, drawn to a communication method comprising transitioning a credential reader from a first mode of operation to a second mode of operation upon determining that a message has been received from an upstream device.

The inventions listed as Groups I, II and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: the unidirectional protocol and predetermined code as claimed therein is not present in the invention of Groups II and III. The special technical feature of the Group II invention: a rolling code/pseudorandom number generator as claimed therein is not present in the invention of Groups I or III. The special technical feature of the Group III invention: transitioning a credential reader from a first mode of operation to a second mode of operation upon determining that a message has been received from an upstream device as claimed therein is not present in the invention of Groups I or II.

Groups I, II and III lack unity of invention because even though the inventions of these groups require the technical feature of a credential reader which comprises a code generator, and a receiver which decodes the coded data, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2007/0046424 A1 (DAVIS et al) 01 March 2007, paragraphs [0043-0044].

Since none of the special technical features of the Group I, II or III inventions are found in more than one of the inventions, unity of invention is lacking.

4. Consequently, this opinion has been established in respect of the following parts of the international application:

   ☐ all parts

   ☒ the parts relating to claims Nos. 1-18

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2009/053430

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims	None	NO
Inventive step (IS)	Claims	9-13, 15	YES
	Claims	1-8, 14, 16-18	NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-4, 8, 16 and 18 lack an inventive step under PCT Article 33(3) as being obvious over DAVIS et al (US 2007/0121943 A1; hereinafter DAVIS) in view of TING (US 2008/0184349 A1).

Regarding claim 1, DAVIS discloses a communication method (Figure 3), comprising: data transmitted in a first message from a first communication device (figure 1; paragraph 0017: transmitting the first message to an upstream device) to a second communication device (Figure 1; paragraph 0017: the upstream device; paragraph 0019: downstream device to transmit a message; upstream device to receive the message), wherein the first and second communication devices communicate using a unidirectional communication protocol (paragraph 0016: Although well suited for use in an access system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol; paragraphs 0017, 0019: secure access system utilizing a unidirectional communication protocol) and wherein the data is effected with a predetermined code (paragraphs 0050, selecting a rolling code from a list of rolling codes; 0055: predetermined rolling code). DAVIS does not explicitly disclose obfuscating data, and the obfuscation of the data being affected with a predetermined code. DAVIS, however, teaches generating message with credential data and a predetermined rolling code data (Figures 3, step 316; paragraph 0054: the reader 112 generates a message containing both the credential data and rolling code data). TING, in disclosing a system and method for identity consolidation (Abstract), teaches the concept of obfuscating data (paragraph 0009: data-obfuscation techniques may also be used...) in a unidirectional communication protocol (paragraph 0056: Wiegand control signals to communicate signals from card readers to one or more control panels that determine whether to grant or deny access in accordance with various access policies; based on these policies, the system generates electrical pulses using the Wiegand protocol [a unidirectional communication protocol] that in turn control the door lock), the obfuscation of the data being affected with a predetermined code (paragraph 0026: obfuscated user-authentication credentials; paragraph 0054: using the hash and the account ID). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of TING to incorporate the above features into the invention of DAVIS in order to maintain the privacy of the credentials and to facilitate the building of cross-reference tables in a secure fashion (TING: paragraph 0009).

Regarding claim 2, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the predetermined code is agreed upon between the first and second communication devices prior to obfuscation of the data in the first message (paragraph 0051: the reader 112 and the control panel 104 may use a previously agreed upon sequence or list of valid rolling codes).

Regarding claim 3, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the predetermined code is one of a plurality of codes within a rolling code sequence (Figure 4: step 336, incrementing to the next valid code in rolling code sequence; paragraphs 0050, 0051; determining what the next valid code is in a rolling code sequence; paragraph 0055: predetermined rolling code selection), wherein the first and second communication devices each have a copy of the rolling code sequence (paragraphs 0050, 51; determining what the next valid code is in a rolling code sequence) and wherein data communicated between the first and second communication devices subsequent to the first message contains (is obfuscated with) a code from the rolling code sequence that is different from the predetermined code (paragraph 0065: database 144; paragraph 0067: unique predetermined rolling code; The upstream device will expect rolling code A from a downstream device at time T in order to determine the authenticity of the downstream device. Then at a time later than time T, the upstream device will expect rolling code B [that is different form the previously predetermined code]...since a valid downstream device will have the rolling code sequence 700, it will know what rolling code to send and when to send it), but is silent on obfuscating data with a code. However, TING teaches obfuscating data with a code as per discussion regarding claim 1. Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of TING to incorporate the above features into the invention of DAVIS in order to maintain the privacy of the credentials and to facilitate the building of cross-reference tables in a secure fashion (TING: paragraph 0009).

Regarding claim 4, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the unidirectional communication protocol comprises the Wiegand protocol (paragraph 0016: Although well suited for use in an access system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol; paragraph 0049).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2009/053430

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 8, DAVIS in view of TING discloses the method of claim 1, and DAVIS further teaches wherein the predetermined code is employed to identify an authenticity of the first communication device and a timestamp (paragraph 0014: The reader stamps any signal sent therefrom with a time stamp indicating when the message was generated. Then the control panel reads the time stamp to ensure that the message is authentic. An attempt to harvest a signal and resubmit that signal again at a later time will result in the control panel determining the signal is invalid; paragraphs 0043, 0057, 0063; claim 19: at least one of said first and second message is time stamped in order to verify to said upstream device that said at least one of said first and second message was transmitted at their respective required time).

Regarding claim 16, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on wherein control signals are used to accommodate bi-directional communications in one of a half-duplex configuration and a full-duplex configuration. However, DAVIS teaches the need for bidirectional capabilities (paragraph 0010: Without bidirectional capabilities, it is very difficult to implement a modern protocol that provides for reader authentication), Furthermore, bidirectional communications in half-duplex or full-duplex configuration is well known in the art and the specifics would be a matter of design choice. Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to incorporate the above features into the invention of DAVIS in view of TING in order to implement a modern protocol that provides for reader authentication (DAVIS: paragraph 0010).

Regarding claim 18, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on wherein the first message maintains the same size before and after being obfuscated. However, choosing the size of a message before and after its modification is well known in the art and the specifics would be a matter of design choice. Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to incorporate the above features into the invention of DAVIS in view of TING in order to avoid the complexity in hardware and software by using the same size message for before and after modification.

Claims 5 and 6 lack an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of DAVIS et al (US 2006/0123466 A1; hereinafter DAVIS'466).

Regarding claim 5, DAVIS in view of TING discloses the method of claim 4, but is silent on wherein the first message comprises a Wiegand message. However, DAVIS'466 discloses a system and method of extending communications with the Wiegand protocol (Abstract) and teaches using a Wiegand message in a Wiegand protocol (paragraph 0011: the processing means is adapted to generate a data message for transmission onto the data bus via the data output means, wherein the data message has a Wiegand message field in accordance with the existing Wiegand protocol). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of DAVIS'466 to incorporate the above features into the invention of DAVIS in view of TING in order to allow improved functionality in the reader such that the user can provide different types of data inputs to the panel (DAVIS'466: paragraph 0007).

Regarding claim 6, DAVIS in view of TING discloses the method of claim 5, and DAVIS further teaches wherein the Wiegand message is encapsulated in one of a TCP and UDP packet and is transmitted over an IP network from the first communication device to the second communication device (paragraph 0036: protocols used to communicate between the control panel 104 and the readers 112 may include one or more of the TCP/IP protocol, RS 232, RS 485, Current Loop, Power of Ethernet (POE), Bluetooth, ZigBee, GSM, WiFi, and other communication methods and protocols known in the art).

Claims 7 lacks an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of DELLOW et al (US 2007/0121943 A1; hereinafter DELLOW).

Regarding claim 7, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on wherein obfuscation comprises computing an XOR of the predetermined code and the data. However, DELLOW discloses data obfuscation (Abstract) and teaches obfuscation comprising XORing the data and a code (Figure 1; paragraph 0017: the data portion may be obfuscated by performing a bitwise exclusive-or (XOR) function between the bits of the data portion and the mask... in hexadecimal format, an input of data portion 'B4675E56' when XORed with a corresponding mask '2DCA2DD8' would produce the output '99AD738E'). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of DELLOW to incorporate the above features into the invention of DAVIS in view of TING in order to provide for a fast and efficient means for modifying data so that unauthorized access to the data is prevented (DELLOW: paragraph 0005).

Claims 14 lacks an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of LEUNG (US 6,487,176 B1).

Regarding claim 14, DAVIS in view of TING discloses the method of claim 1, but DAVIS is silent on further comprising: detecting a message collision on a communication path between the first and second communication devices; and initiating a cooperative transmission of messages over the communication path such that the first communication device transmits a message to the second communication device over the communication path at a different time than the second communication device transmits a message to the first communication device over the communication path. However, LEUNG discloses Methods for preventing and detecting message collisions in a half-duplex communication system (Abstract) and teaches transmission of a message at a later time if a message collision is detected (Abstract; col. 7, line 63 – col. 8, line 17: controller 104, upon receipt of the status signal indicating a high likelihood of a message collision, terminates transmission of the message, continuously monitors the status signal, and retransmits the message at a later time after it has been determined that communication channel 134 is clear). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of LEUNG to incorporate the above features into the invention of DAVIS in view of TING in order to detect message collisions regardless of the amount of channel delay and regardless of the source of the interfering signal (LEUNG: col. 4, lines 9-11).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US2009/053430

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claims 17 lacks an inventive step under PCT Article 33(3) as being obvious over DAVIS in view of TING and further in view of ONG et al (US 2006/0083228 A1; hereinafter ONG).

Regarding claim 17, DAVIS in view of TING discloses the method of claim 1, but is silent on wherein the obfuscation is accomplished by the use of a stream cipher. However, ONG discloses a one time passcode system (Abstract) and teaches obfuscation (paragraphs 0092, 0100: the one time passcode is generated from CT... using a simple permutation function or an obfuscation function) by the use of a stream cipher (paragraphs 0091, 0098: PT is encrypted to produce ciphertext CT..., encryption can be done with any block cipher algorithm in any block or stream cipher mode). Therefore, it would have been obvious to a person of ordinary skill at the time of the invention to use the teachings of ONG to incorporate the above features into the invention of DAVIS in view of TING in order to protect against an attacker who could have captured the shared secrets (ONG: paragraph 0007).

Claims 9-13 and 15 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest:

Regarding claim 9, the feature of determining is performed by one or more of (i) analyzing an out-of-band communication received at the first communication device from the second communication device and (ii) analyzing a special code that identifies the second communication device is an advanced communication device in an advanced communication mode; and based on determining that the message was transmitted by the second communication device, transitioning the first communication device from a first mode of operation to a second mode of operation.

Regarding claims 10-13, each claim depends either directly or indirectly from claim 9.

Regarding claim 15, the feature of wherein out-of-band communications are transmitted from the second communication device to the first communication device at a timing different from message timing used in the unidirectional protocol.

Claims 1-18 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Acknowledgement Receipt	
EFS ID:	10151220
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Carrie Steward
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	23-MAY-2011
Filing Date:	11-AUG-2009
Time Stamp:	17:53:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_03.pdf	332864 193ec4a6954220902af1fee9fe9adabba4df3809	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Filed (SB/08)		4	4	
Warnings:					
Information:					
2	NPL Documents	IPRP_WO.pdf	1027642 3679e5da4de43a2d1a2c70264aecd25c41393222	no	8
Warnings:					
Information:					
		Total Files Size (in bytes):	1360506		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2432
Michael Davis	)	Confirmation No.: 9292
Serial No.: 12/539,431	)	Examiner: Gilberto Barron Jr.
Filed: August 11, 2009	)	
Atty. File No.: 2943-178	)	SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Entitled: "Secure Wiegand Communications"	)	Electronically Submitted

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references cited on attached Form PTO-1449 are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☐ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☐ To the best of applicants' belief, the pertinence of the foreign-language references are believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☐ Examiner's attention is drawn to the following related applications:

Serial No. _____ filed _____ (Attorney Ref. No. _____)

Serial No. _____ filed _____ (Attorney Ref. No. _____)

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be

WAVELYNX EX. 1003, Pg. 1347
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

drawn as to the pertinence of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☒	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry into the national stage of an international application as set forth in 37 CFR 1.491 or ☒ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☐	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of one of the following conditions: (1) a final action under 37 C.F.R. 1.113 or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☐ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

WAVELYNX EX. 1003, Pg. 1348
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: May 23, 2011

WAVELYNX EX. 1003, Pg. 1349
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Gilberto Barron Jr.
Sheet	1	of	1	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	5696909	12/9/1997	Wallner	
	2	2007/0109101	5/17/2007	Colby	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	
	3	ANASHIN "Non-Archimedean Ergodoci Theory and Pseudorandom Generators," Oct. 07, 2007, 39 pages, available at http://arxiv.org/abs/0710.1418v1
	4	BARKER, Cryptanalysis of Shift-Register Generated Stream Cipher Systems, Cryptographic Series No. 39, Aegean Park Press, 1984, Chapters 1-3, pages 1-38
	5	BLUM, M. et al., "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits," SIAM Journal on Computing, Nov. 1984, Vol. 13, No. 4, pp. 850-864.
	6	KOBLITZ, N., p-Adic Number, p-Adic Analysis and Zeta Functions, Chapter 3, Building up Ω, Springer, New York, (1977), pages 52-74.
	7	KUIPERS, et al., Uniform Distribution of Sequences, John Wiley & Sons (1974), 400 pages (Submitted in 3 Parts)
	8	LUBY, M., Pseudorandomness and Cryptographic Applications, Princeton University Press (1996), pages ix-55

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Acknowledgement Receipt

EFS ID:	10483002
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	08-JUL-2011
Filing Date:	11-AUG-2009
Time Stamp:	18:06:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_04.pdf	171946 48f29c4e66f1d871d6d90e5343e99a83288f8f02	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
2	Non Patent Literature	Anashin_non_archimedean_ergodic_theory_2007.pdf	478864 d40398057edb665c13c1dac828202442873b4d28	no	39
Warnings:					
Information:					
3	Non Patent Literature	Barker_Cryptanalysis_of_Shift-Register_Generated_Stream_Cipher_Systems.pdf	4845898 72a1ec00d3d4581e7920476063692330933d4a81	no	40
Warnings:					
Information:					
4	Non Patent Literature	Blum_How_To_Generate_Cryptographically_Strong_Sequences_of_Pseudo-random_Bits.pdf	2337647 4f45da918719925e64adecf4b3f7c46ee8d9afa3	no	15
Warnings:					
Information:					
5	Non Patent Literature	KOBLITZ_p-adic_Numbers_p-adic_Analysis_and_Zeta-Funtions.pdf	5660136 93aece9ffe029223033d05739723d958ca3e6d84	no	25
Warnings:					
Information:					
6	Non Patent Literature	KUIPERS_pt1_Uniform_Distribution_Sequences.pdf	25085022 a1c8913acce46400f6a8861b8a0a35178d636e15	no	181
Warnings:					
Information:					
7	Non Patent Literature	KUIPERS_pt2_Uniform_Distribution_Sequences.pdf	15109528 437374d526477d05a677d139ef602c2af805212f	no	136
Warnings:					
Information:					
8	Non Patent Literature	KUIPERS_pt3_Uniform_Distribution_Sequences.pdf	11354923 0af4c018fe54b2ef2a4a049e0be3038a96b730f5	no	84
Warnings:					
Information:					

9	Non Patent Literature	LUBY_Pseudorandomness_and_Cryptographic_Applications.pdf	7216438 769df51837fa4f49dad1f51a5b746af0aab8535d	no	62

Warnings:	
Information:	
Total Files Size (in bytes):	72260402

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2432
Michael Davis	)	Confirmation No.: 9292
Serial No.: 12/539,431	)	Examiner: Gilberto Barron Jr.
Filed: August 11, 2009	)	
Atty. File No.: 2943-178	)	SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Entitled: "Secure Wiegand Communications"	)	Electronically Submitted

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references cited on attached Form PTO-1449 are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☐ To the best of applicants' belief, the pertinence of the foreign-language references are believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☐ Examiner's attention is drawn to the following related applications:

Serial No. _____ filed _____ (Attorney Ref. No. _____)

Serial No. _____ filed _____ (Attorney Ref. No. _____)

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be

WAVELYNX EX. 1003, Pg. 1354
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

drawn as to the pertinence of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☒	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry into the national stage of an international application as set forth in 37 CFR 1.491 or ☒ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☐	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of one of the following conditions: (1) a final action under 37 C.F.R. 1.113 or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☐ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

WAVELYNX EX. 1003, Pg. 1355
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: July 8, 2011

WAVELYNX EX. 1003, Pg. 1356
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/539,431	08/11/2009	Michael Davis	2943-178	9292

22442 7590 01/26/2012

SHERIDAN ROSS PC
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

EXAMINER	
ZECHER, CORDELIA P K	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
01/26/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

WAVELYNX EX. 1003, Pg. 1357
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Office Action Summary	Application No.	Applicant(s)	
	12/539,431	DAVIS ET AL.	
	Examiner	Art Unit	
	CORDELIA ZECHER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *1* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-40* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☒ Claim(s) *1-40* are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

WAVELYNX EX. 1003, Pg. 1358
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1 – 29, drawn to obfuscating data using a rolling code.

   II. Claims 30 – 36, drawn to using credential communication between two devices.

   III. Claims 37 – 40, drawn to synchronizing pseudo random number generators.

2. The inventions are distinct, each from the other because of the following reasons:

3. Inventions I, III and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, subcombinations I and III has separate utility such as securing data transmitted between the two devices. See MPEP § 806.05(d).

4. The examiner has required restriction between subcombinations usable together. Where applicant elects a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to

provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

5. Inventions I, II and III are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because resynchronization of the code generators is not required. The subcombination has separate utility such as synchronizing pseudo random number generators for other uses, synchronizing random number generators used for identification purposes.

6. The examiner has required restriction between combination and subcombination inventions. Where applicant elects a subcombination, and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

7. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above

and there would be a serious search and/or examination burden if restriction were not required because at least the following reason(s) apply:

- *the inventions have acquired a separate status in the art due to their recognized divergent subject matter*
- *the inventions require a different field of search (e.g., searching different classes /subclasses or electronic resources, or employing different search strategies or search queries).*

8. **Applicant is advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined** even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

9. The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

10. Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable

over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

11. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CORDELIA ZECHER/
Examiner, Art Unit 2432

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Michael Davis
Art Unit	2432
Examiner Name	Cordelia P.K. Zecher
Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	1	EP 0697491	2/21/1996	NIPPON DENSO CO		
	2	WO 02/082367	10/17/2002	PITTWAY CORP		
	3	WO 2008/043125	4/17/2008	MICROLATCH PTY LTD		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

	Complete if Known
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Michael Davis
Art Unit	2432
Examiner Name	Cordelia P.K. Zecher
Sheet 1 of 1	Attorney Docket Number 2943-178

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	4	European Search Report and Opinion for European Patent Application No. EP09807178, dated Nov. 08, 2011 (Attorney's Ref. No. 2943-178-PEP) 6 pages
	5	Official Action for U.S. Patent Application No. 11/464,912, mailed Jun. 2, 2010 (Attorney Ref. No. 2943-114)
	6	Official Action for U.S. Patent Application No. 11/464,912, mailed Nov. 23, 2010 (Attorney Ref. No. 2943-114)
	7	Notice of Allowance for U.S. Patent Application No. 11/464,912, mailed Jan. 20, 2012 (Attorney's Ref. No. 2943-114) 5 pages

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO:**
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	12018837
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Robert Roe-Pachirat
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	07-FEB-2012
Filing Date:	11-AUG-2009
Time Stamp:	15:31:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	EP0697491.pdf	877197 f9bdaf385267038b790b2535d016c72014a a1e59	no	17

Warnings:	
Information:	

2	Foreign Reference	WO02082367.pdf	749509 85a6ec486f3732d29a66b0ca0f565a131e5826d7	no	24
Warnings:					
Information:					
3	Foreign Reference	WO2008043125.pdf	2519120 8eeb784d7a60e31f966ed823813fcd189b463929	no	62
Warnings:					
Information:					
4	Non Patent Literature	2943-178-PEP_SR_11-08-2011.pdf	246896 80100249ab1f91629667f55a1a74480e4a743de7	no	6
Warnings:					
Information:					
5	Non Patent Literature	2943-114_OA_6_2_10.pdf	465565 379709af7a5b7b5d3762c6190a02c2423a377dc7	no	13
Warnings:					
Information:					
6	Non Patent Literature	2943-114_OA_11-23-2010.pdf	595337 99ceb2d1972ec4a8bcbc03d92b2e46d81146aca1	no	17
Warnings:					
Information:					
7	Non Patent Literature	2943-114_NOA_1-20-2012.pdf	330314 6c0a54801be5c25f7e2a1d06fc09b885f4c1664c	no	5
Warnings:					
Information:					
8		IDS_05.pdf	489586 3461f572a8257021c10a854ff7584dbf2d6cbcc0	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	5
Warnings:			
Information:			
	Total Files Size (in bytes):	6273524	