SECURE WIEGAND COMMUNICATIONS

CROSS REFERENCE TO RELATED APPLICATIONS

This Application claims the benefit of U.S. Provisional Application Number 61/087,941, filed August 11, 2008, the entire disclosure of which is hereby incorporated herein by reference.

FIELD OF THE INVENTION

The present invention is generally directed to authentication of a reader and the security, privacy and efficiency of messaging in a secure access control system. More specifically, the present invention provides extensions to unidirectional security protocols, such as the Wiegand protocol.

BACKGROUND

The Wiegand protocol is the predominant method by which physical access control card readers communicate with upstream devices such as local controllers, access control panels and host computer systems. Because of the popularity and almost universal support of the Wiegand protocol in access control panels, other devices besides access control readers are also available that support the Wiegand protocol. Such devices include biometric-based devices such as fingerprint, hand-geometry, iris, facial recognition, and vein scan. Other devices that utilize the Wiegand protocol include motion sensors, thermostats and smoke detectors.

Both the electrical and logical aspects of the Wiegand communication protocol are codified in the Security Industry Association (SIA) standard AC-01 entitled "Access

Control Standard Protocol for the 26-Bit Wiegand Reader Interface", the entire contents of which are incorporated herein by this reference in their entirety and will henceforth be referred to as the "SIA standard".

Subsequent to the issuing of this standard, both the electrical and logical portions of the standard have been used to transmit bit stream messages, often called formats, longer than 26 bits. 35- and 37-bit formats are found widely and the US Government's PIV standard defines some formats of up to 300 bits. The evolution of upstream devices and middleware to use these longer formats has been slow and is still taking place.

Although other methods are utilized for carrying the informational aspects of the Wiegand protocol over communication bearers such as RS-485, F/2F, and various Internet protocols such as TCP/IP and UDP, none has achieved the widespread usage that Wiegand has in the security and access control market segments This is primarily because each manufacturer utilizes their own proprietary protocols even when using standardized communication bearers such as TCP/IP.

The widespread adoption of the Wiegand protocol is due to several advantages with the primary advantages of the Wiegand protocol being that its implementation in devices is very economical and that it allows very long cable runs which, depending on the gage of the wire used, can be as long as 500 feet.

The electrical aspect of the Wiegand protocol uses five wires. Two of these wires are used to provide power to the reader. The remaining three wires are used for data communication and signaling and use the open collector electrical standard, which means that the circuit acts as either an infinite resistance or a short circuit to ground. Typically the upstream device employs a pull-up resistor, which keeps the signal at a high voltage

WAVELYNX EX. 1003, Pg. 2
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(+5) when it is in the open circuit state. When the signal is asserted, the output is forced to 0 volts. Note that the open state (+5 volts) represents a data value of zero and the asserted state (0 volts) represents the data value of one. This is generally referred to as an "active low" configuration where the active state is the low voltage.

Two of the three data communication and signaling wires are used by the reader to transmit data to an upstream device *e.g.*, control panel, intermediate device, routing device, lock control mechanism, computing platform, host, or the like. These two wires are referred to as DATA0 and DATA1. As the names suggest, the DATA0 signal transmits the "0" bits of the data stream to the upstream device, and the DATA1 signal transmits the "1" bits. Fig. 1 graphically illustrates the representation of a Wiegand data stream for the binary data of "01101". Each dip in the line represents a change from 5V to 0V, thus communicating a single bit of data of the entire message.

The third data communication and signaling wire is used by the upstream device to signal the reader. This wire is called LEDCTL because it is often used by the upstream device to control a light-emitting diode (LED) in the reader and provides feedback to the card holder.

SUMMARY

The SIA standard defines the timing of the signals on the DATA0 and DATA1 lines as shown in Fig. 2 and Table 1 shown below:

SYMBOL	DESCRIPTION	MIN	MAX
TPW	Pulse Width Time	20 μs	100 μs
TPI	Pulse Interval Time	200 μs	20 mS

Table 1: Timing Characteristics of DATA0 and DATA1

WAVELYNX EX. 1003, Pg. 3
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The typical timing uses a pulse width of 50 μs and a 1 ms gap between pulses. The pulse timing between gaps determines the data rate and, as longer bit streams are used, may be reduced from the 1 ms gap typically used. An effective baud rate table calculated using various values for TPW (pulse width time) and TPI (pulse interval time) is depicted in Table 1A shown below:

TPI	TPW	BAUD
200 μs	50 μs	4000.00
250 μs	50 μs	3333.33
1 ms	50 μs	952.38
2 ms	50 μs	487.80
5 ms	50 μs	198.02
10 ms	50 μs	99.50
20 ms	50 μs	49.88

Table 1A: Effective Baud Rate

The baud rates depicted in Table 1A represent a TPI from 200 μs to 20 ms, which is the range of allowable TPI values defined by the SIA standard. All of the baud rates in Table 1A were calculated using a TPW value of 50 μs. However, as noted above, the TPW value may range between 20 μs and 100 μs.

Since TPW and TPI are specified as a range by the SIA standard, this fact can be exploited to provide a secondary covert communication channel over the existing communication and signaling wires. If the spacing of TPI and/or width of length TPW, for example, were to vary, this variance could be tracked by the host. As an example, using a TPI of 1 ms to represent a binary zero bit and a TPI of 2 ms to represent a binary one bit, the reader could send at least as many bits of data as there are in the primary

WAVELYNX EX. 1003, Pg. 4
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

communications path by varying TPI between 1 and 2 ms. This data could simply be additional format data or, as described below, this data could be security and authentication data, or the presence of this data can be used by the upstream device to realize that is communicating with a reader capable of supporting all of the improvement described herein. Because these secondary signals conform to the SIA standard, utilizing this method would always be backwards compatible with existing legacy systems. Another use for this secondary communications channel would be to inform the host device that the reader supports the security improvement inventions contained herein. Any host capable of detecting this could use any of the Wiegand control signals as an acknowledgement

The SIA standard defines signal levels on the LEDCTL line but does not set forth any method of encoding data on this line as it does for the DATA0 and DATA1 lines. Thus, implementers of the SIA standard are free to use the LEDCTL line for arbitrary communication between the upstream devices and middleware and the reader. Moreover, the SIA standard does not preclude manufacturers from including additional features on either readers or upstream devices (*i.e.*, panels). The SIA standard defines the minimum set of features a reader or panel must provide to be in compliance. Manufacturers may have additional features so long as they do not conflict with the SIA standard.

Access control panels may connect to as many as eight readers. The hardware cost trade-offs intrinsic to the panel-to-reader ratio has caused most panel manufacturers to support just two readers in a single panel.

It is important to point out that, if a reader is controlling an exterior door to a premise and consequently mounted on the outside of the premises, the wiring from the

WAVELYNX EX. 1003, Pg. 5
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

reader to the upstream device may be accessed by unauthorized persons.

As popular as the Wiegand interface has become, it has shortcomings. One such shortcoming arises due to the use of open collector signaling makes it very easy to connect a "listening" device to the communication and signaling wires to monitor communications between a card reader and an upstream device and thereby harvest data streams that can be used to compromise the system. Once a rogue device has been connected to monitor communications between the reader and an upstream device, an attacker can note when the door has been unlocked and record the most recent data stream as one that will open the door. Then, whenever illicit entry is desired, the attacker can replay the recorded data stream causing the door to unlock. The attacker need not remove the rogue device from the communication wires to gain unauthorized entry because of the Wiegand communications open collector data interface allows both the monitoring of messages and generation of messages from the same connection.

Furthermore, an attacker can harvest more than one valid message to gain unauthorized entry using different cardholder data so that no suspicions are aroused. Unauthorized access to the Wiegand communications wires is aided by the fact that at least one reader is typically deployed 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 include any tamper detection mechanisms so that the removal of a reader to access the internal wiring or even to replace the reader with another compromised reader or illicit device is undetectable. Even when tamper detection mechanisms are included in a reader, they are often not activatedutilized because the installer of the reader does not

WAVELYNX EX. 1003, Pg. 6
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

want to incur the additional costs associated with installing additional wiring from the tamper detection mechanism back to the upstream device

Certain weaknesses of the existing Wiegand protocol have been publicly exploited by hackers, such as Zac Franken. Mr. Franken has developed a device (known as the Gecko) that is capable of capturing and storing communications transmitted by a reader, , and transmitting the stored communication at a later time thereby allowing unauthorized access to assets secured by the reader. This type of attack is known as a man-in-the-middle store-and-forward attack. Details of this attack will be described in further detail below along with ways that embodiments of the present invention ameliorate and/or eliminate susceptibility to such attacks.

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 format. These additional bits can provide supplementary information from the reader to the upstream device as well as error detection and/or correction bits for the transmitted data. The '203 patent further describes transmitting data back to the reader from the upstream device via an LED control line.

Additionally, in PCT Application No. WO 2005/038729 to Merkert, which is herein incorporated by this reference, an access control 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

WAVELYNX EX. 1003, Pg. 7
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

indicating when the message was generated. Then the control panel reads the time stamp to ensure that the message is current and not the replaying of a previously recorded message. 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 requires additional hardware to support implementation thereby increasing the overall cost of the system.

In the current art and in US 2007/0046424, the entire contents of which are incorporated herein by this reference, encryption techniques are posited to obscure the data sent from the card reader to the access control panel. Each such encryption technique assumes a managed key infrastructure for its operation and proper functioning.

There are a number of disadvantages in using keyed encryption techniques to protect the data in transmission from the reader to the panel. First, creating, administering and managing a key infrastructure can be complex and costly. The additional implementation and administration costs of a key management system to accompany the physical access control system can be a disincentive for purchasing a physical access control system that uses keyed encryption techniques.

Second, the physical access control systems, of which the reader and the panel are a part of, are typically installed and managed by personnel that are not familiar with handling and protection of cryptographic keys. Thus, there is a high likelihood that the encryption keys used to protect the data in transmission would be compromised without this compromise being detected. As a result, the data protection feature of using encryption in reader-to-panel communication may be rendered ineffective and yet the

WAVELYNX EX. 1003, Pg. 8
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

overhead performance and administration costs of the feature would endure.

Third, the amount of executable computer code needed to implement encryption techniques is not insignificant.. Additional memory has to be added to each reader to contain this executable code thereby increasing the cost of the reader.

Fourth, execution of the encryption computer code will take additional processing time and thereby lengthen the response time of the reader and consequently reduce the rate at which, for example, people can pass through the door protected by the reader. Furthermore, the additional processing may require the use of a more capable microprocessor in the reader thereby further increasing the costs of each reader and the overall physical access control system.

Some security issues associated with the Wiegand protocol have been addressed in U.S. Patent Application No. 11/464,912 to Davis et al., the entire contents of which are incorporated herein by this reference. For example, the '912 application helps upstream devices determine whether Wiegand data is being received from a valid device or is simply a replay attack. This security feature is accomplished through the use of rolling codes to obfuscate the Wiegand data. The implementation of the technique mixes some bits known only to the reader and the panel (*i.e.*, the rolling codes) into the existing format data.

In a first aspect of the present invention, the particular rolling code that is mixed into the format data serves to identify the reader sending the data and to time-stamp the transmission. This first aspect is henceforth referred to as *stamping*.

In a second aspect of the present invention, the manner in which the rolling code is mixed into the format data serves to obfuscate the true values of the data contained in

WAVELYNX EX. 1003, Pg. 9
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the message and thus hide these values from prying eyes. This second aspect is henceforth referred to as *blinding*. In accordance with at least one embodiment of the present invention, the rolling code is exclusive OR'd (XOR'd) with the format data to obfuscate the format data sent in the message. This obfuscation requires significantly less processing power and processing time than traditional encryption techniques such as DES or AES

In accordance with at least some embodiments of the present invention, by using the rolling codes both for authentication (stamping) and privacy (blinding), a marked improvement may be obtained in a number of security aspects of the overall system with the addition of very little added system complexity or administration cost.

In accordance with at least one embodiment of the present invention, a security method and system are provided where the rolling code used to authenticate the reader is also used to shroud, obscure and otherwise obfuscate data sent from the reader to the upstream device. This inventive method offers a number of improvements over using keyed encryption techniques to protect the data. First, dual-purposing the rolling code avoids the cost of implementing an independent key infrastructure to secure the data. This helps reduce the overall cost of the system while increasing the security associated therewith.

Second, as the rolling code changes with every transmission, discovering the rolling code for a particular transmission will not enable the discovery of any other transmissions, either before or after the broken transmission, since the codes will be different for each transmission.

Thirdly, data blinding and obfuscation techniques require fewer computer

WAVELYNX EX. 1003, Pg. 10
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

instructions to implement and execute faster than keyed encryption techniques. While data blinding and obfuscation techniques may, in some cases, provide a lower level of data security than keyed cryptography techniques, they are certainly an improvement over no data protection at all and, in many instances, may be deemed appropriate relative to the value of the underlying data or facility being protected.

In accordance with still further embodiments of the present invention, two devices may be enabled to use a synchronized pseudo-random number generator (PRNG) to secure the communication between them, for example. Synchronization of the PRNG between the two devices is lost, for example, when one device suffers a power cycle (*i.e.*, loss of power). In accordance with at least some embodiments of the present invention, the two devices can regain synchronization of the pseudo-random number sequence without opening the possibility of a replay attack on the pseudo-random number sequence. This may be accomplished by having the two devices share one or more different PRNGs. The PRNG used to secure the communication between them is used every time they communicate and may therefore be called the primary communication or "fast" PRNG. Another PRNG may only be used when the devices need to resynchronize the fast PRNG. This second PRNG may be called the secondary synchronization or "slow" PRNG. By implementing a fast and slow PRNG, the two devices that are connected to one another, for example through Wiegand wires, may be adapted to automatically synchronize and re-synchronize with each other dynamically and without user intervention.

Table 2 lists the features and benefits of the stamping aspect of embodiments of the present invention:

WAVELYNX EX. 1003, Pg. 11
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FEATURE	BENEFIT
Each message includes a time-based unique identifier by virtue of the fact that rolling codes are sequential	Access events can be reliably associated with time for accounting and forensic purposes without a secure logging facility. The system is protected against replay of previous messages
Each reader or group of readers can use a different sequence of unique identifiers	The unique identifier serves to authenticate the reader or reader group that sent the message

Table 2: Features and Benefits of Wiegand Stamping

Table 3 lists the features and benefits of the blinding aspect of embodiments of the present invention:

FEATURE	BENEFIT
Personal identification data (PID) in the message is obfuscated	The privacy of the system is improved since no PID is revealed
The blinding can carry additional information	More information can be carried from the reader to the upstream device without altering the current message size or the current message format. Authentication information is added via use of the rolling code (*e.g.*, which is XOR'd with the card data).

Table 3: Features and Benefits of Wiegand Blinding

Table 4 lists how embodiments of the present invention addresses a number of attacks on physical access control systems using the Wiegand protocol.

THREAT	PROTECTION
Rogue Reader: A rogue or non-certified reader could be substituted for the original reader.	Embodiments of the present invention are operable to detect rogue readers due to the authentication mechanisms provided by the rolling code.
Man-in-the-Middle (MIM) Attack: The broadcast of an exact copy of a	Embodiments of the present invention prevent MIM attacks due to the

WAVELYNX EX. 1003, Pg. 12
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

message between a reader and an upstream device that was previously captured. 1. A person presents their card and an unauthorized MIM device inserted between the reader and the upstream device captures this message and subsequently passes it along unmodified. 2. If the host asserts the LEDCTL signal indicating that the cardholder will be granted access, then the MIM device keeps a copy of the message otherwise it is discarded. 3. Whenever illicit entry is desired, the MIM device simply replays the saved message.	authentication mechanism provided by the rolling code; a replay attack would contain an earlier sequenced rolling code.
MIM Store and Forward Attack: The broadcast of an exact copy of a Wiegand message between a reader and an upstream device that was previously captured. This type of attack is more sophisticated than the previous MIM attack scenario because it uses social engineering in an attempt to defeat the rolling code protection. 1. A person presents their card and an unauthorized MIM device inserted between the reader and the upstream device captures this message and blocks its transmission to the upstream device 2. The user presents their card again since the door was not unlocked the first time it was presented. 3. The MIM device releases the first Wiegand message which results in the door being unlocked yet the MIM	The MIM Store and Forward attack is prevented by the periodic assertion of the LEDCTL signal which requests the next rolling code from the reader causing the retained message to be out of sequence when it is used.

device still retains the second message which is in proper rolling code sequence to unlock the door at a later time for a perpetrator. 4. Whenever illicit entry is desired, the MIM device simply replays the saved message.	
MIM Data Substitution Attack: Another form of the man-in-the-middle attack in which the Wiegand message is altered as it transmitted from the reader to the upstream device; alteration could be, for example, altering the card number data.	Embodiments of the present invention mitigate this risk due to its obfuscation of the card number by blinding, making it extremely difficult to alter data without destroying the integrity of the rolling code.
MIM Spoof Attack: A specialized form of the man-in-the-middle attack in which the Wiegand messages from one reader are copied and replayed at another reader.	Embodiments of the present invention are essentially immune to this type of attacks because the rolling code will not be in sync with another reader.
Passive eavesdropping / Privacy leakage: Attack in which the Wiegand messages between a reader and an upstream device can be surreptitiously observed by a third-party.	If the Wiegand wires are cut during attachment of any in-line device, this may be detected depending upon the frequency of the periodic assertion of the LEDCTL signal. However, if a device is merely "attached" to the Wiegand data lines to passively monitor the data, attachment of the device will not be detected but the data itself will remain private due to its obfuscation by blinding with the rolling code.
Tracking: The capture of a Wiegand message between a reader and an upstream device and optionally extracting the card number, its association with a person, and the subsequent correlation of the person's whereabouts using Wiegand messages obtained from other readers.	Embodiments of the present invention mitigate this risk due to its obfuscation of the card number by blinding since the message is essentially different even if the same person presents the same card at the same reader.
Targeting: The ability to perform an action based on identifying an individual from the card	Embodiments of the present invention mitigate this risk due to its obfuscation of the card number by blinding since the

WAVELYNX EX. 1003, Pg. 14
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

number obtained from the passive eavesdropping of the Wiegand messages sent from the card reader to the upstream device.	message is essentially different even if the same person presents the same card at the same reader.
Denial of Service (DOS): An attack in which the reader is made unavailable. As it relates to the Wiegand protocol, DOS may be accomplished by cutting power to the reader, cutting or shorting the DATA0 and DATA1 signals, or connecting a rogue device that continuously sends Wiegand data to jam the channel possibly causing the host to become inoperable because it may be continuously responding to bogus Wiegand data.	Unlike the current Wiegand Protocol, the host is able to detect when the reader becomes non-responsive due to a denial of service attack in which the reader power is interrupted or the integrity of the data lines are compromised because the reader will no longer respond to the periodic assertion of the LEDCTL signal. Jamming can be detected and reported by judicious firmware in the upstream device or by converting back to a legacy Wiegand operational mode. In accordance with at least some embodiments of the present invention, all of the features of the secure Wiegand can be implemented in an intermediate device located between the reader and control panel. Thus, the intermediate device can filter against DOS attacks directed toward the host, control panel, or similar upstream devices.
Buffer Overflow Attack: Attack in which an unexpectedly long Wiegand message causes data to be stored beyond the boundaries of a fixed-length buffer resulting in unexpected and undesirable behavior by the upstream device.	Working with panel manufacturers can help ensure that firmware is not susceptible to this type of attack and tests for susceptibility to buffer overrun attacks could be included in any validation tools provided to test for compliance with the embodiments of the inventions contained herein. Also, updated firmware designed to detect and react to these kinds of attacks may be included in an intermediate device between the legacy reader and upstream device. Thus, the intermediate device can filter against buffer overrun attacks directed toward the host, control panel, or similar upstream devices.

Table 4: Resistance to common threats

In accordance with at least one embodiment of the present invention, systems and methods are provided that allow existing physical access control systems using Wiegand

WAVELYNX EX. 1003, Pg. 15
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

wires for communication between readers and upstream system components such as control panels to be modified to also support data communication from the upstream components back to the readers This may be affected by making modifications solely to the software and firmware contained in the readers and upstream devices and thus without making any changes to existing hardware. As an immediate consequence of the application of these inventive means, methods and systems, two-way, communication may be realized between card readers and upstream devices.

More specifically, in the current art, Wiegand wires are used to carry format and reader status data read from an access control credential such as a Prox or iCLASS® card by a card reader to an upstream component of an access control system which is often an access control panel. The upstream device analyzes this data and may perform operations based on this analysis such as unlocking a door located near the reader that sent the data. As described in the SIA standard and as implemented by the physical access control industry, Wiegand wires provide only a one-way channel for the communication of digital data, namely from the card reader to the upstream device.

A number of advanced features of physical access control systems can be realized if communication in the other direction, namely from the upstream device to the card reader, can be achieved. The realization of these advanced features would be particularly attractive if the communication from the upstream device to the card reader could be achieved in the following manner:

1. without modifying or changing in any way the hardware of existing components of the system including readers and upstream devices;
2. using the physical and electrical properties of any existing Wiegand wires and still operating within the electrical characteristics of the industry standard Wiegand protocol;
3. continuing compliance with the SIA standard; and

WAVELYNX EX. 1003, Pg. 16
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

4. maintaining complete backward compatibility with all existing system functionality.

At least some embodiments of the present invention help to achieve these desirable advantages. Elements of this particular aspect include electrical and logical digital encoding techniques that enable the transmission of digital data to card readers in access control systems from upstream devices such as control panels. This is accomplished by utilizing one or more of the Wiegand wires currently defined to carry only a high-low indicator signal with pre-defined semantics to carry packets of digital data.

The existing methods of communication on Wiegand wires as described by the SIA standard only provide for the transmission of a single high- low indicator to be sent from an upstream device to the reader, in particular on the LEDCTL wire. The meaning of this high- low signal as described by the SIA standard is the on/off control of a cardholder feedback indicator such as an LED and does not include the encoding of digital data.

Consequently, there are a number of advanced features of physical access control systems that are not implemented in systems using Wiegand wires because of the lack of a digital communication path from the upstream device to the card reader other than the high-low LEDCTL signal. For example, it is impossible for the upstream device to send the reader messages to reconfigure the reader's operating characteristics. Nor is it possible for the upstream device to reconfigure the security properties of the communication from the reader to the upstream device. And finally, without true bi-directional data communication, there is no way that a reader can receive new

WAVELYNX EX. 1003, Pg. 17
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

configuration data, keys, or firmware without human intervention such as, for example, presenting a special configuration card to the reader or removing the reader from the wall to connect to a serial communication port reserved for this purpose.

In the current art, as defined by the SIA standard, a reader need only sense a high-low level signal on the LEDCTL wire and the response of the reader to changes in this signal is defined by the SIA standard. According to the SIA standard, for readers with a single color LED, when a high signal is sensed on the LEDCTL, the reader's LED is turned off. For readers with bi-color (or tri-color) LEDs, when a high signal is sensed on the LEDCTL, the reader's LED is illuminated in red or some other color, for example. Similarly, according to this standard, when a low level is present on the LEDCTL signal, the LED in a reader with a bi-color LED will be illuminated in green and is illuminated in red for readers with a single red color LED. Although it is not defined in the standard, some manufacturers will treat oscillation of the LEDCTL signal as an indication to illuminate the reader's LED in a third color (usually yellow in readers with a tri-color LED or perceived as yellow in readers with a bi-color LED by quickly alternating the flashing of the red and green LEDs). In accordance with at least some embodiments of the present invention, additional meaning is given to both the levels and transitions of the LEDCTL signal. By programming these additional meanings into the software of the reader, packets of digital data can be sent from the upstream components including control panels back to the reader.

Additionally, the frequency with which these control signals are transmitted from the upstream device to the reader can be altered in such a way as to communicate data from the upstream device to the reader. More specifically, PSK, and FSK may be utilized

WAVELYNX EX. 1003, Pg. 18
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

for transmitting data or other types of signals and data from the upstream device to the reader. A transition in signal frequency, duty cycle, or phase, for example, may provide a certain meaning to the signal that can be interpreted by the reader. Alternatively, predetermined frequencies or amplitudes may correspond to different signals and based on the frequency, for instance, of the signal transmitted from the upstream device to the reader the reader may react differently.

If hardware modifications of the host are permitted, then amplitude and voltage levels could also be utilized on the Wiegand control signals by the upstream devices to communicate back to the reader while still using existing wiring. If the voltage levels stayed within the standards, then this method of communications would still be within the defined standards and, if compliance with the strict letter of the standards is not desired or required, then amplitudes and voltage levels outside of the standards may be utilized. Additionally, a reader and an upstream device can even operate according to the SIA standard when legacy backwards compatibility is desired but operate outside the defined electrical characteristics of the standard when these improvements are desired.

The data transmission of packets of data from an upstream device back to a reader via the Wiegand LEDCTL line or any of the other Wiegand control signal is described in the following in three aspects.

1. mode change protocol
2. data encoding
3. packet structure

For each aspect, there are one or more mechanisms by which the aspect can be realized in practice.

WAVELYNX EX. 1003, Pg. 19
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

In the SIA standard, there is no defined method for upstream devices to communicate digital data to a reader, in order to, for example, change the operating characteristics of said reader. Currently it is required that a person visit the card reader and perform various maintenance procedures (*e.g.*, update software/firmware in the reader, change operating characteristics, change keys, etc.) in the presence of and with physical access to the card reader. In the present state of the art, these maintenance procedures may include entering updated data into the reader using the radio frequency (RF) communication capabilities of the reader together via a special credential, NFC-based device, or via a communications port using infrared communications. Additional less-convenient methods may be employed such as wired communications which may require removal of the reader from the wall to connect the configuring device to the reader. These maintenance procedures may also require opening the reader enclosure or removing power from the reader and then restoring power to the reader.

As it is costly to send a technician to visit every reader in a system, this method of updating readers is avoided if at all possible. One of the primary advantages of this invention is that these operations can be performed -- and performed securely -- over the Wiegand wires thus avoiding a trip to the reader. Because the cost of performing a maintenance procedure at the card reader goes from very expensive to virtually nothing, the possibility of more frequent changes to the reader configuration and operating parameters becomes possible through the two-way packet mode communication provided by embodiments of the present invention. Moreover, remote updating of readers can be performed from anywhere in the world if there is Internet connectivity at the upstream device associated with the reader.

WAVELYNX EX. 1003, Pg. 20
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Another advantage offered by embodiments of the present invention is that the transmission of sensitive cardholder authentication information from the reader to the upstream devices, such as the 26-bit Wiegand format data discussed in the SIA standard, can be secured using proprietary as well as conventional and standardized security protocols that require two-way communications between the sender and the receiver. Bi-directional communications enables the ability to utilize mutual authentication, a well established mechanism commonly used to authenticate communication devices.

The present invention is generally directed toward a method, apparatus, and system that provide the additional security features described above to unidirectional security protocols. Although well suited for use in a physical access control system utilizing the Wiegand protocol, embodiments of the present invention may be suitable for use in any system utilizing a unidirectional protocol.

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

Fig. 1 is a waveform diagram for transmitting binary data over Wiegand wires in accordance with embodiments of the present invention;

Fig. 2 is a waveform diagram for timing characteristics of Wiegand data transmitted in accordance with embodiments of the present invention and as described in

WAVELYNX EX. 1003, Pg. 21
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the SIA Standard;

Fig. 3 is a block diagram depicting a communication system in accordance with embodiments of the present invention;

Fig. 4 is a block diagram depicting a half-duplex configuration of a reader and host in accordance with at least some embodiments of the present invention;

Fig. 5 is a block diagram depicting a full-duplex configuration of a reader and host in accordance with at least some embodiments of the present invention; and

Fig. 6 is a block diagram depicting one or more data structures used in accordance with at least some embodiments of the present invention.

DETAILED DESCRIPTION

The present invention is generally directed toward a communication method, device, and system. Embodiments of the present invention address deficiencies of the prior art and may be utilized within the context of physical access control or security systems, as well as be equally efficiently utilized in a broad range of other applications that use a unidirectional communications protocol.

One compelling aspect of the present invention is that it yields so many benefits without dramatically altering the Wiegand protocol. Not only are existing deployed hardware and wiring unchanged but the size and therefore the transmission properties of the message are not significantly changed.

WAVELYNX EX. 1003, Pg. 22
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Obscuring Wiegand Data

There are in the art many rolling code generators. Rolling code generators are also known as pseudo-random number generators (PRNG). A rolling code generator is a function, algorithm or procedure that creates the next elements in a sequence of numbers given one or more of the previous elements together with some ancillary information such as the indices in the sequence of the elements being used.

For example, the rolling code algorithm

$$x_{i+1} = (1 + x_i + 2(g(x_i+1)-g(x_i) \bmod 2^n))$$

where

$$g(x) = x \oplus 2x+1$$

shows how to generate the next element, x_{i+1}, in a sequence given the current element, x_i. ($\oplus$ is the logical XOR or exclusive OR operation.) Such a procedure is given an initial value, x_0, to initiate the generation.

For use in a preferred embodiment in the context of this disclosure, the rolling code generator should be what is known in the art as cryptographically strong. There are in the art alternative definitions of cryptographically strong but to a first approximation it means that: 1) many elements are generated before the sequence starts to repeat, 2) each possible number that the generator can generate appears as often as other numbers that the generator can generate, and 3) the minimum number of distinct values in contiguous subsequences is large.

All of these criteria and others describing cryptographically strong rolling code generators can be given strict mathematical definitions and rolling code generators satisfying these definitions can be constructed.

WAVELYNX EX. 1003, Pg. 23
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Which particular cryptographically strong rolling code generator is used in a particular embodiment of the invention depends on the security context in which the embodiment is to be used and on the resources available for the embodiment's implementation.

In accordance with at least some embodiments of the present invention, the rolling code generator may provide a sequence of numbers. In one embodiment of the data obfuscation, each number may be represented in binary notation; i.e., to the base 2, with a fixed number of digits (i.e., length). If, for example, the fixed number of binary digits were 6, then the number 3 would be represented by 000011. Thus, the obfuscated message produced by the rolling code generator is the same length as the original message and it yields a fixed-length sequence of 0's and 1's.

The message from the reader to the upstream device may also be a fixed-length sequence of 0's and 1's, called a format. Said format comprises a number of data fields including the unique identification of the card presented to the reader, the location of the reader, a unique identification of the reader, etc.

The contribution of the data obfuscation portion to embodiments of the present invention is to combine the 0's and 1's produced by the rolling code generator with the 0's and 1's of the format to be sent from the reader to the upstream device in such a way that the upstream device, with knowledge of the rolling code, can recover the original, un-combined format data but an attacker only in possession of the combination of rolling code and format data cannot recover the original, uncombined format data.

There are in the art many ways of performing this combination. Many of these means are known in the art as stream ciphers. In one embodiment, the rolling code

WAVELYNX EX. 1003, Pg. 24
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

generator is configured to generate a string of 0's and 1's that was exactly as long as the format data and the two binary strings are combined using the logical exclusive OR operation (XOR).

As with rolling code generators, combination mechanisms can be used in a particular embodiment of the invention. The combination used may depend on the security context in which the embodiment is to be used and on the resources available for the embodiment's implementation.

Two-Way Packet-Mode Communication

Possible System Configurations

In accordance with at least some embodiments of the present invention, two-way communications between a reader and an upstream device may be facilitated utilizing existing Wiegand wires that currently connect the reader with the upstream device and have been previously used to facilitate unidirectional communications from the reader to the upstream device. One aspect of current Wiegand wires that can be exploited to facilitate two-way communications is the fact that Wiegand wires use open collector signals. This means that a reader or upstream device can either transmit messages on the Wiegand wire or receive messages being transmitted on the Wiegand wireeven though the SIA standard only describes data transmission from the reader to the upstream device. As can be seen in Figs. 4 and 5, two types of system configurations can be utilized to facilitate bi-directional data communications using Wiegand wires, namely a half-duplex configuration (Fig. 4) and a full-duplex configuration (Fig. 5).

In the full-duplex system configuration, 4 wires may be used to connect the reader

WAVELYNX EX. 1003, Pg. 25
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

to the upstream device. Two of the wires may be utilized to carry data communications from the reader to the host as per the Wiegand standard. These wires correspond to the DATA0 and/or DATA1 lines, which carry DATA0 and/or DATA1 signals, respectively. In the simplest method, two of the Wiegand signaling wires can be utilized to carry data communications from the host to the reader in the same method that is defined in the Wiegand standard. These wires may correspond to the LEDCTL signal lines, a buzzer signal line, a hold/inhibit signal, or the like. In another embodiment, these wires may be used to conduct bi-directional communications using level-based communications or modulation-based communications (*e.g.*, asynchronous serial data, FSK, PSK, ASK, *etc.*). In the full-duplex configuration, both the reader and host may be enabled to simultaneously send messages to the other device without incurring message collision problems

In a half-duplex configuration, however, unless the reader and the upstream device use a mechanism preventing them from trying to communicate with each other at the same time, message collisions resulting in data alteration may occur since the communication lines (*e.g.*, DATA0 and DATA1) between the reader and host are shared and used to support bi-directional message traffic. By nature, Wiegand communications are relatively low volume traffic and collisions will be rare. However, since there is still a statistical probability that message collisions can occur, embodiments of the present invention provide a number of different ways to enable half-duplex communications while also accounting for possible message collisions.

In accordance with at least one embodiment of the present invention, both the reader and upstream device may be enabled to send messages to the other device at any

WAVELYNX EX. 1003, Pg. 26
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

time. When a collision is detected (*e.g.*, because a corrupted or unrecognizable message has been received) then a predefined protocol may be followed whereby, for example, the reader re-transmits its message within 5 seconds of detecting the collision and then the host transmits its message between 5 and 10 seconds after detecting the collision. In an alternative re-transmission scenario, both the reader and upstream device wait a random amount of time and retry their transmission. Collisions may be detected by any type of known error checking and correcting algorithm. If the messages contain error correction data and the message can be reliably constructed without resorting to a retransmission, then the other sender will be able to retransmit, if necessary, without the possibility of a resultant second collision.

In a preferred embodiment, the reader and upstream device operate in predefined sending and listening modes and only change their sending/listening mode upon the occurrence of a predefined event. As one example, the reader may be in a default send mode and the upstream device may be in a default listen mode. Each device may maintain its respective default mode until a predetermined event occurs (*e.g.*, a card is presented to the reader, read by the reader, and/or card data is sent to the upstream device). When the event does occur, the devices may switch to the alternative mode such that the reader goes into a listen mode and the upstream device goes into a sending mode for a predetermined amount of time after the occurrence of the event. During this window of time, the upstream device may be free to send any necessary messages to the reader since the reader is in listen mode and is otherwise prohibited from sending messages. By having synchronized, alternating, and mutually exclusive operating modes, collisions on the Wiegand wires are avoided.

WAVELYNX EX. 1003, Pg. 27
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Another type of predetermined event that may initiate a change in listening/sending modes of the upstream device and reader may be the transmission of a heart beat message from the reader to the upstream device via the LEDCTL signal or other method. As discussed herein, the heart beat message transmitted from the reader to the upstream device is essentially an empty Wiegand message (because it does not actually contain card data) that is utilized to allow the reader to check-in with the upstream device. Of course, in accordance with at least some embodiments of the present invention, the heart beat message may contain a rolling code to verify the identity of the reader to the upstream device. The heart beat messages are essentially used by the reader to prove to the upstream device that it is still alive and functioning as well as insuring that the communications wires are intact and that the reader has operating power. Each time a heart beat message is transmitted from the reader to the upstream device, the devices may alternate sending and listening roles for a predetermined amount of time after the occurrence of the event. However, if the periodicity with which heart beat messages are transmitted is relatively fast such that the upstream device wouldn't be able to send a message to the reader between heart beat messages, then the operating modes of the devices may only be switched after every other, every third, every fourth, *etc.* heart beat message. The parameters used to define when the devices switch listening and sending roles may vary depending upon other system characteristics and should not be limited to the examples discussed herein.

Although the half-duplex configuration depicted above shows the connection of the LED control signals to the DATA lines as being external to the host and reader, one skilled in the art will appreciate that these connections may also be made internally

WAVELYNX EX. 1003, Pg. 28
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

within the host and/or reader. More specifically, internal connections between the LED modules in the host and/or reader may be made to the DATA0 and/or DATA1 modules in the host and/or reader.

Mode Change Protocol

In the teachings of the current disclosure, communications between the reader and upstream systems is modal. Embodiments of the present invention contemplate at least two modes of communication. One mode is the communication of the current art according to the SIA standard. The other mode is the advanced two-way packet-mode of communication described herein. In another embodiment, one mode is the standard Wiegand communication mode and the other mode is the secure Wiegand mode.

Modal communication necessitates a method of changing from one mode to the other and then optionally back to the original mode. In the teachings of the current disclosure, either the card reader or the upstream device can initiate mode change from Wiegand-format mode to packet-mode or from legacy Wiegand mode to secure Wiegand mode (*i.e.*, the secure use of rolling codes in accordance with the Wiegand mode).

Upstream Device-Initiated Mode Change

It is desirable for communications to occur using the inventions described herein. Since a mix of readers that both support and do not support the inventions described herein may be present, the upstream device can use the out-of-band communications channel in which the timing characteristics are changed to detect which readers support the inventions described herein. Any such reader can be directed by the upstream device to switch to these improved methods using the following methods. Note that this is very

WAVELYNX EX. 1003, Pg. 29
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

desirable because it allows a manufacturer to sell a single reader that support *both* legacy communications and these new communications methods and the improved methods will *automatically* be turned on by upstream devices that also support these improved communication methods.

As described in the SIA standard, the LEDCTL signal can be in one of two states, high or low. Each state of the LEDCTL signal is associated with the state of the illumination of an LED on the card reader. This illumination is intended to provide information about the state of the physical access control system to a human being presenting a card to the reader. Thus the state of the LEDCTL signal as currently defined in the standard and used for purpose in the field must be constant long enough to be supraliminally acquired by a human observer. Supraliminal visual acquisition time in humans is determined by many factors such as the nature of the symbol and the age of the human but the psychophysical literature generally agrees that presentation times below 10ms may be subliminal or not perceived at all.

As the visual presentation controlled by LEDCTL is not intended to be subliminal, if the state of the LEDCTL is constant for less than 10ms a reader implementing the means and methods of the current disclosure on the LEDCTL Wiegand wire can safely conclude that this is the beginning of the protocol to switch to the packet-mode of communication on LEDCTL and not a signal to change the state of the illumination of the LED. Additionally, data may be sent to the reader in a secure fashion (i.e., through obfuscation with a rolling code) within the 10 ms window.

Conversely, if the reader does not implement the means and methods of the current disclosure on the LEDCTL Wiegand wire, presentation of a voltage level on the

WAVELYNX EX. 1003, Pg. 30
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

LEDCTL line of less than 10ms by the upstream device will either be ignored by the reader or will cause the illumination of an LED to change beneath the threshold of conscious awareness of the cardholder and therefore will not alter the understanding of the cardholder in the state of the access control system.

Thus, by the means and methods of the current disclosure, the addition of readers or upstream devices to existing physical access control systems is completely backward compatible with existing system components. A reader implementing the teachings of this disclosure will behave exactly as a reader of the current art when used with an upstream device of the current art with respect to the signals on the LEDCTL wire. The upstream device of the current art will send LEDCTL signals, levels, and/or communication data with stable times of greater than 10ms and the reader implementing the teachings of this disclosure will interpret these to be commands for changes in the illumination of an LED. Conversely, an upstream device implementing the teachings of the current disclosure sending a level change on the LEDCTL wire of less than 10ms of duration indicating a request to transition to digital data transition mode will not receive a reply from a reader in the current art and therefore will henceforth treat the reader as a reader of the current art.

In order to support the means and methods of the current disclosure, the software in a reader will not change the state of the LED immediately upon receipt of a change in the LEDCTL voltage level. Rather, upon detection of change in LEDCTL, the reader software/firmware will sample the LEDCTL line approximately 10ms later. If the voltage is still at the new level, then this is an indication from the upstream device to change the state of illumination of the LED. If the voltage has returned to the value

WAVELYNX EX. 1003, Pg. 31
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

before the detected change then this is an indication from the upstream device to switch to the digital transmission mode. In telecommunications art, the 10ms signal is called a START signal.

A reader implementing the teachings of the current disclosure having detected a voltage level duration on the LEDCTL wire of less than 10ms sends an acknowledgement message, which may be obfuscated with a rolling code, on the DATA0 and DATA1 wires indicating that it has detected the request to change to packet-mode communication on the LEDCTL wire and has switched to this mode of reception on the LEDCTL wire.

The change back to the interpretation of signals on the LEDCTL described in the SIA standard by either the reader or the upstream device is accomplished either by sending a message in packet-mode to terminate packet-mode communication. Furthermore, once the reader is in a secure Wiegand mode (*i.e.*, a packet transmission mode or any other secure Wiegand mode discussed herein), the reader and/or upstream device will set a flag that indicates the change to the secure Wiegand mode has been executed. In accordance with at least some embodiments of the present invention, when the reader powers up, the reader stays in this mode so that a power cycle, for example, cannot be used to attack the reader and send it back to an unsecured mode of operation. While there may be some secure way of causing a reader to go back to its initial mode of operation (*i.e.*, resetting the flag), it should not be due to a power down of the reader, which could be easily exploited by an attacker to compromise the system.

Reader-Initiated Mode Change

The DATA0/DATA1 channel from the reader to the upstream device carries

WAVELYNX EX. 1003, Pg. 32
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

digital data according to existing standards and usage so, unlike the panel-to-reader channel, it is not necessary to configure the channel for the transmission of digital data. There are circumstances however wherein which it is advantageous for the reader to signal a switch from the Wiegand format of described in the SIA standard to a more flexible packet format such as the datagrams of the Internet Protocol (IP).

This is accomplished by sending a special format message, for example a message consisting of all 1's. Such a message may be referred to as a STOP signal. The upstream device would acknowledge the change to packet mode by sending the upstream device-initiated packet-mode START signal as above.

In accordance with at least some embodiments of the present invention, the host may detect when a message has been received to determine that the line is secure. Once a message is received at the host, the host may initiate a mode change by sending a mode-change message to the reader.

Data Encoding

There are in the current art methods of encoding sequences of 0's and 1's or digital data bits on a single wire such as LEDCTL. There are also in the current art methods of forming these streams into finite-length blocks of 8-bit elements called bytes.

The blocks of digital data received on the LEDCTL wire are called frames. In the interest of simplicity and ease of implementation, a preferred embodiment would employ frames consisting of constant and fixed number of bytes in every block of data; i.e. a fixed frame length.

In the case that software/firmware in the upstream device is used to interpret the encoding of the digital data on the LEDCTL wire (a software UART), it is advantageous

WAVELYNX EX. 1003, Pg. 33
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

that the frames be short because the reader will have to devote all of its resources to this task for example by turning off interrupts and thus will not be in a mode to receive signals on its other inputs, for example on the input that reads cards presented to it.

For the purposes envisioned for packet-mode communication using the LEDCTL line, message lengths on the order of 8 to 16 bytes are deemed sufficient. If error detection and correction (packet framing below) posed a 100% overhead, then a frame length of 32 bytes would be required. Assuming a transmission rate of 200k bits/second, such a frame would take the reader off-line for approximately ½ of a millisecond. With a hardware UART, there is essentially no off-line time.

In alternative embodiments of the current disclosure, frames are of variable length and the data encoding methodology includes the determination of the number of bytes in the frame, message length, symbols, etc.

Packet Framing

A frame is an undifferentiated finite sequence of bytes. In order to turn the frame into a message, the values of the bytes need to be given meaning. Imputing meaning to the bytes in a frame is called packet framing and results in a packet of data. Both the upstream device and the card reader have to agree on the semantics of the bytes in the frame for a packet to be formed and for packet-mode communication to take place.

In one embodiment of the current disclosure, there is a single, fixed agreement within the access control system as to the structure of a packet of data on the LEDCTL wire. In an alternative embodiment, the only fixed aspect of the structure of the packet is an indication of what type of packet is to be found in the frame. This could, for example, be the first byte in the frame wherein the value of this byte indicates the type of packet

WAVELYNX EX. 1003, Pg. 34
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

encoded in the following bytes.

In the case that a fixed frame length is used, the packet length may be different than the frame length, in particular the packet length may be less than the frame length. In this case the packet has to be found within the frame. One method of doing this is to reserve specific byte values to mark the beginning and end of the packet. The SLIP protocol is a method of packet framing using special byte values.

There are in the art other packet framing protocols that would be appropriate for use on two-way, packet-mode serial communication means for Wiegand wires described in the current disclosure such as the serial line internet protocol (SLIP) described in RFC 1055 and the point-to-point protocol (PPP) described in RFC 1661.

In a preferred embodiment of the current disclosure, packet framing also includes error checking and error correction using means and methods of the current art such as cyclic redundancy codes (CRC) and Hamming encoding.

Serial Line Internet Protocol (SLIP)

The following code excerpted from RFC 1055 implements a small and efficient packet framing protocol called SLIP. Due to the short frames envisioned in the application of the current disclosure, no flow control is needed or defined. SLIP can be used effectively with Van Jacobsen TCP header compression when the IP datagrams are carrying TCP packets (See IP over Wiegand below).

```
 /* SLIP special character codes
 */
#define END             0300    /* indicates end of packet */
#define ESC             0333    /* indicates byte stuffing */
#define ESC_END         0334    /* ESC ESC_END means END data byte */
#define ESC_ESC         0335    /* ESC ESC_ESC means ESC data byte */

/* SEND_PACKET: sends a packet of length "len", starting at
 * location "p".
 */
```


WAVELYNX EX. 1003, Pg. 35
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

```
void send_packet(p, len)
        char *p;
        int len; {

  /* send an initial END character to flush out any data that may
   * have accumulated in the receiver due to line noise
   */
     send_char(END);

  /* for each byte in the packet, send the appropriate character
   * sequence
   */
        while(len--) {
                switch(*p) {
                /* if it's the same code as an END character, we send a
                 * special two character code so as not to make the
                 * receiver think we sent an END
                 */
                case END:
                        send_char(ESC);
                        send_char(ESC_END);
                        break;

                /* if it's the same code as an ESC character,
                 * we send a special two character code so as not
                 * to make the receiver think we sent an ESC
                 */
                case ESC:
                        send_char(ESC);
                        send_char(ESC_ESC);
                        break;

                /* otherwise, we just send the character
                 */
                default:
                        send_char(*p);
                        }

                p++;
                }

        /* tell the receiver that we're done sending the packet
         */
        send_char(END);
        }


/* RECV_PACKET: receives a packet into the buffer located at "p".
 *      If more than len bytes are received, the packet will
 *      be truncated.
 *      Returns the number of bytes stored in the buffer.
 */
int recv_packet(p, len)
        char *p;
        int len; {
        char c;
        int received = 0;

        /* sit in a loop reading bytes until we put together
```


WAVELYNX EX. 1003, Pg. 36
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

```
 * a whole packet.
 * Make sure not to copy them into the packet if we
 * run out of room.
 */
while(1) {
        /* get a character to process
         */
        c = recv_char();

        /* handle bytestuffing if necessary
         */
        switch(c) {

        /* if it's an END character then we're done with
         * the packet
         */
        case END:
                /* a minor optimization: if there is no
                 * data in the packet, ignore it. This is
                 * meant to avoid bothering IP with all
                 * the empty packets generated by the
                 * duplicate END characters which are in
                 * turn sent to try to detect line noise.
                 */
                if(received)
                        return received;
                else
                        break;

        /* if it's the same code as an ESC character, wait
         * and get another character and then figure out
         * what to store in the packet based on that.
         */
        case ESC:
                c = recv_char();

                /* if "c" is not one of these two, then we
                 * have a protocol violation.  The best bet
                 * seems to be to leave the byte alone and
                 * just stuff it into the packet
                 */
                switch(c) {
                case ESC_END:
                        c = END;
                        break;
                case ESC_ESC:
                        c = ESC;
                        break;
                        }

        /* here we fall into the default handler and let
         * it store the character for us
         */
        default:
                if(received < len)
                        p[received++] = c;
                }
        }
}
```


WAVELYNX EX. 1003, Pg. 37
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

IP over Wiegand

In order to support Internet transport and network protocols such as TCP and UDP and application Internet protocols such as HTTP and SNMP, embodiments of the present invention may utilize an IP packet called IP-over-Wiegand.

Arbitrary protocols including proprietary protocols and industry-specific protocols can be carried in IP packets. Those familiar with the art of digital data communication will understand that the means and methods of the current disclosure include the transmission of packets that are not Internet packets but may designed explicitly for use in physical access control systems.

The intent of the current disclosure is to cover all methods for the serial communication of digital data on the LEDCTL line in conformance to three constraints.

The first constraint is that there be no changes to the existing hardware comprising either the physical access control reader or the upstream device communicating with the reader.

The second constraint is that components implementing the means and methods of the disclosure are in full compliance with the SIA standard.

The third constraint is that card readers and upstream devices such as control upstream devices that implement the teachings of the current disclosure interoperate seamlessly with card readers and upstream devices complying with the SIA standard that do not implement the teachings of the current disclosure.

By adding hardware to either the card reader or the upstream device or by inserting additional hardware components such as gateways and translators into the physical access control system, there are alternative methods of achieving the

WAVELYNX EX. 1003, Pg. 38
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

communication of packet data from upstream devices to card readers using Wiegand wires. Indeed there are such devices in the art.

The advantage provided by embodiments of the present invention is that two-way, packet-mode communication can be achieved on existing hardware and thus without adding hardware components to the physical access control system and without changing existing hardware or wiring in the physical access control system.

The commonly accepted and widely held view of the physical access control industry is that the Wiegand protocol described in and constrained by the SIA standard can achieve the communication of digital data in only one direction, namely from the reader to the upstream device. By describing the communication of digital data in the other direction, from the upstream device to the reader, and by defining communication between the card reader and the upstream device while maintaining conformance to the SIA standard and on existing hardware, embodiments of the present invention connect the end nodes of physical access control systems to the Internet and thereby drastically decrease their maintenance and administration costs and greatly increase their security. Additionally, a party line may be provided to detect collisions if the readers and/or upstream device are operating in a packet mode. Thus, multiple readers can be connected to the upstream device via a single wire and the communication time on that wire may be shared among the readers.

Blind Synchronization

In accordance with at least some embodiments of the present invention, two devices may be using a synchronized PRNG to, for example, secure the communication

WAVELYNX EX. 1003, Pg. 39
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

between them. Synchronization of the PRNG between the two devices can be lost if any number of disruptions occur at either the reader or upstream device or any intermediary device. By utilizing at least one embodiment of the present invention, the two devices can regain synchronization of the pseudo-random number sequence without opening the possibility of a replay attack on the pseudo-random number sequence.

The PRNG used to secure the communication between them is used every time they communicate and therefore is called the "fast" PRNG. The other PRNG is only used when the devices need to resynchronize the fast PRN. This second PRNG is called the "slow" PRNG.

In the current art, an element generated fast PRNG or some function of an element generated by the fast PRNG is used to resynchronize the PRNG. An attacker listening on the communication line between the two devices can capture and replay the resynchronization sequence. Thus, and in accordance with at least some embodiments of the present invention, when the fast PRNG needs to be resynchronized, the slow PRNG is stepped to the next value. This next element of the slow PRNG shared by the two devices may be used to restart the fast PRNG from some predetermined beginning point, for example the element of the slow PRNG itself or some function thereof.

Data Transfer Reduction

In accordance with at least some embodiments of the present invention, a method and system for reducing the amount of data transferred from a reader to an upstream device is provided. Although the following method will be described in relation to the transmission of Wiegand format data, one skilled in the art will appreciate that the

WAVELYNX EX. 1003, Pg. 40
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

inventive data transmission methods described herein can be applied to other types of data transmission and security protocols.

The specific formatting of card data may have certain redundancies from card to card. For example, many cards distributed at a common location or site may be assigned the same site code. While each card has a unique card code, the site code is common among a plurality of cards used at a particular site. However, according to the SIA standard, the upstream device typically analyzes both the site code and card code transmitted from a reader (which was obtained from a card presented thereto). Accordingly, it is typically required that a reader transmit both the site code and card code to the upstream device so that the identity of the card presented to the reader can be determined.

In accordance with at least some embodiments of the present invention, the data redundancies between cards within a card population is identified and used to reduce the amount of data transmitted from the reader to the upstream device. An exemplary method of reducing data transmissions between the reader and upstream device will be described in accordance with data structures depicted in Fig. 6.

According to the SIA standard for 26-Bit Wiegand, the first bit is an even parity for the following 12 bits. Bits 2-9 are the site code and bits 10-25 are the card number. The final bit (*i.e.*, bit 26) is an odd parity over the previous 12 bits. Accordingly, the 26-bit Wiegand standard comprises at least two data fields (*i.e.*, a site code and card number data field). Data from common data fields of different cards may be identical, for example if both cards are issued the same site code or if the same card is presented to the same reader at two different times.

WAVELYNX EX. 1003, Pg. 41
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

As can be seen in Fig. 6, when a site code or other data field is redundant between two cards, there may be an opportunity to reduce the amount of data transmitted from the reader to the upstream device. More specifically, if the reader and upstream device can maintain a synchronized accounting of the cards that have been previously presented to the reader and had their entire data set transmitted to the upstream device, then the reader may be enabled to replace data from an entire field with an indicator which indicates that the omitted data from a particular field is redundant with a previously presented card. Upon recognizing the indicator, the upstream device can reference its cache to find the redundant data from a data field of a previously presented card. Thus, instead of sending a plurality of bits of data (*e.g.*, 8 bits for the site code), the reader is enabled to send an indicator, which will be comprised of data that cannot ordinarily appear in the message. Alternatively, other methods of detecting that a field has been compressed can be employed such as the message receiver noting that the fixed length message is shorter or even including an additional field comprised of single bits indicating whether or not a field is present or has been reduced. This allows the reader to reduce the amount of data transmitted when a card currently presented to a reader comprises a field of data that matches a field of data from a previously read card.

In another more aggressive scheme, reduction of data can be utilized *within* a field. For example, if the card number field is 16 bits but only cards 1 through 100 are actually in use, the card number field will always have many high-order zero bits that can be reduced.

In accordance with at least some embodiments of the present invention, the reader may be required by internal logic to at least send certain portions of the card data

WAVELYNX EX. 1003, Pg. 42
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

regardless of whether or not it is found in its cache. For example, if the reader reads the same card two times in a row, the reader may still be required to send at least the card number. Without such a requirement an attacker could send illicit indicators to the upstream device for all data fields that should be transmitted by the reader after the reader had previously sent valid card data. Upon receiving all of the indicators, the upstream device would simply refer to the previously read card data and allow the attacker access to the asset. Of course, the use of security techniques, some of which are described herein, in connection with the indicators would help to alleviate the risk of improperly allowing entry to an attacker that simply transmits indicators to the upstream device.

As can be appreciated by one skilled in the art, this may work for many different types of data organizational schemes used, for example, in Wiegand data transmissions. For instance, embodiments of the present invention may be utilized to reduce the amount of data transmitted in a 26-bit Wiegand data transmission scheme where three data fields (i.e., site code, card code, and parity bits) are typically transmitted from the reader to the upstream device. Alternatively, embodiments of the present invention may also be utilized in data transmission schemes that utilize significantly more data fields, such as PIV and other evolving standards, where a relatively large amount of data is transmitted from a reader to an upstream device when a card has been read by the reader. Any logical separation of data may be used to determine whether fields have been previously submitted from the reader to the upstream device

In accordance with at least some embodiments of the present invention, the reader may compare data fields of a currently read card with data fields of a card that was read immediately before the currently read card. For example, the reader may comprise a

WAVELYNX EX. 1003, Pg. 43
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

cache for only one set of card data at a time. Thus, only a single comparison between the data fields of the currently read card and data fields of the previously read card needs to be performed. Alternatively, the reader may comprise a list of cards that have been previously read along with an order identifier (*e.g.*, last read card, second-to-last read card, third-to-last read card, *etc.*). Data fields of a currently read card may be compared to data fields from all of the other cards that are maintained in the reader's cache. A comparison may be performed for each card in the cache until a match between fields has been identified.

While utilization of multiple comparisons does increase the amount of processing required by the reader, it may further reduce the amount of data that is transmitted to the upstream device, thereby decreasing the overall traffic on the system. When the reader contains the records of multiple previously read cards and data from a currently read card is not being sent since it matched at least some data in one of the previously read cards, the reader may also need to include in its transmission of card data the identifier of the card from which the match was found. Accordingly, the upstream device should maintain a cache that is substantially consistent and synchronized with the cache of the reader.

In the event that a data transmission error occurs (*e.g.*, because of a network failure, because of a power outage at the upstream device, *etc.*), and the reader attempts to transmit less than all of the data from a currently read card (because the reader determined that at least some of the data matched data from a previously read card), the upstream device may no longer be synchronized with the reader and the instant data transmission may be determined to be erroneous by the upstream device. If such a

WAVELYNX EX. 1003, Pg. 44
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

situation occurs, the upstream device may communicate to the reader using any of the methods described herein that it did not recognize the partial transmission and/or could not find the matching field to replace the non-transmitted field. This communication may be in the form of an error message. Alternatively, the upstream device may transmit a re-send entire data message to the reader. Upon receiving such a message from the upstream device, the reader may re-transmit all of the data from the currently read card. As an alternative reaction, the reader may clear its cache upon receiving such a message, request a re-read of the card, and transmit the entire card data. Either reader reaction will allow both the reader and upstream device to re-synchronize with one another as well as allow the upstream device to fully analyze the card data.

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.

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

WAVELYNX EX. 1003, Pg. 45
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

WAVELYNX EX. 1003, Pg. 46
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

What is claimed is:

1. A communication method, comprising:

obfuscating data transmitted in a first message from a first communication device to a second communication device, wherein the first and second communication devices communicate using a unidirectional communication protocol and wherein the obfuscation of the data is effected with a predetermined code.

2. The method of claim 1, wherein the predetermined code is agreed upon between the first and second communication devices prior to obfuscation of the data in the first message.

3. The method of claim 1, wherein the predetermined code is one of a plurality of codes within a rolling code sequence, wherein the first and second communication devices each have a copy of the rolling code sequence and wherein data communicated between the first and second communication devices subsequent to the first message is obfuscated with a code from the rolling code sequence that is different from the predetermined code.

4. The method of claim 1, wherein the unidirectional communication protocol comprises the Wiegand protocol.

5. The method of claim 4, wherein the first message comprises a Wiegand message.

WAVELYNX EX. 1003, Pg. 47
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

6. The method of claim 5, 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.

7. The method of claim 1, wherein obfuscation comprises computing an XOR of the predetermined code and the data.

8. The method of claim 1, wherein the predetermined code is employed to identify an authenticity of the first communication device and a timestamp.

9. The method of claim 1, wherein the first communication device is upstream of the second communication device, the method further comprising:

receiving a message at the first communication device;

determining that the message received at the first communication device was transmitted by the second communication device, wherein 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.

WAVELYNX EX. 1003, Pg. 48
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

10. The method of claim 9, wherein the message transmitted by the second communication device comprises an alteration of a control line signal between the first and second communication devices for a predetermined amount of time.

11. The method of claim 10, wherein the predetermined amount of time is less than a human-perceivable amount of time.

12. The method of claim 9, wherein the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode.

13. The method of claim 9, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

14. The method of claim 1, 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.

WAVELYNX EX. 1003, Pg. 49
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

15. The method of claim 1, 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.

16. The method of claim 1, wherein control signals are used to accommodate bi-directional communications in one of a half-duplex configuration and a full-duplex configuration.

17. The method of claim 1, wherein the obfuscation is accomplished by the use of a stream cipher.

18. The method of claim 1, wherein the first message maintains the same size before and after being obfuscated.

WAVELYNX EX. 1003, Pg. 50
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

19. A reader, comprising:

a rolling code generator operable to generate a plurality of distinct rolling codes; and

a message formatting engine, wherein the message formatting engine is operable to retrieve a first rolling code from the rolling code generator and obfuscate data with the first rolling code prior to transmitting the data to an upstream device.

20. The reader of claim 19, wherein the upstream device also has a copy of the rolling codes, wherein data communicated to the upstream device after using the first rolling code is obfuscated with a code from the rolling code sequence that is different from the first rolling code.

21. The reader of claim 19, wherein a unidirectional communication protocol is used to facilitate communications between the reader and the upstream device, and wherein the unidirectional communication protocol comprises the Wiegand protocol.

22. The reader of claim 19, wherein obfuscation comprises computing an XOR of the first rolling code and the data.

23. The reader of claim 19, wherein the first rolling code is used to confirm an identity of the reader to the upstream device.

WAVELYNX EX. 1003, Pg. 51
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

24. The reader of claim 19, wherein the reader is further operable to receive a message from the upstream device, determine that the received message received was transmitted by the upstream device, and based on determining that the message was transmitted by the upstream device, transition from operating in a first mode of operation to a second mode of operation.

25. The reader of claim 24, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

26. The reader of claim 25, wherein the predetermined amount of time is less than a human-perceivable amount of time.

27. The reader of claim 24, wherein the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode.

28. The reader of claim 24, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

29. The reader of claim 19, wherein the reader is further operable to detect a message collision on a shared communication path between the reader and upstream device and initiate a cooperative transmission of messages over the shared communication path with the upstream device.

WAVELYNX EX. 1003, Pg. 52
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

30. A communication method, comprising:

operating a credential reader in a first mode of operation;

receiving, at the credential reader, a message from an upstream device;

determining, by the credential reader, that the message was transmitted by the upstream device; and

based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation.

31. The method of claim 30, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol.

32. The method of claim 31, wherein the unidirectional communication protocol is the Wiegand protocol.

33. The method of claim 30, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

34. The method of claim 33, wherein the predetermined amount of time is less than a human-perceivable amount of time.

WAVELYNX EX. 1003, Pg. 53
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

35. The method of claim 30, wherein the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode.

36. The method of claim 30, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

37. A method, comprising:

enabling first and second communication devices with first and second PRNGs, respectively, wherein the first and second PRNGs are synchronized and used to secure communications between the first and second communication devices;

determining that synchronization between the first and second PRNGs has been lost; and

invoking third and fourth PRNGs at the first and second communication devices respectively, wherein the third and fourth PRNGs are used to resynchronize the first and second PRNGs.

38. The method of claim 37, wherein the first and second PRNGs are fast PRNGs and the third and fourth PRNGs are slow PRNGs.

39. The method of claim 37, wherein determining that resynchronization has been lost comprises determining that power has been lost at one or more of the first and second PRNGs.

WAVELYNX EX. 1003, Pg. 54
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

40. The method of claim 37, wherein the first and second communication devices utilize a unidirectional communication protocol to facilitate communications between the first and second communication devices.

WAVELYNX EX. 1003, Pg. 55
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ABSTRACT

The present invention is directed toward secure access systems. Specifically, a method and system is provided that enhances the security of unidirectional communication protocols used in access control systems, such as the Wiegand protocol. The enhancements may include obfuscation of data, a two-way packet-mode communications, and blind synchronization of pseudo-random number generators.

WAVELYNX EX. 1003, Pg. 56
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

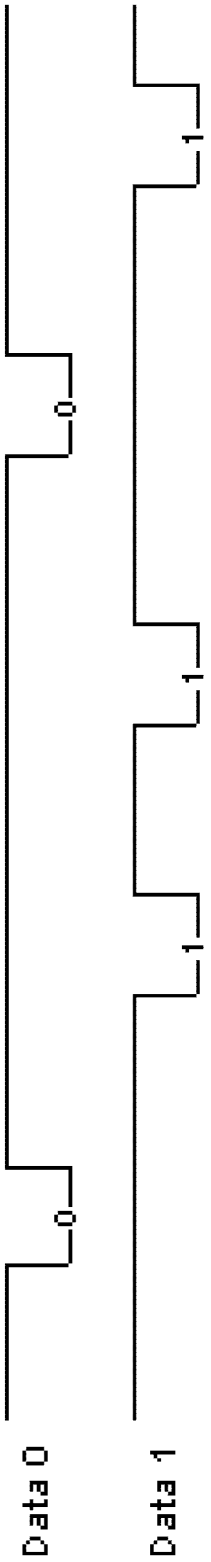


Fig. 1

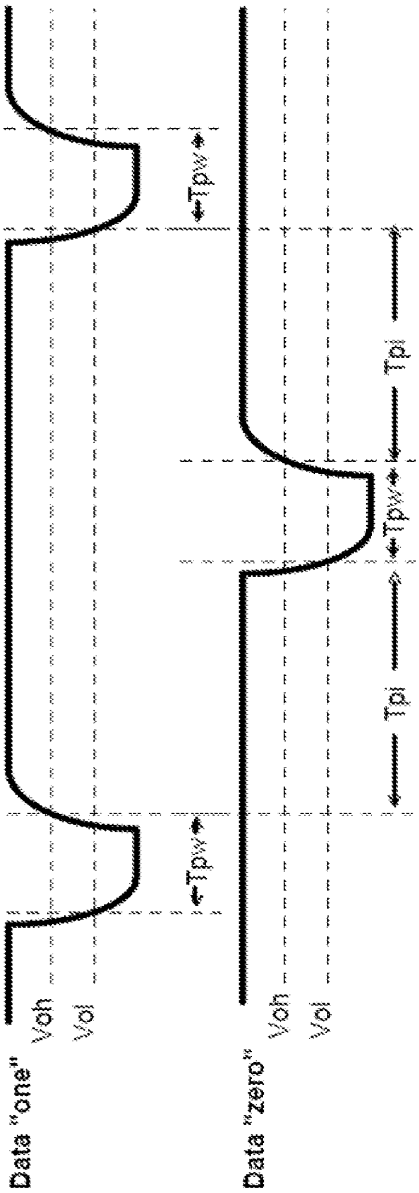


Fig. 2

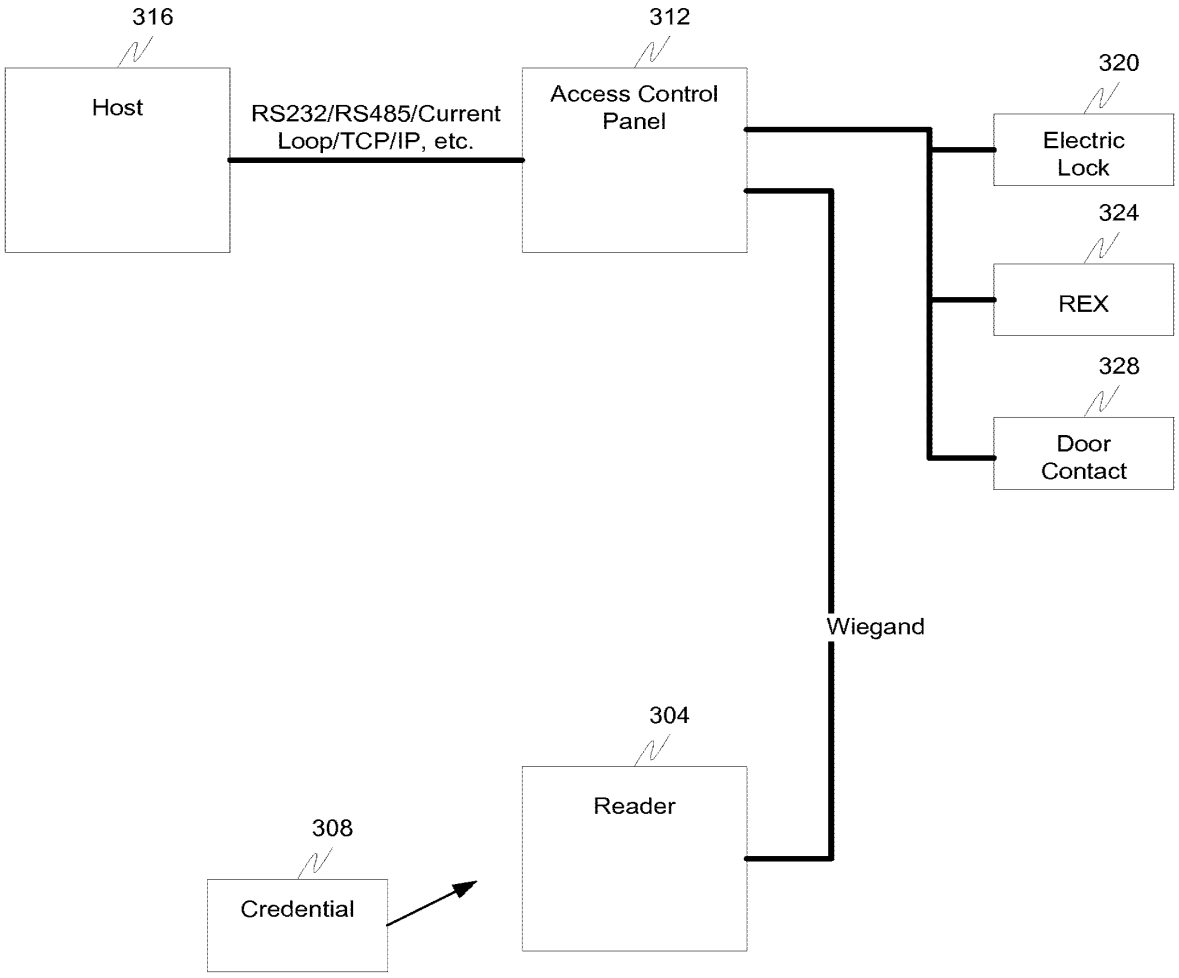

316
Host
RS232/RS485/Current Loop/TCP/IP, etc.
312
Access Control Panel
320
Electric Lock
324
REX
328
Door Contact
Wiegand
304
Reader
308
Credential

Fig. 3

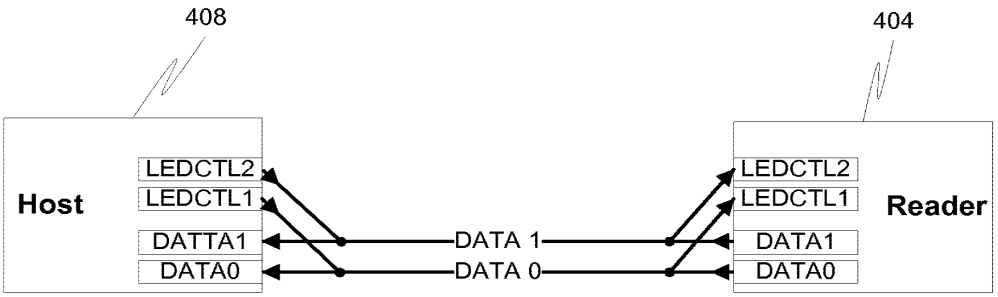

408
404
Host
LEDCTL2
LEDCTL1
DATTA1
DATA0
DATA 1
DATA 0
LEDCTL2
LEDCTL1
DATA1
DATA0
Reader

Fig. 4

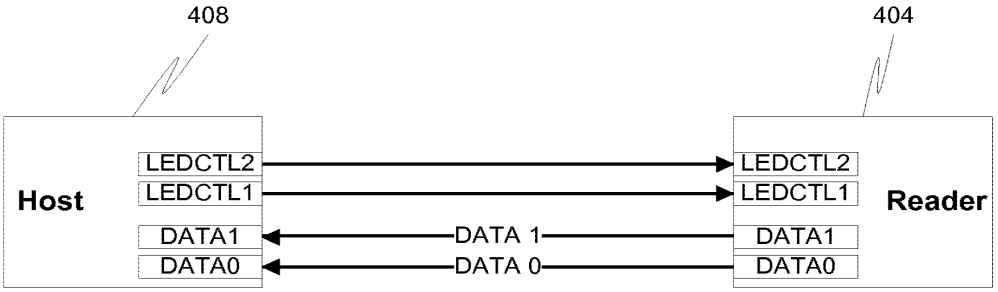

408
404
Host
LEDCTL2
LEDCTL1
DATA1
DATA0
DATA 1
DATA 0
LEDCTL2
LEDCTL1
DATA1
DATA0
Reader

Fig. 5

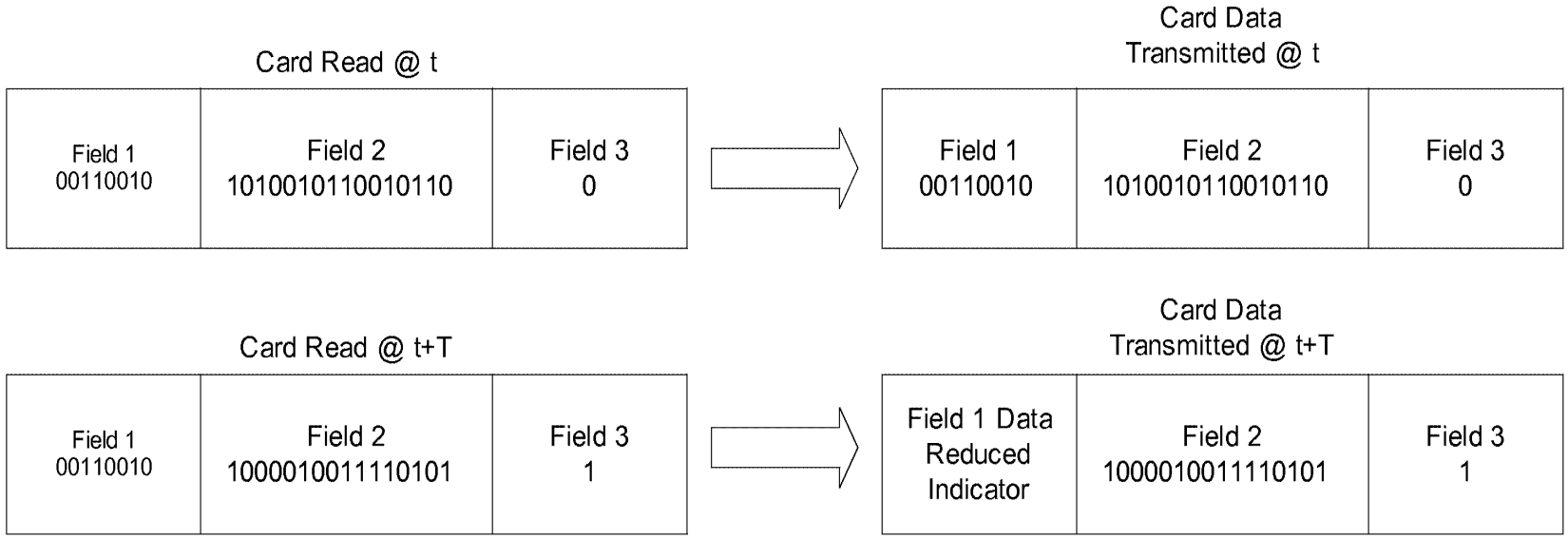


Fig. 6

WAVELYNX EX. 1003, Pg. 61
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2943-178
	Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Scott	B.	Guthery	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Chestnut Hill	State/Province	MA	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i: US

Mailing Address of Applicant:

Address 1	2400 Beacon #208		
Address 2			
City	Chestnut Hill	State/Province	MA
Postal Code	02467	Country i	US

Applicant 2 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Mark		Robinton	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Somerville	State/Province	MA	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i:

Mailing Address of Applicant:

Address 1	897 Broadway, Apt. 2		
Address 2			
City	Somerville	State/Province	MA
Postal Code	02144	Country i	US

Applicant 3 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael		Davis	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Amherst	State/Province	NY	Country of Residence i	US

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2943-178
	Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS	

Citizenship under 37 CFR 1.41(b) i	US				
Mailing Address of Applicant:					
Address 1	12 Hummingbird Lane				
Address 2					
City	Amherst	**State/Province**	NY		
Postal Code	14228	**Country**i	US		

Applicant 4 Remove

Applicant Authority (•) Inventor ( ) Legal Representative under 35 U.S.C. 117 ( ) Party of Interest under 35 U.S.C. 118

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	David		Andresky	

Residence Information (Select One) (•) US Residency ( ) Non US Residency ( ) Active US Military Service

City	Lafayette	**State/Province**	CO	**Country of Residence** i	US
Citizenship under 37 CFR 1.41(b) i	US				
Mailing Address of Applicant:					
Address 1	533 Whitetail Circle				
Address 2					
City	Lafayette	**State/Province**	CO		
Postal Code	80026	**Country**i	US		

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	22442		
Email Address	srlaw@sheridanross.com	Add Email	Remove Email

Application Information:

Title of the Invention	SECURE WIEGAND COMMUNICATIONS		
Attorney Docket Number	2943-178	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	5	**Suggested Figure for Publication (if any)**	

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2943-178
	Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	22442		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61087941	2008-08-11

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2943-178
	Application Number	
Title of Invention	SECURE WIEGAND COMMUNICATIONS	

If the Assignee is an Organization check here. ☒			
Organization Name	Assa Abloy AB		
Mailing Address Information:			
Address 1	Klarabergsviadukten 90 - P.O. Box 70340		
Address 2			
City	Stockholm	**State/Province**	
Country [i]	SE	Postal Code	S107 23
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the **Add** button.		Add	

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature	/Matthew R. Ellsworth/			Date (YYYY-MM-DD)	2009-08-11
First Name	Matthew	Last Name	Ellsworth	Registration Number	56345

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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, U.S. Department of Commerce, 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

WAVELYNX EX. 1003, Pg. 66
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Electronic Acknowledgement Receipt	
EFS ID:	5869289
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth
Filer Authorized By:	
Attorney Docket Number:	2943-178
Receipt Date:	11-AUG-2009
Filing Date:	
Time Stamp:	17:47:02
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		PATENT_APPLICATION.pdf	274259 55ea42c7bd268cecd07ad955d97453680f14c4db	yes	56

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	46
	Claims	47	55
	Abstract	56	56

Warnings:					
Information:					
2	Drawings-only black and white line drawings	FIGS.pdf	85944 24062a24b5188474e8079a833bddc6fcda6dae29	no	5
Warnings:					
Information:					
3	Application Data Sheet	ADS.pdf	1203940 586cc8c3c0c88b6e898e2de4ac5ffb9d735f1f67	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	1564143		

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.

PTO/SB/06 (12-04)

Filing Date: 08/11/09

Approved for use through 7/31/2006. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 12/539,431

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	540
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220
TOTAL CLAIMS (37 CFR 1.16(i))	40 minus 20 =	20	x$26		OR	x$52	1040
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	x$110			x$220	220
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $260 ($130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			195			390	
			TOTAL			TOTAL	2350

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. 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 12 minutes 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, U.S. Department of Commerce, 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 and select option 2.

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/539,431	08/11/2009	Scott B. Guthery	2943-178

CONFIRMATION NO. 9292

22442
SHERIDAN ROSS PC
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

FORMALITIES LETTER

OC000000037455120

Date Mailed: 08/27/2009

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  *Applicant must submit $**330** to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of $**1260** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**130** for a non-small entity, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is $**2480** for a non-small entity
- $**330** Statutory basic filing fee.
- $**130** Surcharge.
- The application search fee has not been paid. Applicant must submit $**540** to complete the search fee.

WAVELYNX EX. 1003, Pg. 70
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- The application examination fee has not been paid. Applicant must submit $**220** to complete the examination fee for a non-small entity.
- Total additional claim fee(s) for this application is $**1260**
  - $**220** for **1** independent claims over 3.
  - $**1040** for **20** total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/tnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

WAVELYNX EX. 1003, Pg. 71
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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/539,431	08/11/2009	2416	0.00	2943-178	40	4

CONFIRMATION NO. 9292

22442
SHERIDAN ROSS PC
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

FILING RECEIPT

OC000000037455119

Date Mailed: 08/27/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;
Michael Davis, Amherst, NY;
David Andresky, Lafayette, CO;

Assignment For Published Patent Application

Assa Abloy AB, Stockholm, SWEDEN

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/087,941 08/11/2008

Foreign Applications

If Required, Foreign Filing License Granted: 08/20/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/539,431**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

WAVELYNX EX. 1003, Pg. 72
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Title

SECURE WIEGAND COMMUNICATIONS

Preliminary Class

370

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

WAVELYNX EX. 1003, Pg. 73
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

WAVELYNX EX. 1003, Pg. 74
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2416
	)	
GUTHERY et al.	)	Examiner: Not Yet Assigned
	)	
Serial No.: 12/539,431	)	Confirmation No.: 9292
	)	
Filed: August 11, 2009	)	SUBMISSION OF MISSING PARTS
	)	
Atty. File No.: 2943-178	)	
	)	***Filed Electronically***

For: "SECURE WIEGAND COMMUNICATIONS"

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

In response to the Notice to File Missing Parts mailed August 27, 2009, in connection with the above-identified application, enclosed for filing is a Declaration. In addition, payment in the amount of $2,480.00 for the required filing fee, surcharge, application search fee and additional claim fees is being submitted via EFS-Web concurrently with the filing of this paper. Although fees submitted are believed to be correct, please charge any underpayment or credit any overpayment to Deposit Account No. 19-1970.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Matthew R. Ellsworth
Registration No. 56,345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: September 23, 2009

PTO/SB/01A (01-09)
Approved for use through 06/30/2010. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SECURE WIEGAND COMMUNICATIONS

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. 12/539,431 filed on August 11, 2009

☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Michael Davis Date: 8/17/2009

Signature: Michael Davis Citizen of: U.S.

Inventor two: David Andresky Date: _____

Signature: _____ Citizen of: U.S.

☐ Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1.11 and 1.14. This collection is estimated to take 1 minute 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, U.S. Department of Commerce, 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 and select option 2.

PTO/SB/01A (01-09)
Approved for use through 06/30/2010. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SECURE WIEGAND COMMUNICATIONS

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. 12/539,431 filed on August 11, 2009

☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Michael Davis Date: _____

Signature: _____ Citizen of: U.S.

Inventor two: David Andresky Date: 8/18/09

Signature: _____ Citizen of: U.S.

☐ Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1.11 and 1.14. This collection is estimated to take 1 minute 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, U.S. Department of Commerce, 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 and select option 2.

PTO/SB/01A (01-09)
Approved for use through 06/30/2010. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SECURE WIEGAND COMMUNICATIONS

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. 12/539,431 filed on August 11, 2009

☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Scott B. Guthery Date: 8/14/2009

Signature: _____ Citizen of: U.S.

Inventor two: Mark Robinton Date: _____

Signature: _____ Citizen of: U.S.

☒ Additional inventors or a legal representative are being named on 1 additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1.11 and 1.14. This collection is estimated to take 1 minute 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, U.S. Department of Commerce, 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 and select option 2.

PTO/SB/01A (01-09)
Approved for use through 06/30/2010. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SECURE WIEGAND COMMUNICATIONS

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. 12/539,431 filed on August 11, 2009

☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Scott B. Guthery Date: _____

Signature: _____ Citizen of: U.S.

Inventor two: Mark Robinton Date: 9/23/09

Signature: _____ Citizen of: U.S.

☒ Additional Inventors or a legal representative are being named on 1 additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1.11 and 1.14. This collection is estimated to take 1 minute 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, U.S. Department of Commerce, 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 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	12539431
Filing Date:	11-Aug-2009
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Filer:	Matthew Ryan Ellsworth/Leslie Frankel
Attorney Docket Number:	2943-178

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	330	330
Utility Search Fee	1111	1	540	540
Utility Examination Fee	1311	1	220	220
Pages:				
Claims:				
Claims in excess of 20	1202	20	52	1040
Independent claims in excess of 3	1201	1	220	220
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Late filing fee for oath or declaration	1051	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2480**

Electronic Acknowledgement Receipt	
EFS ID:	6132724
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Scott B. Guthery
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Frankel
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	23-SEP-2009
Filing Date:	11-AUG-2009
Time Stamp:	17:54:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2480
RAM confirmation Number	4123
Deposit Account	191970
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SUBMISSION_MISSING_PARTS.pdf	657348 c5a34870803a2f16d8bf65b5daec824dd9c18b65	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Response to Pre-Exam Formalities Notice	1	1
	Oath or Declaration filed	2	5

Warnings:

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	40117 09a4d91b1ec847d288a6acddfe09cf61d5c87628	no	2

Warnings:

Information:

Total Files Size (in bytes):	697465

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.

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/539,431	08/11/2009	2416	2480	2943-178	40	4

CONFIRMATION NO. 9292

UPDATED FILING RECEIPT

22442
SHERIDAN ROSS PC
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

OC000000038056800

Date Mailed: 10/05/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Michael Davis, Amherst, NY;
David Andresky, Lafayette, CO;
Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;

Assignment For Published Patent Application

Assa Abloy AB, Stockholm, SWEDEN

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/087,941 08/11/2008

Foreign Applications

If Required, Foreign Filing License Granted: 08/20/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/539,431**

Projected Publication Date: 02/11/2010

Non-Publication Request: No

Early Publication Request: No

WAVELYNX EX. 1003, Pg. 84
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Title

SECURE WIEGAND COMMUNICATIONS

Preliminary Class

370

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

WAVELYNX EX. 1003, Pg. 85
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

WAVELYNX EX. 1003, Pg. 86
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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/539,431	08/11/2009	Michael Davis	2943-178

CONFIRMATION NO. 9292

22442
SHERIDAN ROSS PC
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

PUBLICATION NOTICE

OC000000040075820

Title:SECURE WIEGAND COMMUNICATIONS

Publication No.US-2010-0034375-A1
Publication Date:02/11/2010

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

WAVELYNX EX. 1003, Pg. 87
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	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	8	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	3694757	9/26/1972	Hanna, Jr.	
	2	4087626	5/2/1978	Brader	
	3	5187676	2/16/1993	DeVane	
	4	5193115	3/9/1993	Vobach	
	5	5258936	11/2/1993	Gallup et al.	
	6	5357528	10/18/1994	Alon et al.	
	7	5420928	5/30/1995	Aiello et al.	
	8	5446683	8/29/1995	Mullen et al.	
	9	5533128	7/2/1996	Vobach	
	10	5541996	7/30/1996	Ridenour	
	11	5577124	11/19/1996	Anshel et al.	
	12	5608801	3/4/1997	Aiello et al.	
	13	5680131	10/21/1997	Utz	
	14	5686904	11/11/1997	Bruwer	
	15	5751808	5/12/1998	Anshel et al.	
	16	5754603	5/19/1998	Thomas et al.	
	17	5802176	9/1/1998	Audebert	
	18	5825882	10/20/1998	Kowalski et al.	
	19	6044388	3/28/2000	DeBellis et al.	
	20	6052786	4/18/2000	Tsuchida	
	21	6079018	6/20/2000	Hardy et al.	
	22	6097307	8/1/2000	Utz	
	23	6154544	11/28/2000	Farris et al.	
	24	6285761	9/4/2001	Patel et al.	
	25	6314440	11/6/2001	O'Toole et al.	
	26	6487176	11/26/2002	Lehmann	
	27	6542608	4/1/2003	Scheidt et al.	
	28	6606386	8/12/2003	Scheidt et al.	
	29	6608901	8/19/2003	Scheidt et al.	
	30	6691141	2/10/2004	Schmidt	
	31	6718038	4/6/2004	Cusmario	
	32	6810123	10/26/2004	Farris et al.	

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.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Scott B. Guthery
Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	2943-178

Sheet 2 of 8

	33	6885747	4/26/2005	Scheidt et al.	
	34	6931533	8/16/2005	Roberts	
	35	6944768	9/13/2005	Siegel et al.	
	36	6947560	9/20/2005	Smeets et al.	
	37	6988203	1/17/2006	Davis et al.	S
	38	7016925	3/21/2006	Schmidt	
	39	7064665	6/20/2006	Woodall et al.	
	40	7085791	8/1/2006	Barry et al.	
	41	7118033	10/10/2006	Merkert	
	42	7120696	10/10/2006	Au et al.	
	43	7170997	1/30/2007	Petersen et al.	
	44	7190787	3/13/2007	Graunke et al.	
	45	7212632	5/1/2007	Scheidt et al.	
	46	7219113	5/15/2007	Bonaccio et al.	
	47	7277543	10/2/2007	Driscoll	
	48	7293698	11/13/2007	Cheng et al.	
	49	7412056	8/12/2008	Farris et al.	
	50	7492898	2/17/2009	Farris et al.	
	51	7492905	2/17/2009	Fitzgibbon	
	52	2001/0041593	11/15/2001	Asada	
	53	2001/0056534	12/27/2001	Roberts	
	54	2002/0016913	2/7/2002	Wheeler et al.	
	55	2002/0184539	12/5/2002	Fukuda et al.	
	56	2003/0014646	1/16/2003	Buddhikot et al.	
	57	2003/0074319	4/17/2003	Jaquette	
	58	2003/0204541	10/30/2003	Shackleford et al.	
	59	2003/0208697	11/6/2003	Gardner	
	60	2004/0153291	8/5/2004	Kocarev et al.	
	61	2004/0162863	8/19/2004	Barry et al.	
	62	2004/0162864	8/19/2004	Nowshadi et al.	
	63	2005/0002533	1/6/2005	Langin-Hooper et al.	
	64	2005/0010624	1/13/2005	Stehle	
	65	2005/0044119	2/24/2005	Langin-Hooper et al.	
	66	2005/0110210	5/26/2005	Soltys et al.	
	67	2005/0129247	6/16/2005	Gammel et al.	
	68	2005/0166040	7/28/2005	Walmsley	

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.

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	3	of	8	Attorney Docket Number	2943-178

	69	2005/0182946	8/18/2005	Shatford	
	70	2005/0265546	12/1/2005	Suzuki	
	71	2006/0083228	4/20/2006	Ong et al.	
	72	2006/0123466	6/8/2006	Davis et al.	
	73	2006/0174184	8/3/2006	Stroud et al.	
	74	2006/0177056	8/10/2006	Rostin et al.	
	75	2006/0179094	8/10/2006	Onaya et al.	
	76	2006/0206554	9/14/2006	Lauter et al.	
	77	2006/0294312	12/28/2006	Walmsley	
	78	2007/0121943	5/31/2007	Dellow et al.	
	79	2007/0016942	1/18/2007	Sakai et al.	
	80	2007/0034691	2/15/2007	Davis et al.	
	81	2007/0043954	2/22/2007	Fox	
	82	2007/0046424	3/1/2007	Davis et al.	
	83	2007/0057057	3/15/2007	Andresky et al.	
	84	2007/0076864	4/5/2007	Hwang	
	85	2007/0099597	5/3/2007	Arkko et al.	
	86	2007/0165847	7/19/2007	Langin-Hooper et al.	
	87	2007/0165848	7/19/2007	Reyes	
	88	2007/0178886	8/2/2007	Wang et al.	
	89	2007/0183593	8/9/2007	Yoshida et al.	
	90	2007/0195952	8/23/2007	Singanamala	
	91	2007/0214293	9/13/2007	Gangstoe et al.	
	92	2007/0269048	11/22/2007	Hsu	
	93	2007/0293192	12/20/2007	De Groot	
	94	2007/0294528	12/20/2007	Shoji et al.	
	95	2007/0294531	12/20/2007	Alten	
	96	2007/0294539	12/20/2007	Shulman et al.	
	97	2007/0296817	12/27/2007	Ebrahimi et al.	
	98	2008/0001778	1/3/2008	Challener et al.	
	99	2008/0046493	2/21/2008	Rosenberg	
	100	2008/0005532	1/3/2008	Liao et al.	
	101	2008/0061941	3/13/2008	Fischer et al.	
	102	2008/0010218	1/10/2008	Zank	
	103	2008/0012690	1/17/2008	Friedrich	
	104	2008/0016363	1/17/2008	Lapstun et al.	

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.

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	4	of	8	Attorney Docket Number	2943-178

	105	2008/0184349	7/31/2008	Ting	

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]
	106	AU 2006203768	3/15/07	Davis et al.		
	107	CA 2556843	2/28/07	Davis et al.		
	108	WO 01/013218	02/22/01	Siemens Aktiengesellschaft		(Translated Abstract Attached)
	109	WO 01/18331	03/15/01	Electec System Aktiebolag		
	110	WO 03/027832	04/03/03	Intel Corporation		
	111	WO 03/042812	05/22/03	Everbee Networks		(Translated Abstract Attached)
	112	WO 04/010373	01/29/04	Banque-Tec International Pty Ltd		
	113	WO 05/001777	01/06/05	SCM Microsystems GMBH		
	114	WO 2004/039119	05/06/04	Anzon Autodoor Limited		
	115	WO 2005/018137	02/24/05	Securicom Pty Ltd		
	116	WO 2005/029315	03/31/05	Globespanvirata Incorporated		
	117	WO 2005/038729	04/28/05	SCM Microsystems, Inc.		
	118	WO 2006/015625	08/09/04	Telecom Italia S.P.A.		

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.

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	5	of	8	Attorney Docket Number	2943-178

	119	WO 2006/032941	03/30/06	Nokia Corporation		
	120	WO 2006/036521	04/06/06	Qualcomm Incorporated		
	121	WO 2006/126668	11/03/06	NEC Corporation		(Translated Abstract Attached)
	122	WO 2007/103906	09/13/07	Imagineer Software, Inc.		
	123	WO 2007/117315	10/18/07	Symbol Technologies, Inc.		
	124	WO 2007/120215	10/25/07	Imagineer Software, Inc.		
	125	WO 2008/001918	01/03/08	Yui et al.		
	126	WO 2008/010441	01/24/08	NEC Corporation		(Translated Abstract Attached)
	127	EP 1043687	11/22/06	CANON KK		
	128	EP 1148644	10/24/01	COMM RES LAB MINISTRY OF PUBLI		
	129	EP 1292882	03/19/03	ANOTO AB		
	130	EP 1398691	03/17/04	TOSHIBA KK		
	131	EP 1420542	05/19/04	ST MICROELECTRONICS SRL		
	132	EP 1460573	09/22/04	Nokia Corporation		
	133	EP 1643643	04/05/06	MICRONAS GMBH		(Translated Abstract Attached)
	134	EP 1696360	08/30/06	SAMSUNG ELECTRONICS CO LTD		
	135	EP 1760985	03/07/07	Davis et al.		

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.

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	6	of	8	Attorney Docket Number	2943-178

	136	EP 0616429	09/21/94	SIEMENS AG		(Translated Abstract Attached)
	137	EP 0843438	05/20/98	THOMSON MULTIMEDIA SA		
	138	EP 0872976	10/21/98	UNITED TECHNOLOGIES AUTOMOTIVE		
	139	EP 0924894	06/23/99	SIEMENS AG		(Translated Abstract Attached)
	140	EP 0949563	10/13/99	LUCENT TECHNOLOGIES INC		
	141	EP 0996928	05/03/00	ASSURE SYSTEMS INC		

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	
	142	Partial European Search Report for European Patent Application No. 06113988 (Atty File No. 2943-114-EP), dated January 10, 2007.
	143	Written Opinion of the International Searching Authority for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	144	International Search Report for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	145	Examiner's First Report for Australian Patent Application No. 2006203768, mailed November 20, 2009.
	146	"Access Control Standard for the 26-Bit Wiegand Reader Interface," Security Industry Association, October 17, 1996, 15 pages.
	147	"Condoplex - The World Leader in Developing Security and Communication Solutions," retrieved from http://web.archive.org/web/20040324112641/http:llcondoplexinc.com/, publication date March 24, 2004, 1 page.
	148	"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance White Paper, October 2002, 36 pages.

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.

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	7	of	8	Attorney Docket Number	2943-178

	149	"Information Technology: Application Profile for Commercial Biometrical Physical Access Control," Project INCITS 1706-D, 2005, 16 pages.
	150	"Technology Basics: Understanding Wiegand," HID Corporation, 2004, 5 pages.
	151	ANASHIN, V. "Uniformly distributed sequences over p-adic integers," Number Theoretic and Algebraic Methods in Computer Science, Moscow 1993 (A.J. van der Poorten, I.Shparlinski, and H.G. Zimmer eds., 1995), pp. 1-18, available at http://crypto.rsuh.ru/papers/anashin-paper1.pdf.
	152	ANASHIN, V., "Pseudorandom number generation by p-adic ergodic transformations" (Jan. 29, 2004), available at http://arxiv.org/abs/cs.CR/0401030.
	153	ANASHIN, V., "Pseudorandom number generation by p-adic ergodic transformations: An addendum" (Feb. 26, 2004), pp. 1-9, available at http://arxiv.org/abs/cs.CR/0402060.
	154	ANASHIN, V., "Uniformly distributed sequences in computer algebra, or how to constuct program generators of random numbers," J. Math. Sci., 89(4):1355–1390 (1998), available at http://crypto.rsuh.ru/papers/anashin-paper5.pdf.
	155	ANASHIN, V., "Uniformly distributed sequences of p-adic integers," II. Discrete Math. Appl., 12(6):527–590 (2002), available at http://arXiv.org/abs/math.NT/0209407.
	156	ANASHIN, V., "Uniformly distributed sequences of p-adic integers," Mathematical Notes, 55(2):109–133 (1994), available at http://crypto.rsuh.ru/papers/anashin-paper2.pdf.
	157	BRIAN, M., "How Remote Entry Works," Howstuffworks.com, retrieved from http://auto.howstuffworks.com/remote-entry.htm, printed on May 19,2005, copyright 2005, 8 pages.
	158	DAMGARD, I., "On the Randomness of Legendre and Jacobi Sequences," Advances in Cryptology (Proceedings of Crypto '88), Lecture Notes in Computer Science (1990), pp. 163-172.
	159	Data Sheet, "26 Bit Weigand Specifications," Essex Electronics Incorporated, April 1, 1998, 1 page.
	160	Data Sheet, "Micro RWD EM4001 'Mag swipe' Decimal Output Version," IB Technology, May 3, 2005, pp. 1-8.
	161	DAVIS, M., "Reader To Panel Authentication," Cartes 2005, Paris, France, Nov. 1, 2005, 33 pages.
	162	GLASS, B., "DMCA Used In Garage Door Battle," Ziff Davis Media, retrieved from http://www.extremetech.com/print_article2/0,2533 on May 19, 2005 (Jan. 23,2003), 1 page.
	163	KNEBELKAMP et al., "Latest Generation Technology for Immobilizer Systems," Texas Instruments, retrieved from www.ti.com/tiris on May 19, 2005, 11 pages.

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.

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	8	of	8	Attorney Docket Number	2943-178

	164	LEVIN, L., "One Way Functions and Pseudorandom Generators," Combinatorica, Vol. 7(4) (1987), pp. 357-363.
	165	Press Release, "Radio Frequency Identification (RFID) based immobilizer systems help to curb auto theft and reduce insurance costs," Texas Instruments, May 7, 1999, 2 pages.
	166	WEINSTEIN, L., "DMCA: Ma Bell Would Be Proud," Wired News, Jan. 20, 2003, 27 pages.
	167	WOODCOCK, F., et al., "p-Adic Chaos and Random Number Generation," Experimental Mathematics, Vol. 7(4), (1998), pp. 334–342.

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.

(12) STANDARD PATENT APPLICATION (11) Application No. **AU 2006203768 A1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Device authentication using a unidirectional protocol

(51) International Patent Classification(s)
H04L 9/32 (2006.01)

(21) Application No: **2006203768** (22) Date of Filing: **2006.08.29**

(30) Priority Data

(31) Number	(32) Date	(33) Country
60/713528	**2005.08.31**	**US**
11/464912	**2006.08.16**	**US**

(43) Publication Date: **2007.03.15**
(43) Publication Journal Date: **2007.03.15**

(71) Applicant(s)
Assa Abloy Identification Technology Group AB

(72) Inventor(s)
Davis, Michael L;Hulusi, Tam

(74) Agent / Attorney
Allens Arthur Robinson Patent & Trade Marks Attorneys, Stock Exchange Centre 530 Collins Street, Melbourne, VIC, 3000

2006203768 29 Aug 2006

ABSTRACT

The present invention is directed toward secure access systems. Specifically, a method and system is provided that allows a control panel of a secure access system to verify the authenticity and fidelity of a reader within the secure access system by utilizing a rolling code agreed upon by the reader and the control panel.

WAVELYNX EX. 1003, Pg. 97
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

P/00/011
Regulation 3.2

AUSTRALIA

Patents Act 1990

ORIGINAL
COMPLETE SPECIFICATION
STANDARD PATENT

Invention title: Device authentication using a unidirectional protocol

The following statement is a full description of this invention, including the best method of performing it known to us:

2006203768 29 Aug 2006

DEVICE AUTHENTICATION USING A UNIDIRECTIONAL PROTOCOL

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

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

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.

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

WAVELYNX EX. 1003, Pg. 99
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 100
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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

WAVELYNX EX. 1003, Pg. 101
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

an upstream device. Without bidirectional capabilities, it is very difficult to implement a modern protocol that provides for reader authentication.

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 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.

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.

There have been some attempts to address the shortcomings of the Wiegand

WAVELYNX EX. 1003, Pg. 102
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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

WAVELYNX EX. 1003, Pg. 103
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 104
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

In accordance with other embodiments of the present invention, a secure access system utilizing a unidirectional communication protocol is provided. The system

WAVELYNX EX. 1003, Pg. 105
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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.

These and other advantages will be apparent from the disclosure of the invention(s) contained herein. The above-described embodiments and configurations are

WAVELYNX EX. 1003, Pg. 106
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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

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.

WAVELYNX EX. 1003, Pg. 107
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

DETAILED DESCRIPTION

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).

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 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.

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

WAVELYNX EX. 1003, Pg. 108
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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,

WAVELYNX EX. 1003, Pg. 109
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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 algorithm(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.

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.

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.

In accordance with embodiments of the present invention, a stand-alone reader

WAVELYNX EX. 1003, Pg. 110
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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.

In operation a credential 116, for example a credential, is brought into an active

WAVELYNX EX. 1003, Pg. 111
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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

WAVELYNX EX. 1003, Pg. 112
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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

WAVELYNX EX. 1003, Pg. 113
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

WAVELYNX EX. 1003, Pg. 114
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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 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.

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

WAVELYNX EX. 1003, Pg. 115
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

valid code is in a rolling code sequence. For example, the reader 112 may use a pseudo-random 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.

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.

WAVELYNX EX. 1003, Pg. 116
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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

WAVELYNX EX. 1003, Pg. 117
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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 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.

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.

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

WAVELYNX EX. 1003, Pg. 118
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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

WAVELYNX EX. 1003, Pg. 119
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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

WAVELYNX EX. 1003, Pg. 120
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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).

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 frequency of update may be required.

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.

WAVELYNX EX. 1003, Pg. 121
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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

WAVELYNX EX. 1003, Pg. 122
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

another valid rolling code at the predetermined time or in a predetermined time window.

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).

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

WAVELYNX EX. 1003, Pg. 123
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

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.

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 downstream device is not valid or is not functioning properly. A valid rolling code generally includes

WAVELYNX EX. 1003, Pg. 124
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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 of 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

WAVELYNX EX. 1003, Pg. 125
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

limited to control panels 104, but also may include a reader 112, an intermediate device 120, and/or a credential 116.

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.

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.

Moreover though the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and

WAVELYNX EX. 1003, Pg. 126
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 127
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

What is claimed is:

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.

3. The method of claim 2, wherein said second message is generated a predetermined amount of time after said first message is generated.

WAVELYNX EX. 1003, Pg. 128
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

WAVELYNX EX. 1003, Pg. 129
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 130
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 131
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

WAVELYNX EX. 1003, Pg. 132
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 133
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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

WAVELYNX EX. 1003, Pg. 134
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

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.

WAVELYNX EX. 1003, Pg. 135
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

WAVELYNX EX. 1003, Pg. 136
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 137
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 138
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

58. The device of claim 46, wherein said upstream device comprises a reader and wherein a credential comprises said code generator.

Assa Abloy Identification Technology Group AB 29 August 2006

WAVELYNX EX. 1003, Pg. 139
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

2006203768 29 Aug 2006

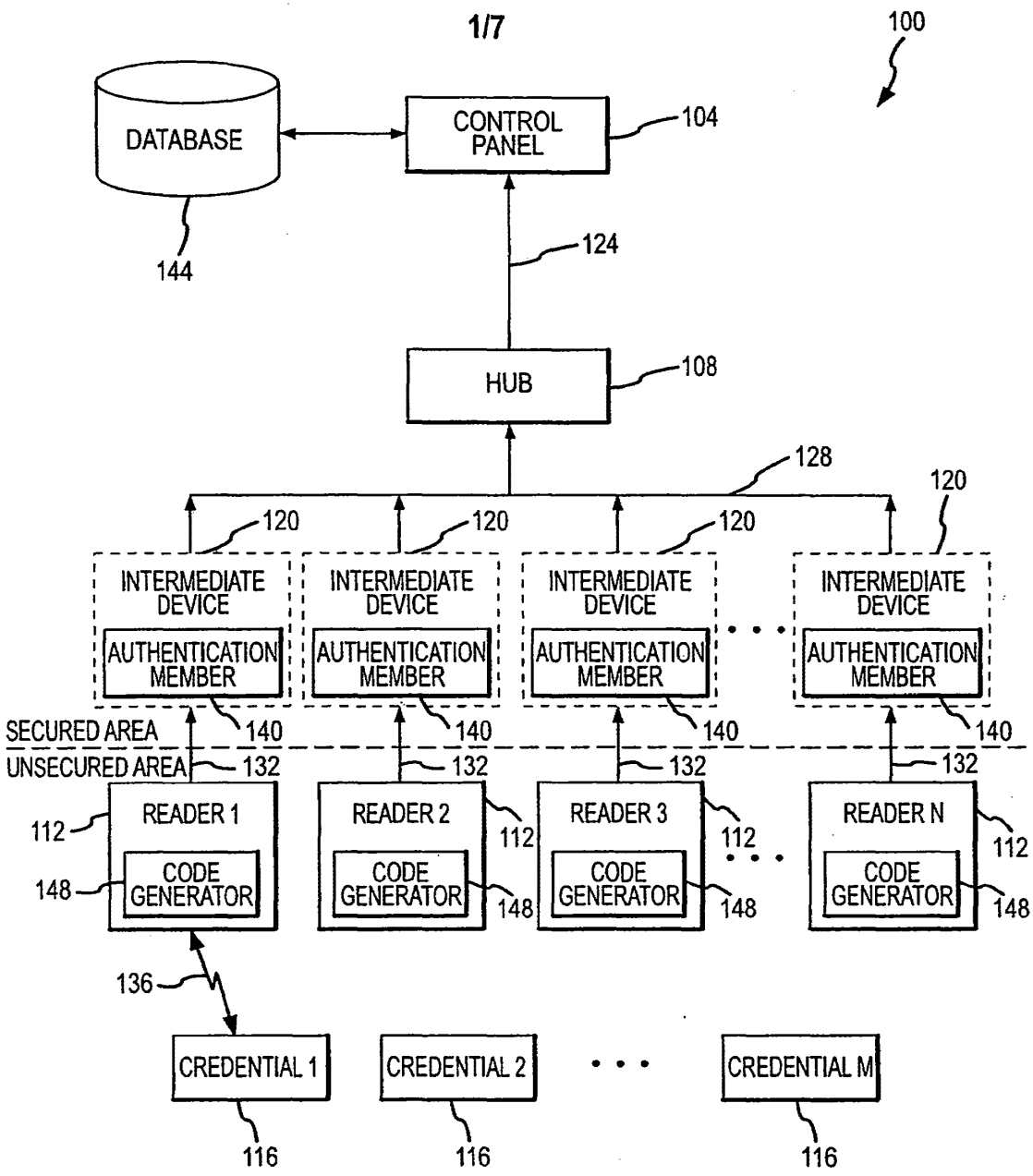


FIG.1

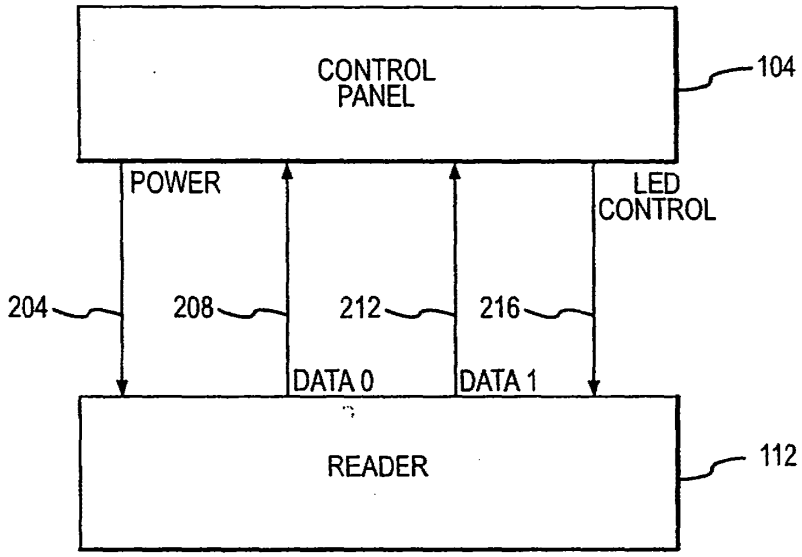


FIG.2
PRIOR ART

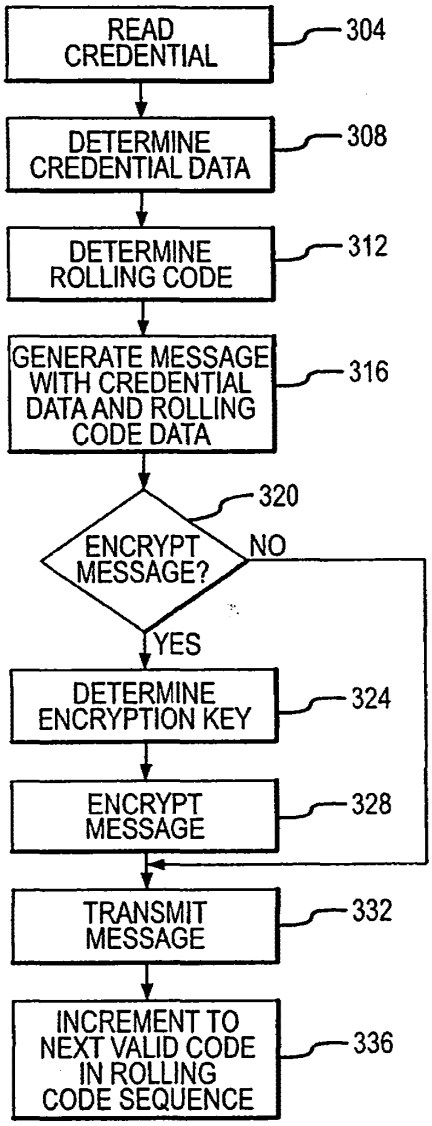

READ CREDENTIAL
304
DETERMINE CREDENTIAL DATA
308
DETERMINE ROLLING CODE
312
GENERATE MESSAGE WITH CREDENTIAL DATA AND ROLLING CODE DATA
316
320
ENCRYPT MESSAGE?
NO
YES
DETERMINE ENCRYPTION KEY
324
ENCRYPT MESSAGE
328
TRANSMIT MESSAGE
332
INCREMENT TO NEXT VALID CODE IN ROLLING CODE SEQUENCE
336

FIG.3

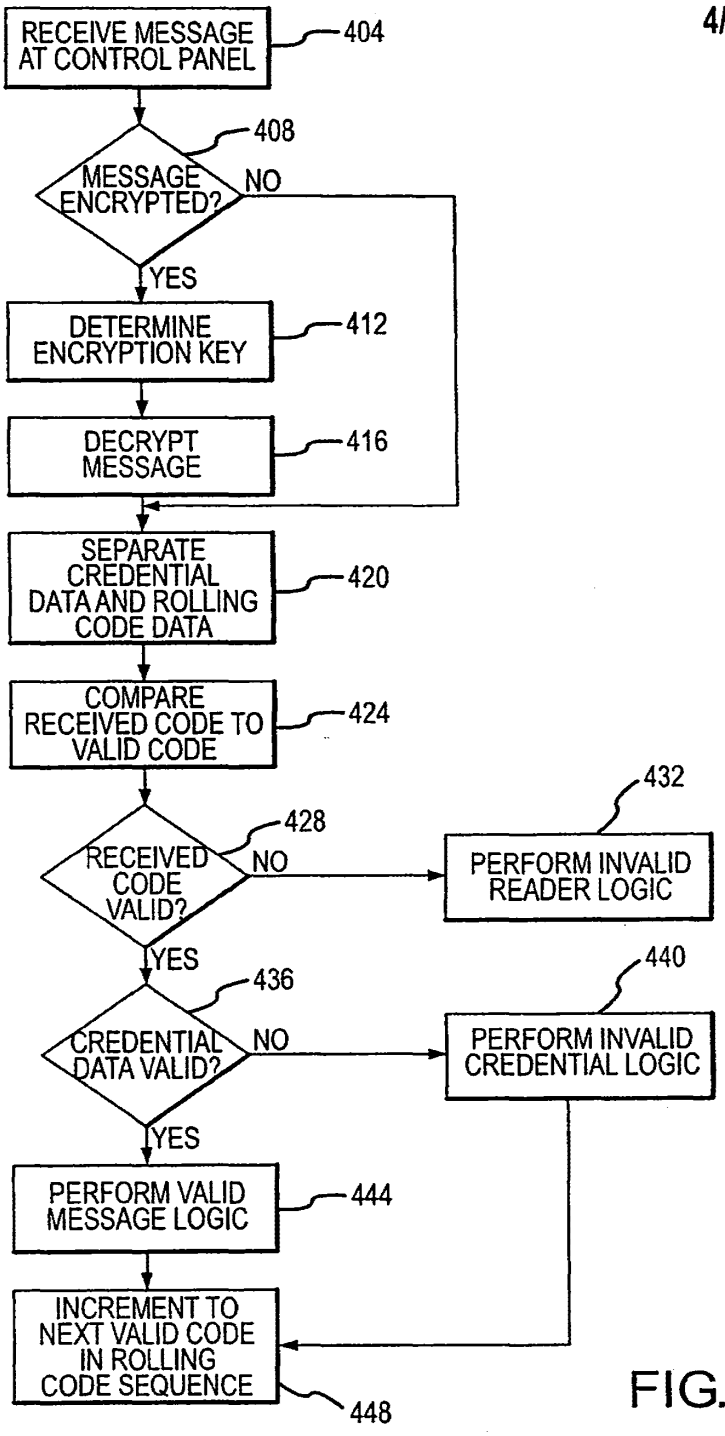

RECEIVE MESSAGE AT CONTROL PANEL
404
MESSAGE ENCRYPTED?
408
NO
YES
DETERMINE ENCRYPTION KEY
412
DECRYPT MESSAGE
416
SEPARATE CREDENTIAL DATA AND ROLLING CODE DATA
420
COMPARE RECEIVED CODE TO VALID CODE
424
RECEIVED CODE VALID?
428
NO
PERFORM INVALID READER LOGIC
432
YES
CREDENTIAL DATA VALID?
436
NO
PERFORM INVALID CREDENTIAL LOGIC
440
YES
PERFORM VALID MESSAGE LOGIC
444
INCREMENT TO NEXT VALID CODE IN ROLLING CODE SEQUENCE
448

FIG.4

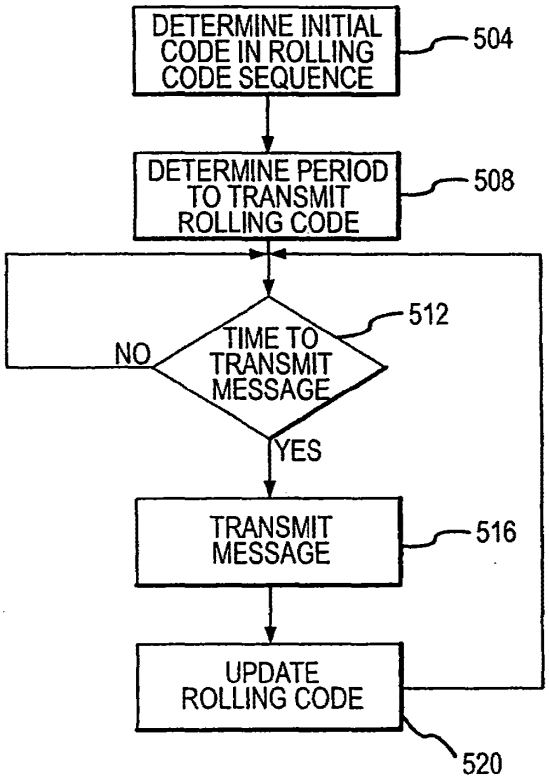

DETERMINE INITIAL CODE IN ROLLING CODE SEQUENCE
504
DETERMINE PERIOD TO TRANSMIT ROLLING CODE
508
TIME TO TRANSMIT MESSAGE
512
NO
YES
TRANSMIT MESSAGE
516
UPDATE ROLLING CODE
520

FIG.5

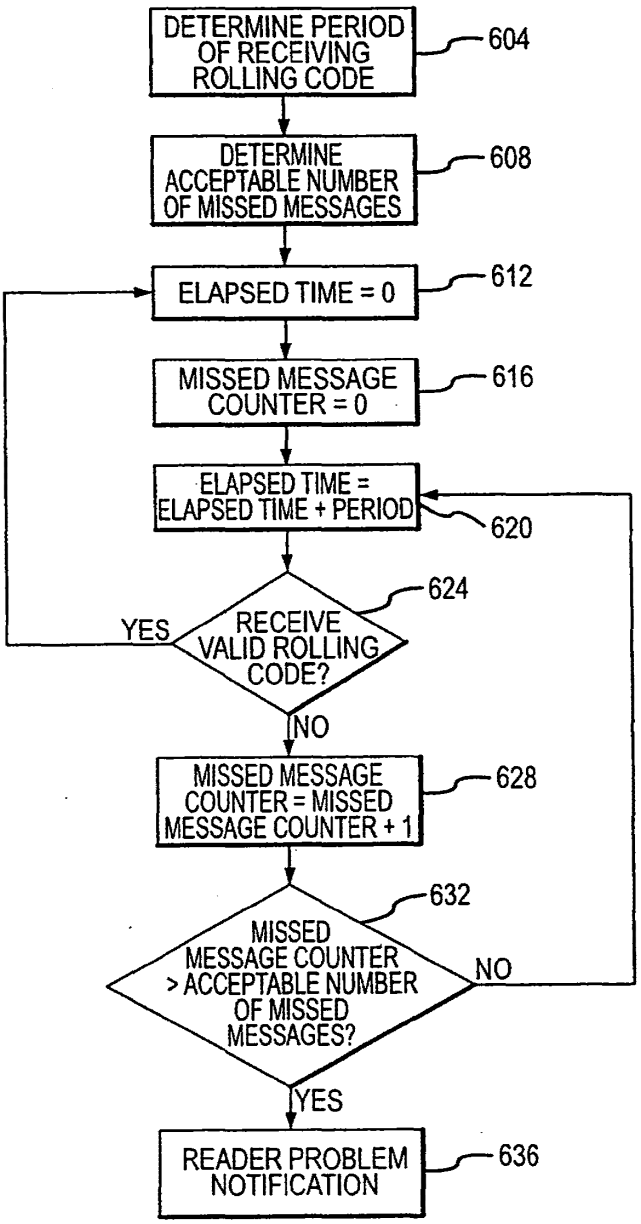
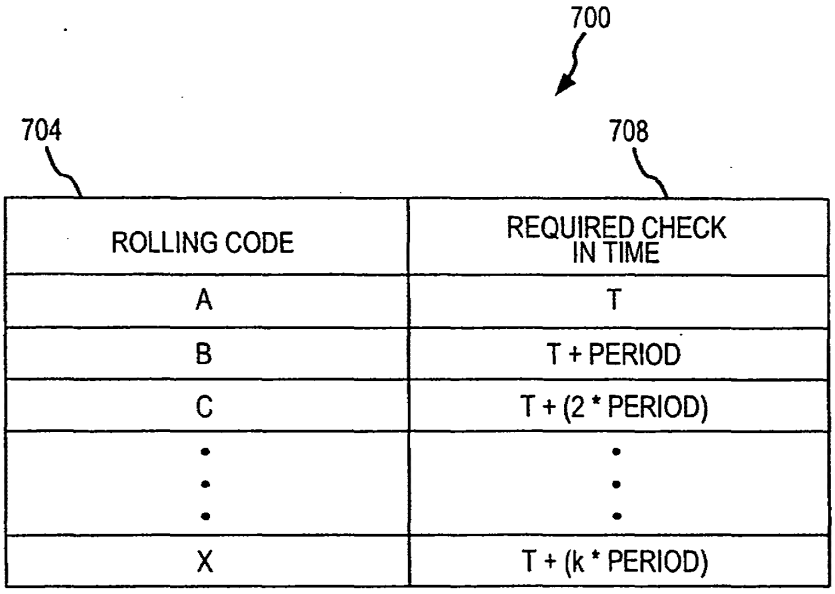

DETERMINE PERIOD OF RECEIVING ROLLING CODE
604
DETERMINE ACCEPTABLE NUMBER OF MISSED MESSAGES
608
ELAPSED TIME = 0
612
MISSED MESSAGE COUNTER = 0
616
ELAPSED TIME = ELAPSED TIME + PERIOD
620
RECEIVE VALID ROLLING CODE?
624
YES
NO
MISSED MESSAGE COUNTER = MISSED MESSAGE COUNTER + 1
628
MISSED MESSAGE COUNTER > ACCEPTABLE NUMBER OF MISSED MESSAGES?
632
NO
YES
READER PROBLEM NOTIFICATION
636

FIG.6



ROLLING CODE	REQUIRED CHECK IN TIME
A	T
B	T + PERIOD
C	T + (2 * PERIOD)
•	•
•	•
•	•
X	T + (k * PERIOD)

FIG.7

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2556843 A1 2007/02/28

(21) 2 556 843

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2006/08/22

(41) Mise à la disp. pub./Open to Public Insp.: 2007/02/28

(30) Priorités/Priorities: 2005/08/31 (US60/713,528); 2006/08/16 (US11/464,912)

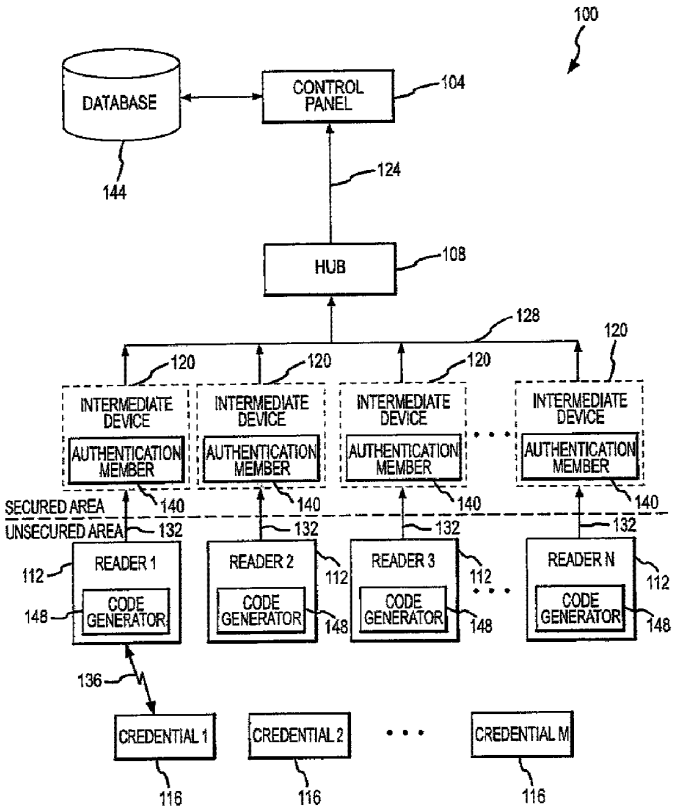
(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01)

(71) Demandeur/Applicant:
ASSA ABLOY IDENTIFICATION TECHNOLOGY GROUP AB, SE

(72) Inventeurs/Inventors:
DAVIS, MICHAEL L., US;
HULUSI, TAM, US

(74) Agent: MBM & CO.

(54) Titre : AUTHENTIFICATION DE DISPOSITIF PAR PROTOCOLE UNIDIRECTIONNEL
(54) Title: DEVICE AUTHENTICATION USING A UNIDIRECTIONAL PROTOCOL



(57) Abrégé/Abstract:
The present invention is directed toward secure access systems. Specifically, a method and system is provided that allows a control panel of a secure access system to verify the authenticity and fidelity of a reader within the secure access system by utilizing a rolling code agreed upon by the reader and the control panel.

WAVELYNX EX. 1003, Pg. 147
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ABSTRACT

The present invention is directed toward secure access systems. Specifically, a method and system is provided that allows a control panel of a secure access system to verify the authenticity and fidelity of a reader within the secure access system by utilizing a rolling code agreed upon by the reader and the control panel.

WAVELYNX EX. 1003, Pg. 148
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

DEVICE AUTHENTICATION USING A UNIDIRECTIONAL PROTOCOL

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

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

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.

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

WAVELYNX EX. 1003, Pg. 149
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

physical reader into a single unit that makes the access decision. This type of device is sometimes referred to as a stand-alone reader.

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 150
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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

WAVELYNX EX. 1003, Pg. 151
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

modern protocol that provides for reader authentication.

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 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.

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.

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.

WAVELYNX EX. 1003, Pg. 152
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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

The present invention is generally directed toward a method, apparatus, and

WAVELYNX EX. 1003, Pg. 153
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 154
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 155
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 156
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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

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.

WAVELYNX EX. 1003, Pg. 157
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

DETAILED DESCRIPTION

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).

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 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.

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

WAVELYNX EX. 1003, Pg. 158
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 159
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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 algorithm(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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 160
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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.

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.

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

WAVELYNX EX. 1003, Pg. 161
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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,

WAVELYNX EX. 1003, Pg. 162
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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

WAVELYNX EX. 1003, Pg. 163
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

Referring now to Fig. 3 a method of generating a signal for transmission to an

WAVELYNX EX. 1003, Pg. 164
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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 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.

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 pseudo-

WAVELYNX EX. 1003, Pg. 165
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

random 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.

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.

Of course different algorithms may be used in a similar fashion. The code

WAVELYNX EX. 1003, Pg. 166
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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

WAVELYNX EX. 1003, Pg. 167
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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 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.

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.

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

WAVELYNX EX. 1003, Pg. 168
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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,

WAVELYNX EX. 1003, Pg. 169
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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

WAVELYNX EX. 1003, Pg. 170
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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).

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 frequency of update may be required.

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.

Referring now to Fig. 6 a method of ensuring that a downstream device is updated

WAVELYNX EX. 1003, Pg. 171
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

WAVELYNX EX. 1003, Pg. 172
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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).

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

WAVELYNX EX. 1003, Pg. 173
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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 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

WAVELYNX EX. 1003, Pg. 174
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

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 of 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

WAVELYNX EX. 1003, Pg. 175
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

120, and/or a credential 116.

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.

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.

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

WAVELYNX EX. 1003, Pg. 176
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 177
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

What is claimed is:

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.

3. The method of claim 2, wherein said second message is generated a predetermined amount of time after said first message is generated.

WAVELYNX EX. 1003, Pg. 178
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 179
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 180
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 181
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 182
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

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.

WAVELYNX EX. 1003, Pg. 183
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 184
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 185
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 186
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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. 187
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.

WAVELYNX EX. 1003, Pg. 188
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 189
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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.

WAVELYNX EX. 1003, Pg. 190
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

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. 191
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

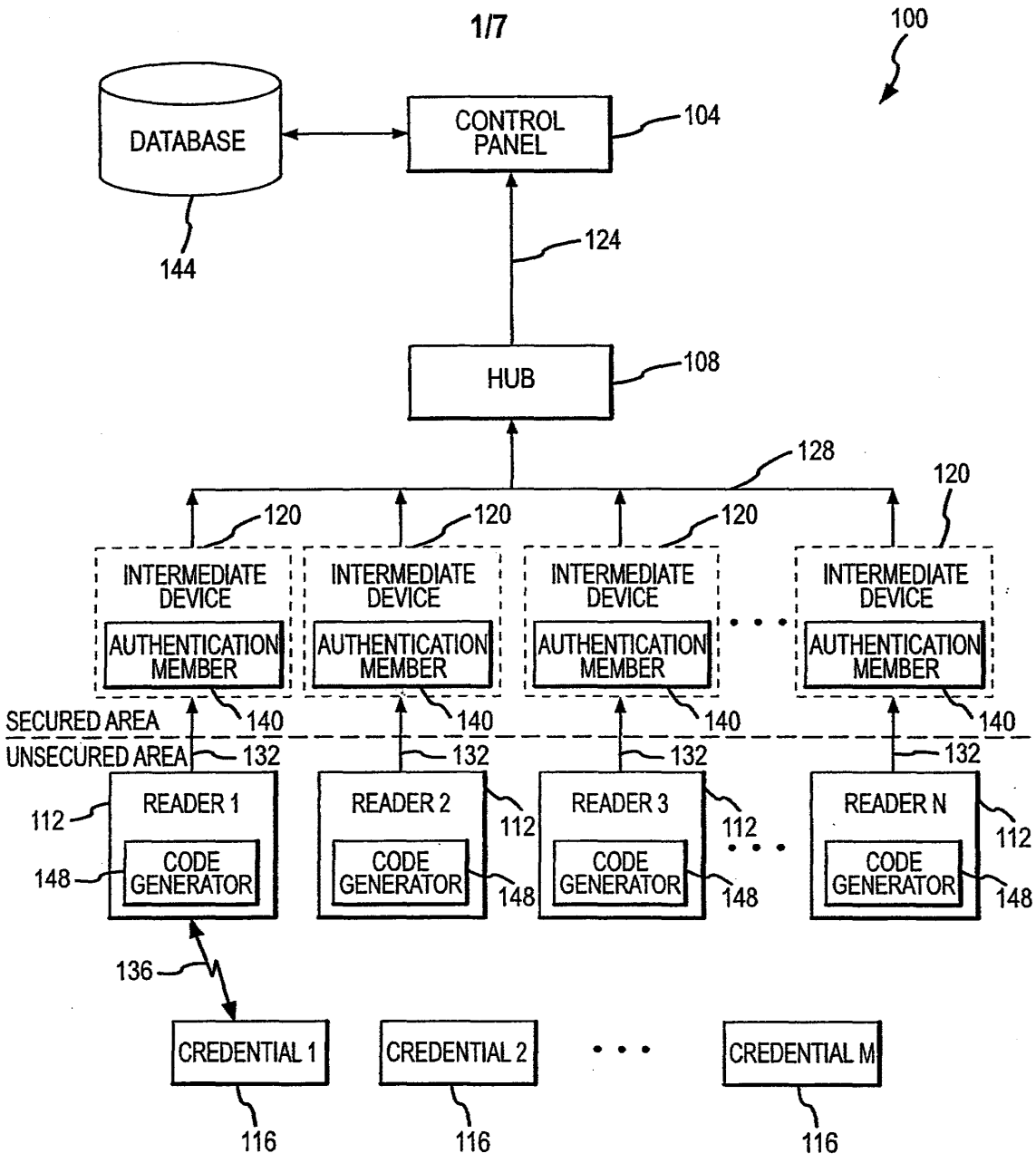

100
DATABASE
CONTROL PANEL
104
144
124
HUB
108
128
120
120
120
120
120
INTERMEDIATE DEVICE
AUTHENTICATION MEMBER
140
SECURED AREA
UNSECURED AREA
132
READER 1
READER 2
READER 3
READER N
112
CODE GENERATOR
148
136
CREDENTIAL 1
CREDENTIAL 2
CREDENTIAL M
116

FIG.1

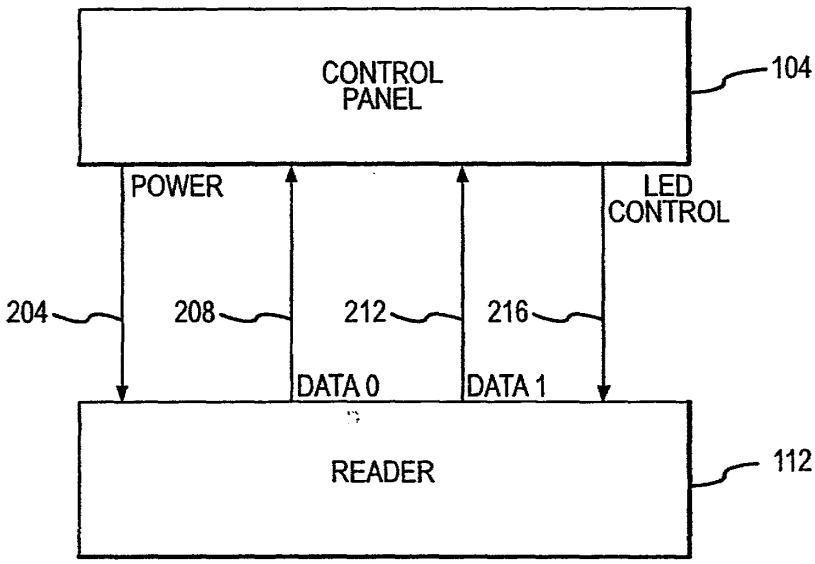


FIG.2
PRIOR ART

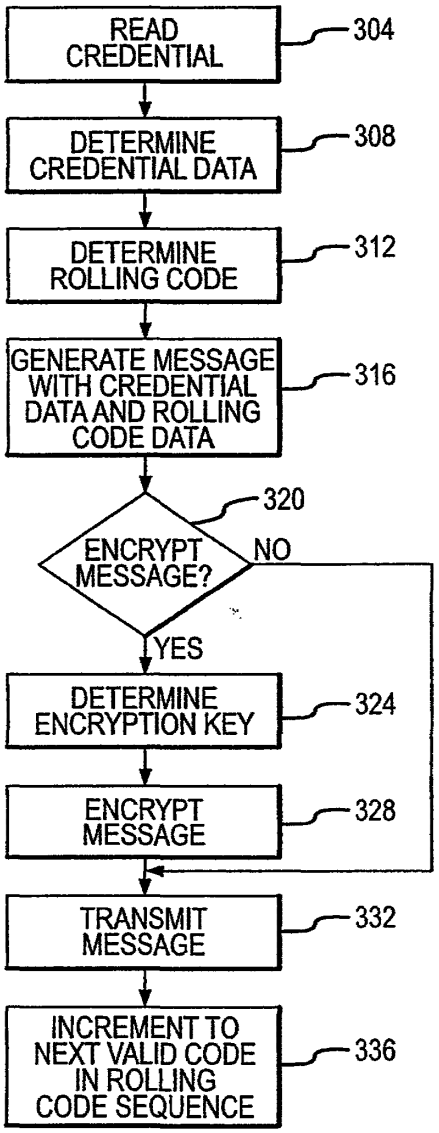

READ CREDENTIAL
304
DETERMINE CREDENTIAL DATA
308
DETERMINE ROLLING CODE
312
GENERATE MESSAGE WITH CREDENTIAL DATA AND ROLLING CODE DATA
316
320
ENCRYPT MESSAGE?
NO
YES
DETERMINE ENCRYPTION KEY
324
ENCRYPT MESSAGE
328
TRANSMIT MESSAGE
332
INCREMENT TO NEXT VALID CODE IN ROLLING CODE SEQUENCE
336

FIG.3

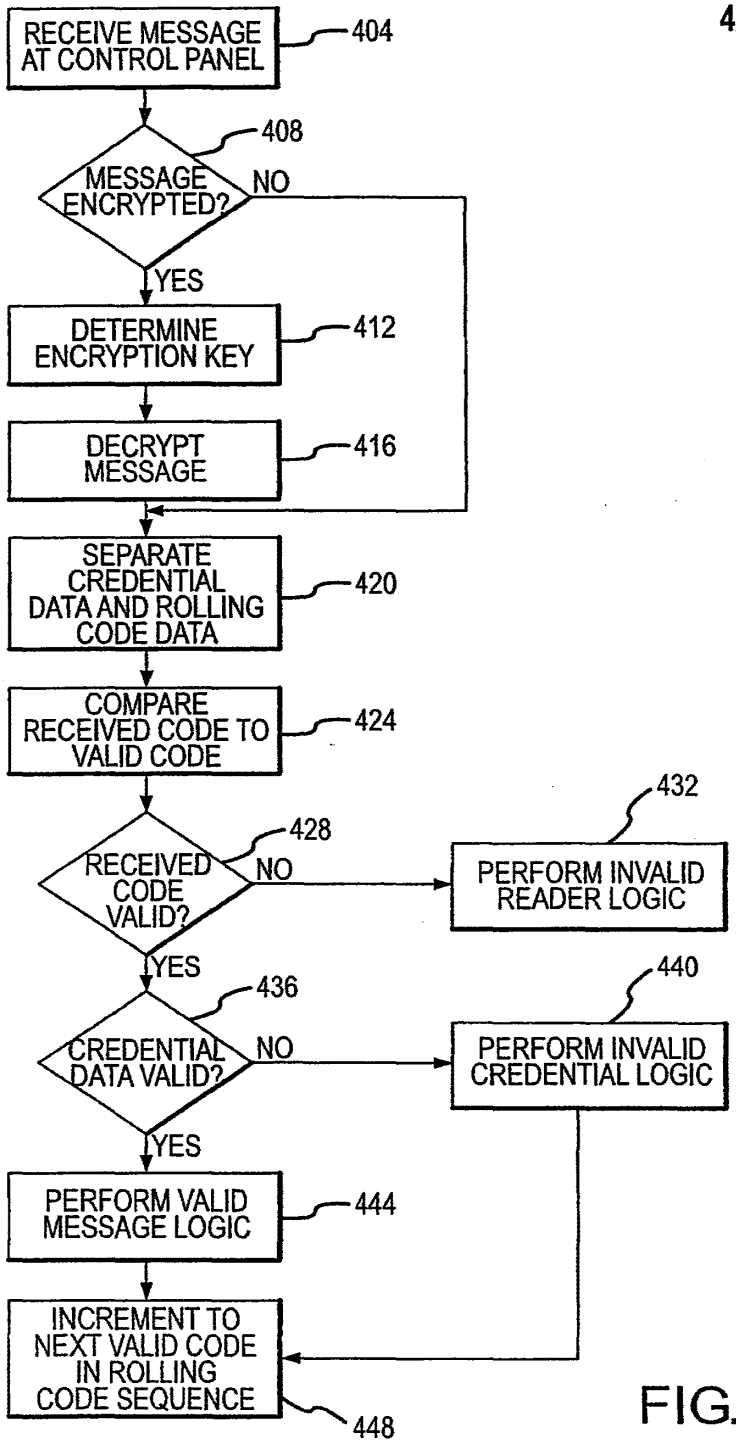

RECEIVE MESSAGE AT CONTROL PANEL
404
408
MESSAGE ENCRYPTED?
NO
YES
DETERMINE ENCRYPTION KEY
412
DECRYPT MESSAGE
416
SEPARATE CREDENTIAL DATA AND ROLLING CODE DATA
420
COMPARE RECEIVED CODE TO VALID CODE
424
428
RECEIVED CODE VALID?
NO
432
PERFORM INVALID READER LOGIC
YES
436
CREDENTIAL DATA VALID?
NO
440
PERFORM INVALID CREDENTIAL LOGIC
YES
PERFORM VALID MESSAGE LOGIC
444
INCREMENT TO NEXT VALID CODE IN ROLLING CODE SEQUENCE
448

FIG.4

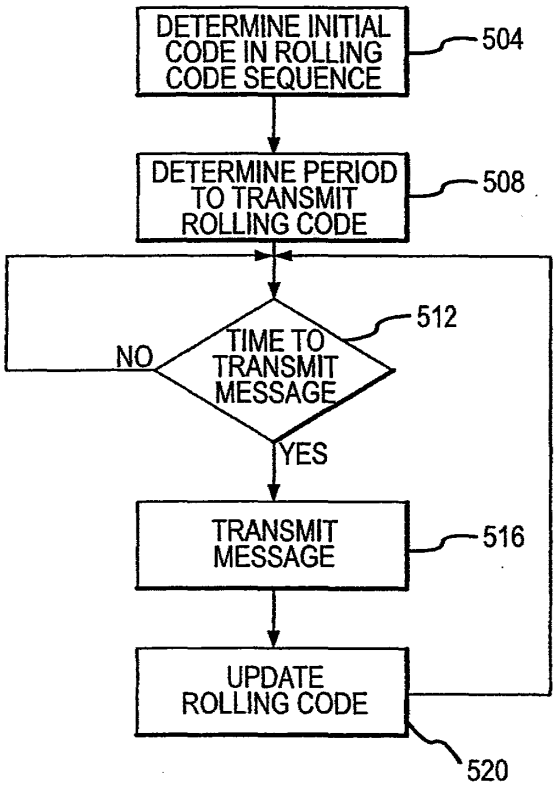

DETERMINE INITIAL CODE IN ROLLING CODE SEQUENCE
504
DETERMINE PERIOD TO TRANSMIT ROLLING CODE
508
TIME TO TRANSMIT MESSAGE
512
NO
YES
TRANSMIT MESSAGE
516
UPDATE ROLLING CODE
520

FIG.5

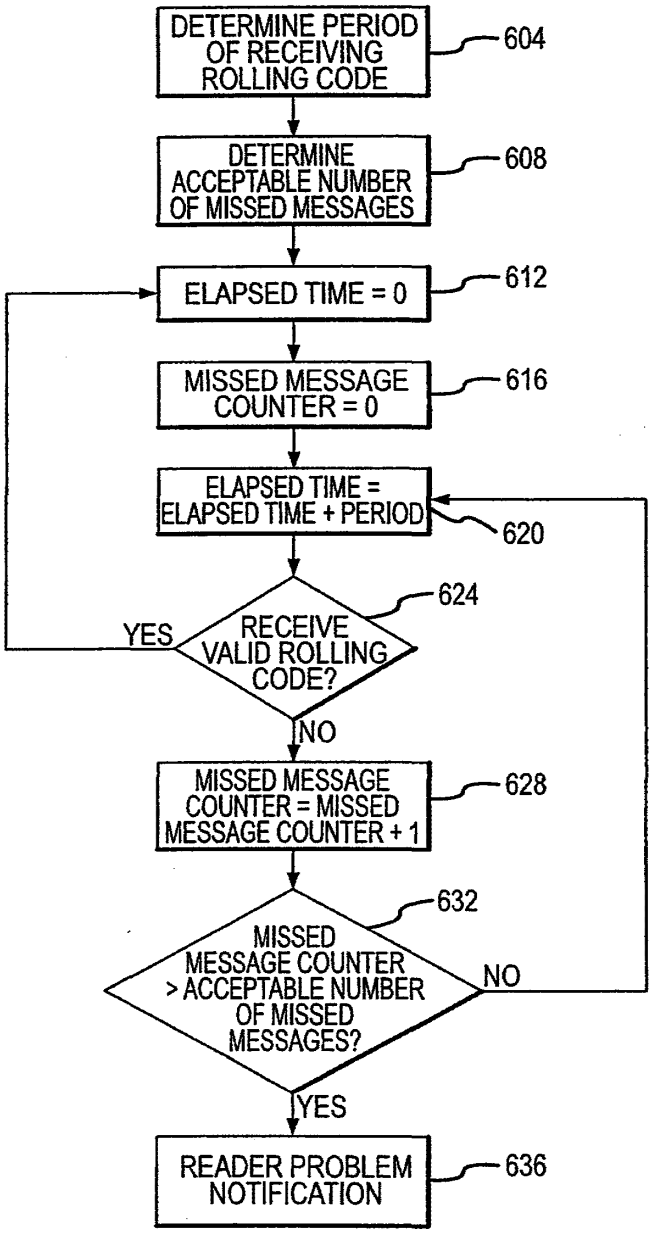
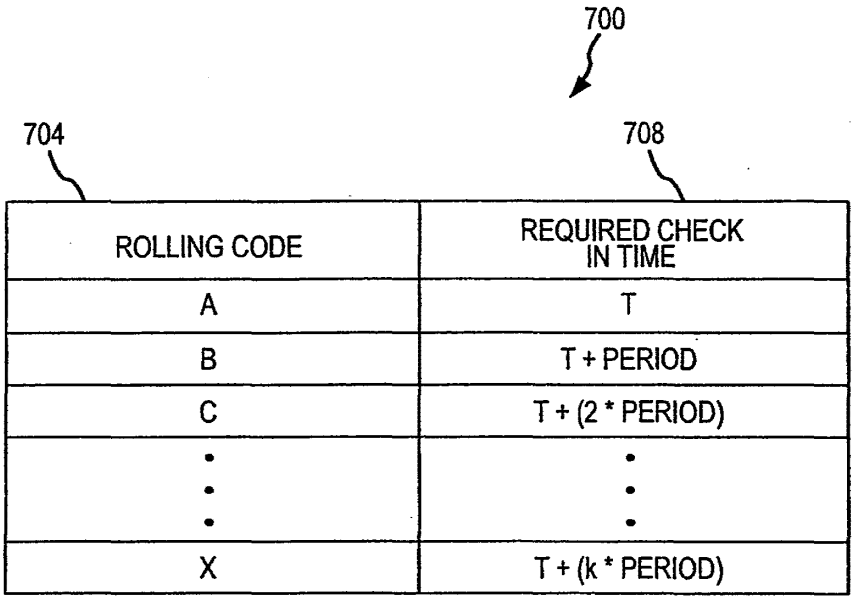
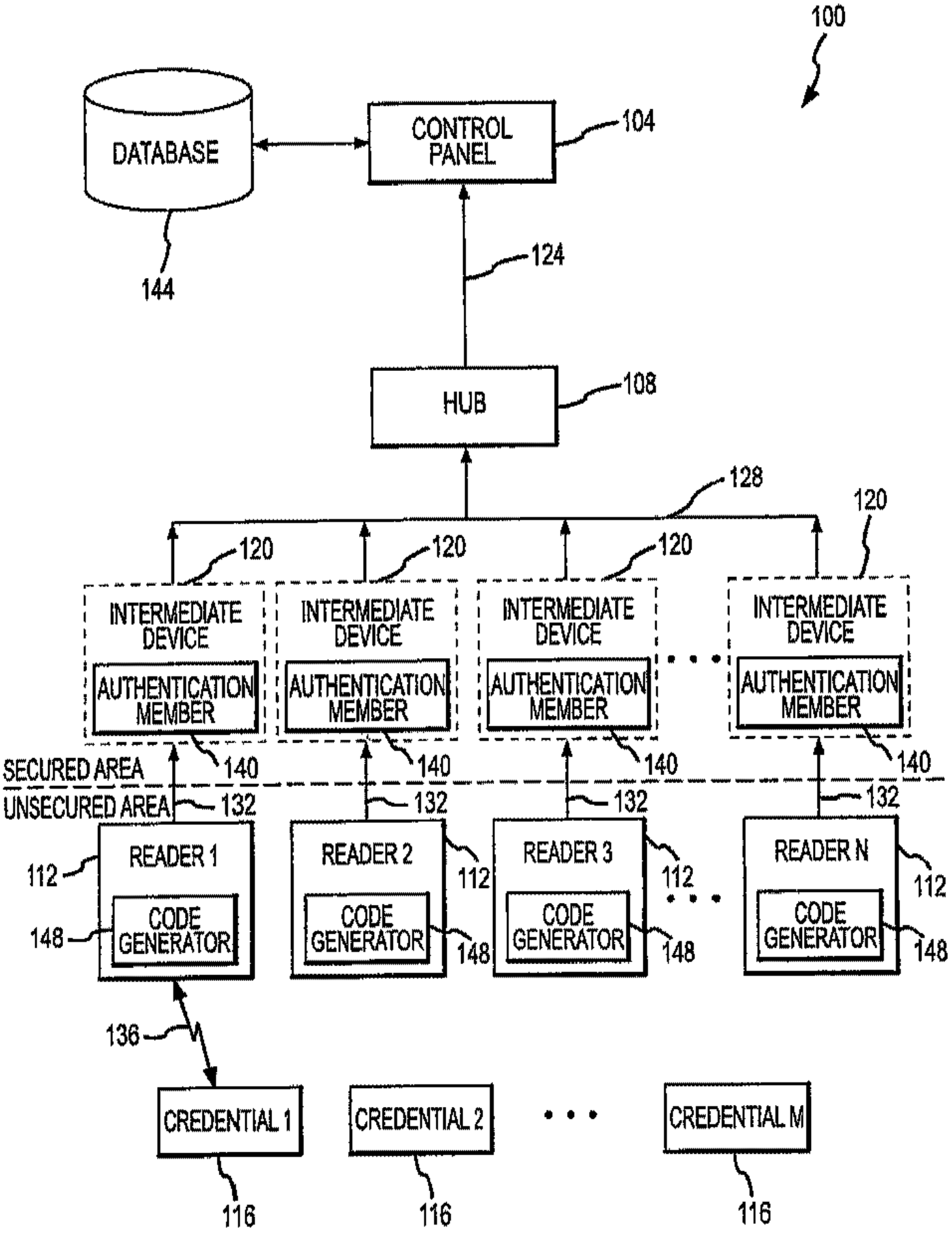

DETERMINE PERIOD OF RECEIVING ROLLING CODE
604
DETERMINE ACCEPTABLE NUMBER OF MISSED MESSAGES
608
ELAPSED TIME = 0
612
MISSED MESSAGE COUNTER = 0
616
ELAPSED TIME = ELAPSED TIME + PERIOD
620
RECEIVE VALID ROLLING CODE?
624
YES
NO
MISSED MESSAGE COUNTER = MISSED MESSAGE COUNTER + 1
628
MISSED MESSAGE COUNTER > ACCEPTABLE NUMBER OF MISSED MESSAGES?
632
NO
YES
READER PROBLEM NOTIFICATION
636

FIG.6



ROLLING CODE	REQUIRED CHECK IN TIME
A	T
B	T + PERIOD
C	T + (2 * PERIOD)
• • •	• • •
X	T + (k * PERIOD)

FIG.7


100
DATABASE
CONTROL PANEL
104
144
124
HUB
108
128
120
120
120
120
120
INTERMEDIATE DEVICE
AUTHENTICATION MEMBER
INTERMEDIATE DEVICE
AUTHENTICATION MEMBER
INTERMEDIATE DEVICE
AUTHENTICATION MEMBER
INTERMEDIATE DEVICE
AUTHENTICATION MEMBER
140
140
140
140
SECURED AREA
UNSECURED AREA
132
132
132
132
READER 1
READER 2
READER 3
READER N
112
112
112
112
CODE GENERATOR
CODE GENERATOR
CODE GENERATOR
CODE GENERATOR
148
148
148
148
136
CREDENTIAL 1
CREDENTIAL 2
CREDENTIAL M
116
116
116

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Februar 2001 (22.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/13218 A1

(51) Internationale Patentklassifikation[7]: G06F 7/58, H04L 9/32 // G06F 7/72

(21) Internationales Aktenzeichen: PCT/DE00/02776

(22) Internationales Anmeldedatum:
16. August 2000 (16.08.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 39 059.2 18. August 1999 (18.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HESS, Erwin** [DE/DE]; Gottfried-Keller-Strasse 36, D-85521 Ottobrunn (DE). **SERF, Pascale** [DE/DE]; Max-Löw-Strasse 61, D-85579 Neubiberg (DE).

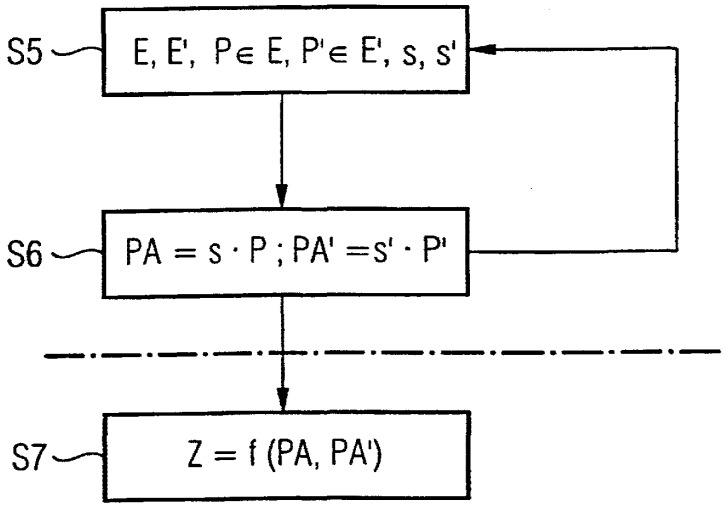
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, D-80506 München (DE).

(81) Bestimmungsstaaten *(national)*: CA, JP, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GENERATING PSEUDO RANDOM NUMBERS AND METHOD FOR ELECTRONIC SIGNATURES

(54) Bezeichnung: VERFAHREN ZUM ERZEUGEN VON PSEUDOZUFALLSZAHLEN UND VERFAHREN FÜR ELEKTRONISCHE SIGNATUR



(57) Abstract: The invention relates to a method for generating pseudo random numbers and a method for electronic signatures. According to the inventive method for generating pseudo random numbers, points are determined on at least two different elliptical curves. A pseudo random number is produced respectively by linking the points. The linking of points of different elliptical curves to generate a pseudo random number makes it impossible to deduce the individual elliptical curves on the basis of the pseudo random numbers. The cryptographic security of the inventive method is thus tremendously increased because the computation of discrete logarithms is made impossible.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen, sowie ein Verfahren für elektronische Signatur. Bei dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen werden Punkte auf zumindest zwei verschiedenen elliptischen Kurven bestimmt, und durch Verknüpfen der Punkte wird jeweils eine Pseudozufallszahl erzeugt. Das Verknüpfen der Punkte von unterschiedlichen elliptischen Kurven zu einer Pseudozufallszahl macht Rückschlüsse aus den so erzeugten Pseudozufallszahlen auf die einzelnen elliptischen Kurven unmöglich, wodurch die kryptographische Sicherheit des erfindungsgemäßen Verfahrens erheblich erhöht wird, weil die Berechnung diskreter Logarithmen unmöglich gemacht wird.

WO 01/13218 A1

WAVELYNX EX. 1003, Pg. 200
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:

- *Mit internationalem Recherchenbericht.*
- *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zum Erzeugen von Pseudozufallszahlen und Verfahren für elektronische Signatur

Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen und ein Verfahren für elektronische Signatur.

Zufallszahlen werden in der Kryptographie zum Verschlüsseln oder Signieren von Nachrichten benötigt. Im Artikel „Vom diplomatischen Code zur Falltürfunktion" von Otto Leiberich, Spektrum der Wissenschaft, Juni 1999, Seite 26 bis 34 wird ein Überblick über die Entwicklung der Kryptographie in Deutschland gegeben. Hierin ist ein früher verwendetes Wurm- oder Stromchiffrierverfahren beschrieben, bei dem eine sehr lange Zeichenfolge, die keinerlei innere Struktur aufweist, ein sogenannter Zeichenwurm oder Zeichenstrom, Zeichen für Zeichen zu einer zu verschlüsselnden Nachricht, dem Klartext, addiert wird. Sind es Buchstaben, werden sie zunächst nach dem Schema a = 0, b = 1, ..., z = 25 in Zahlen verwandelt. Damit keine größeren Zahlen als 25 entstehen, wird eine Addition modulo 26 durchgeführt. Im Zeitalter der Computer werden die Texte in binäre Zahlen verwandelt und Nullen und Einsen modulo 2 addiert. Der Empfänger subtrahiert vom empfangenen Geheimtext den Zeichenstrom - modulo 26 bzw. 2 - und gewinnt dadurch den Klartext zurück.

Der Zeichenstrom wird mit Hilfe von Zufallszahlengeneratoren erzeugt. Diese beruhten früher auf hochfrequenten Spannungsschwankungen bestimmter Röhren, sogenannter Thyratrons, und später auf radioaktiven Zerfallsereignissen.

Da jedoch die Zeichenströme jeweils parallel vom Sender zum Empfänger sicher übertragen werden müssen, ist ein erheblicher Durchsatz an sicherem Datentransfer notwendig.

WAVELYNX EX. 1003, Pg. 202
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Man hat deshalb Verfahren zum Erzeugen von Pseudozufallszahlen, sogenannte Pseudozufallszahlengeneratoren, entwikkelt, die in Abhängigkeit von einem Schlüssel eine im wesentlichen beliebig lange Folge von Pseudozufallszahlen erzeugen können. Hierdurch mußte bei obigem Codierverfahren lediglich ein Schlüssel zwischen den Kommunikationspartnern geheim übermittelt werden, was wesentlich einfacher handhabbar ist, als jeweils einen kompletten Zeichenstrom zu übermitteln.

Für heutige offene Netze, insbesondere das Internet, sind Verfahren entwickelt worden, bei denen zwei Kommunikationspartner, die zum ersten Mal miteinander kommunizieren wollen, sich verschlüsselte Nachrichten übersenden können. Diese Verfahren sind sogenannte asymmetrische Schlüsselverfahren, die auch als Public-Key-Verfahren bezeichnet werden, bei welchen der Empfänger seinen Schlüssel, den sogenannten Public Key, veröffentlicht.

Eines der bekanntesten Verfahren dieses Typs ist das sogenannte RSA-Verfahren, bei dem Teile der Schlüssel, die sogenannten Schlüsselmoduln, Produkte zweier großer Primzahlen sind. Der Sender der Nachricht kennt lediglich den Schlüsselmodul, also das Produkt, und kann mit diesem nach einer bestimmten mathematischen Funktion die Nachricht verschlüsseln. Zur Entschlüsselung der Nachricht genügt jedoch nicht die Kenntnis des Produktes, sondern man benötigt die beiden Primzahlen. Mit Hilfe dieser Primzahlen und einer entsprechenden Umkehrfunktion kann nur der richtige Empfänger, der den Schlüssel erzeugt hat, die verschlüsselte Nachricht entschlüsseln.

Die Zerlegung des Schlüsselmoduls in seine Teiler, die beiden Primzahlen, ist bei großen Moduln mit normalem Rechenaufwand praktisch nicht möglich. In „Faktorisierung großer Zahlen" von Johannes Buchmann, Spektrum der Wissenschaft, September 1996, Seite 80 - 88 ist das Problem der Zerlegung großer Zahlen in ihre Primzahlen ausführlich beschrieben und der Auf-

wand zur Zerlegung einer 129stelligen Zahl dargelegt. Diese Zahl wurde mit Hilfe von 600 Freiwilligen, die ihre Computer zur Verfügung gestellt haben, in die einzelnen Primzahlen zerlegt.

Nachteilig an dem RSA-Verfahren ist, daß es zu langsam für die Nachrichtenverschlüsselung ist, da zur Gewährleistung einer ausreichenden Sicherheit sehr große Zahlen - ungefähr 1000 Binär- oder 300 Dezimalstellen - verwendet werden müssen. Es sind derart große Zahlen mit anderen gleicher Größenordnung zu potenzieren, was zur Verschlüsselung von zu übertragenden Daten nicht schnell genug erfolgen kann. Das RSA-Verfahren wird deshalb lediglich zur verschlüsselten Übertragung von geheimzuhaltenden Schlüsseln für ein herkömmliches Verfahren verwendet, das dann die eigentliche Verschlüsselung vollzieht.

Als Alternative zu dem RSA-Verfahren sind Verfahren auf Grundlage von elliptischen Kurven entwickelt worden. Für die Kryptographie sind lediglich elliptische Kurven über endlichen Körpern relevant. Diese elliptischen Kurven über endlichen Körpern bilden Punktgruppen, in denen eine Addition und eine Multiplikation definiert sind, die mit der landläufigen Addition und Multiplikation nichts gemeinsam haben als die Rechenregeln. Die Multiplikation auf einer elliptischen Kurve über einem endlichen Körper ist eine Einwegfunktion, das heißt, daß die Umkehrung - die Berechnung sogenannter diskreter Logarithmen - im Normalfall rechentechnisch undurchführbar ist, wohingegen die Multiplikation sehr einfach und schnell ausgeführt werden kann. Diese Tatsache wird bei den auf elliptischen Kurven basierenden kryptographischen Verfahren ausgenutzt, indem der Empfänger sich eine Zufallszahl t wählt und auf Grundlage dieser Zufallszahl t und einer Multiplikation mit t auf der elliptischen Kurve einen Kurvenpunkt T bestimmt. Der Kurvenpunkt T wird als Schlüssel veröffentlicht, wohingegen die Zufallszahl t vom Empfänger geheimgehalten wird. Ein Sender kann mit Hilfe des Kurvenpunktes T

seine Nachricht verschlüsseln, die dann lediglich der Empfänger, der die dem Kurvenpunkt T zugrundeliegende Zufallszahl t kennt, entschlüsseln kann.

Solche auf elliptischen Kurven basierende Verfahren benötigen bei gleicher Sicherheit wie das RSA-Verfahren wesentlich weniger Rechenleistung. Derartige Verfahren können in Kleinstrechnern implementiert werden, wie z.B. in Chipkarten. Die Siemens AG vertreibt eine Chipkarte mit der Markenbezeichnung SLE44CR80S, in der ein Signaturverfahren auf der Basis elliptischer Kurven implementiert ist.

Zur Erzeugung der Schlüssel, des öffentlichen Schlüssels, den der Empfänger veröffentlicht, und seines entsprechenden privaten Schlüssels, werden wiederum Zufallszahlen benötigt.

Der Erfindung liegt deshalb die Aufgabe zugrunde, auf Basis elliptischer Kurven ein Verfahren zum Erzeugen von Pseudozufallszahlen zu schaffen, das einfach und schnell ausführbar ist und mit dem eine große Menge qualitativ hochwertiger Zufallszahlen erzeugt werden kann.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1 gelöst.

Ferner liegt der Erfindung die Aufgabe zugrunde, ein Verfahren für elektronische Signatur auf Basis elliptischer Kurven sowie eine entsprechende Vorrichtung zu schaffen, die weniger Speicherplatz als bekannte Verfahren und Vorrichtungen für elektronische Signatur auf Grundlage elliptischer Kurven benötigen und auf kleinen Rechensystemen, insbesondere Chipkarten, implementiert werden können.

Die Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 11 und eine Vorrichtung mit den Merkmalen des Anspruchs 12 gelöst.

WAVELYNX EX. 1003, Pg. 205
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

Beim erfindungsgemäßen Verfahren nach Anspruch 1 zum Erzeugen von Pseudozufallszahlen werden Paare von Punkten bestimmt, die auf zumindest zwei unterschiedlichen elliptischen Kurven über einem endlichen Körper liegen, und in Abhängigkeit von jeweils einem solchen Paar von Punkten wird eine Zufallszahl ermittelt.

Da erfindungsgemäß zwei verschiedene elliptische Kurven benutzt werden, und die Pseudozufallszahl aus einem Paar von Punkten abgeleitet wird, wobei die beiden Punkte des Paares auf unterschiedlichen elliptischen Kurven liegen, ist es unmöglich, aus den derart ermittelten Pseudozufallszahlen auf die Kurvenpunkte zurückzuschließen. Bei Verwendung lediglich einer einzigen elliptischen Kurve zum Ableiten von Pseudozufallszahlen könnte durch Berechnen diskreter Logarithmen aus den Pseudozufallszahlen auf die Kurvenpunkte zurückgeschlossen werden. Hierdurch wäre es möglich, daß Dritte die Rechenregel der Pseudozufallszahlen bestimmen könnten und die weiteren Pseudozufallszahlen voraussagen könnten. Dies würde ein erhebliches Sicherheitsrisiko darstellen, das mit der vorliegenden Erfindung vermieden wird.

Das erfindungsgemäße Verfahren für elektronische Signatur kombiniert ein an sich bekanntes Signaturverfahren mit dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen. Die gleichen Routinen bzw. Einrichtungen können sowohl beim Signaturverfahren als auch bei der Erzeugung der Zufallszahlen verwendet werden, wodurch erheblich Programmcode und Speicherplatz eingespart werden kann. Zudem wirkt sich eine Optimierung der EC(=elliptic curve)-Arithmetik sowohl bei der Erzeugung der Pseudozufallszahlen als auch bei der unmittelbaren Ausführung des Signaturverfahrens vorteilhaft aus. Durch diese doppelte Verwendung der

Routinen und Einrichtungen auf Basis elliptischer Kurven werden somit Synergieeffekte erzielt.

Ferner sind die erfindungsgemäß erzeugten Pseudozufallszahlen nicht von Zufallszahlen eines echten Zufallsgenerators zu unterscheiden und können mit relativ geringem Rechenaufwand erzeugt werden.

Die Erfindung wird nachfolgend beispielhaft anhand der Zeichnungen näher erläutert. In denen zeigen schematisch:

Fig. 1 eine elliptische Kurve über den reellen Zahlen,

Fig. 2 eine elliptische Kurve über einem endlichen Körper,

Fig. 3 die Addition zweier Punkte einer elliptischen Kurve über den reellen Zahlen,

Fig. 4 die Punkte der elliptischen Kurve $y^2=x^3+2x+9$ über dem Körper mod 13, die eine zyklische Gruppe mit 17 Punkten bilden,

Fig. 5 den Verfahrensablauf eines Ausführungsbeispiels der Erfindung in einem Flußdiagramm,

Fig. 6 das Grundprinzip des erfindungsgemäßen Verfahrens zum Erzeugen von Pseudozufallszahlen in einem Flußdiagramm, und

Fig. 7 den Aufbau eines Programmes zum Ausführen eines erfindungsgemäßen Signaturverfahrens.

Zunächst werden kurz die mathematischen Grundlagen zum Rechnen auf elliptischen Kurven erläutert. Eine elliptische Kurve E über einem Körper K ist eine Kurve, die durch eine kubische Gleichung der Form:

WAVELYNX EX. 1003, Pg. 207
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$y^2=x^3+ax+b$,

beschrieben werden kann mit a und b aus K, $4a^3+27b^2 \neq 0$. Paare (x, y) aus K x K, welche die Gleichung erfüllen, sowie das formale Paar (∞,∞) nennt man Punkte der Kurve E über K.

Eine elliptische Kurve über den reellen Zahlen ist in Fig. 1 gezeigt. Man beachte, daß elliptische Kurven keine Ellipsen sind.

Fig. 2 zeigt eine elliptische Kurve über einem endlichen Körper. Der algebraische Begriff Körper definiert einen „Zahlenbereich", in dem man nach den von den rationalen Zahlen bekannten formalen Rechenregeln addieren, subtrahieren, multiplizieren und dividieren kann. Es gibt unendliche Körper, wie z.B. die rationalen Zahlen, die reellen Zahlen, die komplexen Zahlen, und endliche Körper. Endliche Körper sind z.B. der Körper GF(p) der Zahlen mod p, wobei p eine Primzahl ist, bzw. der Körper $GF(2^n)$ der Binärvektoren der Länge n. („GF" steht für „Galois field", was ein Synonym für „endlicher Körper" ist.) Für die Kryptographie sind nur elliptische Kurven über endlichen Körpern relevant.

Fig. 3 zeigt die Addition zweier Punkte P_1, P_2 auf einer elliptischen Kurve über den reellen Zahlen, wobei sich der Punkt P_3 ergibt. Bei dieser Addition wird die Verbindungsgerade der Punkte P_1 und P_2 gebildet und deren 3. Schnittpunkt mit der elliptischen Kurve ermittelt. Dieser Schnittpunkt wird an der x-Achse gespiegelt und ergibt das Resultat P_3 der Addition von P_1 und P_2.

Diese Addition der Punkte auf elliptischen Kurven kann durch folgende Formeln ausgedrückt werden:

$x_3=r^2-x_1-x_2$, $y_3=r(x_1-x_3)-y_1$ mit
$r=(y_2-y_1)/(x_2-x_1)$, falls $x_1 \neq x_2$
$r=(3x_1^2+a)/2y_1$, falls $P_1=P_2$

wobei x_i, y_i die Koordinaten des Punktes P_i (i=1,2,3) sind.

Diese Formeln gelten auch für elliptische Kurven über endlichen Körpern.

Durch Iteration der Punktaddition wird eine Multiplikation von Kurvenpunkten mit ganzen Zahlen k definiert:

k*P=P+P+...+P (k-fache Summe).

Diese Multiplikation von Kurvenpunkten mit ganzen Zahlen kann leicht und schnell ausgeführt werden, wohingegen die Umkehraufgabe, die Berechnung sogenannter diskreter Logarithmen, normalerweise nur mit außergewöhnlichem Rechenaufwand gelöst werden kann. Hierfür gibt es keinen Algorithmus mit subexponentieller Laufzeit. Diese Punktmultiplikation stellt somit eine Einwegfunktion dar, weshalb sie bei Verfahren mit öffentlichen Schlüsseln, den sogenannten Public-Key-Verfahren, verwendet wird.

Nachfolgend wird anhand eines in Fig. 5 gezeigten Ausführungsbeispieles das erfindungsgemäße Verfahren zum Erzeugen von Pseudozufallszahlen erläutert.

Eine erste elliptische Kurve E über dem Körper GF(p) ist durch die folgende Gleichung gegeben:

$(y^2) \bmod p = (x^3 + 6x +$
$6050679034418465473882149660454552069529384067 71) \bmod p,$
wobei $p = 2^{160}-47=$
1461501637330902918203684832716283019655932542929.
p ist eine Primzahl mit 160 Bits.

Die elliptische Kurve E über GF(p) besitzt als Gruppenordnung
#E(GF(p)) = 7*q mit
q=208785948190128988314812461240940947434505754881.
q ist wiederum eine Primzahl mit 128 Bits.

Die Gruppenordnung einer elliptischen Kurve ist die Anzahl der Elemente der Punktgruppe, also die Anzahl der Lösungen der definierenden Gleichung der elliptischen Kurve E über GF(p). Je größer der maximale Primteiler der Gruppenordnung ist, desto schwieriger ist die Berechnung diskreter Logarithmen. Die Größe der Gruppenordnungen und ihrer maximalen Primteiler stellt somit ein Qualitätsmerkmal des erfindungsgemäßen Verfahrens dar, wobei die Gruppenordnungen vorzugsweise zumindest 2^{100} oder besser 2^{130} betragen sollten.

Eine zweite elliptische Kurve E' über GF(p) ist durch folgende Gleichung gegeben:

$$(y^2) \bmod p = (x^3 + 3x + 168756385740498547400152923318200148712149363991) \bmod p.$$

Die Kurve E' ist isogen zur Kurve E, das heißt, wenn die Kurve E die Form

$$y^2=x^3+ax+b$$

aufweist, besitzt die Kurve E' die Form

$$y^2=x^3+ac^2x+bc^3,$$

mit a, b, c aus GF(p), wobei c ein quadratischer Nichtrest modulo p ist. Im vorliegenden Fall gilt für c:

$$c= 503145425704462245322517599589013227703324936803.$$

Die Verwendung zweier isogener Kurven statt zweier beliebiger Kurven bietet wesentliche Vorteile. So kann man die Ordnung der elliptischen Kurve E' über GF(p) einfach aus der Gruppenordnung von E ableiten, da nämlich die Summe der beiden Ordnungen 2p+2 ist, womit sich folgende Gleichung ergibt:

WAVELYNX EX. 1003, Pg. 210
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

#E'(GF(p)) = 2p+2 - #E(GF(p))

Im vorliegenden Fall ergibt sich für die Gruppenordnung von E':

#E'(GF(p)) = 2p+2 - #E(GF(p)) = 11 * 19 * q'
mit
q'= 458150983489311259624978820296545268736778934 7.

q' ist eine Primzahl mit einer Länge von 152 Bits.

Man wählt nun zwei Punkte P, P' der Kurven E, E', wie z.B.:

P =(27,1199480719563308855489368355308026541006624847440)
P' =(318,767790262932904318810390534329377261151321453045),
und
zwei Startwerte s, s', z.B. s=s'=2.

Durch die Bestimmung der elliptischen Kurven E, E', der Punkte P, P' und der Startwerte s, s' ist der Schritt S1 aus Fig. 5 abgeschlossen. Der Verfahrensablauf geht nun auf den Schritt S2 über, bei dem die Punkte P, P' mit s bzw. s' multipliziert werden, wobei das Ergebnis als PA bzw. PA' bezeichnet wird. Die Multiplikation wird als s-fache bzw. s´-fache Addition gemäß der in Fig. 3 gezeigten Addition ausgeführt.

Die Punkte PA und PA' werden der Vorschrift zum Ermitteln von Zufallsbits übergeben (Schritt S3). Im vorliegenden Fall werden die x-Koordinaten der beiden Punkte PA und PA' mit XOR verknüpft und durch c geteilt.

Für isogene elliptische Kurven E und E´ gilt, daß für ein beliebiges x aus GF(p) x entweder x-Koordinate von zwei verschiedenen Punkten auf E ist, oder aber x ist x-Koordinate eines Punktes auf E und cx ist x-Koordinate eines Punktes auf E', oder aber x ist nicht x-Koordinate eines Punktes auf E,

aber cx ist x-Koordinate von zwei Punkten auf E'. Wenn man also die x-Koordinaten auf E' durch c teilt, dann kommt jedes beliebige x aus GF(p) genau 2x als x-Koordinate vor. Das heißt, wenn man eine x-Koordinate auf E mit einer x-Koordinate auf E' geteilt durch c verknüpft, ist das äquivalent zum Verknüpfen zweier beliebiger, zufälliger Werte zwischen 0 und p-1. Die hierdurch abgeleiteten Pseudozufallsbits verhalten sich also wie echte Zufallsbits.

Vom Schritt S2 werden die Punkte PA und PA' auch an den Schritt S4 übergeben, bei dem die Punkte P, P' unverändert bleiben und s bzw. s' jeweils um eins erhöht wird.

Vom Schritt S4 geht der Verfahrensablauf wieder auf den Schritt S2 über, bei dem wiederum neue Punkte PA und PA' gebildet werden, die dann wieder an den Schritt S3 zur Berechnung weiterer Zufallsbits und an den Schritt S4 übergeben werden. Dieser Verfahrensablauf kann vielfach wiederholt werden, wobei immer wieder neue Zufallsbits erzeugt werden.

Die Erfinder der vorliegenden Erfindung haben mit dem oben beschriebenen Verfahren zum Erzeugen von Zufallszahlen 20 x eine Million Zufallsbits erzeugt und diese Zufallsbits verschiedenen statistischen Tests unterzogen. Mit den Tests konnten keine Abweichungen von echten Zufallsbits festgestellt werden.

Für die Erfindung ist wesentlich, daß im Schritt S3 die Zufallszahl Z aus den beiden Punkten PA und PA' ermittelt wird, die von unterschiedlichen elliptischen Kurven E und E' stammen. Durch das Verknüpfen dieser beiden Punkte PA und PA' wird sichergestellt, daß anhand der erzeugten Pseudozufallszahlen nicht die der Berechnung der Punkte PA und PA' zugrunde liegenden Punkte P und P´ durch diskrete Logarithmen ermittelt werden können. Von dem Ergebnis aus S3 kann somit nicht auf das Verfahren zum Erzeugen der Punkte PA, PA' mit

den Schritten S1, S2 und S4 geschlossen werden, was durch die gestrichelte Linie in Fig. 5 dargestellt ist.

Die Erfindung ist nicht auf das in Fig. 5 dargestellte Ausführungsbeispiel beschränkt. Im Rahmen der Erfindung ist es z.B. möglich, im Schritt S3 eine andere Verknüpfung der x-Koordinaten zu wählen. So können z.B. die beiden x-Koordinaten durch eine Addition modulo p miteinander verknüpft werden. Oder aber man verknüpft die y-Koordinaten. Oder aber x- und y-Koordinaten. Im Rahmen der Erfindung ist es auch möglich, daß anstelle von fest vorgegebenen elliptischen Kurven E, E' mit Punkten P, P' nach jeder Berechnung von PA und PA' neue Kurven E*, E*' und Punkte P*, P*' bestimmt werden, die zur Berechnung der nächsten Punkte PA* und PA*' herangezogen werden. Auch die Werte s, s' können an sich beliebig verändert werden. Für die Erfindung ist lediglich wesentlich, daß die Werte s, s' ganze Zahlen sind. Zu Beginn des Verfahrens können sie beispielsweise mit einem einfachen Zufallsgenerator erzeugt werden, der keinen hohen Ansprüchen genügen muß. In Fig. 6 ist das grundsätzliche Prinzip der vorliegenden Erfindung dargestellt, das eine Schleife bestehend aus den Schritten S5 und S6 aufweist, wobei in Schritt S5 zwei elliptische Kurven E, E', zwei Punkte P, P' auf den beiden Kurven und zwei Startwerte s, s' gewählt werden. Im Schritt S6 werden die Punkte P, P' mit s bzw. s' multipliziert, woraus sich PA und PA' ergibt. Bei jeder Wiederholung der Schleife S5, S6 wird zumindest eines der Paare E, E' bzw. P, P' bzw. s, s' verändert. Es ist auch möglich, zwei oder alle 3 Paare nach einer festzulegenden Regel zu verändern.

Bei jeder Wiederholung der Schleife wird ein neues Zahlenpaar PA, PA' erzeugt und dem Verfahrensschritt S7 übergeben, bei dem die beiden Punkte PA und PA' jeweils zu einer Pseudozufallszahl Z verknüpft werden.

Verfahren auf Basis elliptischer Kurven verwenden als Einwegfunktion die Multiplikation auf elliptischen Kurven, weshalb

Vorrichtungen zum Durchführen solcher Verfahren mit Routinen und Einrichtungen für Arithmetik auf elliptischen Kurven versehen sind. Solche Verfahren benötigen zudem Zufallszahlen zum Erstellen der privaten und öffentlichen Schlüssel. Durch Verwenden des erfindungsgemäßen Verfahrens zum Erzeugen dieser Zufallszahlen können zum einen qualitativ hochwertige Pseudozufallszahlen erzeugt, und zum anderen kann der Programmcode gering gehalten werden, da die vorhandenen Routinen doppelt verwendet werden können. Hierdurch werden erhebliche Ressourcen eingespart, und gleichzeitig wird die Sicherheit des Verfahrens deutlich gesteigert.

Fig. 7 zeigt schematisch den Aufbau eines Programmes zum Ausführen des erfindungsgemäßen Verfahrens in einem Blockschaltbild. Das Programm besteht aus einem Teil P1 zum Durchführen des Signaturverfahrens, das auf einen Programmteil P2 zurückgreift, mit dem Multiplikationen auf elliptischen Kurven über endlichen Körpern durchgeführt werden. Der Programmteil P1 wird von einem weiteren Programmteil P3 mit Zufallszahlen versorgt, wobei der Programmteil P3 wiederum auf den Programmteil P2 zum Multiplizieren auf elliptischen Kurven zurückgreift. Am Programmteil P1 ist ein Dateneingangsstrom I und ein Datenausgangsstrom O dargestellt, wobei der Dateneingangsstrom eine zu signierende Nachricht sein kann und der Datenausgangsstrom die Signatur. Ferner kann der Programmteil P1 am Datenausgangsstrom O seinen privaten und öffentlichen Schlüssel ausgeben. Diese Funktionen des Programmteils P1 entsprechen den an sich bekannten Signaturverfahren und -vorrichtungen auf Basis elliptischer Kurven. Das erfindungsgemäße Verfahren kann insbesondere bei Recheneinrichtungen mit geringerer Rechenkapazität, wie z.B. Chipkarten eingesetzt werden, da der entsprechende Programmcode äußerst kompakt ist und die Länge der zu verarbeitenden Zahlen wesentlich kürzer als bei einem RSA-Verfahren gleicher Sicherheitsstufe. Es ist jedoch auch möglich, die Programme auf elektronisch lesbaren Datenträgern zu vertreiben.

WAVELYNX EX. 1003, Pg. 214
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Patentansprüche

1. Verfahren zum Erzeugen von Pseudozufallszahlen, bei dem zumindest zwei Punkte (P, P´) von zumindest zwei unterschiedlichen elliptischen Kurven (E, E´) über einem endlichen Körper (GF) bestimmt werden und eine Pseudozufallszahl durch Verknüpfen dieser Punkte (P, P´) erzeugt wird.

2. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 1, d a d u r c h g e k e n n z e i c h n e t, daß zur Bestimmung der Pseudozufallszahl jeweils ein Paar von Punkten (P, P´) bestimmt wird, wobei zur Bestimmung der einzelnen Paare jeweils dieselben zwei elliptischen Kurven (E, E´) verwendet werden.

3. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 2, d a d u r c h g e k e n n z e i c h n e t, daß die beiden elliptischen Kurven (E, E´) zueinander isogen sind.

4. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 3,
d a d u r c h g e k e n n z e i c h n e t, daß die Punkte (P, P´) eines ersten Paares in Abhängigkeit zweier Startwerte (s, s´) bestimmt werden.

5. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 4,
d a d u r c h g e k e n n z e i c h n e t, daß die Punkte (P, P´) der weiteren Paare durch Variieren der Startwerte gemäß einer vorbestimmten Regel bestimmt werden.

6. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 4,
d a d u r c h g e k e n n z e i c h n e t, daß die weiteren Paare von Punkten (P, P´) durch Variieren der elliptischen

Kurven und/oder der Punkte (P, P´) nach einer vorbestimmten Regel bestimmt werden.

7. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 6,
d a d u r c h g e k e n n z e i c h n e t, daß zum Ermitteln einer Zufallszahl die Koordinaten der beiden Punkte (P, P´) miteinander verknüpft werden.

8. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 7,
d a d u r c h g e k e n n z e i c h n e t, daß die x-Koordinaten der beiden Punkte (P, P´) miteinander verknüpft werden, wobei die beiden elliptischen Kurven (E, E´) isogen sind.

9. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 8,
d a d u r c h g e k e n n z e i c h n e t, daß die Punktgruppen (E(GF (p)), E´(GF (p))) der elliptischen Kurven (E, E´) über einem endlichen Körper GF(p) Gruppenordnungen (q bzw. q´) von zumindest 2^{100} und vorzugsweise mindestens 2^{130} aufweisen.

10. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 9,
d a d u r c h g e k e n n z e i c h n e t, daß die elliptischen Kurven über dem endlichen Körper GF(p) definiert sind, wobei p eine Primzahl ist, die größer als 3 ist.

11. Verfahren für elektronische Signatur auf Basis elliptischer Kurven, bei dem die Schlüssel auf Grundlage von Zufallszahlen erzeugt werden,
d a d u r c h g e k e n n z e i c h n e t, daß die Zufallszahlen nach einem Verfahren der Ansprüche 1 bis 10 ermittelt werden.

12. Vorrichtung zur Durchführung des Verfahrens für elektronische Signatur auf Basis elliptischer Kurven nach Anspruch 11, mit

einer Einrichtung zum Ausführen von Multiplikationen in der Punktgruppe einer elliptischen Kurve (E, E´) über einem endlichen Körper (GF(p)),

einer Einrichtung zum Signieren, die die Einrichtung zum Ausführen der Multiplikation verwendet, und

einer Einrichtung zum Erzeugen von Pseudozufallszahlen nach dem Verfahren nach einem der Ansprüche 1 bis 9, wobei auch diese Einrichtung die Einrichtung zum Ausführen der Multiplikation verwendet.

FIG 1

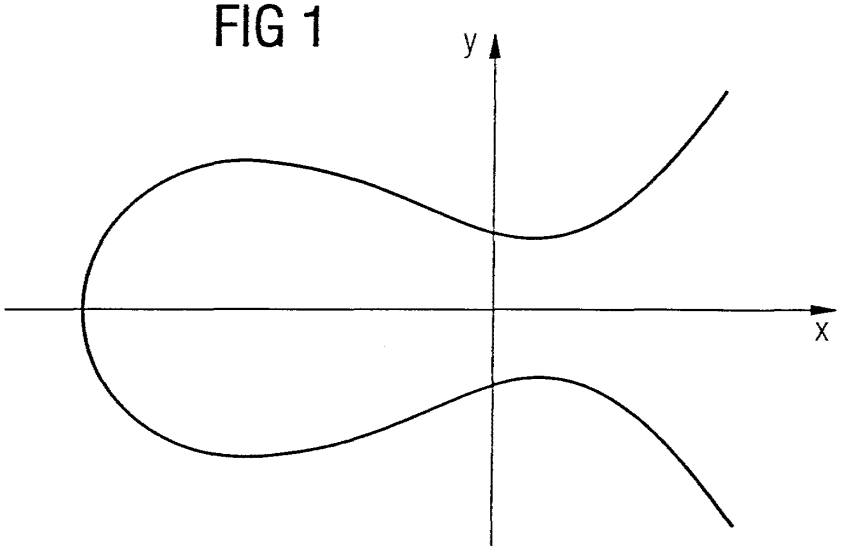


FIG 2

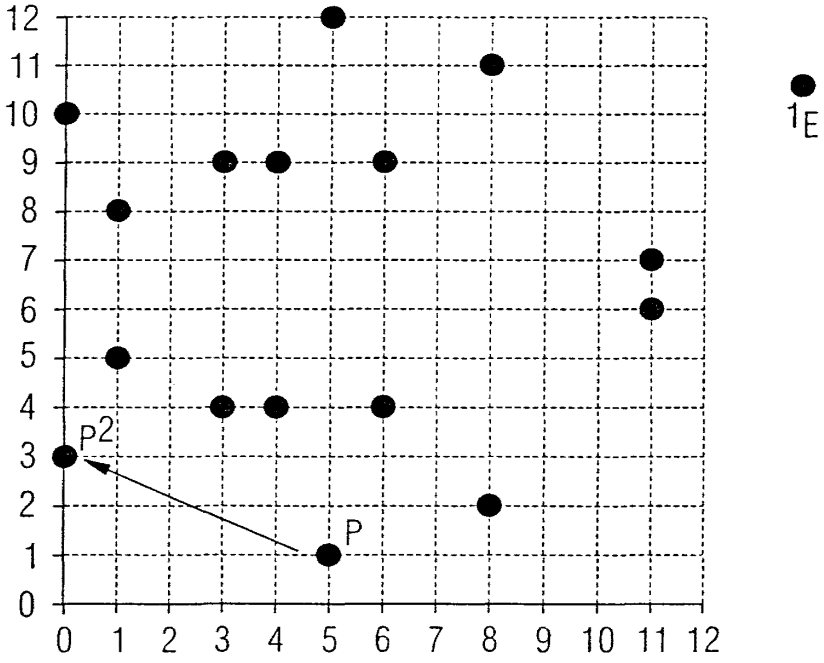


FIG 3

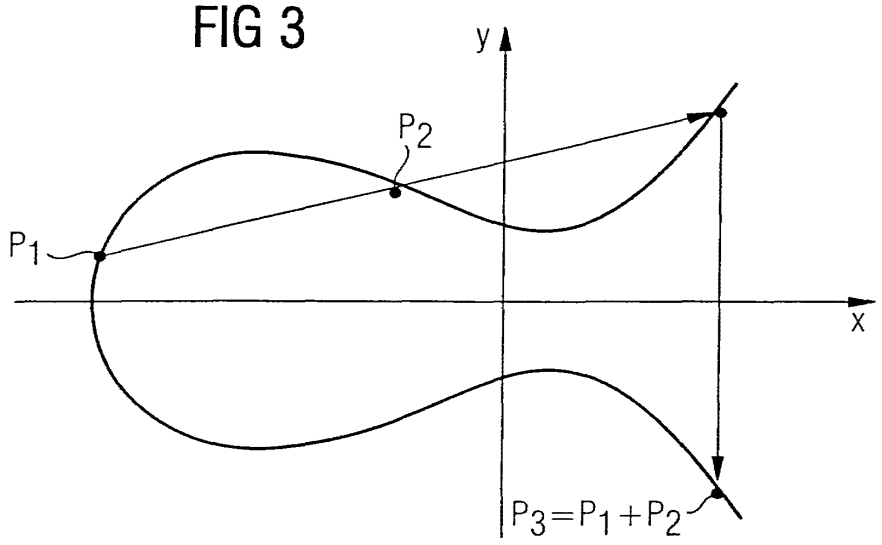


FIG 4

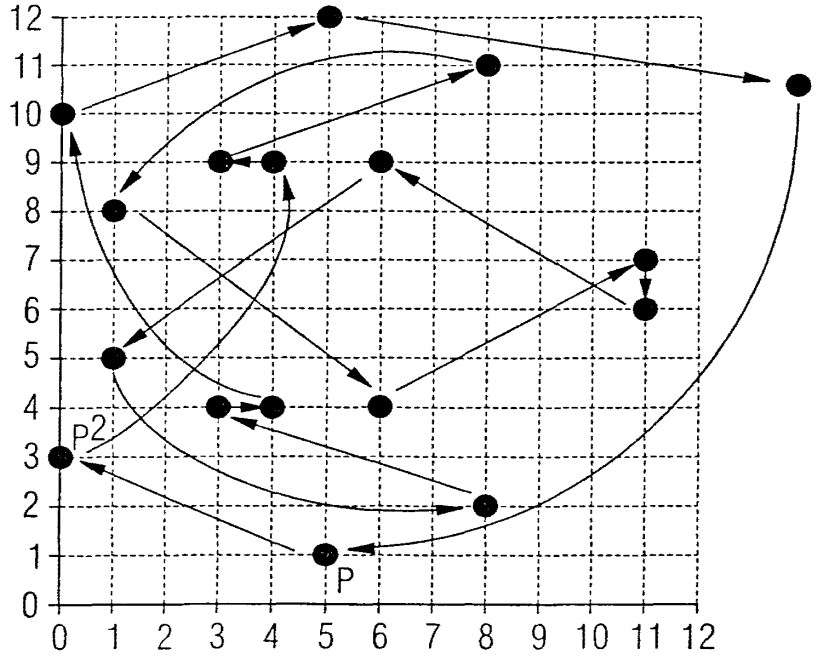


FIG 5

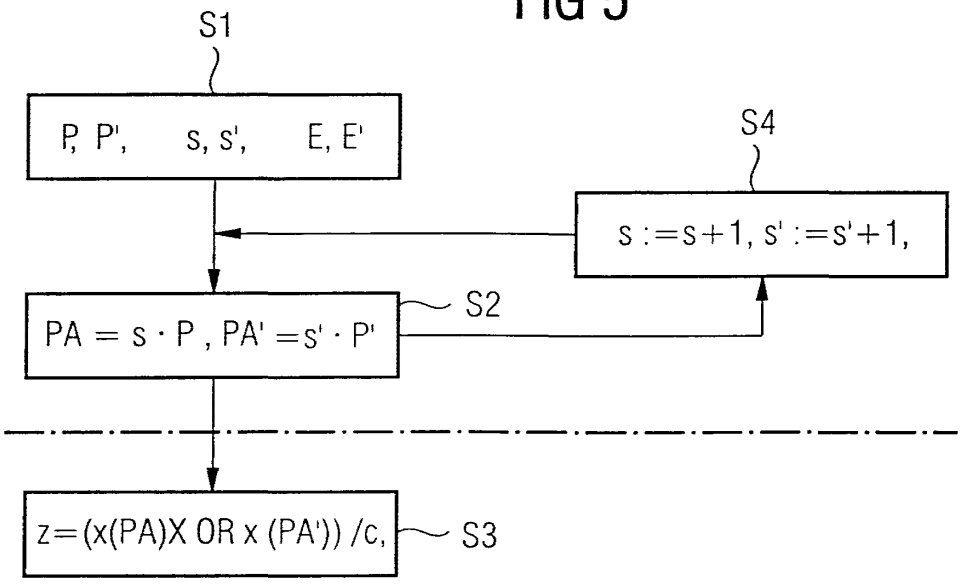

S1
P, P', s, s', E, E'
S4
s :=s+1, s' :=s'+1,
PA = s · P , PA' =s' · P'
S2
z=(x(PA)X OR x (PA')) /c,
S3

FIG 6

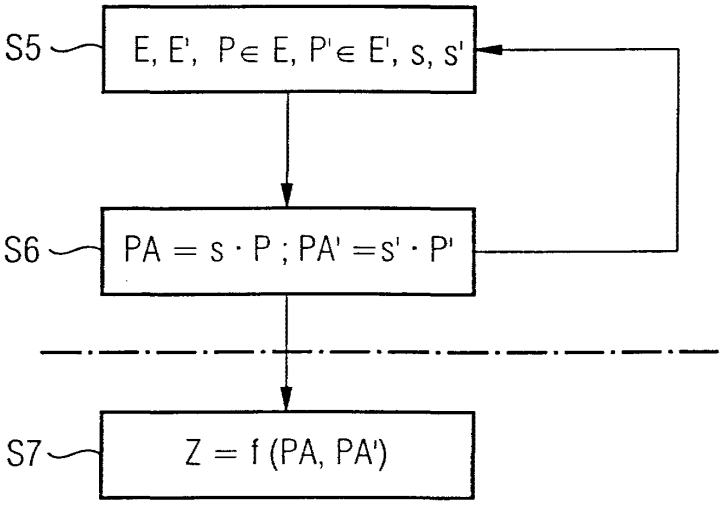
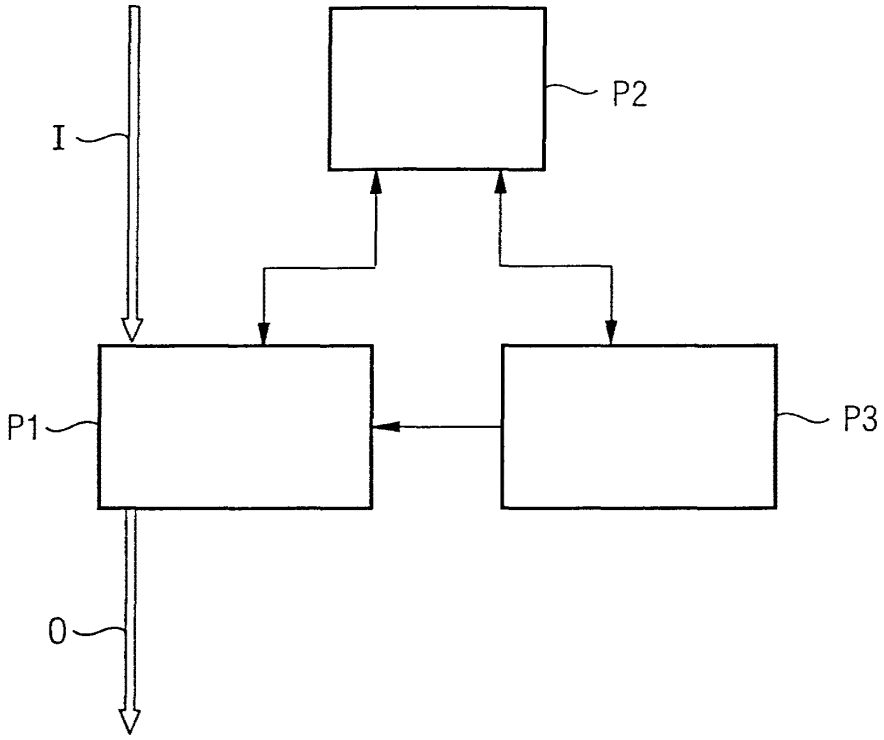

S5
E, E', P∈ E, P'∈ E', s, s'
S6
PA = s · P ; PA' =s' · P'
S7
Z = f (PA, PA')

FIG 7



WAVELYNX EX. 1003, Pg. 221
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/DE 00/02776

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58 H04L9/32 //G06F7/72

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 7 G06F H03K

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 practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 3, no. 3, pages 187-199, XP000972491 ISSN: 0933-2790 page 187, paragraph 1 page 188, paragraph 7 page 194, paragraph 2 -page 196, paragraph 1 ---	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 6, 1986, pages 84-103, XP000090665 page 98, line 20 - line 33 ------	1-12

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in 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 document 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
8 December 2000	20/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoof, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/DE 00/02776

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F7/58 H04L9/32 //G06F7/72

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H03K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, Bd. 3, Nr. 3, Seiten 187-199, XP000972491 ISSN: 0933-2790 Seite 187, Absatz 1 Seite 188, Absatz 7 Seite 194, Absatz 2 -Seite 196, Absatz 1 ---	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, Bd. CONF. 6, 1986, Seiten 84-103, XP000090665 Seite 98, Zeile 20 - Zeile 33 -----	1-12

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. Dezember 2000	20/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoof, P

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/18331 A1

(51) International Patent Classification[7]: E05B 41/00, 47/00, 41/00

(21) International Application Number: PCT/SE00/00949

(22) International Filing Date: 12 May 2000 (12.05.2000)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
9903127-0 3 September 1999 (03.09.1999) SE

(71) Applicant *(for all designated States except US)*: **ELECTEC SYSTEM AKTIEBOLAG** [SE/SE]; Box 307, S-662 27 Åmål (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GUSTAFSSON, Niclas** [SE/SE]; Elisebergsgatan 29, S-662 35 Åmål (SE).

(74) Agents: **HYNELL, Magnus** et al.; Hynell Patenttjänst AB, Patron Carls Väg 2, S-683 40 Hagfors/Uddeholm (SE).

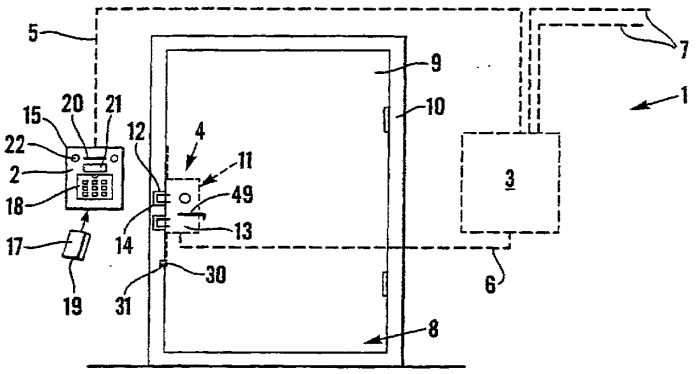
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD FOR CONTROL OF IN AND OUT PASSAGE BY MEANS OF A LOCKING SYSTEM, A LOCKING SYSTEM FOR PERFORMING THE METHOD AND A MOTOR-LOCK INTEGRATED INTO SAID LOCKING SYSTEM



(57) Abstract: The invention relates to a method in which in and out passage to or from a certain room or area, preferably a building or an enclosure, is controlled via an automatic door system, in which automatic door system a locking system (1) is provided, which comprises at least three main components including at least an operating panel (2), a control unit (3) and a motor-lock (4). The method is characterized in that a random code (H1, H2, H3) is transmitted from one main component (2, 3, 4) to another after a user has entered an authorization code (B1) via a registration device (16), which code is converted in an activation circuit card (23) to a first random code (H1), which varies randomly between each such main component (2, 3, 4) and in addition each time an authorization code (B1, B2) etc. is entered, which random code (H1) is received and verified by the control unit (3), following which another random code (H2) is transmitted to the motor-lock (4), which transmits its current status back to the control unit (3), following which a third random code (H3) is transmitted to the motor-lock (4) for opening its latch bolt (14) by means of an electric motor (47).

WO 01/18331 A1

A METHOD FOR CONTROL OF IN AND OUT PASSAGE BY MEANS OF A LOCKING SYSTEM, A LOCKING SYSTEM FOR PERFORMING THE METHOD AND A MOTOR-LOCK INTEGRATED INTO SAID LOCKING SYSTEM

TECHNICAL FIELD

The invention relates to a method, in which in and out passage to or from a certain room or area, preferably a building or enclosure, is controlled via an automatic door system, in which automatic door system a locking system is provided, which comprises at least three main components including at least an operating panel, a control unit and a motor-lock.

The invention also relates to a locking system comprising at least three main components including at least an operating panel, a control unit and a motor-lock.

Furthermore, the invention relates to an electromechanical motor-lock for use in a method or in a motor-locking system according to claims 1 or 2, which motor-lock is intended to be fitted to a device closing an opening, preferably a door, which motor-lock comprises a rotary lock mechanism and a motor-lock mechanism.

PROBLEM AND BACKGROUND TO THE INVENTION

Several different designs of locking systems are known, by means of which control of in and out passage through an opening into or out of a closed room or defined area, for example a building or an enclosure, can be executed via an automatic door system. A typical feature of such locking systems is that they comprise three main components, to be precise an operating panel, which comprises a receiver for registration via transmission, reading or entry of an authorization code, for example a card reader or key set, a control unit with a microprocessor, which receives the signal from the operating panel for verifying that an approved authorization code has been entered, and one or more electromechanical motor-locks, which are fitted to at least a door, outer door or the like at said room or enclosure. Motor-locks are distinguished from normal locks in that they have an electric motor for retracting and extending a latch bolt, usually in the form of a catch bolt. Motor-

locks can also have a further catch bolt, the open and locking position of which is controlled via a key-operable cylinder mechanism, a handle and/or a turning door handle, and in addition more often than not a normal spring bolt. Catch bolt means a bolt with a generally rectangular cross-section and a level end face, which bolt has at least two fixed end positions, which consist of a position barring and a position releasing the door, while a spring bolt is understood to mean a bolt, likewise with a usually rectangular cross-section but with a bevel-cut end face, which bolt is adjusted by means of the door handle between two end positions, which consist of a retracted and a projected spring end position. The function of the control unit's microprocessor is to emit a signal following checking and possible approval of the authorization code received to put the latch bolt of the motor-lock into its open or locking position.

One problem is that all locks which are intended to be used in type-approved doors, outer doors or the like must have a lock compartment of which the outer dimensions have an upper limit in accordance with the prefabricated and thus standardized recesses of the type-approved door or outer door for the lock compartment, in order thereby to always fit into these recesses. The lock compartment thus has a set, limited inner space, which cannot be filled completely without reservations as to what can or must be included. The contents of the lock compartment must therefore be optimized according to the intended use of the lock, where a compromise has to be made between the desired requirements for the strength of the lock compartment and for example the number of latch bolts included, etc. Hitherto it has thus proved difficult to combine both a considerable content, comprising followers, cylinders, springs, several latch bolts, a number of other necessary or at least desirable electrical and mechanical components etc. with a satisfactory capacity for resisting external damage. To meet the requirements for Swedish standards and for the lock to be approved by insurance companies, it is required for example that the projected latch bolt withstands a pressure of 500 kg and that the lock compartment is able to withstand a side load of 700 kg. To increase the strength of the lock compartment by using thicker sheet metal for the lock compartment's walls, bottom and cover only results in the already very limited inner space being limited further owing to the fact that the external dimensions of the lock compartment

are fixed. The inner space in a motor-lock, compared with a normal mechanical lock, is also filled by components required for the function, such as an electric motor and other necessary components for this, such as cabling, which is why there is no motor-lock on the market up to now which meets all the requirements set for Swedish standards and for approval by the insurance companies for mounting in a conventional lock compartment for a type-approved door.

Another significant problem is that the electrical signals transmitted in the cables between the individual main components forming part of the locking system, the components being arranged at a distance from one another and suitably protected against break-in, can be read relatively easily by an unauthorized person. The door lock can then be tampered with in that the signals read are quite simply repeated, the latch bolt being caused to move to an unlocked position for the door. In this case, whether the signal is coded or not makes no difference, since it only needs to be compared with a signal approved for opening the lock which has already been previously stored in a memory for illegal entry to be possible.

A further problem is that in all previously known and comparable motor-locks, the user has had to wait a relatively long time for the latch bolt to reach the appropriate end position before the door can be opened, or is locked. The required locking time, i.e. the bolt movement from the unlocked to the locked position and vice versa, takes up to several seconds in many known motor-locks. The reason for this is that the electric motor for these locks has been optimized for extending and retracting the latch bolt even when the door panel is not in the fully closed position, i.e. the door panel continues to stand slightly ajar so that the recess for the latch bolt in the door frame is not exactly in line with the latch bolt, for which reason the friction forces which occur in this case have to be overcome by the electric motor. A lock of this kind requires a larger and slower electric motor, on the one hand to overcome said friction forces and on the other to prevent the lock from jamming fast if pushed in too quickly. However, it is desirable for opening and locking to be able to be executed much more quickly, even up to 10 times faster. Even a wait of just 2-3 seconds can be found to be highly irritating by certain users, especially if passage in

and out takes place often. The latch bolt is therefore often set to the open (unlocked) position during the daytime, as doors of this kind otherwise tend to be set in the open position by means of an obstruction in the door spring by certain users, resulting in the lock not only being unlawfully disabled but also in the risk of the lock being forgotten altogether in the open position, or of the alarm being triggered unnecessarily if one is installed. Owing to the problems of the known motor-locks with latching times which are too long, it is thus common for them rather to be used only in the capacity of "night locks".

Finally, there is a potential problem if motor-locks with a higher speed should be used, since there is a risk of damage occurring to the motor shaft and to the transmission of power to the latch bolt, i.e. to the gear unit and pinions, due to the forces which arise at high speeds of the latch bolt when opening and locking the lock.

PURPOSE AND CHARACTERISTICS OF THE INVENTION

The object of the present invention is to eliminate or at least reduce the aforementioned problems.

The method according to the present invention is characterized in that a random code is sent from one main component to another after a user has entered an authorization code at a registration device, which code is converted in an activation circuit card to a first random code, which varies randomly between each such main component and also each time an authorization code is entered, which random code is received and checked by the control unit, following which yet another random code is sent to the motor-lock, which transmits its current status back to the control unit, following which a third random code is transmitted to the motor-lock to open its latch bolt by means of an electric motor.

The locking system according to the present invention is characterized in that each main component comprises at least an activation circuit card for receiving authorization codes and/or random codes, for conversion between these authorization codes and random codes

and for transmitting random code from one main component to another, which motor-lock includes reinforcement plates for reinforcing the lock compartment of the motor-lock.

The motor-lock according to the present invention is characterized in that the motor-lock furthermore comprises reinforcement plates, a blocking arm for blocking of a latch bolt, which is disposed via an operating device to be guided in a linear movement between a projected position latching the device and a retracted position releasing the device by means of an electric motor, which movement is controlled by the control unit, which is disposed to transmit a random code based on an authorization code from one main component to another, and that each such main component comprises at least one activation circuit card for conversion between authorization codes and said random codes.

ADVANTAGES OF THE SOLUTION

A locking system is achieved due to the present invention in which the motor-lock cannot be tampered with only by repeating a read signal in one of the cables between the main components forming part of the locking system, i.e. the operating panel, control unit and motor-lock, to achieve unauthorized lock opening.

Since the locking system always senses that the device which closes the opening to the lock-protected room or area, for example a door, is really in the correct position before the electric motor is started, the motor latch bolt does not need to align the door panel in relation to the door frame, for which reason no greater strength of the electric motor is required. The electric motor is therefore a considerably smaller model than that of the motor-locks otherwise obtainable on the market, and it is also specially adapted to guide the latch bolt forwards and backwards between its end positions considerably more quickly than in comparable motor-locks. It has been possible surprisingly to reduce the locking time to approx. 10 % of the corresponding locking time for comparable motor-lock designs, i.e. it has virtually been eliminated.

Thanks to the use of the much smaller and also considerably cheaper electric motor, the invention solves not only the problem of the extremely long locking time of up to several seconds at present, but also the problem of the minimal space inside the lock compartment is solved, as the smaller motor automatically gives extra space for greater reinforcement of the lock housing to make breaking in more difficult, which is achieved by the fitting of reinforcement plates, which are specially formed according to the components to be found in the lock compartment. In a conventional motor-lock, there is no space for extra protection in the form of reinforcement plates around the most essential design components of the lock with regard to protection against break-in, since its large electric motor takes up far too much room. The extended latch bolt is also blocked by a locking device which resists a pressure of over 500 kg, for which reason the lock can be approved by the insurance companies. Further "night locks" are thus not required.

By laminating several reinforcement plates of mutually diverging width, thickness and length on top of and/or at a set distance adjacent to one another, the advantage is also gained that predetermined geometrical spaces, tracks, surfaces or ducts can be created with optional extension in all directions for laying cables or for accurate three-dimensional mounting of defined components or sliding surfaces. The stationary or moving parts arranged in the lock compartment can thus be formed to be considerably thinner than previously, as they do not need to have the same thickness as the lock compartment to obtain the required supporting and /or sliding surfaces, at the same time as all the previously unutilized empty space is now filled with reinforcement material. The present motor-lock therefore copes with considerably greater loads in all directions than the corresponding conventional lock compartments, in spite of the external dimensions being essentially identical to one another to fit in the same recess.

LIST OF DIAGRAMS

The invention will be described in greater detail below with reference to the enclosed diagrams:

WAVELYNX EX. 1003, Pg. 230
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Fig. 1 shows a door in diagrammatic form with parts of a locking system according to the present invention, which locking system comprises a motor-lock, an operating panel and a central control unit with cables laid between the integral components.

Fig. 2 is a block diagram, which shows the connection between certain essential parts of the locking system shown in Figure 1.

Fig. 3 is a diagrammatic plan view of parts of a lock compartment for a motor-lock according to the present invention, with the cover of the lock compartment removed, in which the latch bolt of the motor-lock is in its outer, fully projected position blocked by means of a locking block.

Fig. 4 is a diagrammatic plan view of parts of the lock compartment for the motor-lock according to Figure 3, but with the latch bolt in a position partly retracted into the lock compartment.

Fig. 5 is a diagrammatic side view of parts of the lock compartment for the motor-lock according to Figure 3, but with the latch bolt in a position almost fully retracted into the lock compartment.

Fig. 6 is a flow chart, which shows in diagrammatic form the sequence of events when opening the lock according to the present invention.

DETAILED DESCRIPTION OF EXECUTION

Fig. 1 shows a locking system 1 according to the present invention, which is intended to control in and out passage through an opening to or from a certain closed room or defined area, for example a building or an enclosure. The locking system 1 comprises three separate main components, to be precise an operating panel 2, a control unit 3 and an electromechanical motor-lock 4, between which main components 2, 3, 4 suitable cables 5, 6, 7 are laid for transmitting signals and a power supply. The main components 2, 3, 4,

which can be more than one of each type, together constitute a complete system 1 in which all main components 2, 3, 4 are integrated with one another. Each main component 2, 3, 4 is unique in such a way that it is prepared so that if one or more of them need to be exchanged, the new component 2, 3 or 4, plus those remaining, can be adapted easily and without the aid of an external computer to function together directly following connection to the system 1 by means of "button pressing", described in greater detail below.

The room or area has a device 8 for closing said opening, such as a door, outer door, window or gate, preferably a type-approved door 8. Type-approved door 8 means a prefabricated door, which comprises a door panel 9, which is fitted in a door frame 10, and in which door panel 9 and door frame 10 predetermined recesses 11, 12 are included for the motor-lock 4, which is standardized with regard to its outer dimensions. The motor-lock 4 comprises a lock compartment 13 and at least one latch bolt 14, for which said recesses 11, 12 of set dimensions are thus provided with a good fit with regard to the height, depth and thickness of the lock compartment 13 and the latch bolt 14 respectively.

The operating panel 2 is arranged outside and at best closely adjacent to the opening through which in and out passage to or from the lock-protected room or area is to take place. The operating panel 2, which is advantageously arranged in an enclosure reinforced against break-in, at best a metal box 15, comprises a registration device 16 for receiving or reading a defined and unique authorization code B1, B2, B3 etc. via an information carrier 17 or via a key set 18 for manual entry of said authorization code B1, B2, B3 etc., see Figure 1. The information carrier 17 can consist for example of an electromechanical key of a known type, which has been personalized in some suitable manner, or, in the case of a registration device 16 consisting of a card reader, of a card with a magnetic strip 19, a bar code, microcircuit or the like, which card is inserted in a known manner into a slit 20 for registering the authorization code B1, B2, B3 etc. The registration device 16 can also consist of an IR receiver for registering the authorization code B1, B2, B3 etc. via remote transmission from the information carrier 17. The main thing is that the distinct authorization code B1, B2, B3 etc., which is at best unique to each user, is disposed in

some way to be transmitted to the registration device 16 of the locking system 1 to generate a first signal S1. The operating panel 2 can also comprise for example display windows 21 and / or lamps 22 for indicating such information as is considered essential for the user, for example that the door 6 is open or locked, that an incorrect authorization code Bx has been registered etc.

Furthermore, a transmitter 23 is provided in the form of an activation circuit card in the enclosure 15 of the operating panel 2 in a manner which is safeguarded against outer damage and against external reading of said first signal S1 generated. The activation circuit card 23 comprises a signal converter 24, for example a microprocessor or a circuit card of the type KEELOQ, for converting the first signal S1 generated in the registration device 16 into a variable, "random" code H1. Random code H1 means a code which is always changed on each new registration of an authorization code B1, B2, B3 etc. in the registration device 16, regardless of whether the authorization code B1, B2, B3 etc. is incorrect, correct, the same or new. The random code H1, which in the embodiment described consists of a 66-bit code, thus varies between each new passage in or out through the opening, including between each attempt to register an authorization code B1, B2, B3 etc., thereby eliminating the risk of unlawful opening of the door 8 by repeating a code H1 which has been read. The signal converter 24 for converting an incoming first signal S1 to a second signal S2 in the form of a random code H1 is a known electrical component, which is freely obtainable on the market. A diagrammatic example of the possible construction of a signal converter 24 is however as follows.

The signal converter 24 comprises a built-in random number generator 25 for generating a binary number of a certain length, which number varies randomly each time the activation circuit card 23 is activated by said first signal S1 from the registration device 16. The signal converter 24 of the activation circuit card 23 is set to utilize the binary number and the first signal S1 for a predetermined numerical calculation, a new, second signal S2, based on the read or entered authorization code B1, B2, B3 etc. and the binary random number provided by the random number generator 25, being set to be generated, which thus

forms the both coded and constantly changed "random" code H1 for each activation occurrence. The activation circuit card 23 can generate at least a million possible random codes H1 in separate combinations for each activation occurrence. Each activation is disposed to last for approx. 3 seconds. An external cable 5 is arranged from the activation circuit card 23 for transmitting the random code H1 to the control unit 3, disposed at a distance from the operating panel 2 inside the lock-protected room or area. This external cable 5 thus does not need to be protected against reading or signal repetition owing to the random codes H1 numbering at least a million, which are varied randomly in time.

The control unit 3, see Figure 2, comprises a receiver in the form of a second activation circuit card 26, which is set to receive the random code H1 from the activation circuit card 23 of the operating panel 2 for "decoding" to the factual authorization code B1 presently entered or read via the registration device 16, a main processor 27 for processing incoming and outgoing signals, for example checking the decoded authorization code B1 against approved authorization codes B1, B2, B3 etc. stored previously in a memory 28 of the main processor 27, and a transmitter in the form of a third activation circuit card 29 for converting a first and a second opening signal S3, S5 from the main processor 27 to a second or third random code H2, H3 (which are changed on each new opening signal S3, S5, and consequently also the code between the control unit 3 and the motor-lock 4 is protected against reading and repetition to achieve unlawful opening of the motor-lock 4 in the manner described in greater detail below), for forwarding via the cable 6 to the motor-lock 4 following completed and approved verification of the decoded authorization code B1. The main processor 27 can consist for example of one of several advanced electrical components, such as circuit cards, microprocessors etc. or of a computer. The main processor 27 is also provided for simultaneous or separate control of other functions of the motor-locking system 1 and the closing device or devices 8 which are arranged therein. Such functions include detection of the open or closed door position, detection of the projected position of the latch bolt 14 barring the door 8 and its retracted position releasing the door 8, locking of one or more motor-locks 4 etc. For this purpose, there are a number of magnetic sensors 30 and/or magnets 31, see Figure 1 and 3, placed for example on the

door frame 10, door panel 9 and/or the lock compartment 13 of the motor-lock. A rectifier, which is not shown, for converting alternating current to direct current is also provided in the control unit 3, thus it makes no difference whether the control unit 3 is supplied with alternating current or direct current.

The motor-lock 4, see Figure 3, comprises a receiver in the form of an activation circuit card 32 for the random codes H2, H3 from the control unit 3. The motor-lock 4 is connected via a connector 33 by means of electric cable 6 to the control unit 3 and to an external power source, which can consist of both an alternating current and a direct current source, the motor-lock 4 being disposed to set itself automatically to different voltages in the voltage ranges normal for motor-locks 4. In embodiments not shown, an internal power source such as a battery can also be located if necessary in the locking system 1 or the motor-lock 4 at one or more suitable points. Furthermore, the motor-lock 4 and its activation circuit card 32 comprise several electrical components and sensors such as magnetic sensors 30, relay 34, signal converter 35 and a microprocessor 36 for control and verification of the function of the lock 4 and for combining separate sub-signals SS1, SS2 etc., which represent the current status of the lock 4 with regard to the positions of the constituent mechanical parts.

All the delicate parts of the motor-lock 4 are arranged inside the protective case of the lock compartment 13, which consists of the box 37 of the lock compartment 13, a cover closing this, not shown, and a lock post 38 for fitting of the lock compartment 13 to the closing device 8, for example the type-approved door with a recess for the standardized lock compartment. The lock compartment 13 therefore has the necessary external dimensions required for said fitting. The lock post 38 has recesses 39, 40 for a spring bolt 41 and/or at least a latch bolt 14. The box 37 and cover of the lock compartment 13 include openings 42, 43, for cabling purposes and for a cylinder or handle follower 44, 45, which forms part of each lock mechanism. The motor-lock 4 shown in Figures 3 to 5 comprises two locking mechanisms, which consist of a motor-lock mechanism 46, which has an electric motor 47

for retraction and extension of the linearly movable latch bolt 14, and a conventional rotary lock mechanism 48.

The rotary lock mechanism 48 comprises a handle or knob 49 for operating the conventional spring bolt 41 via the handle follower 45, which is fitted rotatably at one end of the lock compartment 13. The handle follower 45 comprises a carrier arm 50, which is inserted into a groove 51 in the rear end part 52 of the spring bolt 41 to interact with this groove 51 in the linear inward and outward movements of the spring bolt 41. One or more springs 53, 54 are arranged inside the lock compartment 13, which springs 53, 54 lie close to the spring bolt 41 and the carrier arm 50 under tension, the springs 53, 54 being provided to hold the spring bolt 41 normally in a position partly projected outside the lock compartment 13, until the handle or knob 49 is used. The spring bolt 41 ensures that the door panel 9 and thereby the latch bolt 14 end up in the right position before the electric motor 47 is started. A door closer, not shown, can also be provided suitably on the door 8 for closing it, following which also said magnets 31 and magnetic sensors 30 detect that the correct position has been assumed. At least one further magnetic sensor 31 and magnet 30 are fitted in the lock compartment 13 and on the spring bolt 41 for detecting the position of the spring bolt 41, i.e. whether it is in its projected or retracted position, which positions provide two of the sub-signals SS1, SS2 etc., which the microprocessor 36 is set to collect and transmit to the control unit 3.

Apart from said cylinder follower 44 and electric motor 47, the motor-lock mechanism 46 comprises an operating device 55 for interaction with the electric motor 47 for said retraction and extension of the latch bolt 14. The operating device 55 comprises an oblong, linearly movable carrier 56, which has an essentially rectangular cross-section. The carrier 56 has a rectilinear cog rail in the form of a rack 57 disposed at its one end and an oblong, continuous recess 58 disposed at its opposite, other end. A cogwheel 59 is mounted on the revolving axle 60 of the electric motor 47 for bearing on the cog rail 57 for said retraction and extension of the linearly movable latch bolt 14. The carrier 56 also comprises a cog segment 61 and two hooks 62, 63 arranged on opposing sides of the recess end 58 of the

carrier 56, where the two hooks 62, 63, which are arranged at a set distance from one another, are turned towards the cylinder follower 44 to engage with a peg 64 raised from the follower 44, turning of the cylinder follower 44, via its knob or via a traditional locking cylinder by means of a main key, offering an opportunity for manual opening of the motor-lock 4, for example in an emergency situation or if the power supply is interrupted. The carrier 56 also has two level sliding surfaces 65, which are at right angles to the two sides which comprise said cog segment 61 and hooks 62, 63, one of which sliding surfaces 65 extends from the cog rail 57 to the end of the recess end 58 and the other, not shown, extends the whole of the carrier's 56 longitudinal extension on the opposite side in relation to the cog rail 57. The cog rail 57 is sunk here in relation to the sliding surface 65 disposed on the same side.

An oblong blocking arm 66 is arranged rotatably at one of its ends by a semicircular cog segment 67 on a pivot 68. The cog segment 61 of the carrier 56 extends in the longitudinal direction of the carrier 56 and has a length which corresponds to at least the peripheral length of the essentially semicircular cog segment 67 of the blocking arm 66. The pivot 68 is arranged to the side of the carrier 56 and at such a distance from it that on activation of the electric motor 47, the two cog segments 61, 67 interact with one another in a movement which is linear for the carrier 56 and rotational for the blocking arm 66. At its free end the blocking arm 66 has a carrier pin 69, which is inserted into an essentially triangular recess 70 in the rear part of the latch bolt 14, termed the operating part 71 below, while the front part of the latch bolt 14 is termed the engagement part 72. On the turning movement forwards and backwards of the blocking arm 66, the carrier pin 69 is disposed to guide the latch bolt 14 forwards and backwards in three stages due to the carrier pin 69 being guided from corner to corner in said triangular recess 70. The engagement part 72 and the operating part 71 both have a rectangular cross-section, the cross-section of the operating part 71 however being thinner than that of the engagement part 72, which parts 71, 72 forming in the present embodiment two level parts 71, 72 fixedly connected to one another, which have a front and a rear part 73, 74, which are disposed in the same plane but displaced laterally in relation to one another, thus basically in the form of a Z. The front

parts 73 of the two parts 71, 72 form the projection of the latch bolt 14, which passes into the recess 12 of the door frame 10. Two magnetic sensors 30 are arranged following one another in the direction of movement of the latch bolt 14 in the lock compartment 13 for sensing the current position of the latch bolt 14 by means of a magnet 31 attached to the latch bolt 14.

The blocking arm 66 is provided to block the projected latch bolt 14, which blocking arm 66 withstands the pressure of 500 kg (applied to the latch bolt 14) required for approval by the insurance companies. A further "night lock", i.e. a manual locking mechanism with a manually operated latch bolt, is thus not needed. The blocking arm 66 comprises a locking surface 75 arranged at the front end of the blocking arm 66 of the latch bolt 14, which locking surface 75 is provided to bear on and interact with a stop ledge 76 in the projected position of the latch bolt 14, see Figure 3. The stop ledge 14 is disposed by the engagement part 72 of the latch bolt 14, more precisely by its rear part 74, the stop ledge 76 and locking surface 75 being arranged parallel to one another in said projected position of the latch bolt 14.

To obtain type approval for the motor-lock 1, this has to conform to certain standardized dimensions and qualifications, i.e. the lock compartment 13 must fit into the standardized recess 12 in the likewise standardized door panel 9. This makes it impractical, for example, to only add further reinforcement to a normal lock to thereby increase its strength. By providing the lock construction with sensors, for example magnetic sensors 30, and a control unit 3 which verifies that the motor-lock 4 is in the correct position before the electric motor 47 is activated, in which case the latch bolt 14 does not have to align the door panel 9 in relation to the recess for the latch bolt 14, which calls for a strong motor 47 which presses the bolt 14 into the recess 12 even if the door panel 9 is in any open position, the lock 4 according to the invention can have an electric motor 47 model which is smaller, creating extra space inside the lock compartment 13.

Disposed inside the lock compartment 13 are a number of reinforcement plates 77 in the form of thin metal plates, which reinforcement plates 77 have each been cut very precisely with regard to cross-section and with varying extension in the plane to fit according to the construction elements to be found inside the lock compartment 13. The reinforcement plates 77 are placed on top of and at a set distance adjacent to one another to form channels and spaces 78 for components of the motor-lock 4 and cables 6 and to fill up essentially the rest of all the empty space inside the lock compartment 13, or to fill one or more defined parts of the lock compartment 13 to thereby increase the resistance capacity over essentially the entire lock compartment 13, or here and there in specially selected places, against external damage by means for example of breaking, drilling or striking tools. One such special place is appropriately around the blocking arm 66, the cog rail 57 and the cylinder follower 44. Considerably better protection is thereby achieved, for which reason the lock compartment 13 is able to withstand loads of over 700 kg, which is one of the requirements set for approval by the insurance companies and to obtain a Swedish standard. A number of pins 79 extend between the box 37 of the lock compartment 13 and its cover, for which pins 79 a number of holes 80 have been made through the reinforcement plates 77.

Since all the main components 2, 3, 4 of the locking system 1 have built-in transmitters and receivers, i.e. the activation circuit cards 23, 26, 29, 32, for the random code H1, H2, H3, they are all prepared to be able to be exchanged easily for a new one, following which the new component 2, 3, 4 is easily integrated into the coded locking system 1 in that necessary data are transferred between the old components 2, 3 and/or 4 and the new ones, for example quite simply by pressing an activation button, not shown, for activating said data transfer, due to which all components 2, 3, 4 are set to be adapted to function only for the same coded and variably random codes H1, H2, H3. The main processor 27 is preprogrammed together with said activation circuit cards 23, 26, 29, 32, which preprogramming is carried out initially by the necessary data being transmitted between the activation circuit cards 23, 26, 29, 32 forming part of the locking system 1 and the main processor 27.

WAVELYNX EX. 1003, Pg. 239
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FUNCTIONAL DESCRIPTION

Fig. 6 shows diagrammatically by means of a flow chart a method according to the present invention for opening of the motor-lock 4 belonging to the locking system 1 described above for controlling in and out passage to or from a certain room or area, preferably a building or an enclosure, via an automatic door system.

The procedure is initiated by a user, via the registration device 16 on the operating panel 2 outside said room or area, registering his defined and unique authorization code B1, which consists of one of several approved authorization codes B1, B2, B3 etc. stored previously in the memory 28 of the control unit 3. If the registration device 16 consists of a card reader, registration is effected for example by an information carrier 17 being guided through the card slot 20 of the card reader 16 to read said code B1, or the current authorization code B1 is entered manually via the key set 18 of the operating panel 2. A first signal S1 containing the read or entered authorization code B1 is generated, which first signal S1 is transmitted to the activation circuit card 23, where a random number generator 25 is activated, so that a binary number of a set length is generated, which number varies randomly each time the activation card 23 is activated by said first signal S1.

The signal converter 24 of the activation circuit card 23, for example a microprocessor, converts by means of a predetermined numerical calculation the first signal S1 and the binary random number to a new and second signal S2, namely the above so-called "random" code H1, which code H1 is thus changed randomly for each activation event, thanks to the effect of the random number generator 25 on the calculation.

The random code H1 is then transmitted via cable 5 to the control unit 3 situated at a distance from the operating panel 2, which unit consists of a personal computer, an advanced microprocessor or similar. The electric cable 5 does not need to be protected against reading, since the random code H1 is always both coded and changed between each attempt to open the door, regardless of whether an incorrect or correct authorization code B1 was originally used.

The random code H1 is received by the receiver 26 of the control unit 3, i.e. the second activation circuit, where it is decoded and then transmitted to the main processor 27. In the main processor 27, the thus recreated authorization code B1 is compared with the database stored in the memory 28 to verify whether the random code H1 received is a calculation result which is based on and agrees with one of the authorization codes B1, B2, B3 etc. stored in the memory 28 and, if such a one is found, that it has approved the authorization for the current motor-lock 4.

If this is the case, a first opening signal S3 , which either consists of the originally received authorization code B1 or a new such code B2, is sent to the transmitter of the control unit 3, i.e. its third activation circuit card 29, which performs a new numerical calculation based on the opening signal S3 and a new binary random number, so that a new, second random code H2 is generated, which is transmitted via cable 6 to the motor-lock 4. In the same way as with the earlier cable 5 between the operating panel 2 and the control unit 3, this cable 6 does not need to be shielded or protected either against reading of this, now second, random code H2.

The second random code H2 is received by the receiver 32 of the motor-lock 4, i.e. the fourth activation circuit card of the locking system 1, which activation circuit card 32 verifies that the incoming random code H2 has the correct authorization, which is carried out in the same way as at the receiving activation circuit card 26 of the control unit 3. In the case of an approved random code H2, the motor-lock 4 sends back a fourth signal S4 to the main processor 27 of the control unit 3, which signal S4 is first combined with several of the sub-signals SS1, SS2, SS3 etc., which together describe the current status of the motor-lock 4 with regard to desired and/or necessary information about the current settings and state of the motor-lock 4.

For example, it is detected by means of the magnetic sensors 30 and the magnets 31 whether the spring bolt 41 or the latch bolt 14 are projected or retracted, whether the latch

bolt 14 has been locked by means of the blocking arm 66 or not (detected by a sensor not shown), whether the movement of the latch bolt 14 is blocked in any direction, so that the electric motor 47 after three closing attempts continues to be prevented from pushing the latch bolt 14 into the recess 12, following which an alarm is triggered, whether the door panel 9 is in the open or closed position, which is simply registered by means of magnets 31 and magnetic sensors 30 arranged on the door panel 9 and on the door frame 10, etc. The combined signal S4 is uncoded in the embodiment described, but can if necessary easily be converted to a random signal by means of a further activation circuit card disposed inside the motor-lock 4.

The combined signal S4 is received by the main processor 27 of the control unit 3, processed by this and if all sub-signals SS1, SS2 etc are correct for door opening, a second opening signal S5 is sent anew to the transmitter 29 of the control unit 3, coded to give a new random code H3, which is transmitted to the motor-lock 4 via cable 6. This time the electric motor 47 of the motor-lock 4 is activated in a direction of rotation which retracts the latch bolt 14.

The function for instead placing the motor-lock 4 in the locking position is executed in a similar manner by means of an authorization code B1, by means of a timer, which triggers locking, via a circuit-breaker inside the protected area or room, for example at the control unit 3, or by means of mechanical projection of the latch bolt 4 by means of a key or knob.

To ensure that the motor axle 60 including power transmission, i.e. the gear unit and pinion 59 etc., shall manage the high speed on opening and locking without being broken, the latch bolt 14 should be braked softly prior to its two end positions, i.e. bolt out/bolt in. Braking is effected preferably by short-circuiting the motor winding and thereby giving the motor 47 the same function as a generator, which means that the desired effect, efficient deceleration, is achieved.

Damage of the type described above can likewise occur in connection with opening/ closing the lock 4 via key or knob 49. This applies both before and after the lock 4 has been connected to a power source. In new buildings under construction, electric locks 4 are often used as a mechanical lock until electrical cables 6 are laid. This means that even before the lock 4 is connected to the power, the electric motor 47 should be short-circuited to thereby keep its braking function.

ALTERNATIVE EMBODIMENTS

The invention is not restricted to the embodiment shown, but can be varied in different ways within the framework of the claims. It is perceived for example that the measures taken and arrangements made to obtain considerably improved protection against break-in, namely the reinforcement plates 77, blocking arm 66 and the fact that the authorization code B1 and all other essential signals S2, S3, S5 in the system outside the protective envelope of the main components always consist of a random code H1, H2, H3, are applicable in a locking system essentially comprising an unlimited number of motor-locks, and that these motor-locks can be formed in different ways with regard to the requirements for standardized dimensions, the number of locking mechanisms and which closing device they are arranged on.

It is also perceived that, if not only a normal relay or electromagnet is used, which only activates or deactivates some type of mechanical block for the latch bolt 14, but if several microprocessors are located in the locking system 1, which code signals using a continuously random code, which cannot be read and then repeated to open the door, considerably better protection is obtained with great security. The combination options of the locking and passage system's random code described above are basically unlimited, as on each new activation of the activation card a new code variable of up to 1 million possible and separate combinations of unique codes is sent off to the respective receiver unit, which can consist of either the lock unit or the control unit.

With the construction described above, a break-in must take place in one of the three main components, i.e. the operating panel 2, control unit 3 or the motor-lock 4, to get at uncoded

signals, and it is only the first signal S1 from the registration device 16 to the activation card 23 inside the operating panel 2 which actually contains an uncoded and correct authorization code B1. Other signals, if they are based in some way on an authorization code, all consist of random codes or only of information regarding the status of the door 8, for example, with regard to its open or closed position in relation to the door frame 10 etc., information which is important in itself but not sufficient to open the motor-lock 4.

None of the electric motor-locks on the market today have utilized the method of increasing the strength of the lock compartment 13 by several layers of reinforcement plates 77 and the shear strength between these and the incorporated, interacting pins 79 to withstand 700 kg of lateral load (Swedish standard requirement), which no existing motor-lock manages today. In the same way, the locking of the latch bolt 14 of the electric motor-lock 4 by means of the blocking arm 66 is unique as it meets the requirements of the standard for 500 kgs of pressure.

The invention is not restricted to what has been described above, but can be varied within the scope of the claims. Thus it is perceived amongst other things that braking mechanisms other than the motor winding can be used to avoid any damage to the motor axle/power transmission, such as mechanical braking devices which take effect close to the respective end position. Furthermore, it is perceived that means other than magnetism, e.g. optical sensors, can be used to detect that the door is in the correct position to be able to be locked. Finally, it is perceived that many of the new functions described in the lock can be utilized in themselves without necessarily being combined with all the other functions described, e.g. it is not necessary to use random codes to exploit the advantages of the new combination of having a fast, smaller motor/ transmission and a mechanism which detects that the door panel is in the correct position, so that the latch bolt can move into the recess quickly and without difficulty.

CLAIMS

1. Method in which in and out passage to or from a certain room or area, preferably a building or an enclosure, is controlled via an automatic door system, in which automatic door system a locking system (1) is provided, which comprises at least three main components including at least an operating panel (2), a control unit (3) and a motor-lock (4), characterized in that a random code (H1, H2, H3) is transmitted from one main component (2, 3, 4) to another after a user has entered an authorization code (B1) via a registration device (16), which code is converted in an activation circuit card (23) to a first random code (H1), which varies randomly between each such main component (2, 3, 4) and in addition each time an authorization code (B1, B2) etc. is entered, which random code (H1) is received and verified by the control unit (3), following which another random code (H2) is transmitted to the motor-lock (4), which transmits its current status back to the control unit (3), following which a third random code (H3) is transmitted to the motor-lock (4) for opening its latch bolt (14) by means of an electric motor (47).

2. Method according to claim 1, characterized in that the latch bolt (14) is braked softly before its two end positions, preferably by the motor winding being short-circuited and the motor (47) thereby being given the same function as a generator.

3. Method according to claim 1, characterized by means (30, 31) for detecting that the latch bolt (14) is in a correct position to be able to be guided into a lock recess (12), incorrect positioning preferably being signalled automatically to the user so that a correction of the door's position is executed by the user before the latch bolt (14) is permitted to be guided into the lock recess.

4. Locking system comprising at least three main components including at least an operating panel (2), a control unit (3) and a motor-lock (4), characterized in that each main component (2, 3, 4) comprises at least an activation circuit card (23, 26, 29, 32) for receiving authorization codes (B1, B2) and/or random codes (H1, H2, H3) for conversion

WAVELYNX EX. 1003, Pg. 245
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

between these authorization codes (B1, B2) and random codes (H1, H2, H3) and for transmission of random code (H1, H2, H3) from one main component to another, which motor-lock (4) comprises reinforcement plates (77) for reinforcement of the lock compartment (13) of the motor-lock (4).

5. Electromechanical motor-lock (4) for use in a method or a motor-locking system according to claim 1 or 2, which motor-lock (4) is intended to be fitted to a device (8) closing an opening, preferably a door, which motor-lock (4) comprises a rotary lock mechanism (48) and a motor-lock mechanism (46), characterized in that the motor-lock also comprises reinforcement plates (77), a blocking arm (66) for blocking a latch bolt (14), which is disposed via an operating device (55) to be guided in a linear movement between a projected position blocking the device (8) and a retracted position releasing the device (8) by means of an electric motor (47), which movement is controlled by the control unit (3), which is set to transmit a random code (H1, H3) based on an authorization code (B1, B2) from one main component (2, 3, 4) to another and that each such main component (2, 3, 4) comprises at least an activation circuit card (23, 26, 29, 32) for conversion between authorization codes (B1, B2) and said random codes (H1, H2, H3).

6. Electromechanical motor-lock (4) for use in a method or a motor-locking system according to claim 1 or 2, which motor-lock (4) is intended to be fitted to a device (8) closing an opening, preferably a door, which motor-lock (4) comprises a linearly movable latch bolt (14) and a motor-lock mechanism (47), characterized in that a first means (31) is arranged on said device (8) and a second means (31) in connection with said opening provided with a recess (12) for the bolt (14), which means (30, 31) interact to detect and signal at least a predetermined given position between said device (8) and opening, with the aim of ensuring that unobstructed movement of said bolt (14) can take place into said recess (12).

WAVELYNX EX. 1003, Pg. 246
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

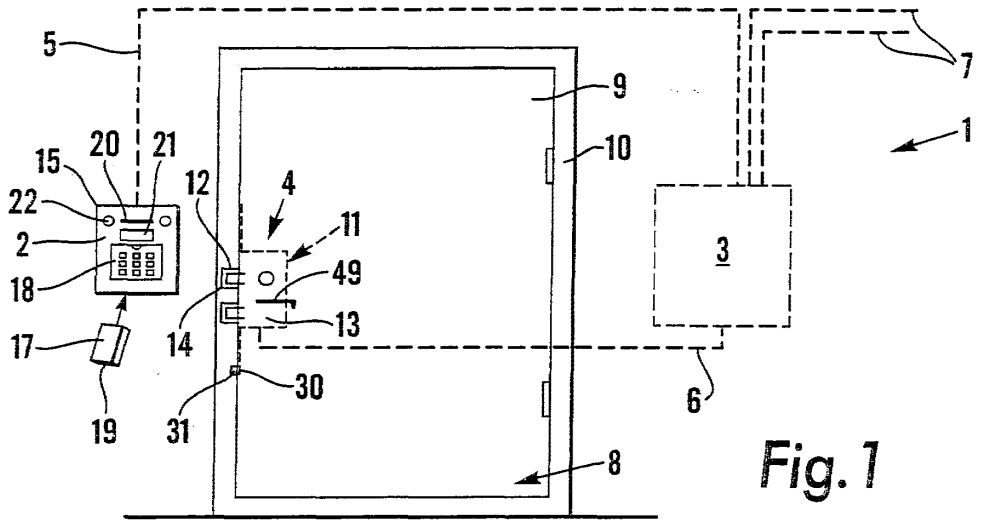

5
7
9
10
1
15
20
21
12
4
22
2
11
49
18
14
13
3
17
19
31
30
6
8

Fig. 1

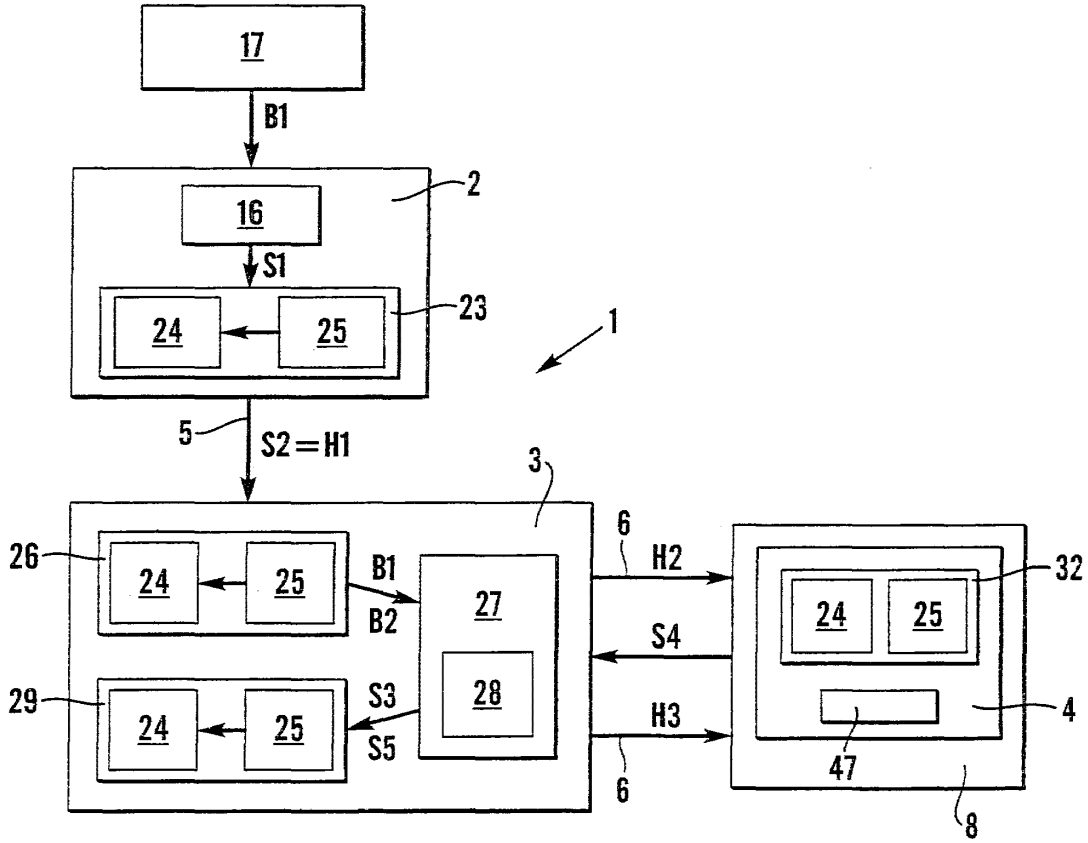

17
B1
2
16
S1
24
25
23
1
5
S2=H1
3
6
26
24
25
B1
B2
27
H2
32
24
25
S4
28
29
24
25
S3
S5
H3
4
47
6
8

Fig. 2

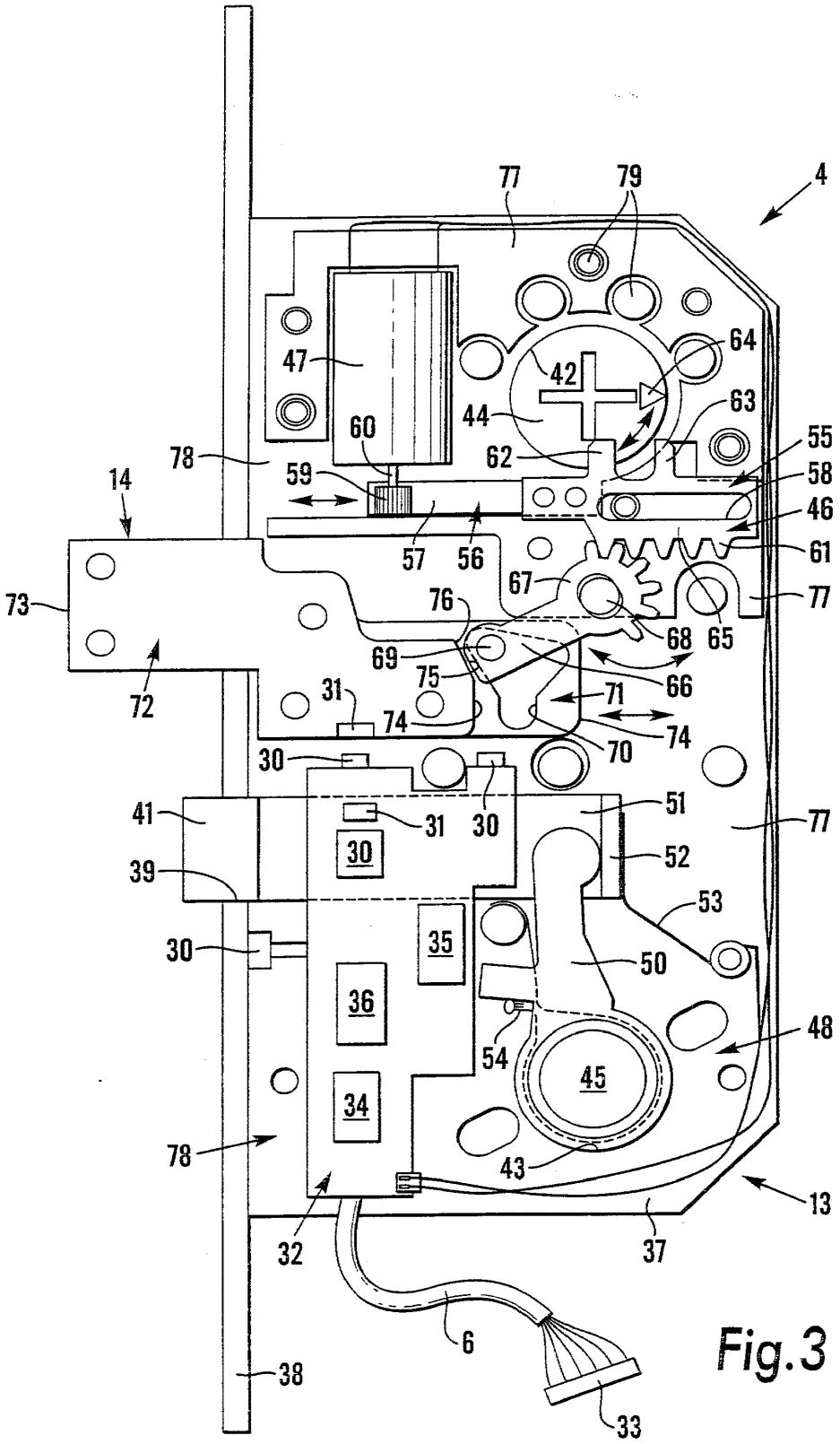

77
79
4
47
42
64
63
44
60
62
55
58
78
59
14
46
57
56
61
67
77
73
76
68
65
69
75
66
31
71
72
74
74
70
30
41
51
77
31
30
30
39
52
53
35
30
50
36
54
48
45
34
78
43
13
32
37
6
38
33

Fig.3

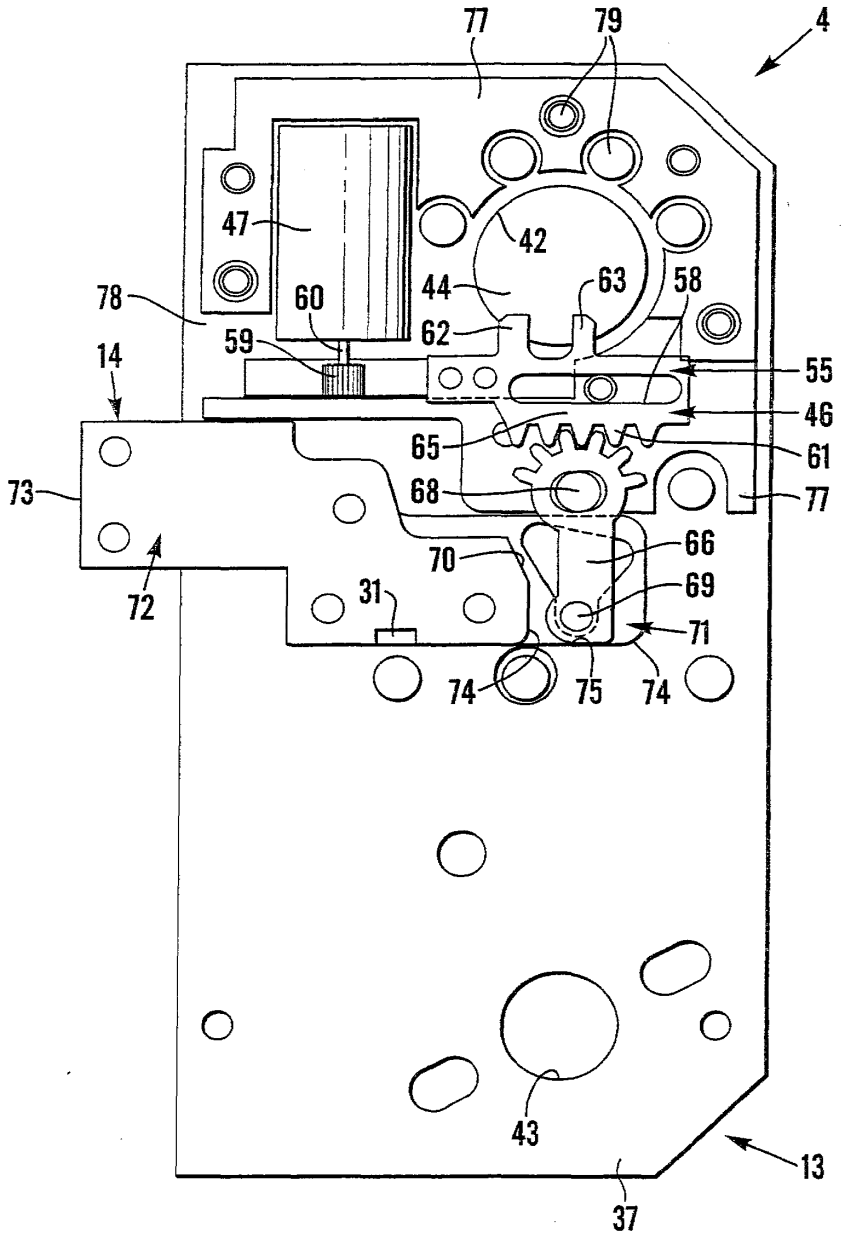

77
79
4
47
42
78
60
44
63
58
59
62
14
55
46
65
61
73
68
77
66
70
69
72
31
71
74
75
74
43
13
37

Fig.4

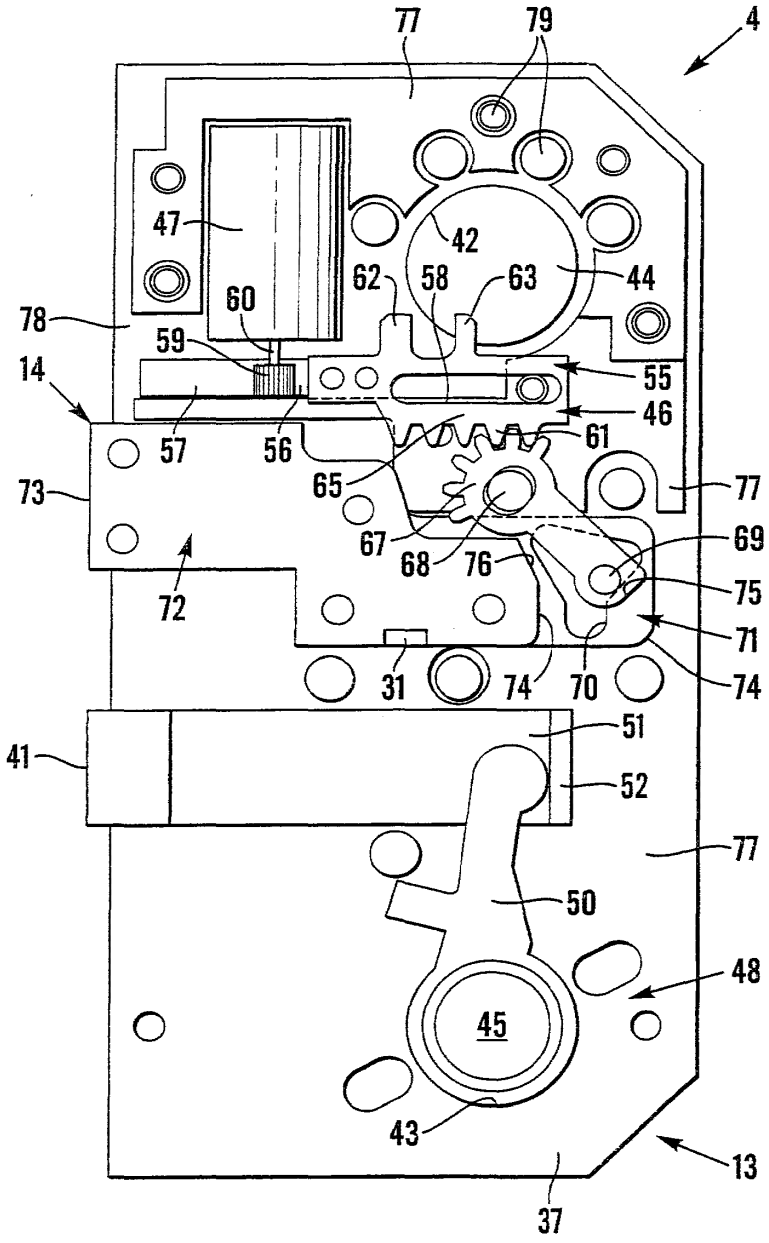

77
79
4
47
42
62
58
63
44
60
78
59
14
55
46
61
57
56
65
77
73
67
68
76
69
75
72
71
31
74
70
74
51
41
52
77
50
48
45
43
13
37

Fig.5

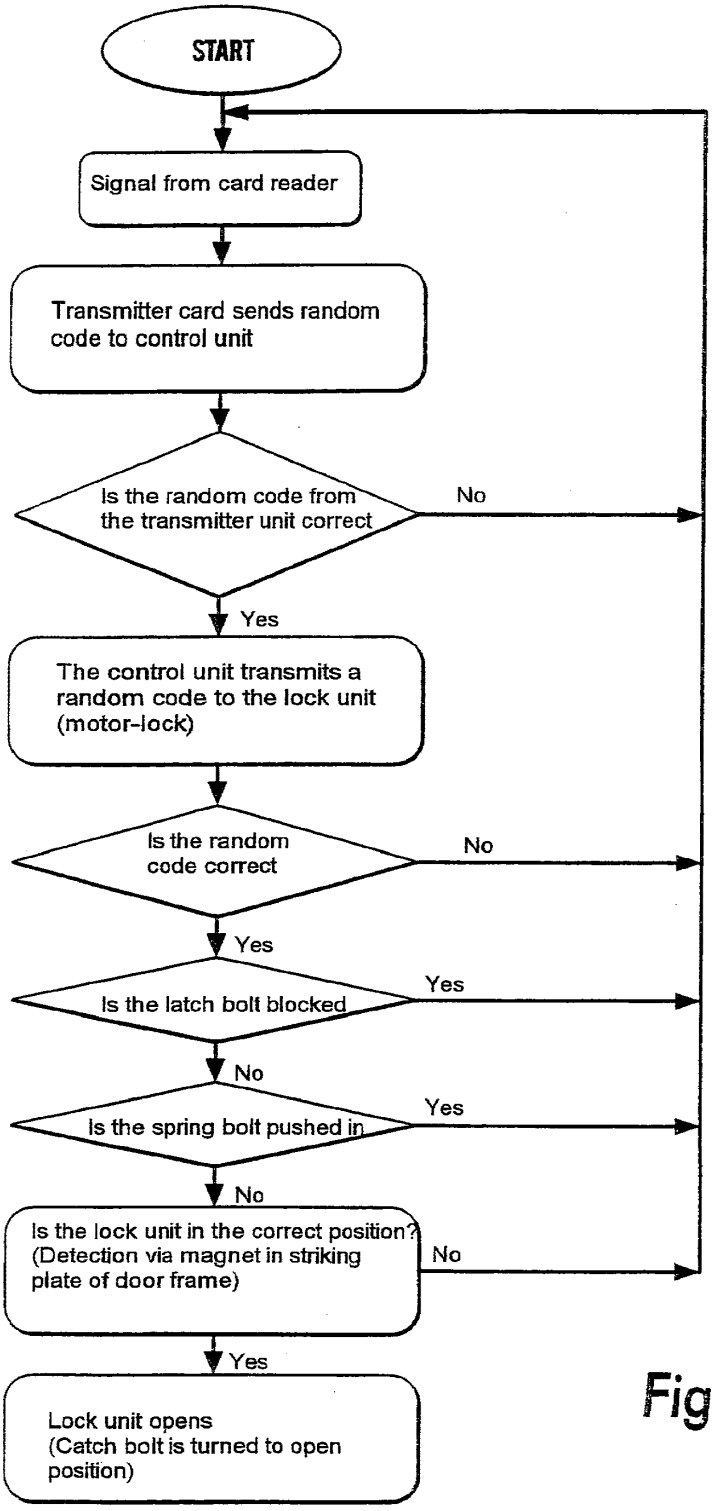

START
Signal from card reader
Transmitter card sends random code to control unit
Is the random code from the transmitter unit correct
No
Yes
The control unit transmits a random code to the lock unit (motor-lock)
Is the random code correct
No
Yes
Is the latch bolt blocked
Yes
No
Is the spring bolt pushed in
Yes
No
Is the lock unit in the correct position? (Detection via magnet in striking plate of door frame)
No
Yes
Lock unit opens (Catch bolt is turned to open position)

Fig.6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/00949

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: E05B 41/00, E05B 47/00, E05B 41/00
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)

IPC7: E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

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	US 4929005 A (HANS-DIETER HEINEN), 29 May 1990 (29.05.90) --	1-6
A	DE 4213141 A1 (VDO ADOLF SCHINDLING AG), 28 October 1993 (28.10.93) --	1-6
A	EP 0733759 A1 (SUMITOMO WIRING SYSTEMS, LTD.), 25 March 1996 (25.03.96) --	1-6
A	EP 0861959 A2 (TALLERES DE ESCORIAZA, S.A.), 2 Sept 1998 (02.09.98) --	1-6

[X] Further documents are listed in the continuation of Box C. [X] 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" erlier document 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
31 July 2000	16 -08- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christer Wendenius/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

WAVELYNX EX. 1003, Pg. 252
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/00949

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4593543 A (RONALD T. STEFANEK), 10 June 1986 (10.06.86) --	1-6
A	DE 3309962 A1 (BECKER EBERHARD), 20 Sept 1984 (20.09.84) -- --------	1-6

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/12/99

International application No.
PCT/SE 00/00949

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4929005 A	29/05/90	DE 3881637 A,T	15/07/93
		EP 0314222 A,B	03/05/89
DE 4213141 A1	28/10/93	NONE	
EP 0733759 A1	25/03/96	JP 2914211 B	28/06/99
		JP 8260783 A	08/10/96
		US 5781121 A	14/07/98
EP 0861959 A2	02/09/98	ES 1036491 U,Y	16/08/97
US 4593543 A	10/06/86	CA 1239803 A	02/08/88
DE 3309962 A1	20/09/84	DE 3338566 A	02/05/85

WAVELYNX EX. 1003, Pg. 254
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 April 2003 (03.04.2003)

PCT

(10) International Publication Number
WO 03/027832 A2

(51) International Patent Classification[7]: G06F 7/58

(21) International Application Number: PCT/US02/29080

(22) International Filing Date:
13 September 2002 (13.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/963,857 26 September 2001 (26.09.2001) US

(71) Applicant: **INTEL CORPORATION** [US/US]; (a Delaware Corpporation), 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor: **RUEHLE, Mike**; 2655 Kaystone Avenue, #30, Santa Clara, CA 95051 (US).

(74) Agent: **MALLIE, Michael, J.**; Blakely, Sokoloff, Tayor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/027832 A2

(54) Title: HASH-BASED PSEUDO-RANDOM NUMBER GENERATOR

(57) Abstract: A pseudo-random number generator (PRNG) with increased randomness. An iterative hash-based PRNG hashes in the output of a numerical sequencer, such as a counter or linear feedback shift register, in each hash stage. To improve the unpredictability of the numerical sequencer output, it may be paused for relatively unpredictable time periods. When the timing of the output of the numerical sequencer is unpredictable, elapsed time cannot be used to reliably predict what the output of the numerical sequencer will be with relation to the hash operation. The unpredictable time period may be related to when a request for a pseudo-random number is received.

WAVELYNX EX. 1003, Pg. 255
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

HASH-BASED PSEUDO-RANDOM NUMBER GENERATOR

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The invention pertains generally to computers. In particular, it pertains to generating pseudo-random numbers.

2. Description of the Related Art

[0002] Many forms of security, such as data encryption, make use of random numbers to increase the difficulty of code-breaking. Such encryption and random number generation is most often performed with computers. However, a computer uses a finite set of known instructions and known timing relationships, so anything produced by a computer is theoretically not random. But by following the right kind of complex algorithm a computer can calculate a sequence of numbers that appears random and is difficult to predict, even when the past history of the number sequence is known. A pseudo-random number generator (PRNG) is called pseudo-random because it produces its output by iterating some complex algorithm on a relatively small set of input data (which may or may not be random), and not by sampling some truly random physical process. The value of a PRNG in security applications is based on the difficulty of determining the value of a particular output number, based on a full or partial history of previous output numbers from the PRNG and/or input numbers to the PRNG.

WAVELYNX EX. 1003, Pg. 256
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0003] Some PRNGs use an iterative one-way hash algorithm, which takes a first number, transforms it through an algorithm into a second number, and then uses the second number as an input to the algorithm to create a third number, which becomes the input to the algorithm to create a fourth number, etc. If the algorithm is sufficiently complex, predicting one number from the previous numbers is very difficult. However, if a hostile attacker learns the PRNG algorithm, he may be able to predict all future outputs because of the inflexible relationship between the input and output of the PRNG.

[0004] A conventional way to reduce this risk is to also hash in the value of a free-running counter at each stage. This increases the difficulty of predicting a given number, and thereby breaking the code, but the output of a counter is predictably linear. With sufficient resources a dedicated attacker can combine the predictability of the counter with the already-known characteristics of the algorithm to determine what a given pseudo-random number will be and thus permit decryption of an encrypted message by a hostile party.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The invention may best be understood by referring to the following description and accompanying drawings that are used to illustrate embodiments of the invention. In the drawings:

[0006] Fig. 1 shows a block diagram of a pseudo-random number generator according to one embodiment of the invention.

[0007] Fig. 2 shows a schematic of a linear feedback shift register according to one embodiment of the invention.

WAVELYNX EX. 1003, Pg. 257
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0008] Figs. 3A, 3B show relative timing between stages and cycles according to one embodiment of the invention.

[0009] Fig. 4 shows a block diagram of a specific embodiment of Fig. 1 according to one embodiment of the invention.

[0010] Fig. 5 shows a flow chart of a method according to one embodiment of the invention.

[0011] Fig. 6 shows a system according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0012] In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it is understood that the invention may be practiced without these specific details. In other instances, well-known circuits, structures and techniques have not been shown in detail in order not to obscure the invention.

[0013] Various embodiments of the invention use the output of a numerical sequencer, such as a counter or linear feedback shift register, as periodic partial input to an iterative hash operation. To increase the randomness of the hash results, the output of the numerical sequencer may be made more random by stopping its operation for unpredictable periods of time. One embodiment runs the hash operation continually, but stops the numerical sequencer when a request for a pseudo-random number is generated and starts the numerical sequencer again at the start of the next hash stage.

[0014] An iterative hash operation is any repeating hash operation that repeatedly produces output numbers from input numbers, with at least part of each output number being fed back as input to produce the next output number. In one embodiment, a

WAVELYNX EX. 1003, Pg. 258
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

modified form of the well-known Secure Hash Algorithm (SHA) is used. A standard SHA is defined in Federal Information Processing Standards Publication 180-1, published April 17, 1995 by the U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.

[0015] Fig. 1 shows a block diagram of a pseudo-random number generator according to one embodiment of the invention. In the illustrated embodiment of Fig. 1, pseudo-random number generator (PRNG) 10 includes hasher 12 in the form of a hashing circuit that receives combined input data at IN-1 and IN-2, performs a hash operation on the combined input data, and produces output data at OUT in the form of a pseudo-random number (PRN). In the illustrated embodiment, the clock signal CLK is used to clock the processing elements of hasher 12, and multiple clock pulses are required to produce each PRN. The PRN produced at the output is latched into register 16, from where it may be made available to devices or operations requesting a PRN. In one embodiment, each new PRN overwrites the data in register 16, thus repeatedly changing the available PRN.

[0016] Hasher 12 may receive input data from two sources. In one embodiment, IN-1 and IN-2 represent parallel groups of bits that receive data simultaneously. In another embodiment, IN-1 and IN-2 represent different inputs received at different times over the same input bits, such as through a multiplexer (not shown). In some embodiments, IN-1 and IN-2 each receive large numbers as a series of smaller numbers received sequentially.

[0017] At least a portion of the output data from hasher 12 is fed back to input IN-2 through feedback circuit 15, for use as an input to hash the next PRN. In one embodiment, feedback circuit 15 consists of direct connections from OUT to IN-2. In another embodiment, feedback circuit 15 performs an active operation on the data, such as

WAVELYNX EX. 1003, Pg. 259
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

but not limited to temporarily storing the output data and providing it in portions as needed.

[0018] To increase the randomness of the hasher output, another source of input data is provided at input IN-1 from numerical sequencer (NS) 14. NS 14 is so named because it outputs a sequence of numbers. The sequence may eventually repeat, even though the period of repetition may be very long. In the illustrated embodiment of Fig. 1, the signal NSCLK is used to clock the processing elements of NS 14. In one embodiment, NSCLK is a derivative of CLK that may be stopped and started by control circuit 18 independently of CLK, so that hasher 12 continues to run while the output of NS 14 is stopped by a first predetermined event (such as receipt of a request for a pseudo random number), and restarted by a second predetermined event (such as the start of the next hash stage). In various embodiments, the ability to stop and start NS 14 independently of hasher 12 eliminates the synchronization that otherwise exists between NS 14 and hasher 12 if they are operated from a common clock source.

[0019] In one embodiment, NS 14 is a counter, such as a 64-bit counter, and NSCLK is used to increment (or decrement) the counter. In another embodiment, NS 14 is a linear feedback shift register (LFSR) and NSCLK is used to advance the bits through the elements of the LFSR.

[0020] Fig. 2 shows a schematic of a linear feedback shift register according to one embodiment of the invention. In the illustrated embodiment of linear feedback shift register (LFSR) 20, flip-flops 21-0 through 21-7 produce an eight-bit number on output bits b0 - b7. The value of the number may change with each pulse of the clock signal CLK as the current value is shifted through the flip-flops and modified by exclusive OR (XOR) gates 22-24. Each XOR gate modifies the input to a given flip-flop by performing an XOR operation on the output of the previous flip-flop with the output of one of the

WAVELYNX EX. 1003, Pg. 260
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

subsequent flip-flops. In the illustrated embodiment, the input to flip-flop 21-6 is modified by gate 22 by performing an XOR operation with the values of b7 and b0, the input to flip-flop 21-5 is modified by gate 23 by performing an XOR operation with the values of b6 and b5, the input to flip-flop 21-3 is modified by gate 24 by performing an XOR operation with the values of b4 and b1, and the value of b3 is fed back to the input of flip-flop 21-7 without modification. Other embodiments may use other feedback arrangements. In one embodiment, the output of multiple flip-flops may be fed back to a single XOR gate that provides the input to flip-flop 21-7.

[0021] Due to the effect of the above-described feedback arrangements and the XOR gates, the normally predictable flow of bits through a shift register may be transformed into a pseudo-random number generator. However, the finite number of bits and the fixed nature of the feedback arrangement eventually results in a repeating sequence of output values, in a similar manner to the way a counter outputs a repeating sequence of output values. A primary difference between the counter and the LFSR in this application is that a counter goes through long periods when the upper bits are the same, thus reducing some of the unpredictability experienced at the output.

[0022] In one embodiment, LFSR 20 includes as many flip-flops as are needed to produce a PRN with the desired number of bits, such as 64 flip-flops to produce a 64-bit number. In another embodiment, multiple LFSRs may be used in parallel, with their outputs combined to form a number with the required number of bits, such as using eight 8-bit LFSRs to produce a 64-bit number. In still another embodiment, several successive output values from LFSR 20 may be combined to form a number with the required number of bits, such as taking eight successive output values from an 8-bit LFSR and combining them into a 64-bit number.

WAVELYNX EX. 1003, Pg. 261
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0023] Figs. 3A, 3B show relative timing between stages and cycles according to one embodiment of the invention. Fig. 3A shows stages and cycles of an iterative hash operation and a numerical sequencer for the illustrated embodiment. A stage includes the operations necessary to produce a PRN at the PRNG output, while a cycle includes the operations necessary to produce a numerical sequencer output value. In one embodiment, a cycle is a clock cycle. In the illustrated embodiment of Fig. 3A, the hash algorithm requires 80 clock cycles to compute a hash value, plus 5 clock cycles of overhead, for a total of 85 clock cycles per stage. The terminology of the illustrated operation may be generically read as *s:c*, with *s* indicating the stage number 1 - n, and *c* indicating the cycle number 1-85 within each stage. After each stage, at least a portion of the hasher output may be placed into a register or other storage device, to be available as a PRN for any device or operation that requires a PRN. In one embodiment, the current PRN is replaced by a new PRN at the end of each stage, so that the PRN that is available to a device or operation repeatedly changes.

[0024] In some embodiments, at the beginning of each stage at least a part of the output from the previous stage is input as starting data, as shown by the looping arrows from cycle 1:85 to cycle 2:1, from cycle 2:85 to cycle 3:1, etc. This input is also shown at input IN-2 in Fig. 1. At the same time, NS 14 may be generating a sequence of new numbers. In one embodiment, each cycle produces a new number at the output of the numerical sequencer. In the illustrated embodiment of Fig. 3A, these cycles are shown as C_0, C_1, C_2, etc. At the time each hashing stage begins, at least a part of the current value of the NS output is used as part of the starting value for that stage, as shown by the right-to-left arrows in Fig. 3A. This input is also shown at IN-1 in Fig. 1. In one embodiment, the output of the NS is unrelated to the output of the hasher (i.e., the value of the NS output does not depend on the value of the hasher output), but the value of the hasher

WAVELYNX EX. 1003, Pg. 262
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

output depends on the value of the NS output. This one-way dependence increases the difficulty of deriving NS outputs based on the history of hasher outputs.

[0025] At the time the hash operation is initialized, there may be no previous result to use as input data, so seed data from any source may be used to initialize stage 1.

[0026] Fig. 3B shows a continuation of the embodiment of Fig. 3A, after the hasher has reached its 9th stage and the NS has produced more than 760 output values. In the illustrated embodiment of Fig. 3B, a request for a PRN is received at the 32nd cycle of the 10th stage. This request may come from any source that needs to be provided with a pseudo-random number for its operation. When the request is received, the operation of the NS may be frozen so that it ceases to produce new output values every clock cycle. In one embodiment, the operation of the NS is restarted at the beginning of the next hash stage. With reference to Fig. 1, stopping and starting NS 14 may be controlled by stopping and starting clock signal NSCLK with control circuit 18. Because the exact timing of a request for a PRN is generally unpredictable, at least with respect to the PRNG, the cycle at which the NS is frozen may also be unpredictable, and therefore the number of cycles it remains frozen may likewise be unpredictable. Thus the previously synchronized operation between the hashing operation and the NS output may be interrupted by a request for a PRN, and they lose synchronization by an unpredictable number of cycles. Loss of synchronization by even one cycle may produce an entirely different set of future outputs from the hasher.

[0027] Continuing with the illustrated embodiment of Fig. 3B, when the next hash stage (stage 11) starts, the frozen value in NS 14 is provided to hasher 12 as part of the hasher's input data. At that point, operation of NS 14 may resume and NS 14 may again start producing a new output value with every clock cycle. In the illustrated embodiment of Fig. 3B, NS 14 is frozen at cycle C_{796} when the request for a PRN is received. When

WAVELYNX EX. 1003, Pg. 263
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

stage 10 is completed, the frozen value of cycle C_{796} is provided to hasher 12 as input to begin stage 11, and NS 14 begins producing new numbers at cycle C_{797}.

[0028] In the illustrated example of Fig. 3B, if NS 14 were not frozen, stage 11 would start with the value of cycle C_{850}. The difference between the values at C_{796} and C_{850} represent 54 iterations of NS 14, and may represent significantly different values with which to start stage 11. Further, the number of iterations that make up the difference is random, and may be limited only by the number of clock cycles per stage.

[0029] In one circuit embodiment, NS 14 is frozen by stopping its clock (e.g., NSCLK in Fig. 1) and restarted by restarting its clock. In one software embodiment of the hasher, NS 14 is frozen by stopping a counter or other incrementing (or decrementing) entity, either in hardware or software, and restarted by restarting that entity.

[0030] In one embodiment, the first PRN requested after the system is initialized does not benefit from freezing the NS, since the PRN is created before the first incidence of freezing, but all subsequent PRN requests do benefit from freezing the NS. This shortcoming with the first requested PRN may be avoided by initially generating one or more false requests for a PRN, which will temporarily freeze the NS and generate sufficient randomness in subsequent PRN values.

[0031] Fig. 4 shows a block diagram of a specific embodiment of Fig. 1 according to one embodiment of the invention. In the PRNG 40 of Fig. 4, hasher 42, NS 44, feedback circuit 45, register 46 and control circuit 48 correspond to hasher 12, NS 14, feedback circuit 15, register 16 and control circuit 18 of Fig. 1, respectively, with specific numbers of bits at various inputs, outputs, and connections in PRNG 40. In the embodiment of Fig. 4, only a portion of the bits produced at various places are completely used, making it more difficult to discern the internal state of the logic. If only a portion of the bits output at a given point are used, and the remaining bits are not exposed, it is more

WAVELYNX EX. 1003, Pg. 264
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

difficult to determine the internal state of any part of the circuit because only partial information is available to aid in such a determination.

[0032] In the embodiment of Fig. 4, hasher 42 receives and internally operates with 512-bit numbers, but outputs only 160 of those bits, all of which are fed back to IN-2 produce a portion of the input for the next hash stage. Only 64 of the 160 bits are placed into register 46 for use as a PRN, and these 64 bits are the only bits that are exposed external to PRNG 40. In the same embodiment, NS 44 internally produces 70 bits, using 7 LFSRs of various lengths in parallel, but only outputs 32 of those bits. In one embodiment, NS 44 outputs 11 consecutive 32-bit values to fill up the 352 bits received by hasher 42 at IN-1. When the 160 bits of hasher 42 are reduced to 64 bits, and when the 70 bits of NS 44 are reduced to 32 bits, various techniques may be used to decide which of the available bits to use. In one embodiment, a group of consecutive bits are used, and the choice of which consecutive bits is a design choice. In another embodiment, the chosen bits are not consecutive, and their order may be rearranged before being output.

[0033] Fig. 5 shows a flow chart of a method according to one embodiment of the invention. In the flow chart 50 of the illustrated embodiment of Fig. 5, at block 51 a new hash stage is started, using the current value of a PRN and the current output of the numerical sequencer as input data. In one embodiment, the input data includes the full 160-bit previous output of the hasher, including the 64-bits of the PRN that that form a part of that output. If the system has just been initiated, these numbers may not exist yet and seed data may be used instead. Decision block 52 determines if a request has been received for a PRN. In one embodiment, once such a request is received, the answer to this decision block continues to be 'yes' until completion of the current hash stage. If a request for a PRN has been received, block 53 stops the numerical sequencer so that its output value remains frozen until the numerical sequencer is restarted. If no request has

WAVELYNX EX. 1003, Pg. 265
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

been received for a PRN, the numerical sequencer continues running and generates a new output value at block 54. Every pass through block 54 may create a new output value for the numerical sequencer, which becomes the current numerical sequencer value until it is changed. Whether or not a request for a PRN was received, the operation of the hash stage continues at block 55. In one embodiment, the clock for the hash operation and the clock for the numerical sequencer are the same frequency. Decision block 56 determines if the current hash stage has completed. If the current hash stage has not completed, control returns to block 52. If the hash stage has completed, the newly-generated PRN is loaded into a register, where it is available for subsequent PRN requests. Block 58 loads the new hasher output, including the new PRN, and the current output value of the numerical sequencer into the inputs of the hasher, where they become the starting values for the next hash stage that begins at block 51. Also, the numerical sequencer is restarted (or continues to run) so that it will be running at the start of the next hash stage.

[0034] Fig. 6 shows a system according to one embodiment of the invention. In the illustrated embodiment of Fig. 6, a system 60 includes a processor 61 coupled to a PRNG 10 through an input-output (I/O) bus 65 and an I/O controller 63. The I/O controller may also be coupled to a main memory 62 and an accelerated graphics processor (AGP) 64. Other devices (not shown) may also be coupled to the system. CPU 61 may execute software to operate PRNG 10. Any device that is capable of accessing PRNG 10 over I/O bus 65 may request a PRN and read the current PRN from PRNG 10.

[0035] In various embodiments, the variability in the precise timing of a call for a PRN introduces additional randomness, or entropy, into the operation of PRNG 10 over the operation of a similar PRNG without this variability. For example, if the timing of such a call varies over just one second, and a clock cycle is 15 nanoseconds (ns) long, a request for a PRN may arrive in any of 67 million cycles of NS 14. Since 67 million is

WAVELYNX EX. 1003, Pg. 266
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

approximately 2^{26}, this represents an entropy, or randomness, of 26 bits. When two calls are made, the two NS clock freezes represent (67 million)^2 possible values from NS 14, or 52 bits of entropy. Each additional call for a PRN creates an additional 26 bits of entropy. At some point, the amount of entropy from the NS will exceed the number of possible hashing sequences. This approximates the maximum amount of randomness available for the particular hash algorithm being used, and further calls may not increase the amount of randomness in the PRNG output. At this point, a brute force approach to determining the PRN may be the most efficient method of determining its value by a hostile attacker. In a data encryption environment, this may represent trying every possible combination of numbers in a decryption key to see if the result is intelligible.

Modified Secure Hash Algorithm

[0036] In various embodiments, a modified Secure Hash Algorithm (SHA) is used in the hasher. In one embodiment that uses the quantities of bits described in Fig. 4, the modified SHA operates in the following manner:

[0037] A 512-bit input (160 bits from the previous output of hasher 42 and 352 bits from NS 44 is used by hasher 42 as input data. The main loop in the modified SHA algorithm has a total of 80 sequential operations (t = 0 to 79) in the form of four groups of twenty operations. The non-linear SHA operations are as follows:

$f_t(B,C,D) = (B \wedge C) \vee (\sim B \wedge D)$ (for t = 0 to 19)

$f_t(B,C,D) = B \text{ xor } C \text{ xor } D$ (for t = 20-39)

$f_t(B,C,D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$ (for t = 40-59)

$f_t(B,C,D) = B \text{ xor } C \text{ xor } D$ (for t = 60-79)

where t = the number of the operation, $\wedge$ = logical AND, $\vee$ = logical OR, $\sim$ = logical complement, and xor = exclusive OR.

WAVELYNX EX. 1003, Pg. 267
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0038] Four constants K and five variables A, B, C, D, and E are used in the algorithms, where their values are shown in hexadecimal notation:

K_t = 5A827999 (for t = 0-19)

K_t = 6ED9EBA1 (for t = 20-39)

K_t = 8F1BBCDC (for t = 40-59)

K_t = CA62C1D6 (for t = 60-79)

Initial values for variables:

A_0 = 67452301

B_0 = EFCDAB89

C_0 = 98BADCFE

D_0 = 10325476

E_0 = C3D2E1F0

[0039] The input data is transformed from sixteen 32-bit words (M_0 - M_{15}) into eighty 32-bits words (W_0 - W_{79}) using the following algorithm:

$W_t = M_t$ (for t = 0-15)

$W_t = (W_{t-3}$ xor W_{t-8} xor W_{t-14} xor $W_{t-16})$ <<< 1 (for t = 16-79),

where <<< 1 = left shift one bit.

[0040] The main loop of the algorithm looks like this:

For t = 0 to 79,

TEMP = (A <<< 5) + F_t(B,C,D) + E_t + W_t +K_t

E = D

D = C

C = B <<< 30

B = A

A = TEMP

WAVELYNX EX. 1003, Pg. 268
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[0041] After 80 loops, the output of the modified SHA algorithm is the 160-bit string represented by ABCDE. In one embodiment, a 64-bit portion of this string is saved in register 46 as the current PRN, while the entire 160 bits is fed back to the input of hasher 42 to serve as part of the initial input data for the next hash stage. As previously described, the bits may be rearranged before being saved and/or fed back.

[0042] The aforementioned description describes one embodiment of the invention using a modified SHA algorithm, but other algorithms may be used without departing from the spirit of the invention.

[0043] The invention may be implemented in circuitry or as a method. The invention may also be implemented as instructions stored on a machine-readable medium, which may be read and executed by at least one processor to perform the operations described herein. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), and others.

[0044] The foregoing description is intended to be illustrative and not limiting. Variations will occur to those of skill in the art. Those variations are intended to be included in the invention, which is limited only by the spirit and scope of the appended claims.

WAVELYNX EX. 1003, Pg. 269
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

I claim:

1. An apparatus, comprising:

a hash circuit to receive first and second input values for a current hash stage and to generate an output value from the current hash stage based on the first and second input values;

a numerical sequencer coupled to the hash circuit to generate a sequence of numbers during the current hash stage and to provide at least a portion of a current one of the sequence of numbers as the first input value for a subsequent hash stage;

a feedback circuit coupled to the hash circuit to provide at least a portion of the output value as the second input value for the subsequent hash stage; and

a control circuit coupled to the numerical sequencer to stop generating the sequence of numbers upon an occurrence of a first predetermined event and to resume generating the sequence of numbers upon an occurrence of a second predetermined event.

2. The apparatus of claim 1, wherein:

the hash circuit is to receive the first and second input values at a beginning of the current hash stage.

3. The apparatus of claim 1, wherein:

the first predetermined event includes receipt of a request for a pseudo-random number.

WAVELYNX EX. 1003, Pg. 270
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

4. The apparatus of claim 1, wherein:

the second predetermined event includes a part of the subsequent hash stage.

5. The apparatus of claim 1, wherein:

the second predetermined event includes a beginning of the subsequent hash stage.

6. The apparatus of claim 1, wherein:

The numerical sequencer includes a counter.

7. The apparatus of claim 1, wherein:

the numerical sequencer includes a linear feedback shift register.

8. The apparatus of claim 1, wherein:

said at least a portion of the current one of the sequence of numbers includes predetermined bits of the current one of the sequence of numbers.

9. The apparatus of claim 1, wherein:

said at least a portion of the output value includes predetermined bits of the output value.

10. A system, comprising:

a processor;

a memory coupled to the processor; and

a pseudo-random number generator coupled to the processor and including:

WAVELYNX EX. 1003, Pg. 271
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

a hash circuit to receive first and second input values for a current hash stage and to generate an output value from the current hash stage based on the first and second input values;

a numerical sequencer coupled to the hash circuit to generate a sequence of numbers during the current hash stage and to provide at least a portion of a current one of the sequence of numbers as the first input value for a subsequent hash stage;

a feedback circuit coupled to the hash circuit to provide at least a portion of the output value as the second input value for the subsequent hash stage; and

a control circuit coupled to the numerical sequencer to stop generating the sequence of numbers upon an occurrence of a first predetermined event and to resume generating the sequence of numbers upon an occurrence of a second predetermined event.

11. The system of claim 10, wherein:

the hash circuit is to receive the first and second input values at a beginning of the current hash stage.

12. The system of claim 10, wherein:

the first predetermined event includes receipt of a request for a pseudo-random number.

13. The system of claim 10, wherein:

WAVELYNX EX. 1003, Pg. 272
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the second predetermined event includes a part of the subsequent hash stage.

14. The system of claim 10, wherein:

the second predetermined event includes a beginning of the subsequent hash stage.

15. The system of claim 10, wherein:

The numerical sequencer includes a counter.

16. The system of claim 10, wherein:

the numerical sequencer includes a linear feedback shift register.

17. The system of claim 10, wherein:

said at least a portion of the current one of the sequence of numbers includes predetermined bits of the current one of the sequence of numbers.

18. The system of claim 10, wherein:

said at least a portion of the output value includes predetermined bits of the output value.

19. A method, comprising:

generating a series of values during each of a previous hash stage, a current hash stage, and a subsequent hash stage;

receiving one of the values as a first hash input;

receiving a hash output from the previous hash stage as a second hash input;

WAVELYNX EX. 1003, Pg. 273
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

hashing the first and second hash inputs during a current hash stage to produce a current hash output;

stopping the generating when a first predetermined event occurs and restarting the generating when a second predetermined event occurs, if the first predetermined event occurs during the current hash stage; and

continuing the generating during the current hash stage, if the first predetermined event does not occur during the current hash stage.

20. The method of claim 19, wherein:

the first predetermined event includes receiving a request for a pseudo-random number.

21. The method of claim 19, wherein:

the second predetermined event includes a beginning of the subsequent hash stage.

22. A machine-readable medium having stored thereon instructions, which when executed by at least one processor cause said at least one processor to perform operations comprising:

generating a series of values during each of a previous hash stage, a current hash stage, and a subsequent hash stage;

receiving one of the values as a first hash input;

receiving a hash output from the previous hash stage as a second hash input;

hashing the first and second hash inputs during a current hash stage to produce a current hash output;

WAVELYNX EX. 1003, Pg. 274
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

stopping the generating when the first predetermined event occurs and restarting the generating when a second predetermined event occurs, if a first predetermined event occurs during the current hash stage; and

continuing the generating if the first predetermined event does not occur during the current hash stage.

23. The medium of claim 22, wherein:

the first predetermined event includes a request for a pseudo-random number.

24. The medium of claim 22, wherein:

the second predetermined event includes a beginning of a subsequent hash stage.

WAVELYNX EX. 1003, Pg. 275
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

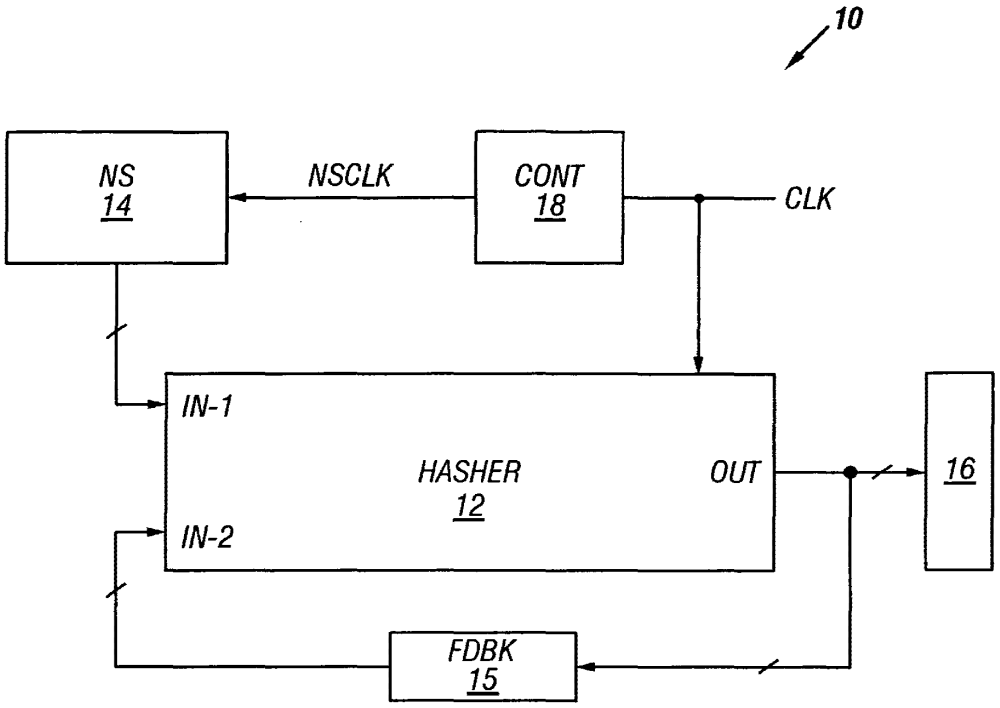


FIG. 1

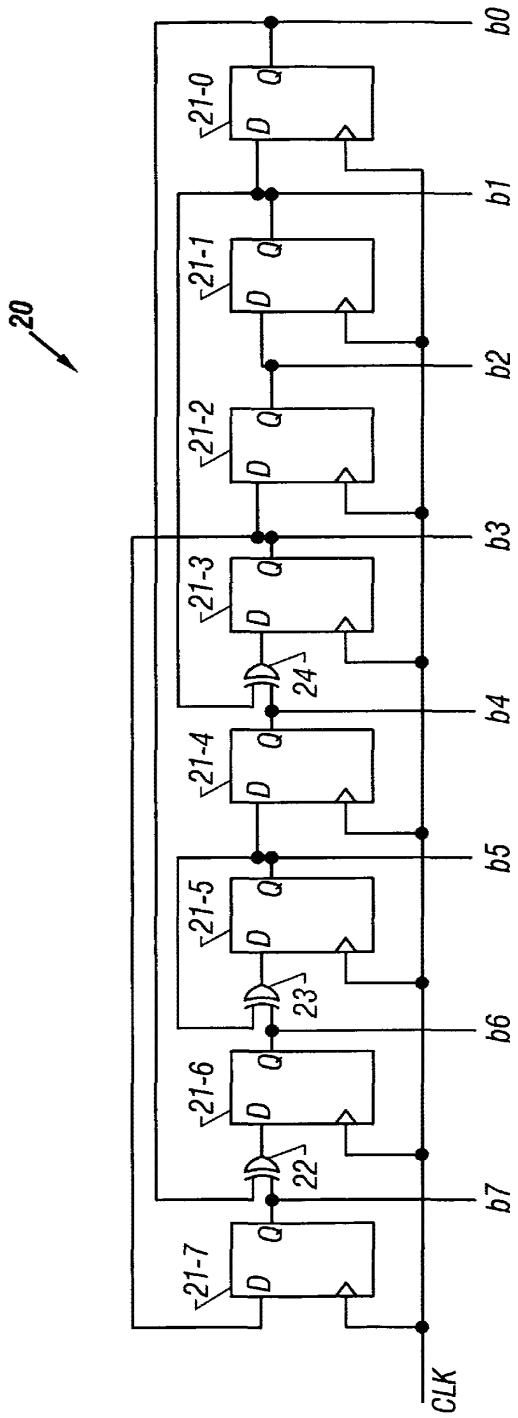

20
21-0
21-1
21-2
21-3
21-4
21-5
21-6
21-7
22
23
24
D
Q
b0
b1
b2
b3
b4
b5
b6
b7
CLK

FIG. 2

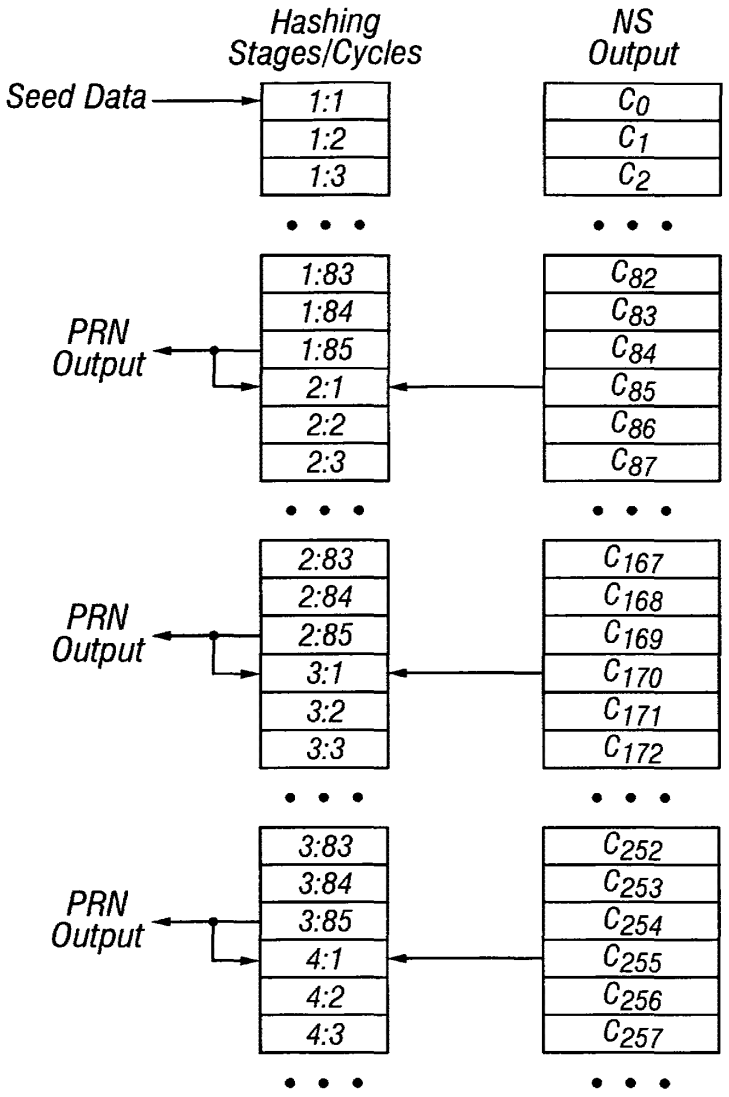

Hashing Stages/Cycles
NS Output
Seed Data
1:1
1:2
1:3
C0
C1
C2
1:83
1:84
1:85
2:1
2:2
2:3
C82
C83
C84
C85
C86
C87
PRN Output
2:83
2:84
2:85
3:1
3:2
3:3
C167
C168
C169
C170
C171
C172
PRN Output
3:83
3:84
3:85
4:1
4:2
4:3
C252
C253
C254
C255
C256
C257
PRN Output

FIG. 3A

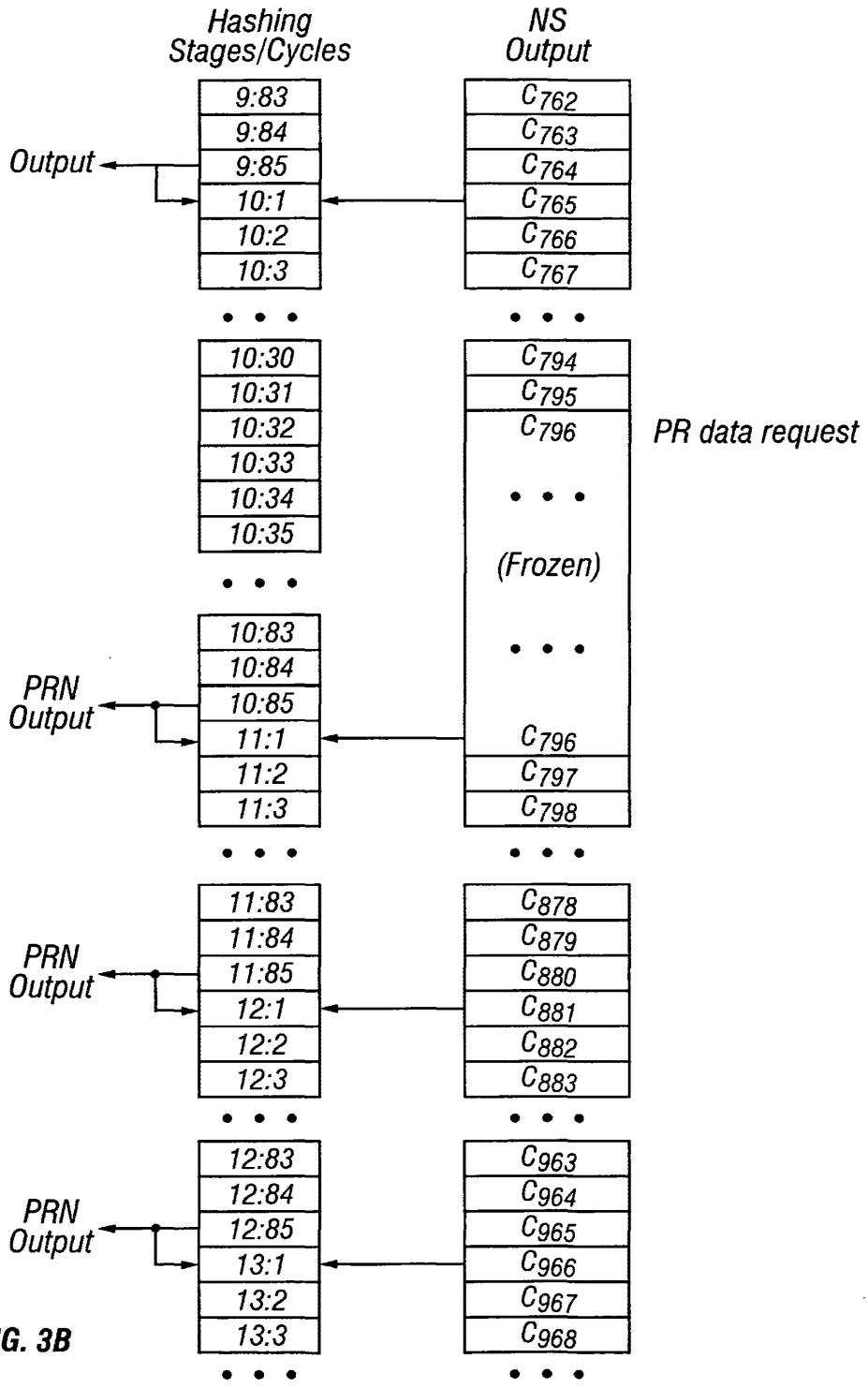

Hashing Stages/Cycles
NS Output
9:83
9:84
9:85
10:1
10:2
10:3
Output
C762
C763
C764
C765
C766
C767
10:30
10:31
10:32
10:33
10:34
10:35
C794
C795
C796
(Frozen)
C796
C797
C798
PR data request
10:83
10:84
10:85
11:1
11:2
11:3
PRN Output
11:83
11:84
11:85
12:1
12:2
12:3
C878
C879
C880
C881
C882
C883
12:83
12:84
12:85
13:1
13:2
13:3
C963
C964
C965
C966
C967
C968

FIG. 3B

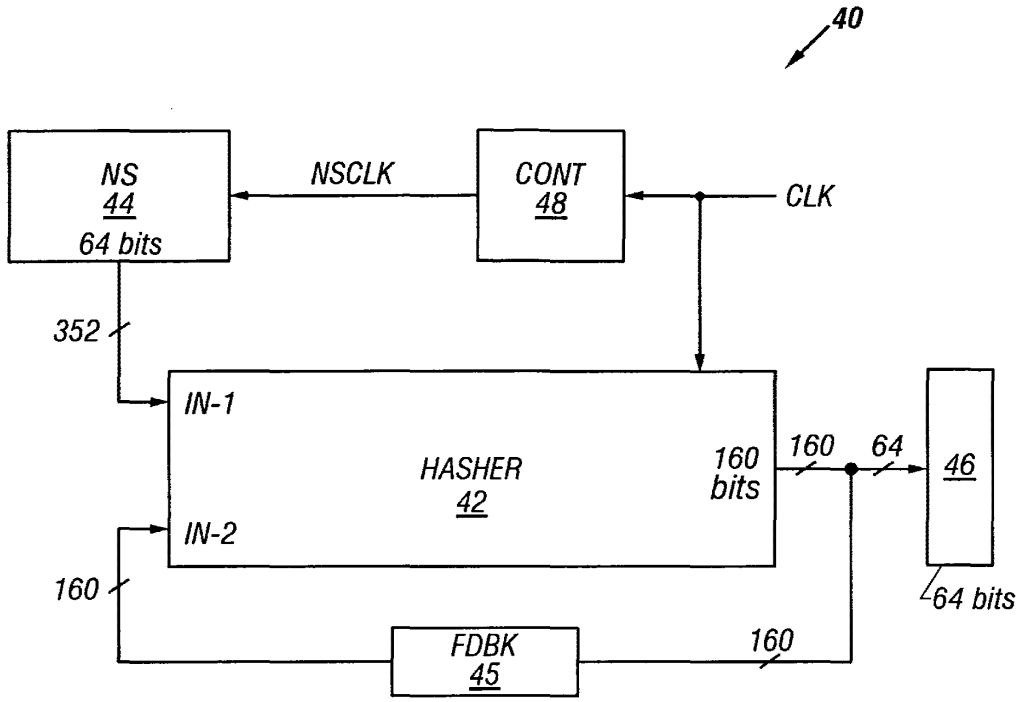

40
NS
44
64 bits
NSCLK
CONT
48
CLK
352
IN-1
HASHER
42
160
bits
160
64
46
IN-2
160
64 bits
FDBK
45
160

FIG. 4

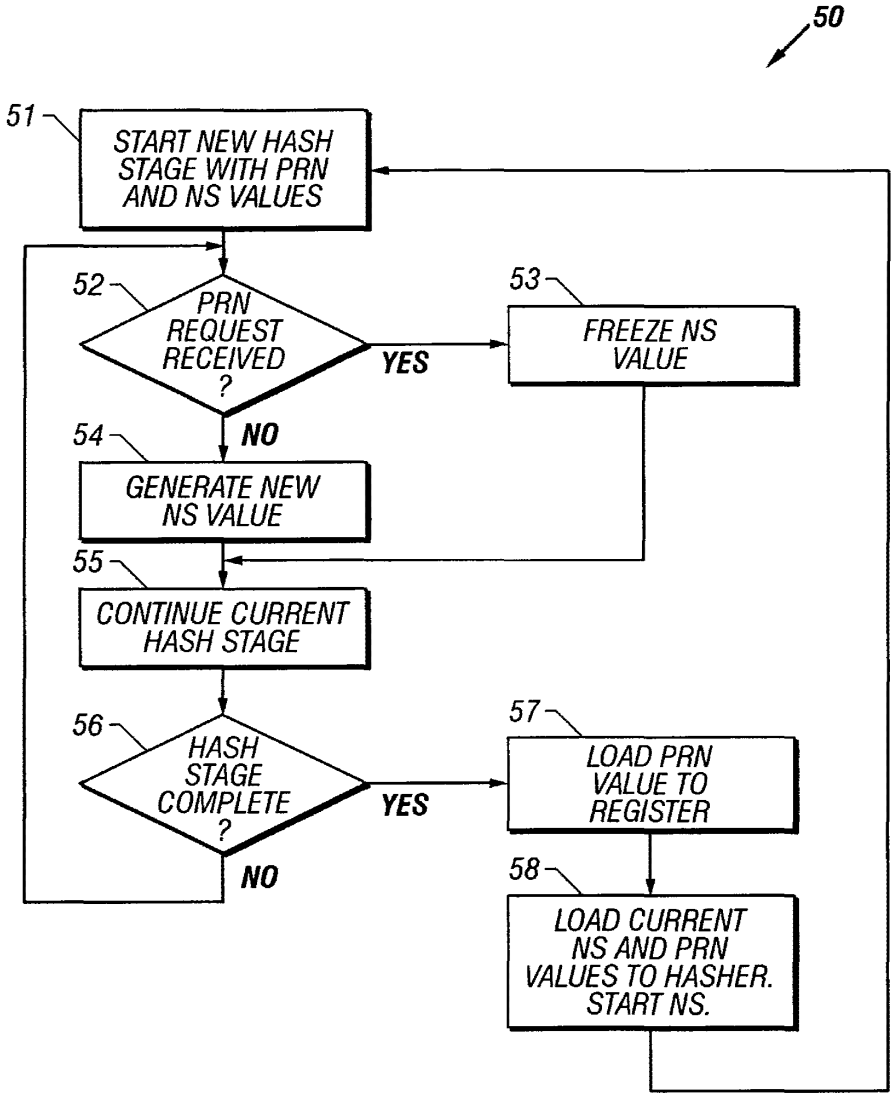

50
51
START NEW HASH STAGE WITH PRN AND NS VALUES
52
PRN REQUEST RECEIVED ?
YES
53
FREEZE NS VALUE
NO
54
GENERATE NEW NS VALUE
55
CONTINUE CURRENT HASH STAGE
56
HASH STAGE COMPLETE ?
YES
57
LOAD PRN VALUE TO REGISTER
NO
58
LOAD CURRENT NS AND PRN VALUES TO HASHER. START NS.

FIG. 5

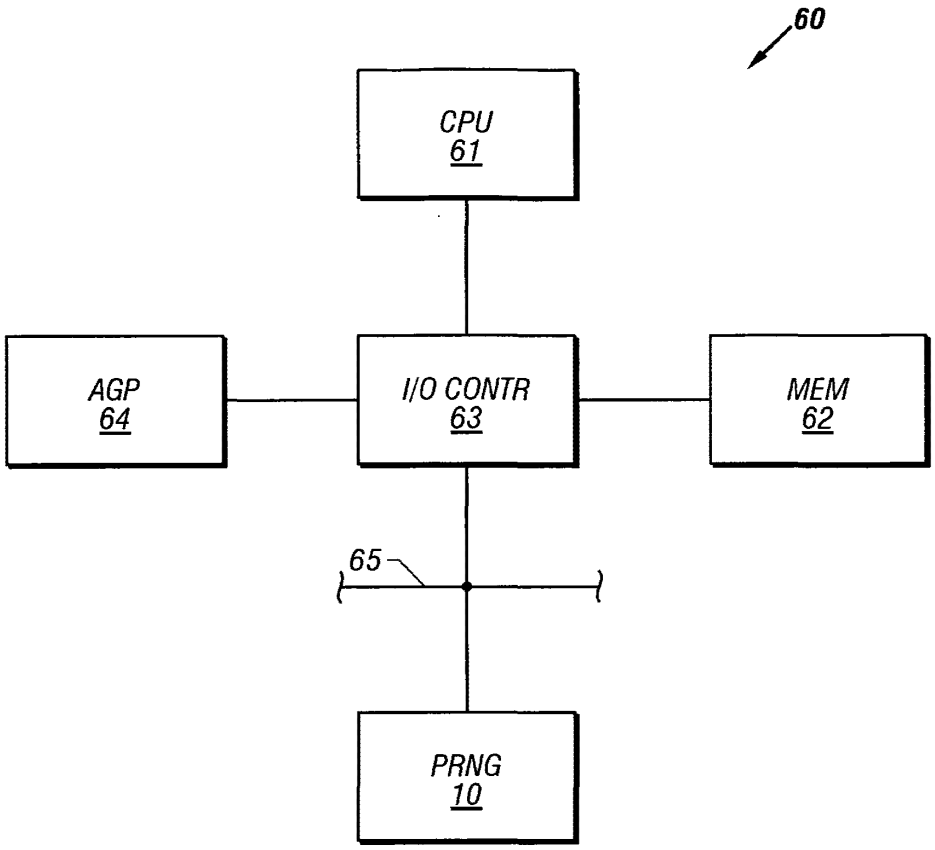


FIG. 6

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
22 mai 2003 (22.05.2003)

PCT

(10) Numéro de publication internationale
WO 03/042812 A2

(51) Classification internationale des brevets[7] : G06F 7/00

(21) Numéro de la demande internationale :
PCT/FR02/03652

(22) Date de dépôt international :
24 octobre 2002 (24.10.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/14785 15 novembre 2001 (15.11.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **EVERBEE NETWORKS** [FR/FR]; 41, boulevard des Capucines, F-75002 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **STEHLE, Jean-Luc** [FR/FR]; 300, rue de Vaugirard, F-75015 Paris (FR).

(74) Mandataire : **GRYNWALD, Albert**; Cabinet Grynwald, 127, rue du faoubourg poissonnière, F-75009 Paris (FR).

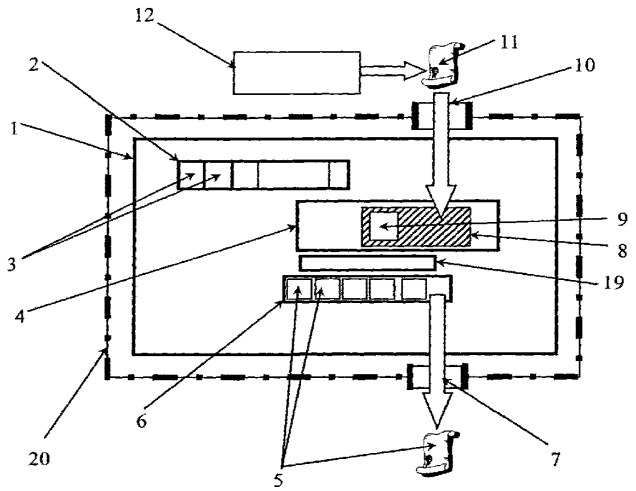
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR MAKING SECURE A PSEUDO-RANDOM GENERATOR

(54) Titre : PROCEDE ET SYSTEME POUR SECURISER UN GENERATEUR PSEUDO-ALEATOIRE



(57) Abstract: The invention concerns a method for making secure a generator (1) generating pseudo-random numbers (5). The generator (1) is characterized by its internal state. The generator (1) comprises: a first storage zone (2) containing state bits (3), representing the internal state of said generator (1); a computing unit (4) performing arithmetic operations on said state bits (3) to produce said pseudo-random numbers (5) and modify the state bits (3); a second storage zone (6) containing said pseudo-random numbers (5); a single output (7) for reading said pseudo-random numbers (5) contained in said second storage zone (6). The inventive method includes the step which consists in irreversibly and unconditionally inhibiting, in particular through logical and/or mechanical and/or electronic means, reading and writing of said state bits (3) from outside said generator (1), including via said single output (7).

[Suite sur la page suivante]

WO 03/042812 A2

eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé sécuriser un générateur (1) générant des nombres pseudo-aléatoires (5). Le générateur (1) est caractérisé par son état interne. Le générateur (1) comprend: - une première zone mémoire (2) contenant des bits d'état (3), représentant l'état interne dudit générateur (1), - une unité de calcul (4) effectuant des opérations arithmétiques sur lesdits bits d'état (3) pour produire lesdits nombres pseudo-aléatoires (5) et modifier lesdits bits d'état (3), - une seconde zone mémoire (6) contenant lesdits nombres pseudo-aléatoires (5), - une sortie unique (7) permettant de lire lesdits nombres pseudo-aléatoires (5) contenus dans ladite seconde zone mémoire (6). Le procédé selon l'invention comprend l'étape d'inhiber de manière irréversible et inconditionnelle, notamment par des moyens logiques et/ou mécaniques et/ou électroniques, la lecture et l'écriture desdits bits d'état (3) depuis l'extérieur dudit générateur (1), y compris via ladite sortie unique (7).

PROCEDE ET SYSTEME POUR SECURISER UN GENERATEUR PSEUDO-ALEATOIRE

Diverses applications nécessitent l'utilisation de nombres tirés au hasard, appelés ci-après nombres aléatoires. Ces nombres aléatoires sont utilisés entre autres dans des applications liées à la sécurité informatique. Ils servent en particulier à générer à la volée des clés de cryptage, par exemple dans le schéma de Diffie Hellman utilisé dans le protocole IPSEC.

Toute la sécurité des transmissions utilisant de tels protocoles repose sur la qualité du générateur de nombres aléatoires. Un générateur de nombres aléatoires fournit des suites d'octets qui doivent vérifier plusieurs caractéristiques. Tout d'abord, ces suites d'octets doivent être statistiquement aléatoires : tous les octets tirés devront être équiprobables. Cela signifie qu'en moyenne, il devra y avoir autant de 1 que de 2, que de 3, etc., et il devra en être de même pour toutes les paires d'octets, pour tous les triplets d'octets, quadruplets d'octets, et ainsi de suite. Plus généralement, une telle suite d'octets aléatoires devra avoir certaines propriétés mathématiques et statistiques bien connues et décrites, par exemple, dans l'ouvrage de Donald Knuth, The art of Computer Programming, volume 2: Seminumerical Algorithms, troisième édition pages 1 à 193, et, en particulier, pages 149 à 183.

WAVELYNX EX. 1003, Pg. 285
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Indépendamment de ces propriétés mathématiques et statistiques, les nombres aléatoires devront être imprédictibles en pratique. Entre autres, la connaissance des nombres préalablement tirés ne doit fournir à un éventuel pirate aucune information lui permettant de deviner que telle séquence pourrait avoir plus de chances d'être tirée que telle autre.

On distingue deux grandes familles de générateurs aléatoires.

La première famille regroupe les générateurs dits physiques. Ceux-ci reposent sur un phénomène physique considéré comme aléatoire. Ce phénomène pourra être par exemple le bruit de fond d'un circuit électronique, l'analyse d'un trafic sur un réseau informatique ou le résultat de calculs divers, entre autres d'algorithmes de hachage, sur le contenu de la mémoire vive d'un ordinateur. Les générateurs physiques peuvent être utilisés pour générer à la volée des clés de cryptage, mais ils sont non reproductibles et, en particulier, ils ne peuvent pas servir directement à générer un masque de cryptage.

Par ailleurs l'utilisation de générateurs physiques basés sur un phénomène physique considéré comme parfaitement aléatoire peut poser quelques problèmes pratiques. Le recueil du bruit de fond d'un élément de circuit électronique nécessite un dispositif électronique onéreux et encombrant pour amplifier ce bruit de fond et s'en servir pour construire des octets vérifiant les propriétés statistiques requises. L'analyse du trafic d'un réseau informatique est susceptible d'introduire des failles de sécurité dans la mesure où un pirate pourrait analyser le même trafic, ce qui lui permettrait d'avoir des informations sur les clés de cryptage. Il en est de même si on utilise des algorithmes de hachage appliqués au contenu de certaines mémoires informatiques, car si un pirate peut accéder à ces mémoires, il pourra en déduire les mêmes nombres aléatoires mettant ainsi à mal la sécurité du système.

La seconde famille regroupe des générateurs connus sous le nom de générateurs pseudo-aléatoires. Ces derniers

WAVELYNX EX. 1003, Pg. 286
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

reposent sur un algorithme mathématique exécuté sur un équipement informatique et peuvent être réalisés soit de manière purement logicielle, soit sur un coprocesseur spécifique. Un générateur pseudo-aléatoire est, au sens mathématique du terme, un automate fini, entièrement déterministe. Pour cette raison les nombres générés par un générateur pseudo-aléatoire sont souvent appelés des nombres pseudo-aléatoires. La suite des nombres pseudo-aléatoires générés dépend de l'état de l'automate, représenté en pratique par un certain nombre de bits appelés ci-après les bits d'état du générateur pseudo-aléatoire. Ces bits d'état sont stockés dans une zone mémoire appelée ci-après première zone mémoire. A chaque tirage d'un nombre pseudo-aléatoire, le générateur pseudo-aléatoire lit la valeur de ses bits d'état, et effectue, à partir de ces valeurs, des calculs dont les résultats permettront, d'une part, de fournir le nombre pseudo-aléatoire recherché et, d'autre part, de fournir de nouvelles valeurs des bits d'état, qui remplaceront les anciennes valeurs de ces bits d'état. Le générateur pseudo-aléatoire sera alors prêt pour le tirage suivant.

Nous nous intéresserons par la suite uniquement aux générateurs pseudo-aléatoires.

L'utilisation des générateurs pseudo-aléatoires pose divers problèmes de sécurité. En effet, une information, même partielle, sur les bits d'état du générateur pseudo-aléatoire permet de prévoir que, parmi les suites de nombres pseudo-aléatoires qui vont être tirées, certaines suites seront plus probables que d'autres, et cette information peut aussi permettre de connaître ces suites plus probables. Une telle information pourrait donc fournir à un éventuel pirate des armes pour attaquer le système informatique. Dans le cas où les bits d'état sont totalement connus, il est possible de prévoir avec certitude tous les nombres pseudo-aléatoires qui vont être tirés par la suite, ce qui rend illusoire toute utilisation de ce générateur pseudo-aléatoire pour des applications visant à sécuriser un système informatique.

WAVELYNX EX. 1003, Pg. 287
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Dans de nombreux générateurs pseudo-aléatoires il est possible, à partir de l'historique des tirages précédemment effectués, de remonter à l'état interne du générateur, donc de déterminer la valeur des bits d'état. On peut alors déterminer avec certitude les résultats de tous les tirages futurs. Même si l'historique ne donne qu'une information partielle, cela permettra de déterminer que certaines configurations des bits d'état sont plus probables que d'autres, et de calculer lesquelles, donc de prévoir que certaines séquences de nombres pseudo-aléatoires seront plus probables que d'autres. Bien évidemment de tels générateurs ne doivent jamais être utilisés pour des applications de sécurité informatique.

D'autres générateurs pseudo-aléatoires sont basés sur des algorithmes mathématiques plus sophistiqués qui ne permettent pas, à partir de l'historique de tirages passés, de remonter à l'état interne du générateur pseudo-aléatoire. Néanmoins d'autres types d'attaques sont possibles.

L'une des attaques possibles consiste à prendre connaissance de l'état interne du générateur pseudo-aléatoire en lisant la zone mémoire qui le contient, ou, ce qui aboutit au même résultat, à écrire dans cette zone mémoire une valeur spécifiée par l'attaquant. Ceci est possible de diverses façons, et en particulier à l'aide de virus ou de chevaux de Troie infectant un poste de travail connecté à un réseau informatique.

Une autre attaque est l'attaque par réinitialisation. Lorsqu'on met sous tension un système informatique, la mémoire vive se retrouve en général dans un état donné (tous les bits à 0 ou tous les bits à 1), et on peut donc connaître l'état interne du générateur pseudo-aléatoire. Si un attaquant peut provoquer une brève coupure de courant, il peut donc connaître l'état interne du générateur pseudo-aléatoire lors de la remise sous tension et il lui est alors possible de prévoir tous les états internes futurs, donc tous les nombres pseudo-aléatoires qui vont être générés.

WAVELYNX EX. 1003, Pg. 288
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Un autre problème lié à l'utilisation des générateurs pseudo-aléatoires provient de ce qu'ils sont, en général, implémentés par logiciel. Lorsqu'une application a besoin d'un nombre aléatoire, elle lance une routine qui va faire fonctionner le générateur pseudo-aléatoire. Cette routine consiste à consulter l'état du générateur puis à faire un calcul qui, d'une part, modifie cet état et, d'autre part, renvoie le nombre pseudo-aléatoire souhaité. Cela signifie que le générateur pseudo-aléatoire ne fonctionne que si l'on s'en sert. Plus précisément, cela signifie qu'il y a eu un nombre relativement petit de tirages aléatoires effectivement réalisés depuis la mise sous tension du système et le pirate n'aura qu'un petit nombre de clés à tester pour casser le système. Si ce nombre de clés est de quelques millions ou de quelques milliards, il suffit de peu de temps à un micro-ordinateur pour les tester toutes.

Un générateur pseudo-aléatoire est souvent considérablement moins coûteux à réaliser qu'un générateur physique. Si la réalisation est purement logicielle, le coût est négligeable. Même en cas de réalisation matérielle, un coprocesseur de faible puissance est suffisant car les algorithmes à mettre en œuvre sont simples et le stockage de l'état interne du générateur, c'est-à-dire des bits d'état, occupe très peu de mémoire. Un générateur pseudo-aléatoire peut être implémenté au sein d'un circuit intégré sur une « puce » en silicium et il occupera alors une place minime et représentera un surcoût négligeable par rapport au coût de conception, de développement et de fabrication du circuit intégré.

L'invention décrite ici, objet du présent brevet, concerne un procédé et un système pour sécuriser des générateurs pseudo-aléatoires, permettant ainsi de les utiliser en palliant aux divers inconvénients décrits ci-dessus. Elle permet de réaliser des générateurs pseudo-aléatoires ayant toutes les qualités requises, entre autres pour des applications liées à la sécurité informatique, cette réalisation étant possible à un

WAVELYNX EX. 1003, Pg. 289
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

coût significativement plus faible que celui d'un générateur aléatoire physique. L'invention peut être utilisée pour n'importe quel type de générateur pseudo-aléatoire, indépendamment de l'algorithme mathématique utilisé, pourvu que cet algorithme soit suffisamment sophistiqué pour empêcher que la connaissance de l'historique des tirages passés puisse donner une quelconque information sur l'état interne du générateur.

L'invention concerne un procédé pour sécuriser un générateur générant des nombres pseudo-aléatoires.

Le générateur est caractérisé par un état interne. Le générateur comprend :

- une première zone mémoire contenant des bits d'état, représentant l'état interne du générateur,
- une unité de calcul effectuant des opérations arithmétiques sur les bits d'état pour produire les nombres pseudo-aléatoires et modifier les bits d'état,
- une seconde zone mémoire contenant les nombres pseudo-aléatoires,
- une sortie unique permettant de lire les nombres pseudo-aléatoires contenus dans la seconde zone mémoire.

Le procédé selon l'invention comprend l'étape d'inhiber de manière irréversible et inconditionnelle, notamment par des moyens logiques et/ou mécaniques et/ou électroniques, la lecture et l'écriture des bits d'état depuis l'extérieur du générateur, y compris via la sortie unique.

De préférence, selon l'invention le procédé est plus particulièrement destiné à sécuriser un générateur. Le générateur comprend en outre des premiers moyens de calcul comportant un opérateur XOR et ayant une entrée unique permettant d'entrer des données provenant d'une source extérieure au générateur. Le procédé comprend l'étape, pour les premiers moyens de calcul, de modifier l'état des bits d'état en mettant en œuvre l'opérateur XOR entre les données et au moins une partie des bits d'état.

WAVELYNX EX. 1003, Pg. 290
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Il résulte de la combinaison des traits techniques que la valeur des bits d'état ne peut être déduite de la connaissance des données.

De préférence, selon l'invention le générateur produit en permanence des nombres pseudo-aléatoires pour les besoins d'un système informatique et mémorise dans la seconde zone mémoire le dernier nombre pseudo-aléatoire produit en le substituant au nombre pseudo-aléatoire précédent.

Le procédé comprend l'étape, pour le système informatique, de lire par intermittence dans la seconde zone mémoire, via la sortie unique, les nombres pseudo-aléatoires de manière asynchrone par rapport à leur production.

Il résulte de la combinaison des traits techniques que le caractère aléatoire et imprévisible des nombres pseudo-aléatoires utilisés par le système informatique est accentué.

Dans le cas d'une autre variante de réalisation de l'invention le générateur produit des nombres pseudo-aléatoires pour les besoins d'un système informatique. Dans le cas de cette variante de réalisation, le procédé comprend en outre un algorithme mis en œuvre, par intermittence, par le système informatique. L'algorithme comporte les étapes suivantes :

- l'étape de lire une partie des nombres pseudo-aléatoires produits par le générateur pour constituer une suite d'arguments,
- l'étape de calculer une suite de bits de perturbation en exécutant des opérations arithmétiques sur les arguments,
- l'étape de modifier les bits d'état en mettant en œuvre l'opérateur XOR entre la suite de bits de perturbation et au moins une partie des bits d'état.

De préférence, dans le cas de cette variante de réalisation selon l'invention, le procédé est tel que pour calculer la suite de bits de perturbation :

- on spécifie une clé de cryptage, notamment au moyen d'une partie des arguments,

WAVELYNX EX. 1003, Pg. 291
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- on spécifie une suite de nombres à crypter, notamment au moyen d'une partie des arguments,

- on met en œuvre un algorithme de cryptage pour produire, au moyen de la clé de cryptage et de la suite de nombres à crypter, la suite de bits de perturbation.

De préférence, le générateur est lui-même constitué de plusieurs générateurs pseudo-aléatoires élémentaires, d'un registre d'adressage et d'une troisième zone mémoire. Chacun des générateurs pseudo-aléatoires élémentaires comprend ses propres bits d'état dénommés bits d'états élémentaires. Les bits d'état du générateur, contenus dans la première zone mémoire du générateur, sont constitués par la réunion du registre d'adressage, de la troisième zone mémoire et des bits d'état élémentaires.

Dans le cas de cette variante de réalisation, le procédé selon l'invention est caractérisé en ce que la génération des nombres pseudo-aléatoires par le générateur comprend les étapes suivantes :

- l'étape d'extraire du registre d'adressage des informations permettant de spécifier, parmi les générateurs pseudo-aléatoires élémentaires, lequel d'entre eux sera utilisé lors de la prochaine itération du procédé,

- l'étape de faire fonctionner le générateur pseudo-aléatoire élémentaire spécifié à l'étape précédente pour en extraire un nombre ci-après dénommé le nombre candidat,

- l'étape d'extraire d'une partie des bits du registre d'adressage et d'une partie des bits du nombre candidat des informations permettant de spécifier une adresse dans la troisième zone mémoire,

- l'étape de lire dans la troisième zone mémoire le contenu de l'adresse spécifiée à l'étape précédente pour fournir les nombres pseudo-aléatoires,

- l'étape de stocker à l'adresse précédemment spécifiée dans la troisième zone mémoire une partie des bits du nombre candidat,

WAVELYNX EX. 1003, Pg. 292
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- l'étape d'utiliser une partie des bits du nombre candidat pour modifier le registre d'adressage.

L'invention concerne un système pour sécuriser un générateur générant des nombres pseudo-aléatoires. Le générateur est caractérisé par un état interne. Le générateur comprend :

- une première zone mémoire contenant des bits d'état, représentant l'état interne du générateur,
- une unité de calcul effectuant des opérations arithmétiques sur les bits d'état pour produire les nombres pseudo-aléatoires et modifier les bits d'état,
- des moyens de mémorisation pour mémoriser les nombres pseudo-aléatoires dans une seconde zone mémoire,
- une sortie unique permettant de lire les nombres pseudo-aléatoires contenus dans la seconde zone mémoire.

Le système comprend des moyens d'inhibition pour inhiber de manière irréversible et inconditionnelle, notamment par des moyens logiques et/ou mécaniques et/ou électroniques, la lecture et l'écriture des bits d'état depuis l'extérieur du générateur, y compris via la sortie unique.

De préférence, selon l'invention le générateur comprend en outre des premiers moyens de calcul comportant un opérateur XOR. Les premiers moyens de calcul ont une entrée unique permettant d'entrer des données provenant d'une source extérieure au générateur. Les premiers moyens de calcul permettent de modifier l'état des bits d'état en mettant en œuvre l'opérateur XOR entre les données et au moins une partie des bits d'état. Il résulte de la combinaison des traits techniques que la valeur des bits d'état ne peut être déduite de la connaissance des données.

De préférence, selon l'invention le système comprend un système informatique. Le générateur produit en permanence des nombres pseudo-aléatoires pour les besoins du système informatique.

Les moyens de mémorisation mémorisent dans la seconde zone mémoire le dernier nombre pseudo-aléatoire produit et

WAVELYNX EX. 1003, Pg. 293
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

substituent ce dernier nombre pseudo-aléatoire au nombre pseudo-aléatoire précédent. Le système informatique comprend des moyens de lecture connectés à la sortie unique pour lire par intermittence dans la seconde zone mémoire, via la sortie unique, les nombres pseudo-aléatoires de manière asynchrone par rapport à leur production.

Il résulte de la combinaison des traits techniques que le caractère aléatoire et imprévisible des nombres pseudo-aléatoires utilisés par le système informatique est accentué.

De préférence, dans le cas d'une variante de réalisation de l'invention le système comprend un système informatique. Le générateur produit des nombres pseudo-aléatoires pour les besoins du système informatique. Le système informatique comprend en outre des moyens de traitement informatique mis en œuvre par intermittence. Les moyens de traitement informatique comprennent :

- des moyens de lecture connectés à la sortie unique pour lire une partie des nombres pseudo-aléatoires et pour constituer une suite d'arguments,
- des seconds moyens de calcul pour calculer une suite de bits de perturbation en exécutant des opérations arithmétiques sur les arguments,
- des moyens de transmission pour transmettre les bits de perturbation aux premiers moyens de calcul via la dite entrée unique.

Les premiers moyens de calcul permettent de modifier les bits d'état en mettant en œuvre un opérateur XOR entre la suite de bits de perturbation et au moins une partie des bits d'état.

De préférence, dans le cas de cette variante de réalisation selon l'invention, les seconds moyens de calcul calculent la suite de bits de perturbation :

- en spécifiant une clé de cryptage, notamment au moyen d'une partie des arguments,

WAVELYNX EX. 1003, Pg. 294
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- en spécifiant une suite de nombres à crypter, notamment au moyen d'une partie des arguments,

- en mettant en œuvre des moyens de cryptage pour produire au moyen de la clé de cryptage et de la suite de nombres à crypter, la suite de bits de perturbation.

De préférence selon une variante de réalisation de l'invention, le générateur comprend plusieurs générateurs pseudo-aléatoires élémentaires, un registre d'adressage et une troisième zone mémoire. Chacun des générateurs pseudo-aléatoires élémentaires comprend ses propres bits d'état dénommés bits d'états élémentaires. Les bits d'état contenus dans la première zone mémoire du générateur sont constitués par la réunion du registre d'adressage, de la troisième zone mémoire et des bits d'état élémentaires.

Le générateur comprend en outre des moyens de traitements informatiques permettant :

- d'extraire du registre d'adressage des informations permettant de spécifier, parmi les générateurs pseudo-aléatoires élémentaires, un générateur pseudo-aléatoire particulier,

- de faire fonctionner un générateur pseudo-aléatoire particulier pour fournir le nombre candidat,

- d'extraire d'une partie des bits du registre d'adressage et d'une partie des bits du nombre candidat, des informations permettant de spécifier une adresse dans la troisième zone mémoire,

- de lire dans la troisième zone mémoire le contenu de l'adresse, spécifiée à l'étape précédente, pour fournir des nombres pseudo-aléatoires,

- de stocker à l'adresse précédemment spécifiée dans la troisième zone mémoire une partie des bits du nombre candidat,

- d'utiliser une partie des bits du nombre candidat pour modifier le registre d'adressage.

L'invention décrite concerne donc un générateur pseudo-aléatoire qui est implémenté de telle sorte qu'il soit

WAVELYNX EX. 1003, Pg. 295
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

impossible d'avoir, depuis l'extérieur, une quelconque information sur les bits d'état c'est-à-dire sur l'état interne du générateur. Ces bits d'état sont stockés dans une première zone mémoire du générateur. De préférence, dans un mode particulier de réalisation de l'invention, le générateur utilisera un processeur dédicacé, utilisant une première zone mémoire qui n'est accessible que par lui seul. Dans ce mode particulier de réalisation le processeur dédicacé et cette première zone mémoire sont physiquement dans un dispositif matériel particulier de type circuit intégré en silicium ou « puce » d'une carte à puce, et ils occuperont tout ou partie de ce dispositif matériel.

Pour augmenter le caractère aléatoire de ce générateur, on le perturbe à intervalles non réguliers par des informations dites informations de perturbation et provenant d'une source extérieure. Cette perturbation consiste à modifier les bits d'état du générateur, contenus dans la première zone mémoire, sans que la connaissance des informations de perturbation puisse apporter une quelconque information sur la valeur des bits d'état, ni avant ni après la perturbation. Pour réaliser cette modification, on utilise un opérateur XOR appliqué entre au moins une partie des bits d'états et les bits de l'information de perturbation. Cette modification par opérateur XOR fonctionne de la manière suivante : pour chacun des bits d'état que l'on souhaite perturber, on consulte un bit dans les informations de perturbation, bit qu'on appellera bit de perturbation. Si le bit de perturbation est à 1, on retourne le bit d'état c'est-à-dire on remplace 0 par 1 et 1 par 0. Si le bit de perturbation est à 1, on ne modifie pas le bit d'état. L'intérêt d'une telle perturbation est qu'il n'y a aucun moyen depuis l'extérieur de connaître la valeur des bits d'état, ni avant, ni après la perturbation. Plus généralement, il est toujours impossible, depuis l'extérieur, d'accéder à quelque information que ce soit concernant le contenu de la première zone mémoire.

WAVELYNX EX. 1003, Pg. 296
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

L'utilisation d'un générateur pseudo-aléatoire utilisant un processeur spécifique présente un autre avantage. Nous avons vu précédemment que si le générateur ne tourne qu'au fur et à mesure des besoins du système qui l'utilise, il n'y aura eu, en général, qu'un petit nombre de tirages aléatoires effectués depuis la mise sous tension du système. Or même si ce nombre est de l'ordre de plusieurs milliards, cela permet une attaque facile si ces nombres pseudo-aléatoires sont utilisés pour des applications de sécurisation d'un système informatique. Une parade est de faire fonctionner le générateur pseudo-aléatoire en permanence, même si on ne l'utilise pas. Néanmoins une telle solution n'est pas toujours possible, car elle consomme des ressources informatiques dans le système utilisateur, ce qui peut être rédhibitoire dans certains cas. Si, par contre, le générateur pseudo-aléatoire possède son propre processeur, il peut tourner en permanence, et de façon totalement asynchrone par rapport à l'utilisation des nombres pseudo-aléatoires au fur et à mesure des besoins du système utilisateur, et ce, sans consommer aucune ressource informatique du système utilisateur.

Dans ce mode de réalisation, le générateur écrit les nombres pseudo-aléatoires successifs dans une seconde zone mémoire, les nombres pseudo-aléatoires nouvellement calculés venant remplacer les nombres pseudo-aléatoires précédemment stockés dans cette seconde zone mémoire. Le système informatique utilisant les résultats du générateur pseudo-aléatoire lira, au fur et à mesure de ses besoins, les nombres stockés dans cette seconde zone mémoire. Il recueillera donc les nombres pseudo-aléatoires qui viennent d'être calculés. Les nombres pseudo-aléatoires plus anciens seront effacés au fur et à mesure du calcul de nouveaux nombres pseudo-aléatoires.

De même qu'on peut recourir à une source extérieure pour perturber, à intervalles non réguliers, les bits du générateur aléatoire, on peut, dans une variante de réalisation de l'invention, calculer les informations de perturbation à

WAVELYNX EX. 1003, Pg. 297
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

partir des nombres pseudo-aléatoires eux-mêmes, tels que fournis par le générateur. Pour ce faire, à intervalles non réguliers, et de façon asynchrone par rapport à la lecture des nombres par le système utilisateur, on lira des nombres pseudo-aléatoires fournis par le générateur pseudo-aléatoire et stockés dans la seconde zone mémoire, puis on appliquera des opérations arithmétiques sur ces nombres pseudo-aléatoires en vue de fournir des informations de perturbation destinées à perturber les bits d'état du générateur pseudo-aléatoire.

Dans une variante particulière de réalisation ces opérations arithmétiques feront appel à un algorithme de cryptage. Dans cette variante particulière de réalisation, certains des nombres pseudo-aléatoires permettront de déterminer une clé de cryptage, d'autres un nombre à crypter, le résultat de cet algorithme de cryptage constituant les bits de perturbation. De préférence, on utilisera un algorithme de cryptage comme le DES (Data Encryption Standard, adopté comme par les autorités américaines le 23 novembre 1976), dont les propriétés statistiques assurent un caractère aléatoire aux informations de perturbations ainsi calculées.

A titre d'exemple purement illustratif et non limitatif, nous décrivons ci-après, un mode particulier de réalisation de l'invention.

Ce mode de réalisation est basé sur le générateur pseudo-aléatoire qui avait été proposé comme standard par Park et Miller (Communications of the ACM 1988) après avoir été primitivement proposé par Lewis, Goodman et Miller en 1969 et, entre autres, implémenté par IBM (par exemple dans le langage APL) dans les années 1970.

Dans ce générateur pseudo-aléatoire de Park et Miller, un « germe » g compris entre 1 et 2^31-2 (a^b désigne le nombre a élevé à la puissance b, c'est-à-dire le produit de b nombres égaux à a) sert à calculer le nombre pseudo-aléatoire. A chaque utilisation du générateur (donc à chaque fois qu'un nombre pseudo-aléatoire est fourni) le germe g est multiplié par

WAVELYNX EX. 1003, Pg. 298
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

7^5 = 16 807 et on en prend le reste modulo le nombre de Mersenne 2^31 - 1 = 2 147 483 647 (qui est un nombre premier). L'état interne du générateur de Park et Miller est défini par le nombre g, et les bits d'état sont les 31 bits constituant ce nombre g.

Le générateur pseudo-aléatoire de Park et Miller est suffisant pour de nombreuses applications, mais il présente quelques inconvénients parfaitement rédhibitoires.

Le premier inconvénient du générateur pseudo-aléatoire de Park et Miller est qu'il a une périodicité d'environ 2 milliards (exactement 2^31 moins 2). A la fin de chaque cycle d'environ 2 milliards de tirages, les mêmes valeurs reviennent dans le même ordre. Si ces valeurs sont utilisées pour sécuriser un système informatique, celui-ci est à la merci d'une attaque, dite « attaque en force », consistant à tester toutes les valeurs possibles (ce qui est à la portée de tout micro-ordinateur). La sécurité du système est alors équivalente à celle que fournirait une clé à 31 bits.

Le second inconvénient du générateur pseudo-aléatoire de Park et Miller est que ce générateur est parfaitement prévisible. La connaissance de la valeur du germe à un moment donné permet de prévoir parfaitement et avec précision les valeurs futures de ce germe et donc tous les nombres pseudo-aléatoires qui seront fournis par le générateur.

Dans le mode particulier de réalisation de l'invention présenté ici à titre d'exemple, plusieurs générateurs pseudo-aléatoires de Park et Miller fonctionnent conjointement. L'invention permet d'éviter les inconvénients évoqués habituels des générateurs de Park et Miller tels qu'ils sont classiquement utilisés. Le générateur objet de la présente invention, dans ce mode particulier de réalisation, se compose, entre autres, des éléments suivants :

- Un registre d'adressage sur 32 bits,
- Une troisième zone mémoire de 512 octets destinée à stocker des octets aléatoires,

WAVELYNX EX. 1003, Pg. 299
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

- Un ensemble de 32 générateurs pseudo-aléatoires de Park et Miller, appelés, par la suite, générateurs pseudo-aléatoires élémentaires. Sur le plan matériel, chacun de ces 32 générateurs pseudo-aléatoires élémentaires dispose de 31 bits d'état, appelés bits d'états élémentaires. Ces générateurs élémentaires se partagent un coprocesseur spécifique unique conçu pour calculer, à partir d'un nombre à 31 bits fourni comme argument, le reste modulo 2^31 - 1 = 2 147 483 647 du produit par 7^5 = 16 807 de ce nombre fourni en argument.

Les bits d'état du générateur objet de la présente invention sont la réunion des bits d'état élémentaires de chacun des 32 générateurs pseudo-aléatoires élémentaires (soit 32 fois 31, donc au total 992 bits), des 32 bits du registre d'adressage et des 512 octets de la troisième zone mémoire.

Le générateur objet de la présente invention fournit à intervalles réguliers des octets pseudo-aléatoires, la fourniture de chaque nouvel octet pseudo-aléatoire se faisant au cours d'une itération qui réalise successivement les opérations suivantes : 5 bits particuliers du registre d'adressage spécifient quel est le générateur pseudo-aléatoire de Park et Miller particulier qui sera utilisé parmi les 32 générateurs pseudo-aléatoires élémentaires présents.

L'état de ce générateur pseudo-aléatoire particulier ainsi spécifié est un nombre à 31 bits, nombre qui est lu et fourni comme argument au coprocesseur spécifique. Ce coprocesseur fournit en résultat un nombre, appelé nombre candidat, qui est le reste modulo 2^31 - 1 = 2 147 483 647 du produit de cet argument par le nombre 7^5 = 16 807.

L'état du générateur pseudo-aléatoire particulier spécifié précédemment prend alors une valeur égale à celle du nombre candidat.

On utilise une partie des bits du nombre candidat et une partie des bits du registre d'adressage pour calculer un nombre à 9 bits qui spécifie une adresse dans la troisième zone mémoire.

WAVELYNX EX. 1003, Pg. 300
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

L'octet de la troisième zone mémoire qui se trouve à l'adresse ainsi spécifiée est le nombre pseudo-aléatoire, résultat de l'itération en cours, nombre qui sera recopié dans la seconde zone mémoire du générateur objet de la présente invention, cette seconde zone mémoire étant destinée à stocker les résultats du générateur pseudo-aléatoire.

8 bits choisis parmi les 32 bits du nombre candidat forment un octet qui sera, par la suite, appelé octet candidat et qui viendra s'écrire dans la troisième zone mémoire à l'adresse précédemment spécifiée, donc à la place de l'octet qui avait été précédemment recopié dans la seconde zone mémoire.

Les 24 autres bits du nombre candidat sont utilisés pour modifier le registre d'adressage, cette modification consistant, d'une part, en l'application d'un opérateur XOR entre certains de ces bits et certains des bits du registre d'adressage et, d'autre part, en des permutations circulaires des bits du registre d'adressage.

Ceci termine l'itération en cours, et le générateur est prêt pour la prochaine itération.

On peut remarquer que la valeur de l'octet candidat résulte des valeurs d'un ensemble de 1024 bits qui sont, d'une part, les bits d'état élémentaires de chacun des 32 générateurs pseudo-aléatoires élémentaires (soit 32 fois 31, donc au total 992 bits) et, d'autre part, les 32 bits du registre d'adressage.

La connaissance des valeurs de ces 1024 bits permet non seulement de connaître l'octet candidat de l'itération en cours, mais toute la suite des octets candidats des itérations suivantes.

Les octets candidats sont recopiés dans la troisième zone mémoire, puis de là, par la suite, ils seront recopiés dans la seconde zone mémoire destinée à recueillir les octets pseudo-aléatoires résultats finaux du générateur objet de la présente invention. La partie du procédé, consistant à stocker provisoirement la valeur des octets candidats dans la troisième zone mémoire avant de les recopier, a pour effet de les

WAVELYNX EX. 1003, Pg. 301
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

mélanger. La suite des octets résultats finaux qui vont être écrits dans la seconde zone mémoire se compose des mêmes octets que la suite des octets candidats, mais dans un ordre différent. Les octets sont donc permutés avant d'être utilisés. Cette permutation a pour effet qu'il devient impossible, de retrouver, à partir des nombres pseudo-aléatoires successifs fournis par le générateur objet de la présente invention, d'en déduire directement des informations concernant l'état des générateurs pseudo-aléatoires élémentaires ou le registre d'adressage. La seule façon de reconstituer l'état interne du générateur objet de la présente invention, ou tout au moins les valeurs des 1024 bits permettant de reconstituer la suite des octets candidats successifs, consiste à procéder par essais et erreurs et à tester toutes les valeurs possibles de ces bits.

Par ailleurs, il résulte de la combinaison des traits techniques que le générateur, objet de la présente invention, dans sa variante de réalisation ci-dessus décrite, a, s'il fonctionne de façon autonome, sans perturbations, une périodicité supérieure à 2^500, ce qui est largement au-delà des besoins actuels et des besoins prévisibles pour les prochaines décennies en sécurité informatique.

De plus si ce générateur est perturbé de la façon décrite précédemment, il donne, pour des applications liées à la sécurité informatique, des résultats de qualité comparables à ceux que donnerait un générateur aléatoire physique basé sur un phénomène aléatoire pur.

Dans une variante particulière d'implémentation du mode de réalisation en cours de description, le générateur objet de la présente invention est réalisé au sein d'un circuit intégré comprenant d'autres composants, dont en particulier un processeur central, ces composants formant le système informatique pour les besoins duquel le générateur fournit des nombres pseudo-aléatoires. La conception même du circuit intégré fait qu'il est impossible d'obtenir une quelconque information sur la valeur des bits d'état du générateur objet de la présente

WAVELYNX EX. 1003, Pg. 302
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

invention, tant depuis l'extérieur du circuit intégré que depuis le système informatique implémenté sur le circuit intégré et utilisant les nombres pseudo-aléatoires fournis par le générateur. Les seules communications du générateur avec l'extérieur se font via une sortie unique qui permet au système informatique de lire les nombres contenus dans la seconde zone mémoire, et via une entrée unique qui permet de perturber les bits d'état du générateur pseudo-aléatoire en appliquant l'opérateur XOR entre ces bits d'état et des informations provenant d'une source externe au générateur, de sorte qu'il n'y a aucun moyen d'avoir une quelconque information sur les valeurs des bits d'état du générateur.

Le générateur fournit approximativement un octet pseudo-aléatoire toutes les 100 nanosecondes (donc dix millions d'octets pseudo-aléatoires par secondes). Les octets pseudo-aléatoires sont stockés dans la seconde zone mémoire et tenus à la disposition du système informatique qui y puisera selon ses besoins. Un octet pseudo-aléatoire, qui n'a pas été lu par ce système informatique avant la fourniture de l'octet suivant, sera effacé et remplacé par l'octet suivant. Compte tenu des vitesses de fonctionnement, d'une part, du générateur pseudo-aléatoire, d'autre part, du système informatique utilisant ces octets pseudo-aléatoires, ce dernier ne lit qu'exceptionnellement deux octets pseudo-aléatoires successifs. Les octets pseudo-aléatoires sont donc fournis de façon totalement asynchrone par rapport au système informatique qui les utilise, ce qui augmente le caractère aléatoire et imprévisible de ceux qui sont effectivement utilisés.

Dans cette variante particulière de réalisation de l'invention, le système informatique situé sur le circuit intégré comprend un bloc de cryptographie utilisant l'algorithme DES (Data Encryption Standard, adopté comme par les autorités américaines le 23 novembre 1976), appelé ci-après bloc DES.

A des intervalles non réguliers, le système informatique réalise sur le générateur pseudo-aléatoire une

WAVELYNX EX. 1003, Pg. 303
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

opération de perturbation consistant à lire des octets pseudo-aléatoires fournis par le générateur, à utiliser certains d'entre eux pour générer une clé de cryptage et d'autres pour générer une suite d'octets à crypter, à utiliser le bloc DES pour crypter cette suite d'octets à crypter en utilisant cette clé de cryptage. Le résultat de ce cryptage est une suite d'octets qui sera transmise au générateur pseudo-aléatoire et qui servira à modifier les bits d'état du générateur pseudo-aléatoire en appliquant un opérateur XOR entre ces bits d'état et le résultat du cryptage. Cette opération de perturbation est réalisée à intervalles non réguliers lorsque le processeur central du système informatique n'est pas occupé à d'autres tâches. Le temps total pour exécuter cette opération est de l'ordre de quelques millisecondes.

Nous allons montrer que le mode particulier de réalisation de l'invention décrit ci-dessus permet de fournir des nombres aléatoires adaptés à des applications visant à sécuriser un système informatique. Pour quantifier la notion de niveau de résistance d'un système à un type d'attaque donné, on définit une notion d'entropie liée au nombre moyen d'essais qu'un éventuel attaquant devra effectuer avant d'arriver à pénétrer le système par une attaque de ce type, ces essais étant effectués en prenant en compte les informations qui sont à la disposition de l'attaquant.

On dira que le système présente une entropie de n bits à un type donné d'attaque s'il faut au moyenne 2^n (2 puissance n) essais à un attaquant utilisant ce type d'attaque pour pénétrer le système. On considère qu'une entropie de 128 bits est largement suffisante pour assurer une sécurité parfaite à un type d'attaque donné, compte tenu de l'état des techniques ou prévisibles ces prochaines décennies. En effet le temps nécessaire à l'ensemble des ordinateurs de la planète, s'ils étaient utilisés conjointement pour mener à bien cette attaque, est significativement supérieur à l'âge de l'univers, même en

WAVELYNX EX. 1003, Pg. 304
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

tenant compte des augmentations des performances informatiques prévisibles pour les prochaines décennies.

Lors de la mise sous tension du générateur objet de la présente invention, dans le mode particulier de réalisation décrit ici, ou lors de sa réinitialisation suite à une coupure de courant, ou lors d'une attaque de type similaire, les bits d'état représentant l'état interne du générateur sont susceptibles de se retrouver dans un état connu. Le générateur réalise environ dix millions d'itérations par seconde. Si on connaît avec une précision parfaite le nombre d'itérations qui sépare l'initialisation ou la réinitialisation du générateur du moment où on utilise des nombres pseudo-aléatoires pour générer des clés de cryptage, et en l'absence de toute perturbation externe, on peut déterminer avec précision cette clé de cryptage. On considère néanmoins en pratique qu'il y a, sur ce nombre d'itérations, une imprécision de l'ordre de la racine carrée de ce nombre. Dans notre exemple 6,4 secondes après la réinitialisation, le nombre d'itération est d'environ 2^26. Si on admet que ce nombre est connu avec une précision de l'ordre de sa racine carrée, il faudra en moyenne 2^13 essais au pirate pour attaquer avec succès le système, c'est-à-dire retrouver les clés de cryptage. L'entropie à ce type d'attaque et donc de l'ordre de 13 bits ce qui est absolument insuffisant. Un an après la mise sous tension, il y aura eu environ 316 000 milliards d'itérations, soit environ 2^48, nombre qui peut être connu avec une précision de l'ordre de 2^24, soit une entropie de 24 bits, ce qui reste toujours absolument insuffisant.

Considérons maintenant une opération de perturbation qui est réalisée à un moment aléatoire, en fonction de l'activité du système informatique, elle-même liée à conditions extérieures telles que la charge du système ou le trafic sur un réseau informatique, et imaginons que l'attaquant puisse connaître avec une précision de l'ordre d'un dix millième de seconde le moment exact de la perturbation. Dans ces hypothèses il y a environ un millier de perturbations de ce type possibles

WAVELYNX EX. 1003, Pg. 305
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(soit 2^10), selon les nombres aléatoires utilisés pour la perturbation (rappelons que les nombres aléatoires situés dans la seconde mémoire sont modifiés tous les dix-millionièmes de seconde). Une telle perturbation introduit alors environ dix bits d'entropie supplémentaire. Il suffit d'une douzaine de telles perturbations pour arriver à une entropie de 128 bits. En fonctionnement normal du circuit intégré, il peut y avoir plusieurs dizaines de perturbations de ce type par seconde. La sécurité du système à ce type d'attaque dépasse donc largement, après quelques secondes, tout ce qu'on pourrait souhaiter.

On va maintenant décrire, à titre d'exemple illustratif et non exhaustif, les figures qui représentent :

- figure 1 : un schéma représentant une variante de réalisation de l'invention,
- figure 2 : un schéma représentant une autre variante de réalisation de l'invention,
- figure 3 : un schéma représentant une autre variante de réalisation de l'invention.

La figure 1 schématise le principe de l'invention, objet du présent brevet. Un générateur pseudo-aléatoire 1 se compose d'une première zone mémoire 2 destinée à stocker l'état interne du générateur 1, cet état interne étant représenté par les bits d'état 3. Une unité de calcul 4 effectue des opérations arithmétiques sur ces bits d'état 3 en vue, d'une part, de modifier ces bits d'état 3 et d'autre part de produire des nombres pseudo-aléatoires 5 qui sont, via des moyens de mémorisation 19, envoyés dans une seconde zone mémoire 6. Ces nombres pseudo-aléatoires 5 peuvent être lus depuis cette seconde zone mémoire 6 via une sortie unique 7. La sécurité du système est assurée par des moyens d'inhibition 20 qui empêchent toute opération qui permettrait, depuis l'extérieur, d'obtenir une quelconque information sur la valeur des bits d'état 3.

Ces bits d'état 3 peuvent cependant être modifiés à l'aide de moyens de calculs 8 situés dans l'unité de calcul 4 et comportant un opérateur XOR 9. Ces moyens de calcul 8 utilisent

WAVELYNX EX. 1003, Pg. 306
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

des données 11 fournies par une source extérieure 12 et lues via une entrée unique 10. Ils appliquent l'opérateur XOR 9 entre les données 11 et au moins une partie des bits d'état 3 en vue de modifier ces bits d'état 3. Notons bien que la connaissance des données 11 qui interviennent lors de l'application de l'opérateur XOR 9 ne fournit aucune information sur la valeur des bits d'état 3 que ce soit avant ou après la perturbation.

La figure 2 schématise la façon dont un générateur pseudo-aléatoire 1 similaire à celui de la figure 1, et protégé par ses moyens d'inhibition 20, peut être utilisé en vue de fournir des nombres aléatoires 5 à un système informatique 13. Ce système informatique 13 comporte des moyens de lecture 21 permettant de lire, via la sortie unique 7, ces nombres aléatoires 5 dans la seconde zone mémoire 6 du générateur 1, tels qu'ils y avaient été mémorisés par les moyens de mémorisation 19. La lecture des nombres aléatoires 5 est faite à fur et à mesure des besoins du système informatique 13, de manière asynchrone à leur production, accentuant ainsi le caractère aléatoire et imprévisible des nombres aléatoires fournis. Au fur et à mesure que de nouveaux nombres aléatoires 5 sont générés par le générateur 1, ils sont mémorisés dans la seconde zone mémoire 6 par les moyens de mémorisation 19, le nombre aléatoire produit le plus récemment venant se substituer au nombre aléatoire précédent, ce dernier étant définitivement oublié.

La figure 3 schématise la façon dont un générateur pseudo-aléatoire 1, similaire à celui des figures 1 et 2, et protégé par ses moyens d'inhibition 20, produisant des nombres aléatoires 5 pour les besoins d'un système informatique 13 peut être perturbé de façon intermittente, de façon à augmenter le caractère aléatoire et imprévisible des nombres pseudo-aléatoires 5 ainsi produits. Le système informatique 13 comprend des moyens de traitements informatiques 22. Ces moyens de traitement informatique 22 comprennent des moyens de lecture 21 qui lisent, via la sortie 7, des nombres aléatoires 5 fournis

WAVELYNX EX. 1003, Pg. 307
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

par le générateur pseudo-aléatoire 1, et les utilisent pour constituer une suite d'arguments 14. Les moyens de traitement informatique 22 comprennent aussi des seconds moyens de calcul 23 permettant de calculer, à partir des arguments 14, une suite de bits de perturbations 15 qui sont transmis, via les moyens de transmission 25 à l'entrée unique 10 du générateur pseudo-aléatoire 1. Cette entrée unique 10 les transmet aux premiers moyens de calcul 8 situés dans l'unité de calcul 4 du générateur pseudo-aléatoire 1. Ces moyens de calcul 8 utilisent ces bits de perturbations 15 pour modifier l'état du générateur en appliquant l'opérateur XOR 9 entre les bits de perturbations 15 et au moins une partie des bits d'état 3 situés dans la première zone mémoire 2.

Dans un mode particulier de réalisation, les bits de perturbation 15 sont calculés à partir de la suite d'arguments 14 à l'aide de moyens de cryptage 24 faisant partie des moyens de traitement informatique 22 et mettant en œuvre un algorithme de cryptage 18 utilisant d'une part une clé de cryptage 16 et d'autre part des nombres à crypter 17, cette clé de cryptage 16 et ces nombres à crypter 17 étant spécifiés à partir d'une partie au moins des arguments 14.

La figure 4 schématise une variante particulière de réalisation de l'invention dans laquelle le générateur pseudo-aléatoire 1 se compose lui-même de plusieurs générateurs pseudo-aléatoires élémentaires 26, d'un registre d'adressage 27 et d'une troisième zone mémoire 28. Chacun des générateurs pseudo-aléatoires élémentaires 26 comprend ses propres bits d'état dénommés bits d'états élémentaires 29. Les bits d'état du générateur 1 sont contenus dans la première zone mémoire 2 et sont constitués par la réunion du registre d'adressage 27, de la troisième zone mémoire 28 et des bits d'état élémentaires 29. Le registre d'adressage 27 contient, d'une part, des informations permettant de spécifier, parmi les générateurs pseudo-aléatoires élémentaires 26, celui qui sera utilisé pour fournir un nombre candidat 30, et d'autre part des informations permettant de

WAVELYNX EX. 1003, Pg. 308
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

spécifier une adresse 31 dans la troisième zone mémoire 2. C'est à cette adresse 31 qu'est lu le prochain nombre pseudo-aléatoire 5 fourni par le générateur pseudo-aléatoire 1. Après lecture de ce nombre 5 une partie des bits du nombre candidat 30, seront stockés à cette adresse 31. Par ailleurs une partie des bits du nombre candidat 30 sont utilisés pour modifier le registre d'adressage 27.

WAVELYNX EX. 1003, Pg. 309
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

REVENDICATIONS

1. Procédé pour sécuriser un générateur (1) générant des nombres pseudo-aléatoires (5) ; ledit générateur (1) étant caractérisé par un état interne ;

ledit générateur (1) comprenant :

- une première zone mémoire (2) contenant des bits d'état (3), représentant l'état interne dudit générateur (1),
- une unité de calcul (4) effectuant des opérations arithmétiques sur lesdits bits d'état (3) pour produire lesdits nombres pseudo-aléatoires (5) et modifier lesdits bits d'état (3),
- une seconde zone mémoire (6) contenant lesdits nombres pseudo-aléatoires (5),
- une sortie unique (7) permettant de lire lesdits nombres pseudo-aléatoires (5) contenus dans ladite seconde zone mémoire (6),

ledit procédé comprenant l'étape d'inhiber de manière irréversible et inconditionnelle, notamment par des moyens logiques et/ou mécaniques et/ou électroniques, la lecture et l'écriture desdits bits d'état (3) depuis l'extérieur dudit générateur (1), y compris via ladite sortie unique (7).

2. Procédé selon la revendication 1 ; ledit procédé étant plus particulièrement destiné à sécuriser un générateur (1) comprenant en outre des premiers moyens de calcul (8) comportant un opérateur XOR (9) et ayant une entrée unique (10) permettant d'entrer des données (11) provenant d'une source extérieure (12) audit générateur (1) ;

ledit procédé comprenant l'étape, pour lesdits premiers moyens de calcul (8), de modifier l'état desdits bits d'état (3) en mettant en œuvre ledit opérateur XOR (9) entre lesdites données (11) et au moins une partie desdits bits d'état (3).

3. Procédé selon l'une quelconque des revendications 1 ou 2 ; ledit générateur (1) produisant en permanence des nombres

WAVELYNX EX. 1003, Pg. 310
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

pseudo-aléatoires (5) pour les besoins d'un système informatique (13) et mémorisant dans ladite seconde zone mémoire (6) le dernier nombre pseudo-aléatoire produit en le substituant au nombre pseudo-aléatoire précédent ;

ledit procédé comprenant l'étape, pour ledit système informatique (13), de lire par intermittence dans ladite seconde zone mémoire (6), via ladite sortie unique (7), lesdits nombres pseudo-aléatoires (5) de manière asynchrone par rapport à leur production.

4. Procédé selon l'une quelconque des revendications 2 ou 3 ; ledit générateur (1) produisant des nombres pseudo-aléatoires (5) pour les besoins d'un système informatique (13) ; ledit procédé comprenant en outre un algorithme mis en œuvre, par intermittence, par ledit système informatique (13) ; ledit algorithme comportant les étapes suivantes :

- l'étape de lire une partie desdits nombres pseudo-aléatoires (5) produits par ledit générateur (1) pour constituer une suite d'arguments (14),
- l'étape de calculer une suite de bits de perturbation (15) en exécutant des opérations arithmétique sur lesdits arguments (14),
- l'étape de modifier lesdits bits d'état (3) en mettant en œuvre ledit opérateur XOR (9) entre ladite suite de bits de perturbation (15) et au moins une partie desdits bits d'état (3).

5. Procédé selon la revendication 4 ; ledit procédé étant tel que pour calculer ladite suite de bits de perturbation (15) :

- on spécifie une clé de cryptage (16), notamment au moyen d'une partie desdits arguments (14),
- on spécifie une suite de nombres à crypter (17), notamment au moyen d'une partie desdits arguments (14),
- on met en œuvre un algorithme de cryptage (18) pour produire, au moyen de ladite clé de cryptage (16) et

WAVELYNX EX. 1003, Pg. 311
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

de ladite suite de nombres à crypter (17), ladite suite de bits de perturbation (15).

6. Procédé selon l'une quelconque des revendications 1 à 5 ; ledit générateur (1) étant lui-même constitué de plusieurs générateurs pseudo-aléatoires élémentaires (26), d'un registre d'adressage (27) et d'une troisième zone mémoire (28), chacun desdits générateurs pseudo-aléatoires élémentaires (26) comprenant ses propres bits d'état dénommés bits d'états élémentaires (29), lesdits bits d'état (3) contenus dans ladites première zone mémoire (2) dudit générateur (1) étant constitués par la réunion dudit registre d'adressage (27), de ladite troisième zone mémoire (28) et desdits bits d'état élémentaires (29),

ledit procédé étant caractérisé en ce que la génération desdits nombres pseudo-aléatoires (5) par ledit générateur (1) comprend les étapes suivantes :

- l'étape d'extraire dudit registre d'adressage (27) des informations permettant de spécifier, parmi lesdits générateurs pseudo-aléatoires élémentaires (26), lequel d'entre eux sera utilisé lors de la prochaine itération dudit procédé,
- l'étape de faire fonctionner ledit générateur pseudo-aléatoire élémentaire spécifié à l'étape précédente pour en extraire un nombre ci-après dénommé le nombre candidat (30),
- l'étape d'extraire d'une partie des bits du registre d'adressage (27) et d'une partie des bits dudit nombre candidat (30) des informations permettant de spécifier une adresse (31) dans ladite troisième zone mémoire (28),
- l'étape de lire dans ladite troisième zone mémoire (28) le contenu de ladite adresse (31) spécifiée à l'étape précédente pour fournir lesdits nombres pseudo-aléatoires (5),
- l'étape de stocker à ladite adresse (31) précédemment spécifiée dans ladite troisième zone mémoire (28) une partie des bits dudit nombre candidat (30),
- l'étape d'utiliser une partie des bits dudit nombre candidat (30) pour modifier ledit registre d'adressage (27).

WAVELYNX EX. 1003, Pg. 312
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

7. Système pour sécuriser un générateur (1) générant des nombres pseudo-aléatoires (5) ; ledit générateur (1) étant caractérisé par un état interne ;

ledit générateur (1) comprenant :

- une première zone mémoire (2) contenant des bits d'état (3), représentant l'état interne du générateur (1),

- une unité de calcul (4) effectuant des opérations arithmétiques sur lesdits bits d'état (3) pour produire lesdits nombres pseudo-aléatoires (5) et modifier lesdits bits d'état (3),

- des moyens de mémorisation (19) pour mémoriser lesdits nombres pseudo-aléatoires (5) dans une seconde zone mémoire (6),

- une sortie unique (7) permettant de lire lesdits nombres pseudo-aléatoires (5) contenus dans ladite seconde zone mémoire (6),

ledit système comprenant des moyens d'inhibition (20) pour inhiber de manière irréversible et inconditionnelle, notamment par des moyens logiques et/ou mécaniques et/ou électroniques, la lecture et l'écriture des bits d'état (3) depuis l'extérieur dudit générateur (1), y compris via ladite sortie unique (7).

8. Système selon la revendication 7 ; ledit générateur (1) comprenant en outre des premiers moyens de calcul (8) comportant un opérateur XOR (9) ; lesdits premiers moyens de calcul (8) ayant une entrée unique (10) permettant d'entrer des données (11) provenant d'une source extérieure (12) audit générateur (1) ; lesdits premiers moyens de calcul (8) permettant de modifier l'état desdits bits d'état (3) en mettant en œuvre ledit opérateur XOR (9) entre lesdites données (11) et au moins une partie desdits bits d'état (3).

9. Système selon l'une quelconque des revendications 7 ou 8 ; ledit système comprenant un système informatique (13) ; ledit générateur (1) produisant en permanence des nombres

WAVELYNX EX. 1003, Pg. 313
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

pseudo-aléatoires (5) pour les besoins dudit système informatique (13) ; lesdits moyens de mémorisation (19) mémorisant dans ladite seconde zone mémoire (6) le dernier nombre pseudo-aléatoire produit et substituant ledit dernier nombre pseudo-aléatoire au nombre pseudo-aléatoire précédent ;

ledit système informatique (13) comprenant des moyens de lecture (21) connectés à ladite sortie unique (7) pour lire par intermittence dans ladite seconde zone mémoire (6), via ladite sortie unique (7), lesdits nombres pseudo-aléatoires (5) de manière asynchrone par rapport à leur production.

10. Système selon l'une quelconque des revendications 8 ou 9 ; ledit système comprenant un système informatique (13) ; ledit générateur (1) produisant des nombres pseudo-aléatoires (5) pour les besoins dudit système informatique (13) ; ledit système informatique (13) comprenant en outre des moyens de traitement informatique (22) mis en œuvre par intermittence ; lesdits moyens de traitement informatique (22) comprenant :

- des moyens de lecture (21) connectés à ladite sortie unique (7) pour lire une partie desdits nombres pseudo-aléatoires (5) et pour constituer une suite d'arguments (14),
- des seconds moyens de calcul (23) pour calculer une suite de bits de perturbation (15) en exécutant des opérations arithmétique sur lesdits arguments (14),
- des moyens de transmission (25) pour transmettre lesdits bits de perturbation (15) auxdits premiers moyens de calcul (8) via la dite entrée unique (10) ;

lesdits premiers moyens de calcul (8) permettant de modifier lesdits bits d'état (3) en mettant en œuvre ledit opérateur XOR (9) entre ladite suite de bits de perturbation (15) et au moins une partie desdits bits d'état (3).

11. Système selon la revendication 10 ; lesdits seconds moyens de calcul (23) calculant ladite suite de bits de perturbation (15) :

- en spécifiant une clé de cryptage (16), notamment au moyen d'une partie desdits arguments (14),

- en spécifiant une suite de nombres à crypter (17), notamment au moyen d'une partie desdits arguments (14),

- en mettant en œuvre des moyens de cryptage (24) pour produire au moyen de ladite clé de cryptage (16) et ladite suite de nombres à crypter (17), ladite suite de bits de perturbation (15).

12. Système selon l'une quelconque des revendications 7 à 11; ledit générateur (1) comprenant plusieurs générateurs pseudo-aléatoires élémentaires (26), un registre d'adressage (27) et une troisième zone mémoire (28), chacun desdits générateurs pseudo-aléatoires élémentaires (26) comprenant ses propres bits d'état dénommés bits d'états élémentaires (29), lesdits bits d'état (3) contenus dans ladite première zone mémoire (2) dudit générateur (1) étant constitués par la réunion dudit registre d'adressage (27), de ladite troisième zone mémoire (28) et desdits bits d'état élémentaires (29),

ledit générateur (1) comprenant en outre des moyens de traitements informatiques permettant :

- d'extraire dudit registre d'adressage (27) des informations permettant de spécifier, parmi lesdits générateurs pseudo-aléatoires élémentaires (26), un générateur pseudo-aléatoire particulier,

- de faire fonctionner un générateur pseudo-aléatoire particulier pour fournir ledit nombre candidat (30),

- d'extraire d'une partie des bits du registre d'adressage (27) et d'une partie des bits dudit nombre candidat (30), des informations permettant de spécifier une adresse (31) dans ladite troisième zone mémoire (28),

- de lire dans ladite troisième zone mémoire (28) le contenu de ladite adresse (31) pour fournir lesdits nombres pseudo-aléatoires (5),

- de stocker à ladite adresse (31) précédemment spécifiée dans ladite troisième zone mémoire (28) une partie des bits dudit nombre candidat (30),

- d'utiliser une partie des bits dudit nombre candidat (30) pour modifier ledit registre d'adressage (27).

FIG.1

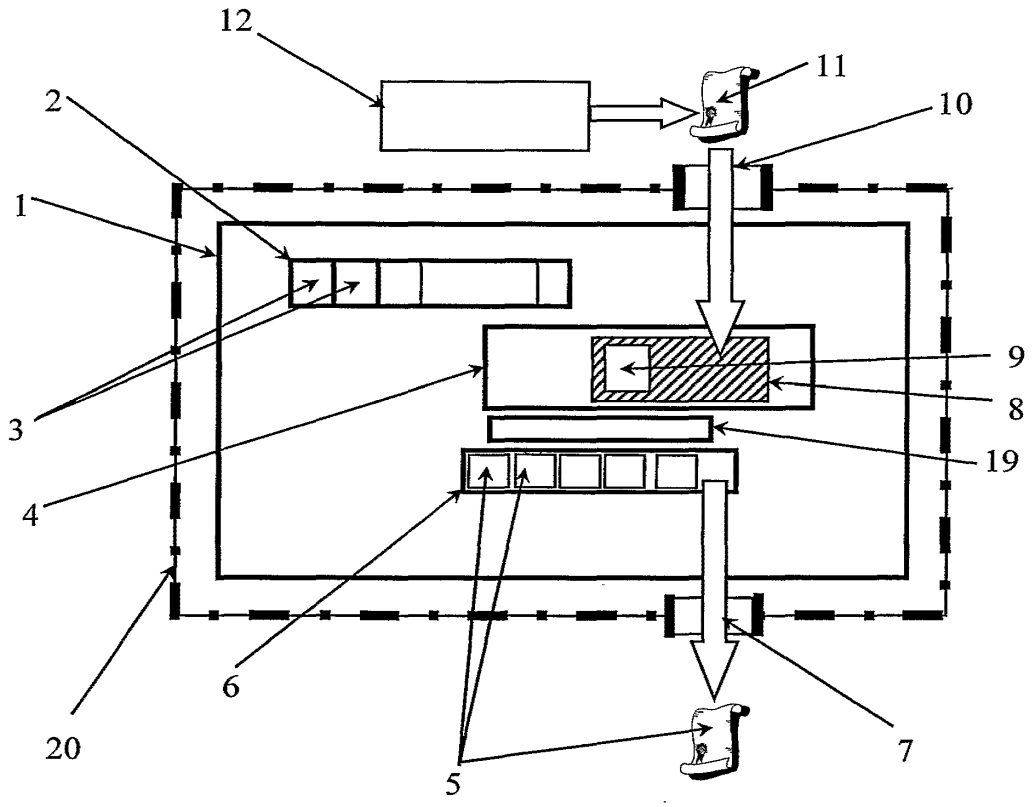
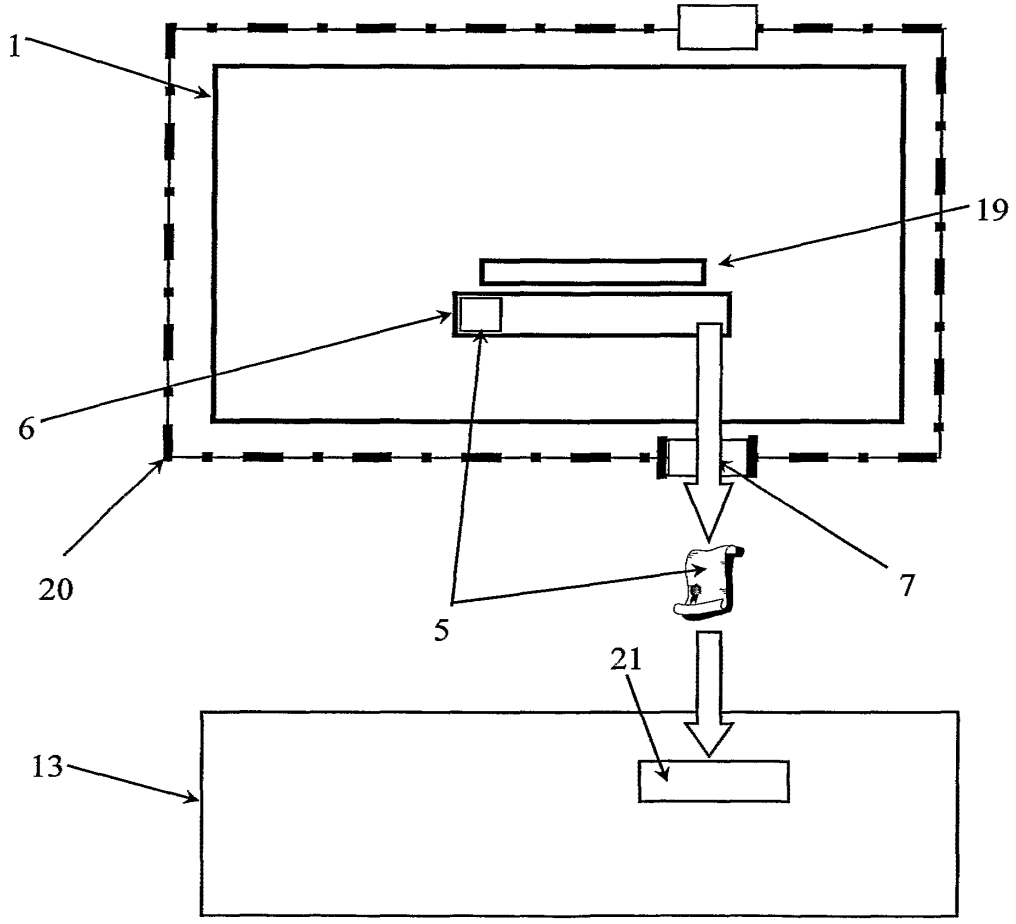


FIG.2



WAVELYNX EX. 1003, Pg. 318
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG.3

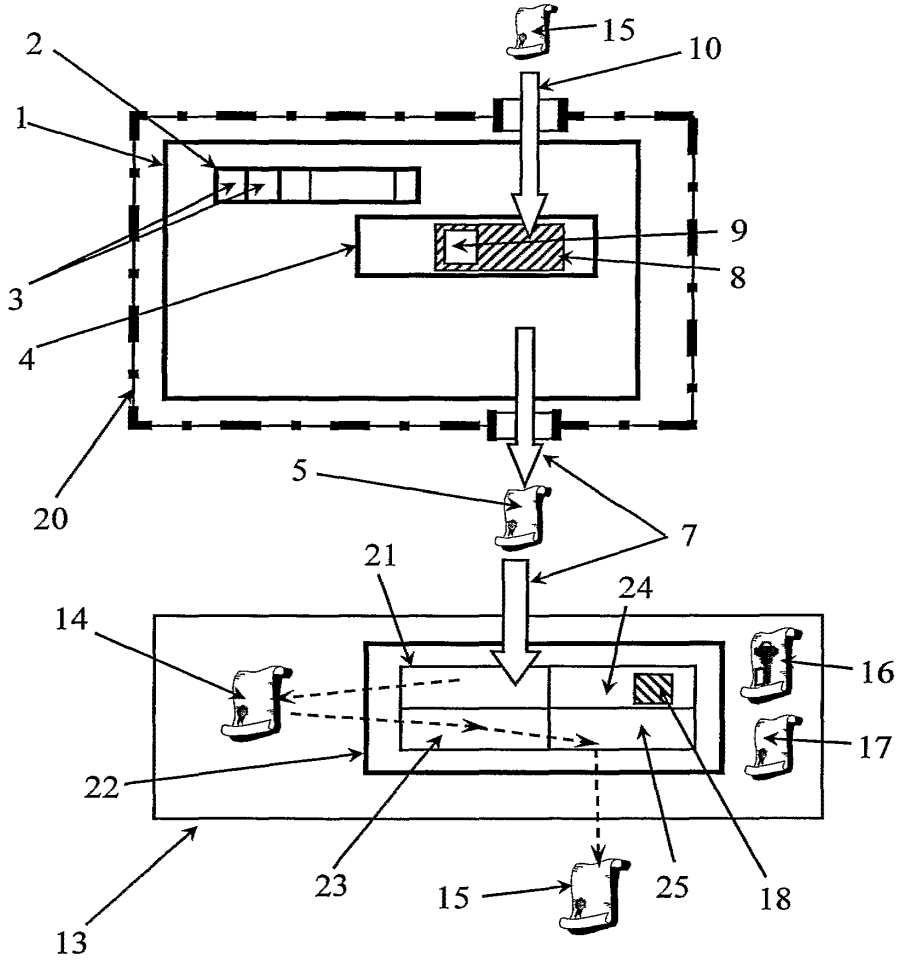
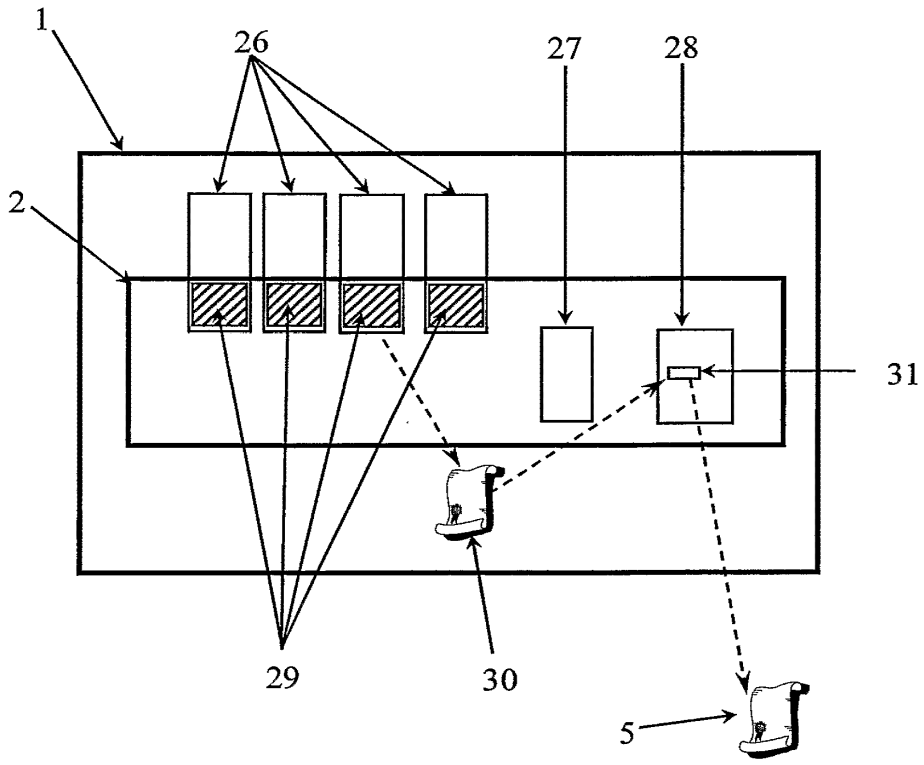


FIG.4



WAVELYNX EX. 1003, Pg. 320
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010373 A1

(51) International Patent Classification[7]: G06K 019/07

(21) International Application Number: PCT/AU2003/000934

(22) International Filing Date: 23 July 2003 (23.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/AU02/00984 24 July 2002 (24.07.2002) AU

(71) Applicant *(for all designated States except US)*: **BANQUE-TEC INTERNATIONAL PTY LTD** [AU/AU]; Unit 5, 12-18 Victoria Street, East Lidcombe, NSW 2141 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BLAKE, Christopher, Ian** [AU/AU]; C/o Banque-Tec International, Unite 5, 12-18 Victoria Street, East Lidcombe, NSW 2141 (AU).

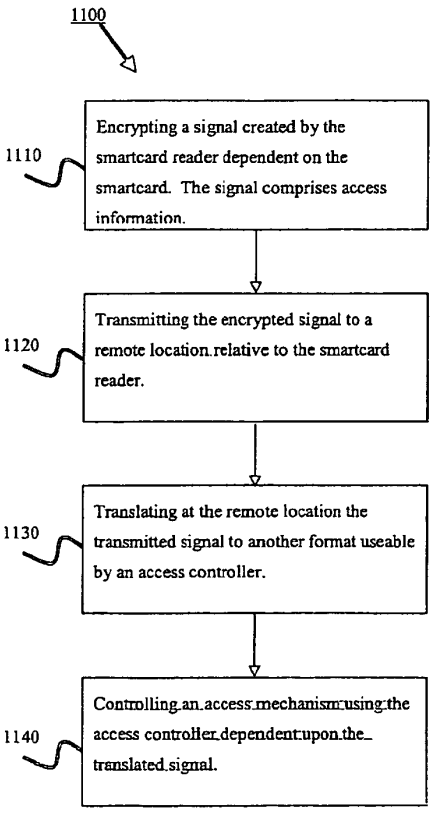
(74) Agent: SPRUSON & FERGUSON; G.P. Box 3898, Sydney, NSW 2001 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD OF SECURE TRANSMISSION



(57) Abstract: A method, a system, and an apparatus for providing secure transmissions from a smartcard reader are described. A signal created by the smartcard reader dependent on the smartcard is encrypted. The signal comprises access information. The encrypted signal is transmitted to a remote location relative to the smartcard reader. The transmitted signal is translated at the remote location to another format useable by an access controller. An access mechanism is controlled using the access controller dependent upon the translated signal.

WO 2004/010373 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD OF SECURE TRANSMISSION

Field of the Invention

The present invention relates generally to security systems and in particular to secure transmission systems and security systems utilising biometric sensors.

Background

Existing security systems are of several different types. One type of security system utilises a smartcard as a key for access to a secure location or secure equipment. The smartcard contains security information providing access via a smartcard reader at the access point. A user presents the reader with the smartcard. If the smartcard is authorised, the reader actuates a control mechanism to provide access. Thus, for example, the reader may signal a controller that controls operation of a latch mechanism controlling access to a door or provide access to a computer terminal. One example of a relevant reader that may be used in such a system is a Wiegand reader. One significant disadvantage of such systems is that the smartcard if stolen or otherwise in the possession of an unauthorised person may allow the unauthorised person to access the secure location or equipment.

Another security system utilises a biometric sensor to control access. A user must provide biometric data, normally a fingerprint, speech, or an eye scan via a sensor at the access point. Other forms of biometric data include facial details and hand geometry. Biometrics is a physical characteristic of a person used as a form of identification. The biometrics data is used in place of, or in addition to a security key, such as a key, card or PIN. A database or central repository of stored biometric data is maintained in a computer, with which the sensor can communicate. The scanned biometric data is compared with the stored biometric data, and if a match is found the user is permitted access. This system is generally more secure than that of the smartcard system, but is disadvantageous in that a central repository of biometric data must be maintained and updated. Further, significant time may be required to conduct such a comparison of the scanned biometric data against the database or central repository to determine whether or not there is a match.

Conventional systems are also disadvantageous in that the products' sizes are bulky. Still a further disadvantage of conventional systems is that such products cannot protect against security breaches arising from a person getting into security lines in a wall to which the reader is connected and providing false authorisation signals and the like to a controller.

Summary

In accordance with an aspect of the invention, there is provided a method of providing secure transmissions from a smartcard reader. The method comprises the steps of: encrypting a signal created by the smartcard reader dependent on the smartcard, the signal comprising access information; transmitting the encrypted signal to a remote location relative to the smartcard reader; translating at the remote location the transmitted signal to another format useable by an access controller; and controlling an access mechanism using the access controller dependent upon the translated signal.

The smartcard may contain biometric data and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data directly. The biometric data may comprise fingerprint data. The biometric data is not transmitted to the remote location from the smartcard reader.

The method may further comprise the step of providing access using the access mechanism if the translated signal is determined by the access controller to authorise access. The access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation. The access information may comprise at least one of a person's name, a facility code, a company code, an access code, and an issue code. The signal may be encrypted using triple DES, Skipjack, or AES Rijndael encryption.

The method may further comprise the step of encrypting communications between the smartcard and the smartcard reader. The encrypted signal may be

transmitted from the smartcard reader to a high security module at the remote location. The high security module translates the encrypted signal to the other format.

The smartcard reader and the high security module may be separated by a distance of up to 1.2 kilometres. Alternatively, the smartcard reader and the high security module are separated by a distance of up to 15 metres.

The translated signal may be in a controller-specified format. Preferably, the controller-specified format is Wiegand format, or clock and data.

In accordance with another aspect of the invention, there is provided a system for providing secure transmissions from a smartcard reader. The system comprises: a smartcard reader for encrypting a signal created by the smartcard reader dependent on the smartcard, the signal comprising access information, and for transmitting the encrypted signal to a remote location relative to the smartcard reader; a high security module for receiving the transmitted signal and translating the transmitted signal to another format useable by an access controller; and an access controller for controlling an access mechanism using the access controller dependent upon the translated signal.

The smartcard may contain biometric data, and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data directly. The biometric data may comprise fingerprint data. The biometric data is not transmitted to the high security module from the smartcard reader.

The system may further comprise an access mechanism providing access if the translated signal is determined by the access controller to authorise access. The access mechanism may be able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation. The access information may comprise at least one of a person's name, a facility code, a company code, an access code, and an issue code.

The signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption. Communications between the smartcard and the smartcard reader may be encrypted. The smartcard reader and the high security module may be separated by a distance of up to 1.2 kilometres. Alternatively, the smartcard reader and the high security module may be separated by a distance of up to 15 metres.

The translated signal may be in a controller-specified format. The controller-specified format may be Wiegand format, or clock and data.

In accordance with still another aspect of the invention, there is provided an apparatus for providing secure transmissions from a smartcard reader. The apparatus comprises: a smartcard reader for encrypting a signal created by the smartcard reader dependent on the smartcard, the signal comprising access information; a module for transmitting the encrypted signal to a remote location relative to the smartcard reader; a module for translating at the remote location the transmitted signal to another format useable by an access controller; and an access controller for controlling an access mechanism dependent upon the translated signal.

The smartcard may contain biometric data and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data directly. The biometric data may comprise fingerprint data.

In accordance with a further aspect of the invention, identification using of biometric data is disclosed. A smartcard encoded with biometric data is read. Actual biometric data is sensed. The biometric data from the smartcard is then compared with the sensed biometric data for verification. Access may be allowed if the biometric data from the smartcard and the sensed biometric data match. This may involve verifying that the biometric data encoded on the smartcard is correct. The biometric data stored in the smartcard is derived by scanning a source of biometric data associated with the smartcard, encoding the scanned biometric data, and storing the encoded biometric data on the smartcard. The biometric data may include a fingerprint. Optionally, a detail level can be specified for scanning the biometric data.

Brief Description of the Drawings

A small number of embodiments are described hereinafter with reference to the drawings, in which:

Fig. 1 is a high-level flow diagram illustrating an enrolment operation of a biometric smartcard system including a biometric smartcard reader or encoder in accordance with an embodiment of the invention;

Fig. 2 is a flow diagram illustrating a process of enrolling a fingerprint on a smartcard using a biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 3 is a flow diagram illustrating a process of verifying a finger on the biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 4A is a block diagram illustrating the structure of storage or memory in a smartcard in accordance with the embodiment of the invention;

Fig. 4B is a table illustrating an arrangement of security keys used in the smartcard of Fig. 4A in accordance with the embodiment of the invention;

Fig. 5 is a functional block diagram showing modules of a biometric smartcard reader or encoder in accordance with the embodiment of the invention;

Fig. 6 is a perspective view of a biometric smartcard reader or encoder in accordance with the embodiment of the invention shown in Fig. 5;

Fig. 7 is a block diagram of a secure transmission system in accordance with a further embodiment of the invention;

Fig. 8 is a flow diagram illustrating a process of secure transmission in accordance with the further embodiment of the invention, which may be practiced with the system of Fig. 7;

Fig. 9 is a block diagram of a secure transmission system in accordance with another embodiment of the invention;

Fig. 10 is a block diagram of a secure transmission system in accordance with still another embodiment of the invention; and

Fig. 11 is a flow diagram illustrating a process of providing secure transmissions from a smartcard reader in accordance with a further embodiment of the invention.

Detailed Description

A method, an apparatus, and a system for biometric smartcard reading and encoding, as well as for secure transmissions are described hereinafter. Numerous specific details are set forth. However, it will be apparent to those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention. Embodiments of the invention provide equipment that synthesise biometric and smartcard technologies to provide a smartcard reader or encoder that eliminates central database communications infrastructure. As the smartcard holds the biometric information, the requirement of central repositories of biometric data and associated security issues are obviated. A significant application of the reader or encoder is as an access control device at security point, whether for access via a door or other portal, or to a computer, network, or other secure equipment or installation.

In the following description, the terms biometric smartcard reader and biometric smartcard encoder are used. A reader is a device that is able to scan a person's biometric data and contactlessly read a smartcard to obtain stored biometric data. The biometric data is preferably a fingerprint. The smartcard is presented to the reader (preferably, 10 mm to 40 mm away), and write/read operations are communicated from the reader to the smartcard. The reader then compares the scanned biometric data and stored biometric data to determine if there is a match. The reader may be located at an access point to provide access to a location or equipment in a security system dependent on the results of the comparison. An encoder is able to perform the functions of a reader including contactless communications with the smartcard, but also is able to encode a smartcard with personal details and biometric data. More particularly, the encoder preferably includes a logical access system where all access in a facility is controlled using a card, i.e. for doors, for PC access, etc. Such a smartcard access system by its nature almost ensures that the user does not forget to leave the smartcard behind. Preferably, an encoder has an appropriate interface to enable the encoder to be connected with a computer to enrol a person's details and biometric data on the smartcard using software running on the computer. The encoder stores biometric data in a two-dimensional structure or template and card holder details on the smartcard. The encoder may have an insert slot in the housing body to receive such a smartcard. The slot allows detection of

the smartcard during an encoding process. A reader cannot be used for enrolment of biometric data and other associated information on a smartcard as can an encoder. For ease of description, the following text uses the two terms biometric smartcard reader and biometric smartcard encoder substantially interchangeably, but the noted distinctions should be borne in mind.

Biometric Smartcard Reader or Encoder

In accordance with an embodiment of the invention, a biometric smartcard reader or encoder is disclosed. Fig. 5 is a block diagram illustrating a smartcard 540 and a biometric smartcard reader 500 in accordance with an embodiment of the invention. This biometric smartcard reader 500 is smaller than other biometric units. The biometric smartcard reader 500 includes a biometric sensor 510 coupled to a sensor control module or printed circuit board 520. The sensor PCB 520 contains modules for processing and encoding scanned biometric data into a suitable digital representation using a given coding algorithm (e.g., Sagem). The fingerprint is stored as a template preferably and not as a digital image. An algorithm is used to generate the template. For fingerprints, examples of relevant algorithms use minutiae reference points, or ridge recognition patterns, for example. In turn, the sensor PCB 520 is coupled to a smartcard reader PCB 530 and sends fingerprint data in a given template to the smartcard reader PCB 530, which is also able to interrogate and obtain data from a smartcard 540. This is preferably done by presenting the smartcard reader PCB 530 with the smartcard 540, in which the smartcard reader PCB 530 energises the smartcard 540 if in close proximity and communicates with the smartcard 540. Preferably, the smartcard reader PCB 530 is a contactless reader using a Philips Chip Mifare® utilising the Wiegand format for its output. Communication between the smartcard 540 and the smartcard reader PCB 530 is encrypted. The encryption utilised with this embodiment involves a proprietary encryption method of Mifare®, which is embedded in the Mifare® smartcards. Another option is to use DES encryption. However, it will be apparent to those skilled in the art in the light of this disclosure that other encryption techniques may be used without departing from the scope and spirit of the invention.

More preferably, the biometric smartcard reader 500 incorporates a biometric finger scan sensor 510 (e.g., for scanning fingerprints) with an accompanying sensor PCB 520. The fingerprint sensor technology may be optical, capacitive, thermal, tactile, or a combination of the foregoing. An example of a sensor arrangement that may be used is a Bioscrypt product provided by Bioscrypt Inc. including an Authentic sensor, a Bioscrypt PCB, and Bioscrypt's own encoding algorithm. Alternatively, the sensor arrangement may be implemented using an ST sensor, a Yuean PCB provided by Yuean Biometrics, and the Sagem algorithm, or a SecuGen product provided by SecuGen Corporation including a SecuGen sensor, a SecuGen PCB, and the SecuGen algorithm. Still further, a SecuGen optical solution may be practiced that enables a rugged and robust design. However, it will be apparent to those skilled in the art in the light of this disclosure that other biometric sensors may be practiced without departing from the scope and spirit of the invention. The sensor 510 and associated PCB 520 scan a person's fingerprint and generate a digital representation of that fingerprint as digital biometric data. Fig. 6 is a perspective view of a biometric smartcard reader 600, which embodies the reader 500 of Fig. 5 including a biometric sensor 610/510, an associated sensor PCB 520 (not shown), and a Mifare® smartcard reader PCB 530 (not shown) in a single unit.

The smartcard 540 is adapted to store a digital representation of the biometric data. Preferably, the smartcard is a Mifare® smartcard for use with the contactless Mifare® reader. The smartcard 540 has approximately 1 Kbyte of storage or memory. Fig. 4A is a block diagram illustrating the structure of the storage 400 in the Mifare® smartcard, which is organised into 16 separate sectors 410-414 – 0 sector 410, 1 sector 412, ..., 15 sector 414. Each of the sectors 410-414 has two keys, Key A and Key B as shown in Fig. 4B. These keys can be designated as read and read/write keys. The keys A and B for each sector are initialised by the manufacturer (e.g. 10 hexadecimal characters each) and can be changed when the sectors are written to to contain biometric data in accordance with the embodiment of the invention. Each Mifare® smartcard 540 also has a unique serial number or identifier. Preferably, the 15th sector 414 contains one or more of the following security parameters for use in the system of Fig. 5: a facility code, a company code, an access code, and an issue code. The facility code can identify a facility that the smartcard permits access to for a given entity or company, which is identified by

the company code. The issue code identifies how many smartcards have been issued to a person. For example, if the issue code is 3, the system may hotlist corresponding smartcards for the person with issue codes of 1 or 2.

Dependent upon the format of the digital biometric data, the smartcard 540 stores such data across two or more sectors with corresponding keys for each sector of data. In the preferred embodiment, 5 to 6 sectors are used to store a digital fingerprint representation or template. For example, an ST sensor and an Yuean PCB produce a digital fingerprint representation that is approximately 320 bytes long. The length of the representation may vary depending on the different biometric sensor products and algorithms used. As noted above, each sector needs a customer specific key to unlock the information.

Optionally, the reader 500/600 incorporates a tamper switch so that if a reader is pulled from a wall, the reader does not function and an alarm flag is activated.

As described in greater detail below, use of the biometrics smartcard encoder 500 enables authorised persons using a properly enrolled smartcard to access to a secure location or equipment, for example. Lost or stolen smartcards 540 are unusable as the person with the lost or stolen smartcard 540 does not have the correct biometrics data (e.g., fingerprint) to match that stored on the smartcard 540. Still further, another advantage of this embodiment is that the biometric smartcard reader 500 of Fig. 5 obviates the need for a central database or repository of biometric data, since the biometrics data is stored on the smartcard 540.

In combination with a computer (not shown), a biometrics smartcard encoder 500 can also be used to enrol a person's fingerprint on a smartcard 540. The biometrics smartcard encoder 500 uses an RS232 or USB communications port, in conjunction with software, to enrol the person's fingerprint onto the smartcard 540. Generally, software or a computer program(s) running on the computer in combination with the biometrics smartcard encoder 500 obtains personal details for a person, scans and records a fingerprint for the person, and then writes the personal details and fingerprint

representation to the smartcard 540. Preferably, this embodiment does not permit fingerprint information to travel to the computer. Instead, the biometric smartcard encoder 500 stores the information and writes the information directly to the smartcard 540. The information is then erased from the memory of the biometric smartcard encoder 500. When enrolling a person's fingerprint, the detail level for scanning by the biometric smartcard encoder 500 can be changed to enable persons with scarred hands or other aberrations to use the encoder 500. This process is set forth in greater detail with reference to Fig. 1.

Fig. 1 is a high-level flow diagram illustrating details of a process 100 of obtaining and storing biometric information in a smartcard 540 using the biometric smartcard encoder (i.e., biometric unit) 500/600. In state 110, the biometric smartcard encoder 500 is initially idle. In step 112, a command is sent to the biometric smartcard encoder 500 to capture a person's fingerprint. This is preferably done by the computer using a communications port. In step 114, the sensor 510/610 of the biometric smartcard encoder 500 captures a fingerprint image. The sensor 510/610 analyses the scanned fingerprint and creates an image. In step 116, the image is coded and the data to be stored is created. This is preferably done by the sensor PCB 520 in combination with the sensor 510. In step 118, the smartcard 540 is presented to the smartcard reader PCB 530, and the biometric data from the sensor PCB 520 is written into the smartcard 540 by the smartcard reader PCB 530. State 120 at the end of the process 100 shows that the digital fingerprint representation is stored on the smartcard 540. This smartcard 540 can then be used as a security key in relation to a biometric security system.

Generally, when verification or access is required using a biometric smartcard reader 500/600, the smartcard 540 is presented to the biometric smartcard reader 500/600 and the fingerprint information is read off the smartcard 540 by the biometric smartcard reader 500/600. The person then presents their finger to the sensor 510/610 of the biometric smartcard reader 500/600 for scanning. The fingerprint representation read off the smartcard 540 is compared by the biometric smartcard reader 500/600 with the fingerprint currently obtained using the sensor 510/610. If there is a match within the detail level set at enrolment, the biometric smartcard reader 500/600 checks access

privileges using the access code from the smartcard 540 and if the holder has appropriate access privileges, access is granted by the biometric smartcard reader 500/600 to the smartcard holder. Verification is strongly dependent on enrolment. A score of 100 applies for a high quality and content template. A medium threshold level may look for a score of 60, for example. The threshold level may be varied to adjust quality and content of a template.

Details of Enrolment Process

Fig. 2 is a more detailed flow diagram of a process 200 of enrolling a fingerprint using a biometric smartcard encoder, based on Fig. 1. In an initial state 210, a biometric software application is run or launched. As noted above, this software is run on a computer connected to a biometric smartcard encoder 500/600, preferably using a RS232 or USB communications port. In step 212, a relevant RS232 or USB port (denoted generally by COM in Fig. 2) is selected by the software. Other interfaces may be practiced without departing from the scope and spirit of the invention. In step 214, the communications link (COM port) is tested to ensure the communications link is operating properly. Communication between the smartcard reader PCB 530 and the computer is preferably triple DES or Skipjack encrypted. Therefore, the information sent for access to the computer is highly difficult to compromise. In step 216, enrolment of a person's fingerprint is commenced. Preferably, this is done by clicking on an enrolment tab in the software application to commence enrolment processing. In step 218, personal details of the person whose fingerprint is to be enrolled are obtained and the type of smartcard being written to is specified. The relevant information may include one or more of the person's name, facility code, company code, access code, and issue code. Alternatively, the smartcard may be pre-encoded with some or all of this information.

In step 220, the desired detail level of the fingerprint is specified using the software application. In particular, this is done using a quality meter in the software where the detail level for the sensor 510 and PCB 520 is specified. Ordinarily, the quality is set as high as possible to avoid misreads. However, the quality can be adjusted downwardly to avoid or reduce the effects of scar tissue and other aberrations on the person's finger. In step 222, the person's fingerprint is presented to the sensor 510/610 of

the biometric smartcard encoder 500/600, and the person's fingerprint is scanned. The data stream for the scanned fingerprint is sent from the sensor 510/610 to the sensor PCB 520. The information is then coded with the specific algorithm within the sensor PCB 520. The coded information is then sent to the smartcard reader PCB 530 and from there encoded onto the smartcard 540.

In decision block 224, a check is made to determine if the quality of the scanned fingerprint image from the sensor 510/610 is adequate. The sensor 510 and PCB 520 determines quality. The biometric smartcard encoder 500/600 indicates this to the computer, since the fingerprint is preferably not transferred to the computer. If the quality is inadequate (NO), the quality is reduced to enable enrolment in step 226 and processing continues at step 222. This may occur multiple times. If decision block 224 determines that the quality is adequate (YES), processing continues at step 228.

In step 228, a smartcard 540 is presented to the smartcard reader PCB 530 of the biometric smartcard encoder 500/600. Presentation of the smartcard 540 to the smartcard reader PCB 530 results in the encoded fingerprint template and related keys for each sector being downloaded onto the smartcard 540. The communication between the smartcard 540 and the reader PCB 530 is encrypted. As noted above, the encrypted, encoded fingerprint representation is normally stored across several sectors in the storage of the smartcard. Also personal details and other information may be stored on the smartcard 540. In step 230, a check is made to determine if the encoding of the smartcard 540 was successful. If decision block 230 returns true (YES), the fingerprint template has been encoded successfully on the smartcard 540 using the encoder 500. If decision block 230 returns false (NO), processing continues at decision block 232. In decision block 232, a check is made to determine if the smartcard type details are correct. For example, the smartcard 540 may be a new or used smartcard. A new smartcard has default values in its storage, while a used smartcard has changed keys A and B for example. Further, or alternatively, a different type of smartcard may be used, for example, from different manufacturers. If decision block 232 returns false (NO) indicating the card type details are incorrect, processing continues at step 234 and the correct smartcard type must be specified to the software. Processing then continues at step 236. If decision block 232

returns true (YES), processing continues at step 236. In step 236, another smartcard is tried or obtained for presentation instead of the smartcard previously presented to the smartcard reader PCB 530 of the encoder 500/600. Processing then continues at step 228.

Details of Verification Process

After a fingerprint representation and associated information are enrolled on a smartcard 540, verification of the enrolment on the smartcard 540 may be required. Fig. 3 is a flow diagram illustrating a process 300 of verifying a fingerprint scanned by the biometric smartcard encoder 500/600 and enrolled on the smartcard 540. In state 310, the biometric application software is loaded. In step 312, the communications link (COM port or USB) between the computer and the biometric smartcard encoder 500 is selected. In step 314, the communications link is tested to ensure the link is operating properly. In step 316, a verification application module in the software is activated. Preferably, this is done by clicking on a verify tab in the biometric application software. In step 318, the smartcard 540 with enrolled fingerprint information is presented to the encoder 500/600, which reads and stores the fingerprint information from the smartcard 540. In step 320, the person's finger is presented to sensor 510/610 of the biometric smartcard encoder 500, and the person's fingerprint is scanned and stored. The biometric smartcard encoder 500 then compares in the smartcard reader PCB 530 the scanned fingerprint template from the sensor 510/610 and the uploaded fingerprint template from the smartcard 540.

In decision block 322, a check is made to determine if the verification passed (OK). The encoder 500/600 provides the comparison result to the computer to establish verification. If decision block 322 returns true (YES), processing continues at state 324 and the fingerprint on the smartcard is verified as that of the fingerprint obtained at the sensor 510/610. Otherwise, if decision block 322 returns false (NO), processing continues at step 326. In step 326, a check is made to determine if the verification bar in the software was raised. Preferably, a quality bar and a verification bar showing current levels are depicted graphically to an operator of the application software on opposite sides of a graphical image of a fingerprint icon, which indicates to the operator when a fingerprint has been properly scanned by the encoder 500/600. Raising the verification bar indicates a better match between the scanned fingerprint and the one from the

smartcard 540. Verification is dependent on the quality level at enrolment. If decision block 326 returns true (YES), processing continues at step 332 and the finger must be positioned correctly for verification, before processing continues at step 320. Otherwise, if decision block 326 returns false (NO), processing continues at step 328. A determination is made that the incorrect finger has been used in relation to the recorded fingerprint information on the smartcard. In step 330, the correct finger is determined before proceeding to step 320.

Secure Transmission System

In a security system, a smartcard reader may be setup to give access on a per door basis or to equipment. The smartcard has unique keys that must also be contained in a smartcard reader's firmware. The smartcard reader communicates with the smartcard and information is read from the smartcard for access. The smartcard reader ordinarily communicates with an access controller, and this controller controls access; for example the controller may preferably activate a door latch for access. Information is sent to the controller. Communication between the smartcard reader and the controller is usually Wiegand. However, the communications may be RS485 or RS232. Still further, another example of a common form of communication back to a controller is Clock and Data. These formats can be cracked or defeated given time, as formats are usually 'known' industry standards. The controller determines whether or not to grant access and activates an access mechanism if granted. When using a security access reader to grant or deny access, a possible breach in security lies in the information that is directly sent to the controller by the smartcard reader. If the smartcard reader is removed from a wall or other connection point and a signal is introduced to the line between the smartcard reader and the controller, then a security breach exists. The signal may provide information to the controller so that the controller improperly grants access. If the smartcard reader has a tamper switch, a degree of added security is provided. A hole in the wall may still be made conditional to the material of the wall, and a security breach may still occur, as this enables access to the cables of the reader. In contrast, a stand-alone reader does not need a controller so this does not apply to such a reader.

In accordance with a further embodiment of the invention, secure transmission from a smartcard reader is provided by encrypting the messages from the smartcard reader in the security system. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The further embodiment of the invention shown in Figs. 7 and 8 addresses this issue. This applies to the embodiments of Figs. 9-11 as well.

Fig. 7 is a block diagram of a secure transmission system 700 in accordance with the further embodiment of the invention. A smartcard reader 702 is coupled to a high security module (HSM) 704. Preferably, the smartcard reader 702 is a biometrics smartcard reader 500/600, but may be a standard smartcard reader. The HSM 704 is located remotely from the smartcard reader 702 and preferably at an inaccessible location relative to the smartcard reader 702, for example on the other side of a wall in a secure area. The distance between the smartcard reader 702 and the HSM 704 may be up to 15 metres. Communications between the reader 702 and the HSM 704 are preferably Triple DES or Skipjack encrypted, but other encryption techniques may be employed. The HSM 704 is in turn coupled to a controller 706. Communications between the HSM 704 and the controller 706 are carried out using the controller-specified format, which is usually Wiegand format but may be another format (e.g., clock and data). In turn, the controller 706 is connected to the door latch 708 to control operation of the door for access. Different access mechanisms may be used in place of a door latch 708, for example to provide access to a computer.

Significantly, the system 700 uses an HSM 704 for each access point and encrypted communications between the smartcard reader 702 and the HSM 704. The smartcard reader 702 preferably reads the information off a smartcard and communicates with the HSM 704 on the secure side of the wall, up to 15 metres away. Again, the communication is encrypted, preferably using a 3DES or Skipjack encrypted protocol. The HSM 704 decrypts the message to obtain the security information from the smartcard, e.g. "Facility Code" and the "Access number", and communicates these values to the access controller 706. Thus, communication between the smartcard reader 702 and the HSM 704 and thus the controller 706 is secure whether the smartcard reader 702 is

removed from the wall or wiring is accessed through a wall. This provides a higher standard of security for access control systems.

Fig. 8 is a flow diagram illustrating a process 800 for secure transmission. In state 810, the smartcard reader 702 is in standby mode. In step 812, a smartcard is presented for access. In step 814, the smartcard reader 702 reads and analyses access information on the smartcard. The smartcard and the reader must have the same keys. If a standard smartcard reader is used, an encrypted transmission is sent to the HSM 704 in step 816. Processing then continues at step 824. Otherwise, if a biometric smartcard reader 500/600 is used, after step 814, processing continues at step 818. In step 818, biometric data is obtained from the cardholder using the biometric sensor of the biometric smartcard reader 500/600 as reader 702. Preferably, the biometric data is fingerprint information. In step 820, the biometric data of the cardholder and the stored biometric data from the smartcard are compared and confirmed to be the same person or not. If the biometric data matches, in step 822, an encrypted transmission for access is sent to the HSM 704 from smartcard reader 702, before processing continues at step 824. In step 824, the HSM 704 decrypts the transmission and communicates it to the controller 706 using the appropriate controller format, e.g. Wiegand. The controller 706 either grants access 828 in step 826 or denies access 832 in step 830 dependent upon the access rights obtained from the smartcard.

Further Embodiments of Secure Transmission System

Fig. 11 is a flow diagram illustrating a method 1100 of providing secure transmissions from a smartcard reader in accordance with an embodiment of the invention. In step 1110, a signal created by the smartcard reader dependent on the smartcard is encrypted. The signal comprises access information. In step 1120, the encrypted signal is transmitted to a remote location relative to the smartcard reader. In step 1130, the transmitted signal is translated at a remote location to another format useable by an access controller. In step 1140, an access mechanism is controlled using the access controller dependent upon the translated signal. The smartcard may contain biometric data and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data

directly. The biometric data may comprise fingerprint data. The biometric data is not transmitted to the remote location from the smartcard reader.

Figs. 9 and 10 are block diagrams of secure transmission systems in accordance with further embodiments of the invention. In these drawings, modules with similar functionality to those of the modules shown in Fig. 7 are indicated with corresponding reference numbers, except that the leading digit(s) is replaced to correspond with the Figure number (e.g., the access controller 906 of Fig. 9 corresponds to the access controller 706 of Fig. 7). For the sake of brevity only, aspects of the smartcard reader and security system are not repeated hereinafter, but reference is made to the description accompanying Figs. 7 and 8. Further, the door latch shown in Fig. 7 (and identified by reference numeral 708) is not depicted in each of Figs. 9 and 10, only to simplify those drawings. However, it is to be understood that such an access mechanism is or can be coupled to each of the controllers 906 and 1006 of Figs. 9 and 10, respectively.

Again, in a security system 900 or 1000, a smartcard reader may be setup to give access on a per door basis or to equipment. In general, the smartcard reader communicates with the smartcard and information is read from the smartcard for access, information is sent to the controller, and the controller determines whether or not to grant access and activates an access mechanism if granted. Secure transmission from a smartcard reader is provided by encrypting the messages from the smartcard reader in the security system. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced.

The system 900 of Fig. 9 comprises a smartcard reader 902, a high security module (HSM) 904, and an access controller 906. While not shown in Fig. 9 to simplify the drawing, the controller 906 may be coupled to an access mechanism able to provide access (e.g., to a door, portal, computer, network, or other secure equipment or installation) at an access point. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The smartcard reader may be a Banque-Tec International reader.

A smartcard 920 (e.g., a Mifare smartcard) is presented to the smartcard reader 902, and the smartcard reader 902 communicates with the smartcard. Preferably, communications between the Mifare smartcard 920 and the smartcard reader 902 are encrypted using Mifare proprietary encryption. However, other forms of encryption may be practiced without departing from the scope and spirit of the invention. The description accompanying Fig. 10 provides examples of other encryption techniques that may be practiced. Also, the smartcard 920 preferably includes biometrics data, as described hereinbefore. The reader 902 reads access information from the smartcard 920. The access information may include one or more of the following: person's name, facility code, company code, access code, and issue code. Other access information and/or authorisation data may be sent from the smartcard reader 902 to the HSM 904 using suitable communications protocols, such as RS232 or RS485. Other communications protocols may be practiced without departing from the scope and spirit of the invention.

The HSM 904 is located remotely from the smartcard reader 902 and preferably at an inaccessible location relative to the smartcard reader 902. Communications between the reader 902 and the HSM 904 are encrypted. The encryption technique used may use one or more of the following techniques: Triple DES (3DES), Skipjack, and AES-Rijndael. Other encryption techniques may be practiced without departing from the scope and spirit of the invention. The distance between the smartcard reader 902 and the HSM 904 may be up to at least 1.2 kilometres, e.g. if RS485 is used. The distance between the smartcard reader 902 and the HSM 904 may be varied dependent on the communications protocol, techniques, and media used.

The HSM 904 is in turn coupled to a controller 906. Communications between the HSM 904 and the controller 906 are carried out using the controller-specified format, which is usually Wiegand format but may be another format (e.g., clock and data). The distance between the HSM 904 and the controller 906 may be up to 500 feet. However, this distance may be varied without departing from the scope and spirit of the invention. In turn, the controller 906 may be connected to an access point (e.g., the door latch 708 of Fig. 7) to control operation of the access point. Different access mechanisms may be used.

The HSM 904 translates the encrypted signal to another format for a controller and communicates the translated signal to the access controller 906. The translation preferably involves decrypting the message to obtain the security or access information from the smartcard, e.g. "Facility Code" and the "Access number" and communicating the values to the access controller. Thus, communications between the smartcard reader 902 and the HSM 904 and thus the controller 906 is secure whether the smartcard reader 902 is removed from the wall or wiring is accessed through a wall. This provides a higher standard of security for access control systems. The process of Fig. 8 applies to this embodiment.

The system 1000 of Fig. 10 comprises a smartcard reader 1002, a high security module (HSM) 1004, and an access controller 1006. While not shown in Fig. 10 to simplify the drawing, the controller 1006 may be coupled to an access mechanism (e.g., to a door, portal, computer, network, or other secure equipment or installation) at an access point. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The smartcard reader may be a Banque-Tec International reader. The system of Fig. 10 is largely identical to that of Fig. 9 and therefore the following description is limited to identifying the points of difference for the sake of brevity.

A smartcard 1020 (e.g., a DESFIRE Mifare smartcard) is presented to the smartcard reader 1002, and the smartcard reader 1002 communicates with the smartcard. Preferably, communications between the Mifare smartcard 1020 and the smartcard reader 1002 are encrypted using triple DES (3DES) encryption. However, other forms of encryption may be practiced without departing from the scope and spirit of the invention. The remainder of the system 1000 is the same as that for the system 900 of Fig. 9, and is not repeated for the sake of brevity. The process of Fig. 8 applies to this embodiment.

A small number of embodiments of the invention regarding methods, devices, and systems for biometric smartcard reading and encoding, as well as for secure transmissions have been described. In the light of the foregoing, it will be apparent to

those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention.

Claims

The claims defining the invention are as follows:

1. A method of providing secure transmissions from a smartcard reader, said method comprising the steps of:

encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information;

transmitting said encrypted signal to a remote location relative to said smartcard reader;

translating at said remote location said transmitted signal to another format useable by an access controller; and

controlling an access mechanism using said access controller dependent upon said translated signal.

2. The method according to claim 1, wherein said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

3. The method according to claim 2, wherein said biometric data comprises fingerprint data.

4. The method according to claim 2 or 3, wherein said biometric data is not transmitted to said remote location from said smartcard reader.

5. The method according to claim 1, further comprising the step of providing access using said access mechanism if said translated signal is determined by said access controller to authorise access.

6. The method according to claim 5, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

7. The method according to any one of claims 1-5, wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

8. The method according to any one of claims 1-7, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

9. The method according to claim 1, further comprising the step of encrypting communications between said smartcard and said smartcard reader.

10. The method according to any one of claims 1-9, wherein said encrypted signal is transmitted from said smartcard reader to a high security module at said remote location.

11. The method according to claim 10, wherein said high security module translates said encrypted signal to said other format.

12. The method according to claim 10, wherein said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometres.

13. The method according to claim 10, wherein said smartcard reader and said high security module are separated by a distance of up to 15 metres.

14. The method according to any one of claims 1-13, wherein said translated signal is in a controller-specified format.

15. The method according to claim 14, wherein said controller-specified format is Wiegand format, or clock and data.

16. A system for providing secure transmissions from a smartcard reader, said system comprising:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information, and for transmitting said encrypted signal to a remote location relative to said smartcard reader;

a high security module for receiving said transmitted signal and translating said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism using said access controller dependent upon said translated signal.

17. The system according to claim 16, wherein said smartcard contains biometric data, and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

18. The system according to claim 17, wherein said biometric data comprises fingerprint data.

19. The system according to claim 17 or 18, wherein said biometric data is not transmitted to said high security module from said smartcard reader.

20. The system according to claim 16, further comprising an access mechanism providing access if said translated signal is determined by said access controller to authorise access.

21. The system according to claim 20, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

22. The system according to any one of claims 16-21, wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

23. The system according to any one of claims 16-22, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

24. The system according to claim 16, wherein communications between said smartcard and said smartcard reader are encrypted.

25. The system according to claim 24, wherein said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometres.

26. The system according to claim 24, wherein said smartcard reader and said high security module are separated by a distance of up to 15 metres.

27. The system according to any one of claims 16-26, wherein said translated signal is in a controller-specified format.

28. The system according to claim 27, wherein said controller-specified format is Wiegand format, or clock and data.

29. An apparatus for providing secure transmissions from a smartcard reader, said apparatus comprising:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information;

means for transmitting said encrypted signal to a remote location relative to said smartcard reader;

means for translating at said remote location said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism dependent upon said translated signal.

30. The apparatus according to claim 29, wherein said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

31. The apparatus according to claim 30, wherein said biometric data comprises fingerprint data.

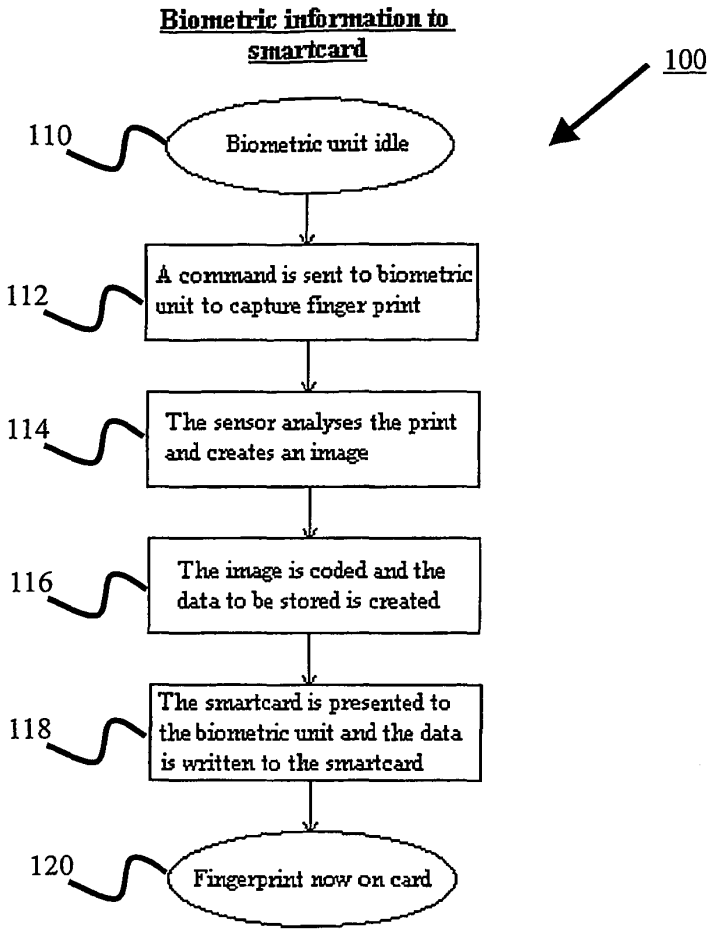

Biometric information to smartcard
100
110
Biometric unit idle
112
A command is sent to biometric unit to capture finger print
114
The sensor analyses the print and creates an image
116
The image is coded and the data to be stored is created
118
The smartcard is presented to the biometric unit and the data is written to the smartcard
120
Fingerprint now on card

FIG. 1

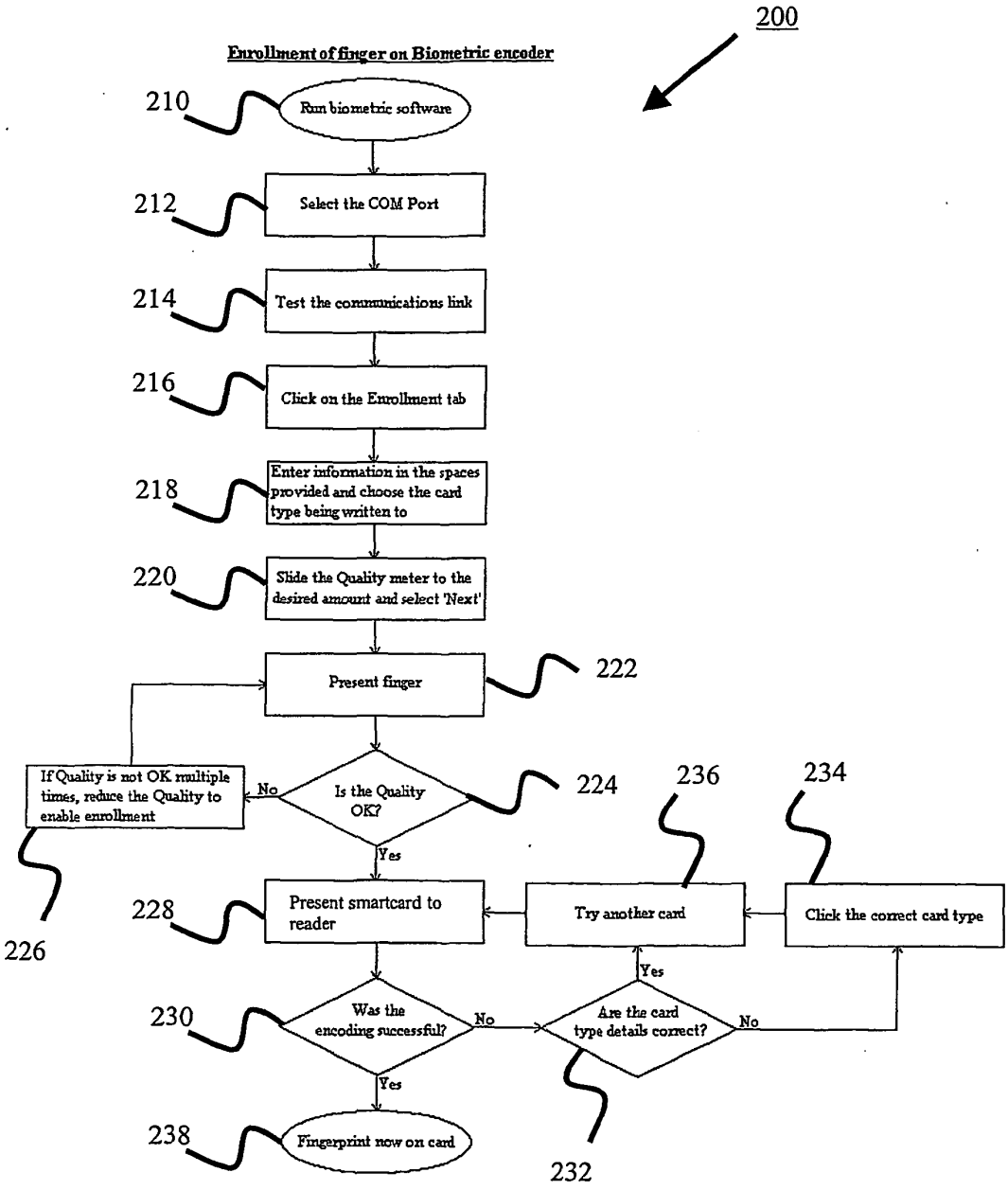

200
Enrollment of finger on Biometric encoder
210
Run biometric software
212
Select the COM Port
214
Test the communications link
216
Click on the Enrollment tab
218
Enter information in the spaces provided and choose the card type being written to
220
Slide the Quality meter to the desired amount and select 'Next'
Present finger
222
If Quality is not OK multiple times, reduce the Quality to enable enrollment
No
Is the Quality OK?
224
Yes
226
228
Present smartcard to reader
Try another card
236
Click the correct card type
234
Yes
230
Was the encoding successful?
No
Are the card type details correct?
No
Yes
232
238
Fingerprint now on card

FIG. 2

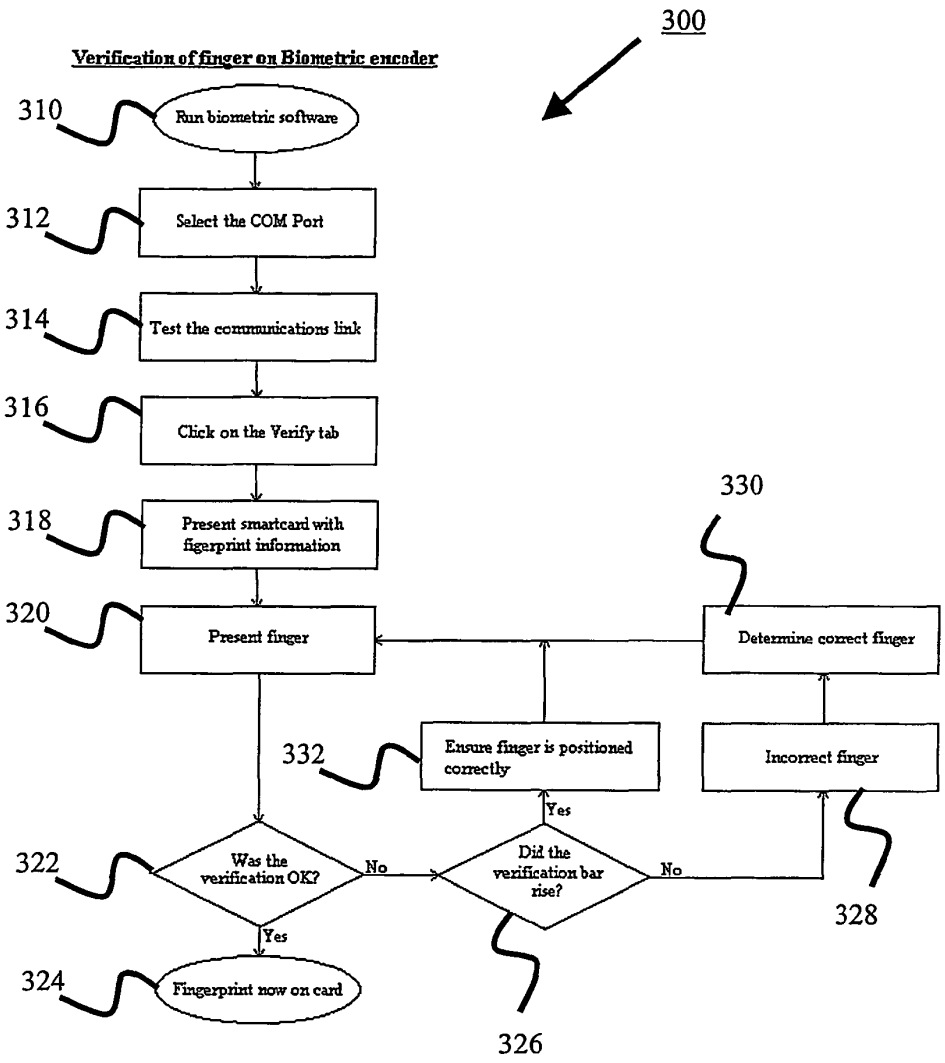

300
Verification of finger on Biometric encoder
310
Run biometric software
312
Select the COM Port
314
Test the communications link
316
Click on the Verify tab
318
Present smartcard with figerprint information
320
Present finger
330
Determine correct finger
332
Ensure finger is positioned correctly
Incorrect finger
Yes
322
Was the verification OK?
No
Did the verification bar rise?
No
328
Yes
324
Fingerprint now on card
326

FIG. 3

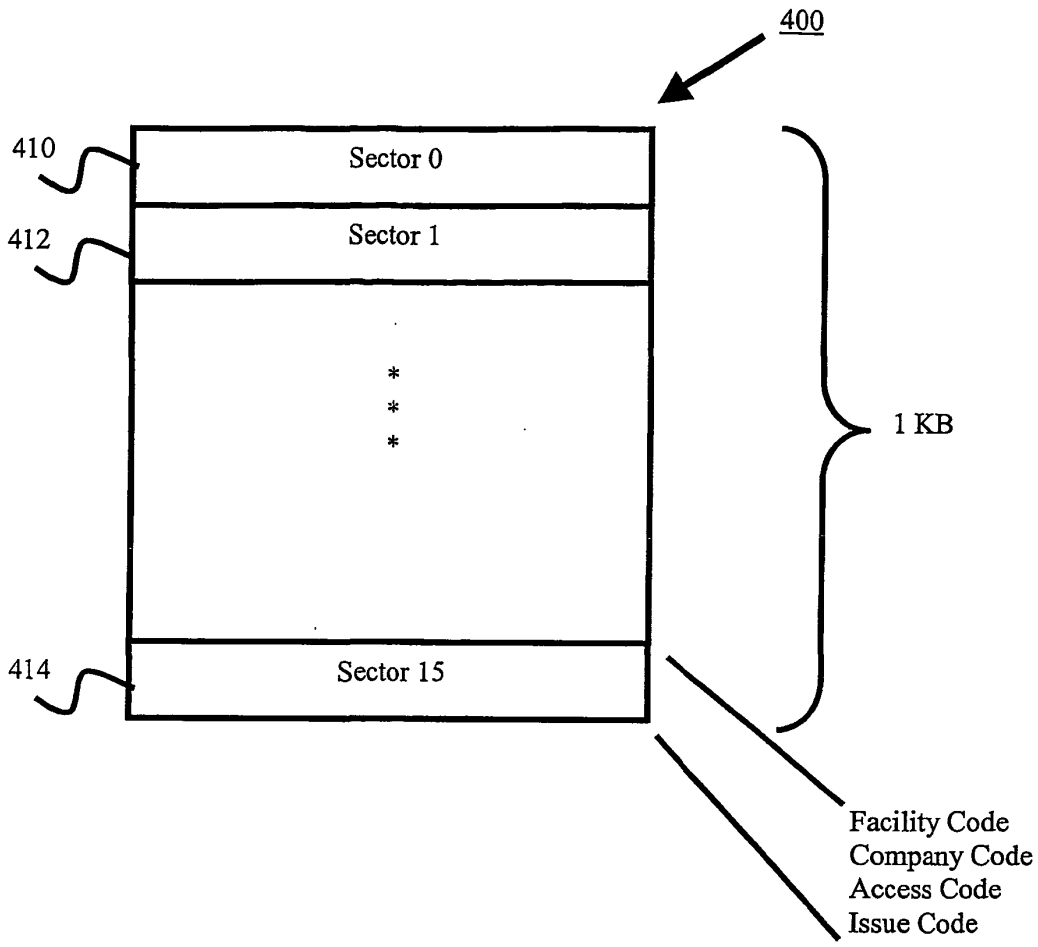


FIG. 4A

Sector	Key A	Key B
0	A0A1A2A3A4	-
	or	
	FFFFFFFFFF	-
*		
*		
*		
15		

450

FIG. 4B

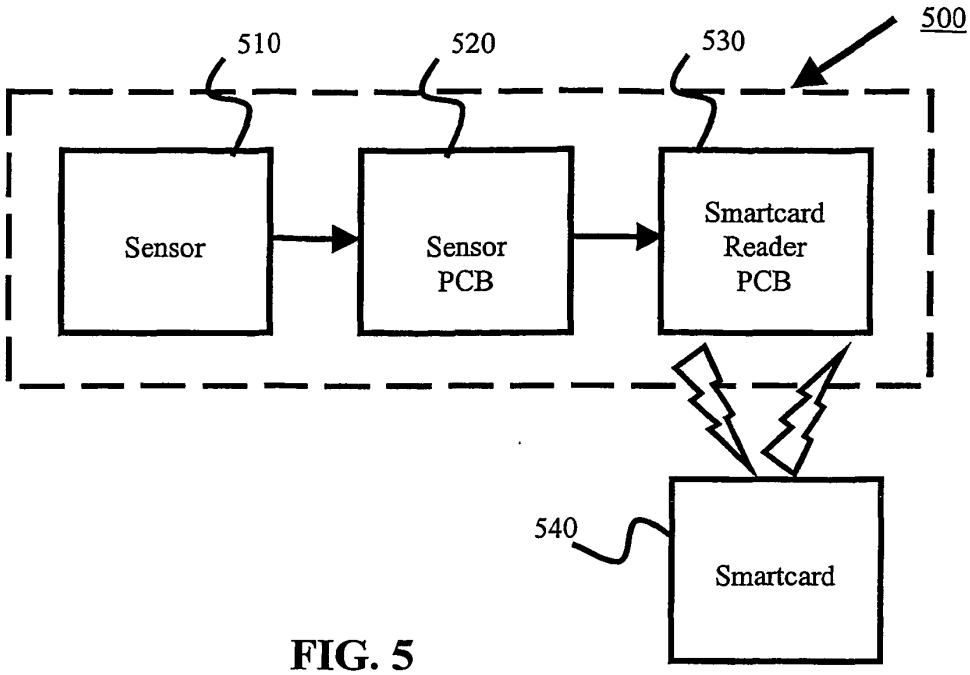

500
510
520
530
Sensor
Sensor PCB
Smartcard Reader PCB
540
Smartcard

FIG. 5

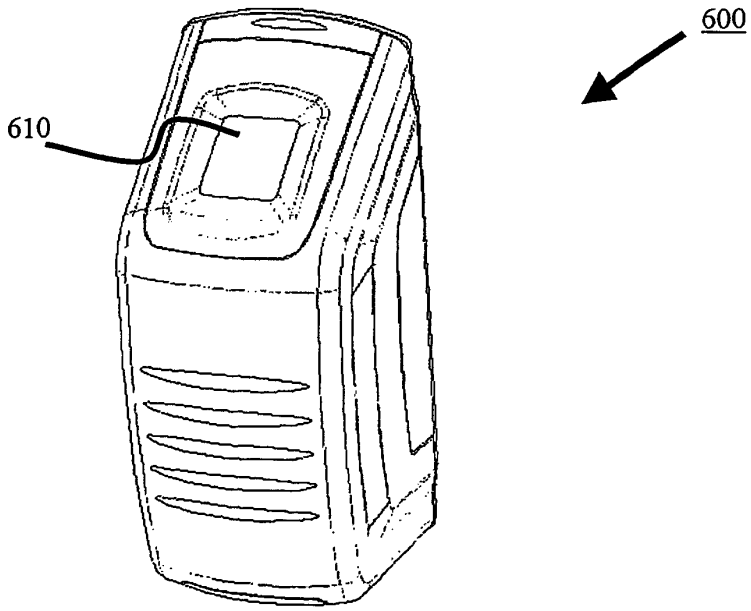

600
610

FIG. 6

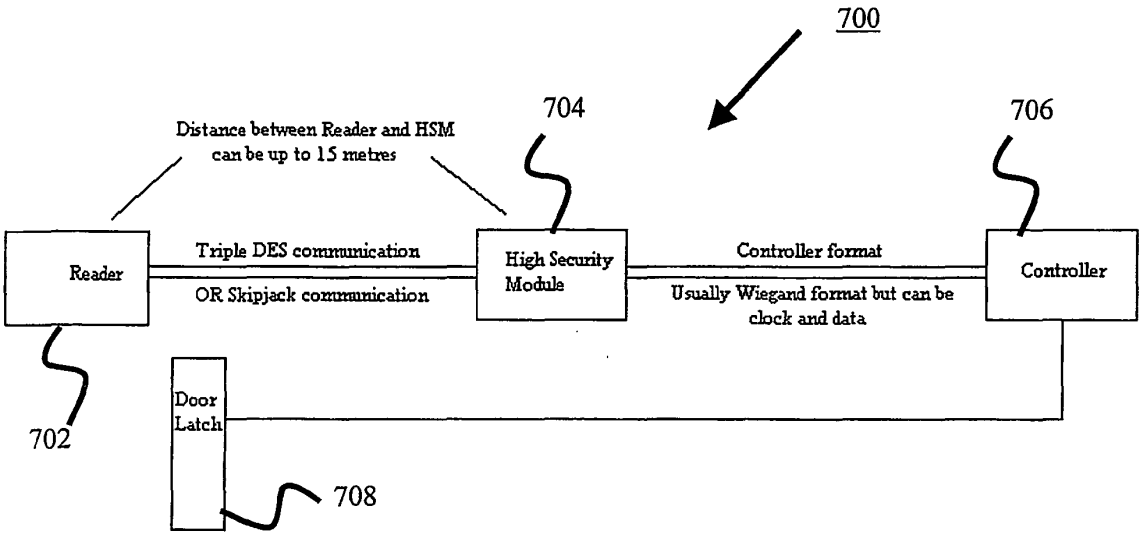

700
704
706
Distance between Reader and HSM can be up to 15 metres
Reader
Triple DES communication
OR Skipjack communication
High Security Module
Controller format
Usually Wiegand format but can be clock and data
Controller
Door Latch
702
708

FIG. 7

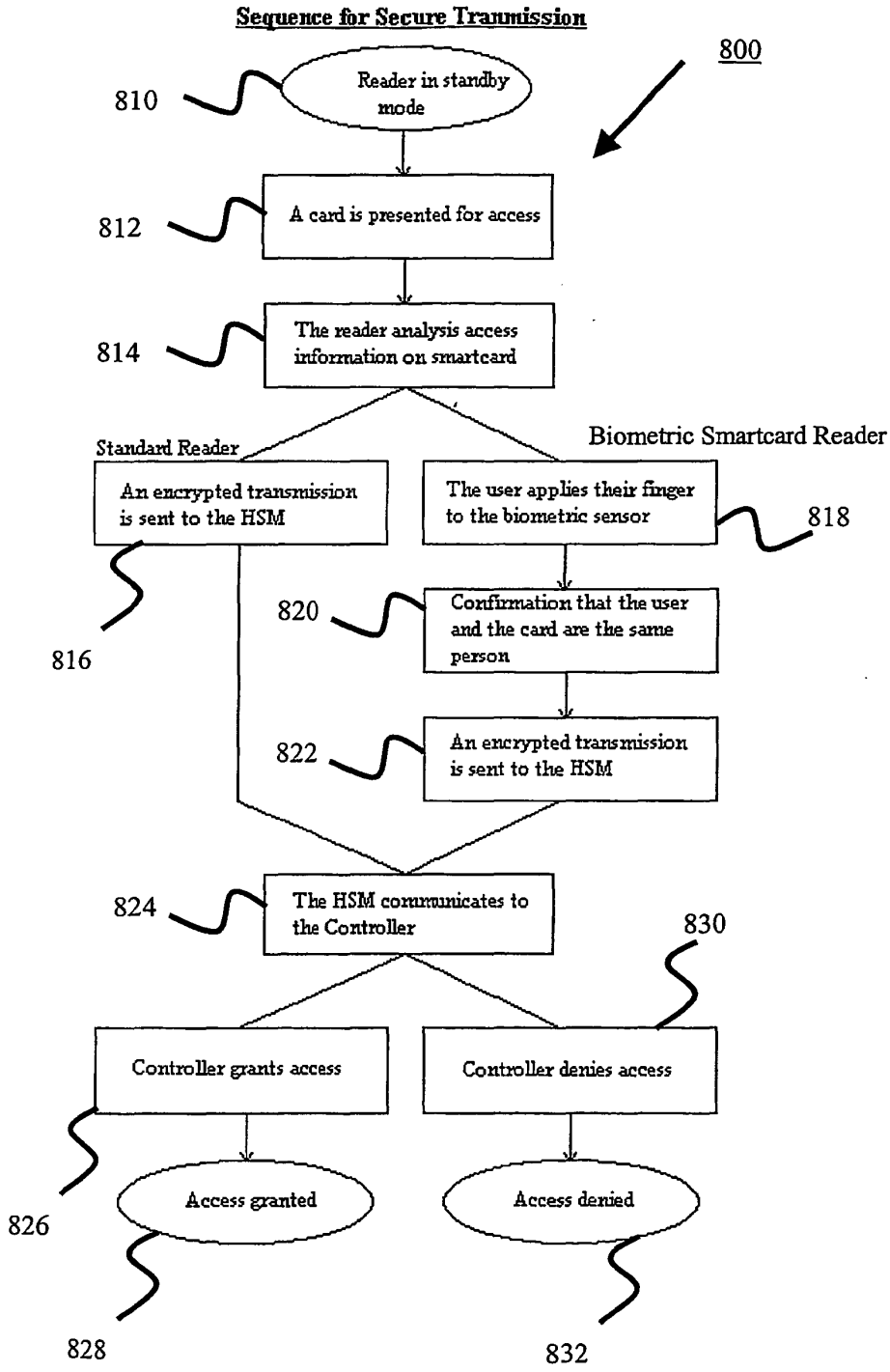

Sequence for Secure Transmission
800
810
Reader in standby mode
812
A card is presented for access
814
The reader analysis access information on smartcard
Standard Reader
Biometric Smartcard Reader
An encrypted transmission is sent to the HSM
The user applies their finger to the biometric sensor
818
816
820
Confirmation that the user and the card are the same person
822
An encrypted transmission is sent to the HSM
824
The HSM communicates to the Controller
830
Controller grants access
Controller denies access
826
Access granted
Access denied
828
832

FIG. 8

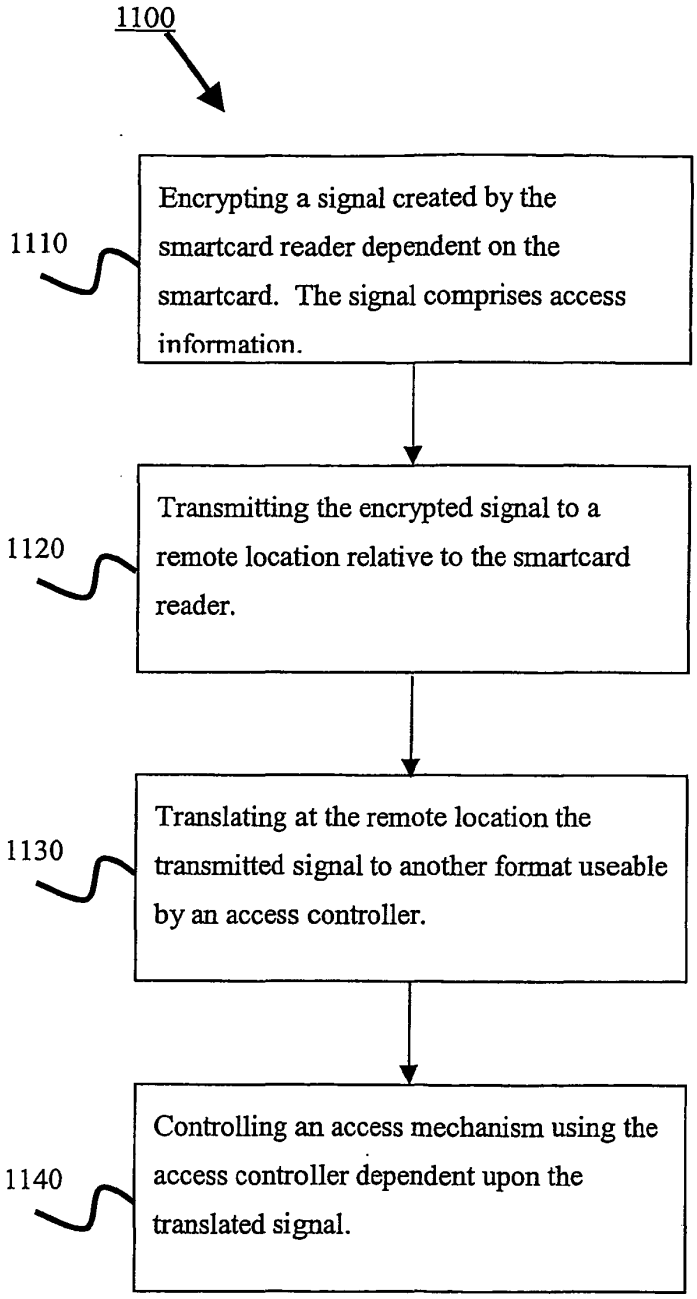

1100
1110
Encrypting a signal created by the smartcard reader dependent on the smartcard. The signal comprises access information.
1120
Transmitting the encrypted signal to a remote location relative to the smartcard reader.
1130
Translating at the remote location the transmitted signal to another format useable by an access controller.
1140
Controlling an access mechanism using the access controller dependent upon the translated signal.

Fig. 11

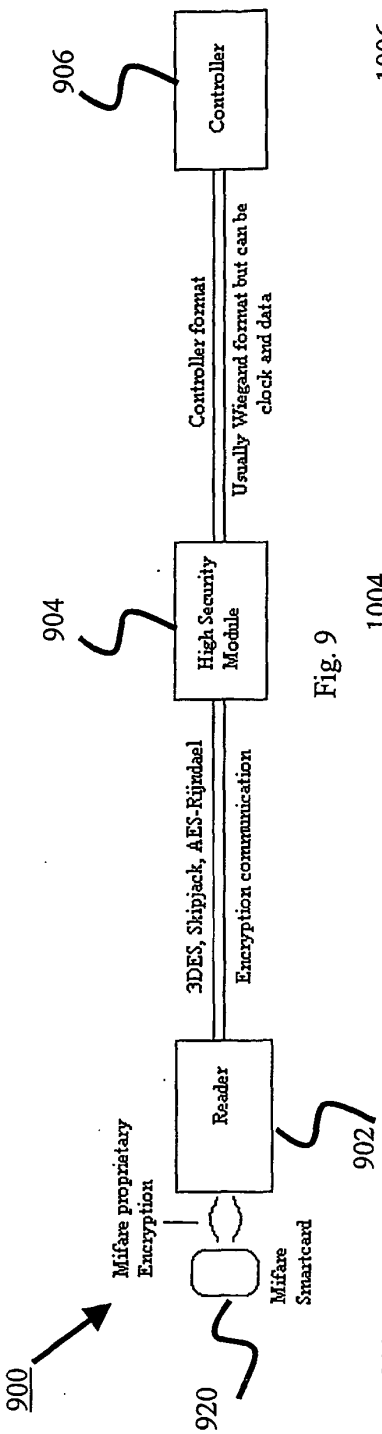

900
Mifare proprietary Encryption
Mifare Smartcard
920
Reader
902
3DES, Skipjack, AES-Rijndael
Encryption communication
High Security Module
904
Controller format
Usually Wiegand format but can be clock and data
Controller
906

Fig. 9

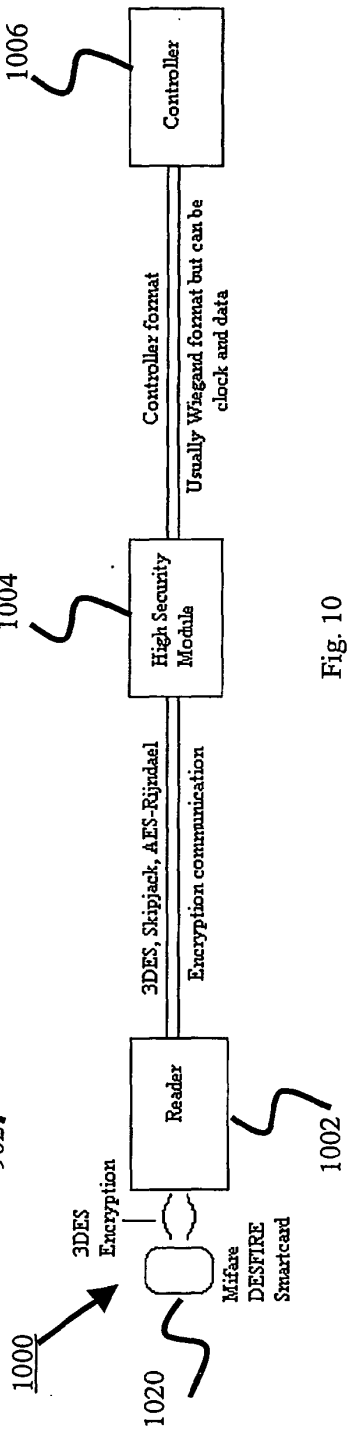

1000
3DES Encryption
Mifare DESFIRE Smartcard
1020
Reader
1002
3DES, Skipjack, AES-Rijndael
Encryption communication
High Security Module
1004
Controller format
Usually Wiegand format but can be clock and data
Controller
1006

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00934

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06K 019/07

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)

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)
DWPI, USPTO (SMARTCARD, ENCRYPT, REMOTE ETC)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5995965 (EXPERTON) 30 November 1999 Column 4, lines 9 to 26 Column 5, lines 50 to 56 Column 10, lines 21 to 33	1, 5 - 7, 29
X	US 5991410 (ALBERT ET AL) 23 November 1999 Column 5, lines 18 - 20 Column 18, lines 45 - 62	1, 5 - 9, 29 - 31

[X] Further documents are listed in the continuation of Box C [X] 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
7 August 2003	-1 SEP 2003
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **M.J. O'ROURKE** Telephone No : (02) 6283 2017

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00934

C (Continuation). **DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6366967 B1 (WAGNER) 2 April 2002 Column 6, lines 11 - 63	1, 5 - 9, 29 - 31
X,P	JP 2002-261749 A (MATSUSHITA ELECTRIC IND CO LTD) 13 September 2002 Paragraph 0010 - 0013 of english translation from Detailed Description (online), (Retreived on 7 August 2003) Retrieved from the Internet < URL: http://www6.ipdl.jpo.go.jp/Tokujitu/PAJdetail.ipdl?N0000=80&N0120=01&N2001=2&N3001=2002-261749>	1 - 9, 14 - 15, 29 - 31

WAVELYNX EX. 1003, Pg. 357
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU03/00934

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5995965	NONE					
US	5991410	US	2002030579				
US	6366967	US	5742845	US	5905908	US	2002032810
		US	2002138430	US	2002198837	US	5898838
JP	2002261749	NONE					

END OF ANNEX

WAVELYNX EX. 1003, Pg. 358
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001777 A1

(51) International Patent Classification[7]: G07C 9/00

(21) International Application Number: PCT/US2004/016616

(22) International Filing Date: 16 June 2004 (16.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
203 09 254.6 16 June 2003 (16.06.2003) DE

(71) Applicant *(for all designated States except US)*: **SCM MICROSYSTEMS GMBH** [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MERKERT, Robert, J., Sr.** [US/US]; 21 Chippenham Drive, Voorhees, NJ 08043 (US).

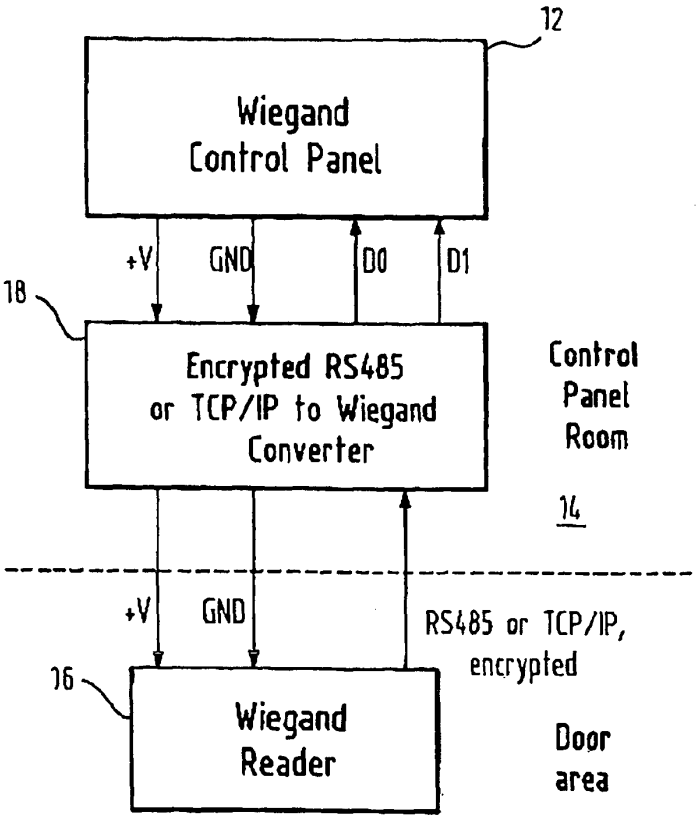
(74) Agent: **GARRETT, Arthur, S.**; Finnegan, Henderson, Farrabow Garrett & Dunner, L.L.P., 1300 I Street, NW, Washington, DC 20005-3315 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: ACCESS SYSTEM



(57) Abstract: An access system includes an input device which is accessible to a user and capable of reading an authentication and/or identification information provided by the user. The access system further includes a Wiegand control panel (12) connected to the input device for evaluation of the information provided by the user. The control panel (12) is located in a secure area (14) remote from the input device. The access system further includes a converter (18) connected to the input device and to the control panel (12). The input device includes encryption means to encrypt the information provided by the user. The converter (18) is capable of converting the encrypted information into a standard Wiegand signal.

WO 2005/001777 A1

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ACCESS SYSTEM

DESCRIPTION OF THE INVENTION

This application claims the right to foreign priority based on German Patent Application No. 203 09 254:6, entitled "ACCESS SYSTEM," filed in the Federal Republic of Germany, on June 16, 2003, which is hereby incorporated herein by reference.

The invention relates to an access system, comprising an input device which is accessible to a user and capable of reading an authentication and/or identification information provided by the user, and a Wiegand control panel connected to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device.

Security systems using Wiegand readers and control panels adapted to evaluate the data read from a Wiegand card are well known and widely employed in various applications like systems for unlocking doors or parking garage gates etc. Usually, the Wiegand reader is located to be accessible to the user (Wiegand card holder) while the control panel, which after a positive evaluation of the data perform a security relevant operation (e.g. unlocking a door) is located in an area which is not accessible to the user, e.g. in a closed room, to guarantee a certain level of security.

US-5 679 945 shows an access system of the type mentioned in the beginning which provides an "intelligent" card reader in order to replace existing magnetic stripe readers, bar code readers and Wiegand readers without the need for retrofitting of existing computer systems which are coupled to the existing readers.

The invention provides an access system with an extremely high level of security.

This object of the invention is attained with a security system of the type mentioned in the beginning wherein the access system further comprises a converter connected to the input device and to the control panel, the input device comprising encryption means to encrypt the information provided by the user, and the converter being capable of converting the encrypted

BEST AVAILABLE COPY

WAVELYNX EX. 1003, Pg. 361
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

information into a standard Wiegand signal. Thus, the access system provides a higher level of security because the data read from the input device is transferred in an encrypted form. Moreover, the system offers more flexibility because it is not limited to Wiegand readers as input devices, while the existing Wiegand control panels can still be used.

Preferably the converter is co-located with the control panel in the secure area. In this configuration there is no chance to intercept and abuse the information.

This guarantees an even higher security with regard to the data transfer from the input device to the control panel because it is not possible to intercept and abuse the authentication/identification information provided by the user since the information is encrypted until it reaches the converter which, together with the control panel, is located in the secure area which is not accessible to a fraud. In other words, a secure communication channel between the input device and the securely located converter is provided.

The input device preferably comprises a smart card reader into which a secure output can be implemented, for example a RS485 or a TCP/IP output.

According to a preferred embodiment of the invention the access system further comprises a host computer connected to and located remote from the input device. Preferably, the host computer is also connected to the control panel and the data between the input device and the host computer is transmitted using a RS485 or a TCP/IP protocol.

Thus, the remote host computer may be an existing access control system host computer which, after a slight modification and/or addition to the system software, can be used to configure and to control the input device in a secure manner.

BRIEF DESCRIPTION OF THE DRAWINGS

Further details of the invention become apparent from the following description in connection with the accompanying drawings. In the drawings:

Fig. 1 shows an access system according to the prior art.

Fig. 2 shows an access system according to an embodiment of the invention.

BEST AVAILABLE COPY

Fig. 3 shows an enhanced access system according to a further embodiment of the invention.

The prior art access system illustrated in Fig. 1 includes a standard Wiegand reader 10 and a Wiegand control panel 12 adapted to retrieve data from a standard Wiegand reader. The control panel 12 is located in a secure area 14 remote from the Wiegand reader 10, which is accessible to a user. In order to gain access the user ins his Wiegand card (not shown), which contains authentication and, if required identification information, into the Wiegand reader 10. The information is transmitted from the reader 10 to the control panel 12 where the information is evaluated. Depending on the result of the evaluation the control panel 12 either perform a security relevant operation, e.g. unlocking a door or the like, to grant the user the requested access, or it denies such operation.

The embodiment of the invention shown in Fig. 2 also makes use of a Wiegand control panel 12. (It has to be understood that the term "Wiegand control panel" is not restricted to a particular hardware configuration but rather includes any suitable control panel which is capable of processing signals/data in a Wiegand format by using corresponding software.) However, the standard Wiegand reader is replaced by another input device, in particular a smart card reader 16 into which a smart card (not shown) containing the authentication/identification information can be inserted. The smart card reader 16 includes means for encrypting the information stored on the smart card and an RS485 or TCP/IP output. The access system according to the invention further comprises a converter 18 connected both to the smart card reader 16 and to the control p el 12. The converter 8 and the control panel 12 are co-located in a secure area 14 remote from the smart card reader 16 and have a direct interface connection.

The operation of the access system of Fig. 1 will now be described. The user inserts his smart card into the smart card reader 16. The information on the smart card is read and encrypted by the encryption means of the smart card reader 16. The encrypted information is transmitted to the converter 18 using a secure RS485 or TCP/IP protocol. Thus, the connection

BEST AVAILABLE COPY

WAVELYNX EX. 1003, Pg. 363
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

between the smart card reader 16 and the converter 18 can be regarded as a "secure channel". The converter 18 converts the encrypted information into a standard Wiegand signal and sends it to the control panel 12. The control panel 12 is able to evaluate the Wiegand signal and decide whether to allow or to deny access.

Fig. 3 depicts a further embodiment of the invention which has substantially the same configuration as the embodiment of Fig. 2, but further includes a remote host computer 20 which is connected both to the input device, preferably a smart card reader 16, and to the control panel 12. The host computer 20 is located outside the secure area 14 of the control panel 12 and the converter 18. The communication between the host computer 20 and the smart card reader 16 is provided by a further secure channel, i.e. data is transferred using an RS485 or a TCP/IP protocol.

The operation of the access system of Fig. 3 to gain access is the same as described above. However, the access system can easily be adapted to various requirements. For example, the secure channel between the remote host computer 20 and the smart card reader 16 is be used to change the configuration of the smart card reader 16 on command from the host computer 20 in a comfortable and secure manner. Moreover, the host computer 20 can be used to define the type of input device that is required to gain access. Suitable input devices include contactless smart card reader, contact smart card reader, PIN pad, biometric device (e.g. fingerprint reader) and combinations thereof. The input devices required can be changed as a function of security threat level, day of week, time of day, or other conditions. The connection between the host computer 20 and the control panel 12 allows to check whether a control panel operation has been successfully executed. Further, the host computer 20 can be used to identify a possible malfunction of the control panel 12 by using test signals.

It has to be understood that the invention is not limited to embodiments using an RS485 or TCP/IP protocol. The communication through the secure channels may be provided by any other suitable protocol.

BEST AVAILABLE COPY

WAVELYNX EX. 1003, Pg. 364
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

WHAT IS CLAIMED IS:

1. An access system, comprising an input device which is accessible to a user and capable of reading an authentication and/or identification information provided by the user, and a Wiegand control panel (12) connected to the input device for evaluation of the information provided by the user, the control panel (12) being located in a secure area (14) remote from the input device, characterized in that the access system further comprises a converter (18) connected to the input device and to the control panel (12), the input device comprising encryption means to encrypt the information provided by the user, and the converter (18) being capable of converting the encrypted information into a standard Wiegand signal.

2. The access system according to claim 1, characterized in that the converter (18) is co-located with the control panel (12) in the secure area (14).

3. The access system according to claim 1, characterized in that the input device comprises a smart card reader (16).

4. The access system according to claim 1, characterized in that the input device comprises at least one of a PIN pad and a biometric device.

5. The access system according to claim 1, characterized in that the encrypted information is transmitted from the input device to the converter (18) using one of a RS485 and a TCP/IP protocol

6. The access system according to claim 1, characterized in that the access system further comprises a host computer (20) connected to and located remote from the input device.

7. The access system according to claim 5, characterized in that the host computer (20) is also connected to the control panel (12).

8. The access system according to claim 7, characterized in that the data between the input device and the host computer (20) is transmitted using one of a RS485 and a TCP/IP protocol.

BEST AVAILABLE COPY

WAVELYNX EX. 1003, Pg. 365
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Fig. 2

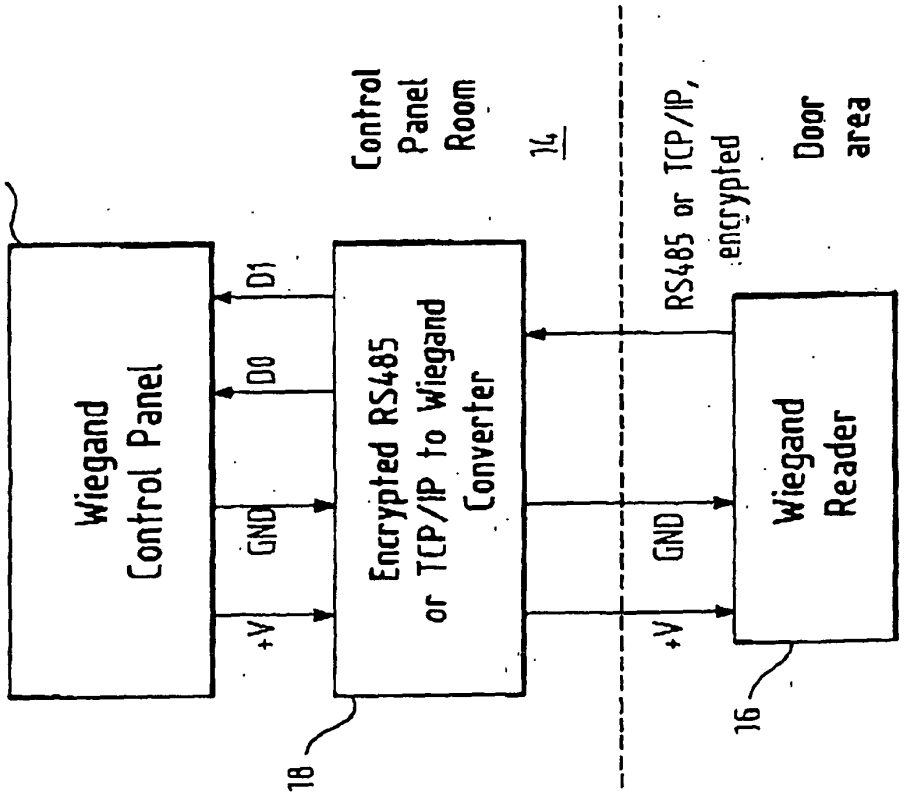
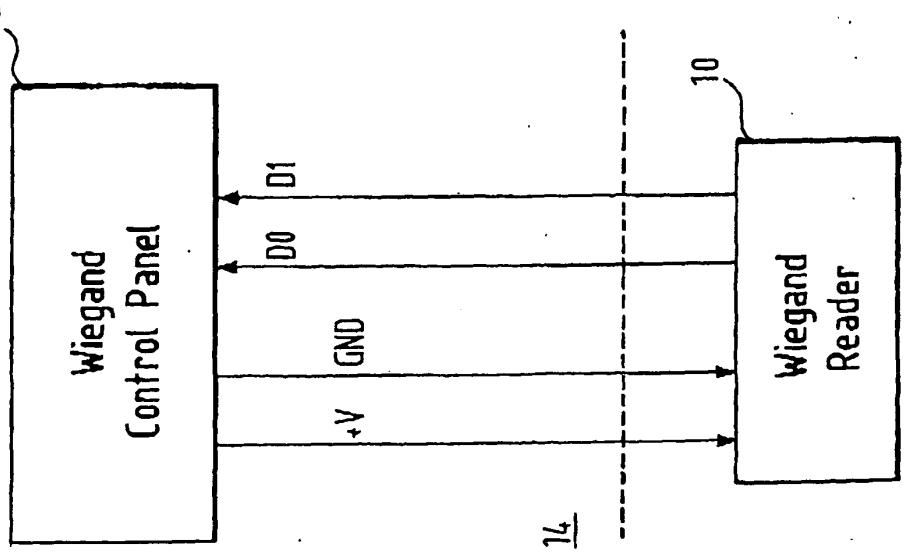


Fig. 1



BEST AVAILABLE COPY

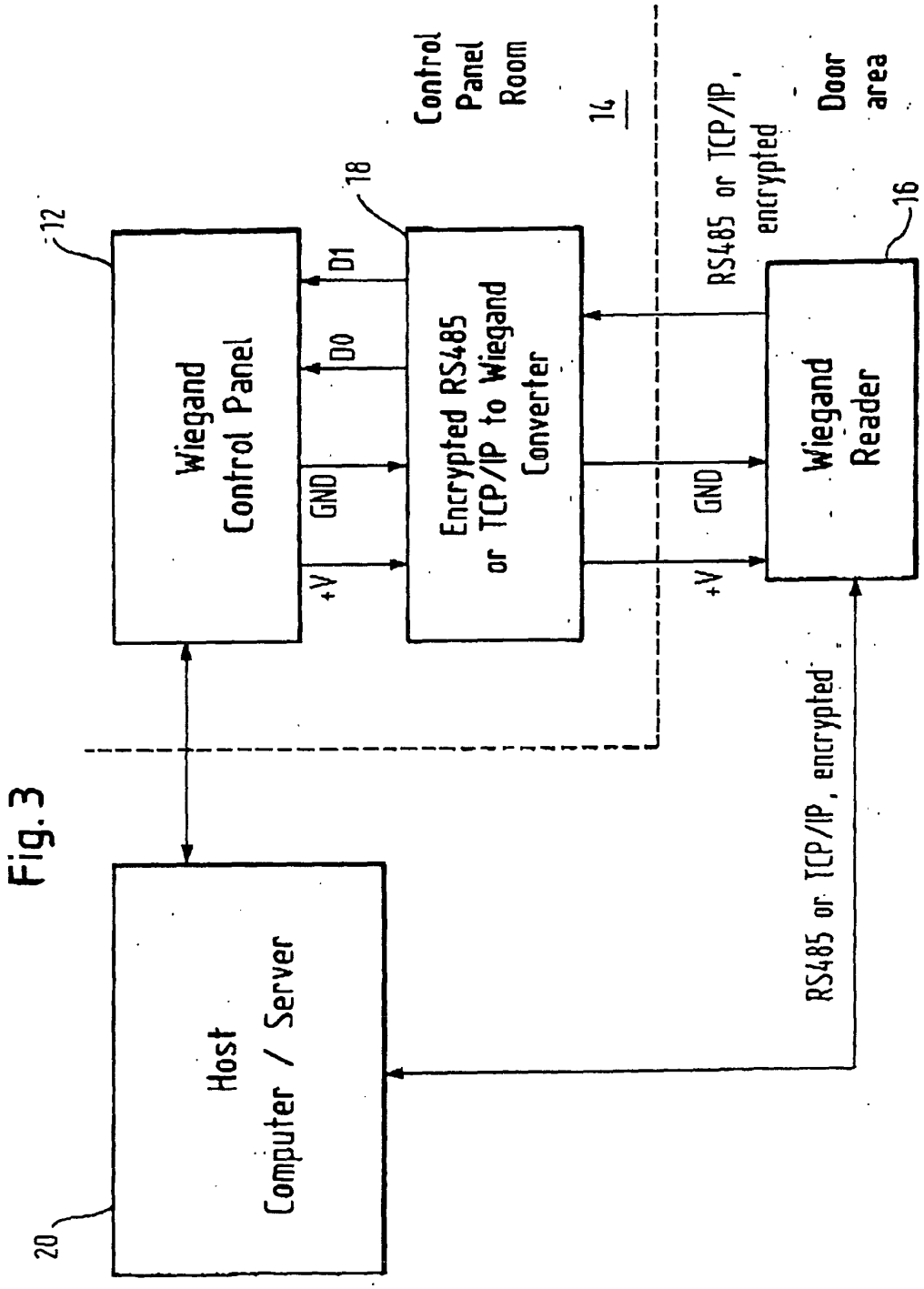

Control Panel Room
14
Door area
12
Wiegand Control Panel
18
Encrypted RS485 or TCP/IP to Wiegand Converter
16
Wiegand Reader
D1
D0
GND
+V
RS485 or TCP/IP, encrypted
GND
+V
RS485 or TCP/IP, encrypted
Host Computer / Server
20

Fig. 3

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

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 7 G07C G07F

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 practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DATABASE WPI Section EI, Derwent Publications Ltd., London, GB; Class T01, AN 2003-145718 XP002299947 "SERIAL COMMUNICATION INTERFACE FOR CONTROLLING ENTRANCE AND EXIT HAVING WIEGAND SIGNAL AUTOMATICALLY GENERATING DEVICE" & KR 2002 073 716 A (SUN SANG GYU) 28 September 2002 (2002-09-28)	1-5
Y	abstract	6-8
Y	US 5 475 378 A (CHARLTON BILL ET AL) 12 December 1995 (1995-12-12)	6-8
A	column 3, line 1 - column 4, line 14 figures	1
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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
8 October 2004	20/10/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Miltgen, E

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	US 2003/200446 A1 (CANNON GREG L ET AL) 23 October 2003 (2003-10-23) paragraph '0021! - paragraph '0029! figures	1-8
A	US 5 517 172 A (CHIU MANFRED F) 14 May 1996 (1996-05-14) column 2, line 35 - column 4, line 10 figure 1	1
A	US 2002/174357 A1 (DAVIS MICHAEL ET AL) 21 November 2002 (2002-11-21)	

WAVELYNX EX. 1003, Pg. 369
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 2002073716 A	28-09-2002	NONE	
US 5475378 A	12-12-1995	CA 2098973 A1	23-12-1994
US 2003200446 A1	23-10-2003	WO 03090403 A1	30-10-2003
US 5517172 A	14-05-1996	NONE	
US 2002174357 A1	21-11-2002	CA 2443086 A1	17-10-2002
		EP 1374157 A1	02-01-2004
		WO 02082367 A1	17-10-2002

WAVELYNX EX. 1003, Pg. 370
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 May 2004 (06.05.2004)

PCT

(10) International Publication Number
WO 2004/039119 A1

(51) International Patent Classification[7]: H04Q 9/00, H04J 13/00

(21) International Application Number: PCT/NZ2003/000211

(22) International Filing Date: 16 September 2003 (16.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
522174 22 October 2002 (22.10.2002) NZ

(71) Applicant *(for all designated States except US)*: **ANZON AUTODOOR LIMITED** [NZ/NZ]; Customhouse, Level 9, 50 Anzac Avenue, Auckland (NZ).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **O'MALLEY, Grant, Craydon** [NZ/NZ]; 232 Remuera Road, Auckland (NZ).

(74) Agents: **ADAMS, Matthew, D.** et al.; A J Park, 6th Floor Huddart Parker Building, PO Box 949, 6015 Wellington (NZ).

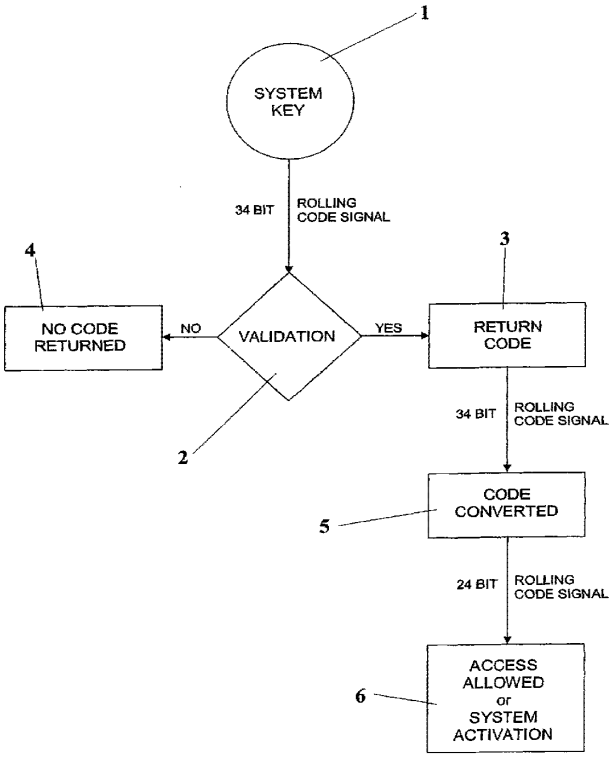
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Continued on next page]

(54) Title: ACCESS CONTROL SYSTEM

(57) Abstract: An access control system having a capability to validate a coded data string wireless transmission using a code hopping or rolling code algorithm and, if the transmission is validated, causing and/or allowing a function to occur responsive to receipt of another code string.



WO 2004/039119 A1

ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

ACCESS CONTROL SYSTEM

Technical Field

The present invention relates to coded entry or access and more particularly access control, security or entry of data logging that involves the validation of a data string.

Background Art

There are many instances where coded entry or access is required. Examples include door and gate systems but such examples are not exhaustive.

For example, with doors or garages it is common to utilise a wireless transmission (e.g. radio, infrared, microwave, etc.) to be detected by a receiver which either validates or does not validate the instruction and consequently respectively actuates or does not actuate.

The present invention recognises an advantage in having for coded entry and/or access purposes means of wirelessly transmitting a coded transmission (e.g. data string) that will vary each time it is used but not to the confusion of its dedicated receiver and only after such verification proceeding through (by any relay means, wired or wireless) to and/or enabling an ancillary data encryption format which has the capability of allowing or causing an action being instructed by and/or substantially together with the original transmission.

It is therefore to such systems that the present invention is directed, on at least to provide the public with a useful choice.

Disclosure of Invention

Accordingly in a first aspect the present invention consists in **an access control system** having a capability to validate a coded data string wireless transmission using a code hopping or rolling code algorithm and, if the transmission is validated, causing and/or allowing a function to occur responsive to receipt of another code string.

In a further aspect the present invention consists in **an access control system** that has, in sequence two code recognitions systems, the first to recognise a wireless

transmission of a data string and the second to be responsive to a related and/or unrelated data string only upon a validated receipt of the first mentioned data string,

wherein the first code recognition system is of a rolling or code hopping type so as to render wireless recording thereof by an authorised person unhelpful without access to the rolling or hoping algorithm.

Preferably the function control data string is shorter than that initially wirelessly transmitted.

In another aspect the invention consists in **an access control system**

having access function(s) controlled by a coded protocol ("function control protocol") system,

and having a coded protocol reliant on wireless transmission and receipt thereof ("the verification protocol") which code hops or rolls reliant on a relating algorithm,

wherein verification by the verification protocol is a prerequisite for access function(s) under the control of the function control protocol being allowed.

Preferably the function control protocol involves fewer coded bits than the verification protocol.

Preferably several transmitters can be verified to enable at least some control of the function control protocol.

Preferably the function(s) include door opening/closing.

Optionally verification protocol can be the or a Wiegand protocol.

Optionally function control protocol can be the or a KEELOQ™ protocol.

The present invention consists in apparatus of a system in accordance with the present invention.

The present invention relates to **methods** of operating an access control which is reliant upon a system in accordance with the present invention.

In still a further aspect the present invention consists in the use of apparatus to transmit verification data and/or instruction data as part of the system of the present invention or as part of the method of the present invention.

In still a further aspect the present invention consists in a door or other access opening responsive to control of the kind contemplated by the present invention.

WAVELYNX EX. 1003, Pg. 374
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

As used herein the term "and/or" means "and" or "or", or both where the circumstances allow.

As used herein the term "(s)" following a noun means both or either the plural and singular forms of that noun.

As used herein the term "/" between nouns (e.g. as used hereinafter as "opening/closing" means both the opening and closing functions or either.

Reference herein to the Wiegand protocol refers to a standard data output format that is an industry standard digital protocol for accessing and transferring data between devices (see published standard of The Security Industry Association of the USA).

Reference herein to a KEELOQ™ protocol refers to a code hopping technology developed specifically for secure remote keyless entry and authentication based on the principle is that the code changes (hops) each time it is transmitted. KEELOQ™ is based on a proprietary, non-linear encryption algorithm that creates a unique transmission on every use, rendering code capture and resend schemes useless. The algorithm uses a programmable 64-bit encryption key unique to each device to generate 32-bit hopping code.

Reference to a protocol that is "or the like" by reference to the Wiegand protocol or the KEELOQ™ protocol means that protocol embodied in Microchip KEELOQ™ products of Microchip technology Incorporated. Reference is made to their website < http://www.microchip.com/1010/index.htm>.

For the purpose of the use of systems of the present invention in garage door openings reference is drawn to the website of *www.merlingo.com/* as demonstrating apparatus and forms appropriate for such control.

Brief Description of Drawings

A preferred form of the present invention will now be described by reference to the two flow diagrams of which

Figure 1 shows a diagram where a data string wirelessly transmitted is detected and verified or not and it is only upon verification that that data string continues into a different coded protocol to effect functions,

Figure 2 shows an alternative where simultaneous or substantially simultaneous transmissions ensure verification prior to allowing a separately transmitted data string to activate the different protocol,

Figure 3 shows a further alternative embodiment whereby a wireless rolling code signal is sent to a receiver which upon positive validation outputs a converted code of a differing rolling code format the signal whether being transmitted in a wired or wireless format then allows access or activates the system, and

Figure 4 is a diagram for use in our explanation of some functions and logic features of a preferred implementation of the present invention.

Best Mode for Carrying Out the Invention

Systems in accordance with the present invention preferably link systems such as that marketed under the trade marks Wiegand and KEELOQ™ so as to provide for the access control system the synergism of initiation to less secure input data strings only upon recognition of a more secure data string protocol. Such a system will enable more transmitters to be made available without any substantial undermining of security. In, for example, a garage door opening scenario or a gate opening scenario, related functions to initiation can be compounded in the scenario of Figure 1 where, for example the code string of the verification protocol may be say of 34 bits whilst that of the function control protocol may be less than half that.

With reference to Figures 1 through 3 is shown varying embodiments of an access control system. The system converts data transmitted wirelessly, for example from a radio transmitter, keypad, or similar 1, in an encrypted code utilising a rolling or code hopping algorithm (such as KEELOQ™). The data is received and validated by a receiver 2 using the appropriate decryption algorithm and then a signal relayed by any means, wired or wireless, in another data encryption format (such as Wiegand) to another access control, security, entry or data logging system 6 for validation and recording by that system such validation may allow activation of a latch or similar means to then allow access by the user or person who originally transmitted the signal. The system also allows for the receiver to learn and store a number of remote

transmitted devices 1. In this way multiple users can gain access with their own code to the system.

The system key 1 sends out a 34 bit rolling code signal, such as that generated by the KEELOQ™ security protocol, this is then received by a receiver 2 which then validates this signal. If the signal is not validated no code is returned 4. If the validation is positive then an output is generated. In the situation where there is a further receiver 5 such as in Figure 1 this receives the code output from 3 as a 34 bit rolling code signal (whether wired or wireless signal). The second receiver 5 then converts the information from the 34 bit rolling code signal and outputs this as a 24 bit rolling code signal (such as that generated by the Wiegand protocol) which then gives the user access or activates the system.

In a situation where the return code is sent to the original system key 1 then this return 34 bit rolling code signal is received and then converted to a 24 bit rolling code signal by 5 which is transmitted to then activate the system or allow access to the system.

A further embodiment allows, upon a positive validation from the receiver 2 generation directly of a 24 bit rolling code system by a conventer 7 which is transmitted either by wired or wireless means to allow further access 6.

In this way a high security protocol such as that provided by a 32 bit rolling code system will allow the user upon positive validation of the user, access to or activation of a further system, the activation of or access to that system occurring via a lower security protocol such as a 24 bit rolling code signal. This two layer security system providing a more secure system.

A description of the function and some underlying logic of the door controller limit system in one preferred or optional embodiment will now be described. It may use hardware as disclosed in our New Zealand Patent Specifications 522578 or 522300 filed 12 November 2002 and 25 October 2002 respectively, or indeed any mounting, assembly, subassembly and system we have disclosed by way of publication or use in respect of our MERLIN™ brand door systems.

Operation before setup

WAVELYNX EX. 1003, Pg. 377
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The manual control button ideally requires to be continuously depressed to move the door. Successive presses result in reversal of door travel direction. This ensures that the door can not accidentally be moved beyond the correct physical end-points of travel.

Set up

To define the limit positions the following process should be performed:

- move the door to the desired open or closed limit position
- store that position in memory
- move the door to the other desired limit position
- store that position in memory

Operation after setup

A brief press of the manual control button will move the door from one limit to the other. Pressing the manual control button while the door is moving stops the door.

Controller overview

The following controller inputs, outputs, and parameters are relevant:

- the state of the reference switch: either 0 or 1
- the state of the motor control relays: opening, closing, or stopped
- the state changes of the position sensor: 0 or 1 for every k mm of door position (where k is a constant dependent on gearing, and type of sensor)
- time
- motor current

From these the controller can infer the position, speed and direction of the door's travel. With knowledge of the motor's torque-speed, and torque-current, characteristics the load placed on the motor can be inferred for any position of the door's travel.

If the controller has been reset, it can not determine whether its stored relative position is correct so it must recalibrate to the reference position. In order to decide which direction to travel first it checks the state of the reference switch and then moves towards the reference point. Once the reference switch has changed state,

normal operation resumes. The user will be unaware of this unless they stop the door and try to move the door in the opposite direction before the reference switch changes state. In this circumstance the user will be required to continuously depress the manual control button.

On every uninterrupted operation from a limit position the counter will be set to zero at the reference switch. The counter values for the open and closed limits will be referenced to the newly calibrated reference position. See Figure 8.

Adaptive travel adjustment

The motor speed and/or current is stored with door position during setup. If during normal operation within a short distance of the bottom limit the speed and/or current does not match the stored values within some percentage then the physical limit position is judged to have been altered. The new limit position replaces the old limit position counter value.

CLAIMS:

1. **An access control system** having a capability to validate a coded data string wireless transmission using a code hopping or rolling code algorithm and, if the transmission is validated, causing and/or allowing a function to occur responsive to receipt of another code string.

2. A system of claim 1 wherein the function control data string is shorter than that initially wirelessly transmitted.

3. **An access control system** that has, in sequence two code recognitions systems, the first to recognise a wireless transmission of a data string and the second to be responsive to a related and/or unrelated data string only upon a validated receipt of the first mentioned data string,

wherein the first code recognition system is of a rolling or code hopping type so as to render wireless recording thereof by an authorised person unhelpful without access to the rolling or hoping algorithm.

4. **An access control system**

having access function(s) controlled by a coded protocol ("function control protocol") system,

and having a coded protocol reliant on wireless transmission and receipt thereof ("the verification protocol") which code hops or rolls reliant on a relating algorithm,

wherein verification by the verification protocol is a prerequisite for access function(s) under the control of the function control protocol being allowed.

5. A system of claim 4 wherein the function control protocol involves fewer coded bits than the verification protocol.

6. A system of claim 4 or 5 wherein several transmitters can be verified to enable at least some control of the function control protocol.

7. A system of any one of claims 4 to 6 wherein the function(s) include door opening/closing.

8. A system of any one of claims 4 to 7 wherein verification protocol can be the or a Wiegand or like protocol.

9. A system of any one of claims 4 to 8 wherein the function control protocol is a KEELOQ™ or like protocol.

10. Apparatus incorporating a system in accordance with any one of the preceding claims.

11. **Methods** of operating an access control which is reliant upon a system in accordance with any one of claims 1 to 9.

12. The use of apparatus to transmit verification data and/or instruction data as part of a system of any one of claims 1 to 9 or as part of the method of claim 11.

13. A door or other access opening obstruction responsive to control of a system of any one of claims 1 to 9.

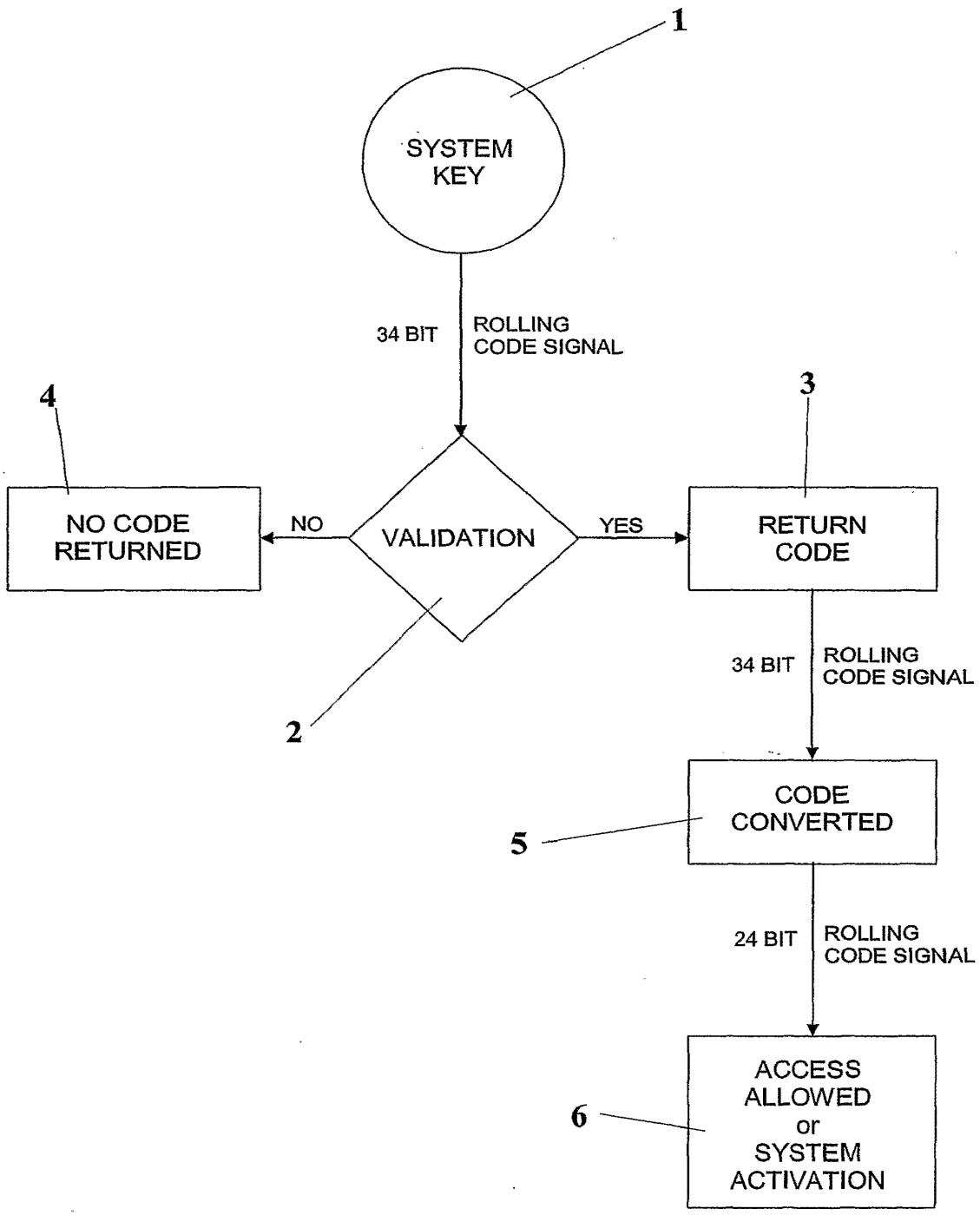

1
SYSTEM KEY
34 BIT
ROLLING CODE SIGNAL
4
3
NO CODE RETURNED
NO
VALIDATION
YES
RETURN CODE
2
34 BIT
ROLLING CODE SIGNAL
CODE CONVERTED
5
24 BIT
ROLLING CODE SIGNAL
ACCESS ALLOWED or SYSTEM ACTIVATION
6

FIGURE 1

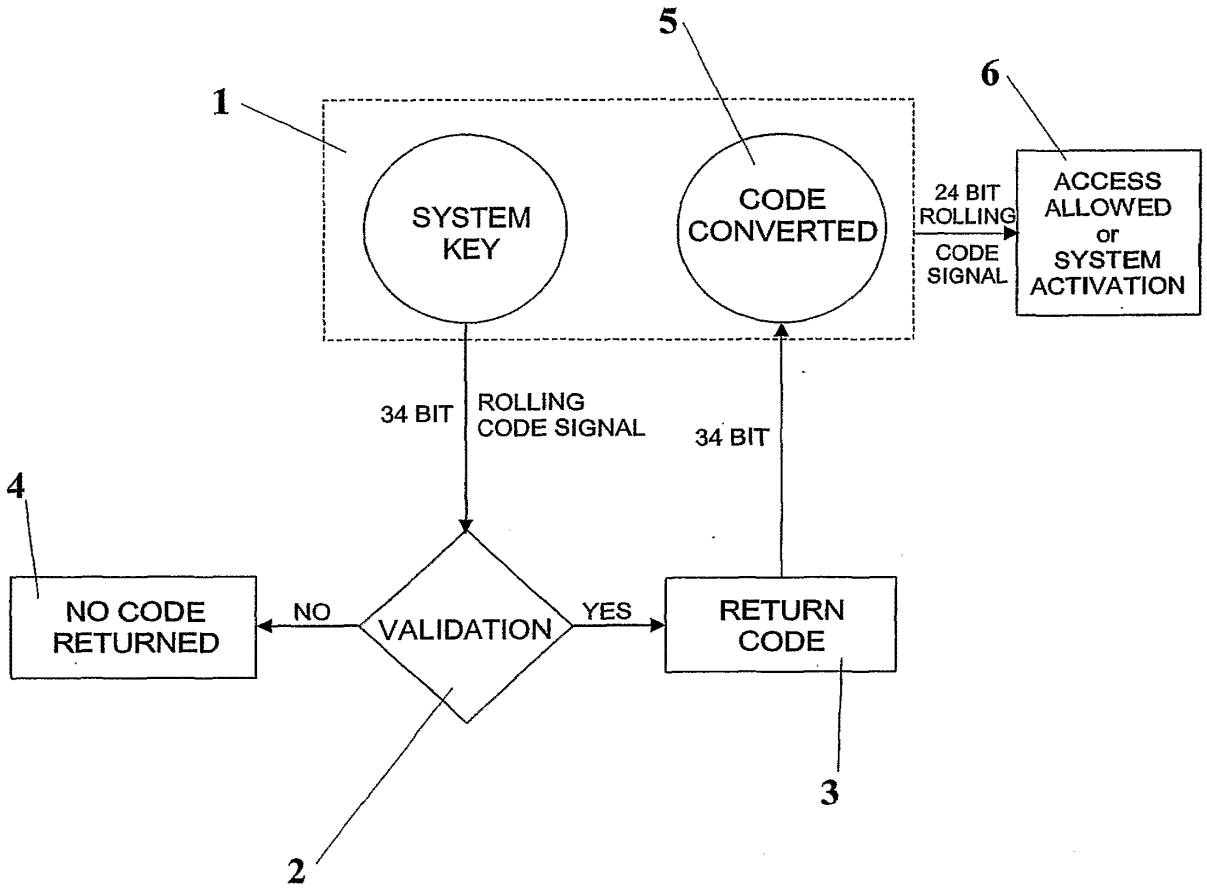

5
6
1
SYSTEM KEY
CODE CONVERTED
24 BIT ROLLING CODE SIGNAL
ACCESS ALLOWED or SYSTEM ACTIVATION
34 BIT ROLLING CODE SIGNAL
34 BIT
4
NO CODE RETURNED
NO
VALIDATION
YES
RETURN CODE
2
3

FIGURE 2

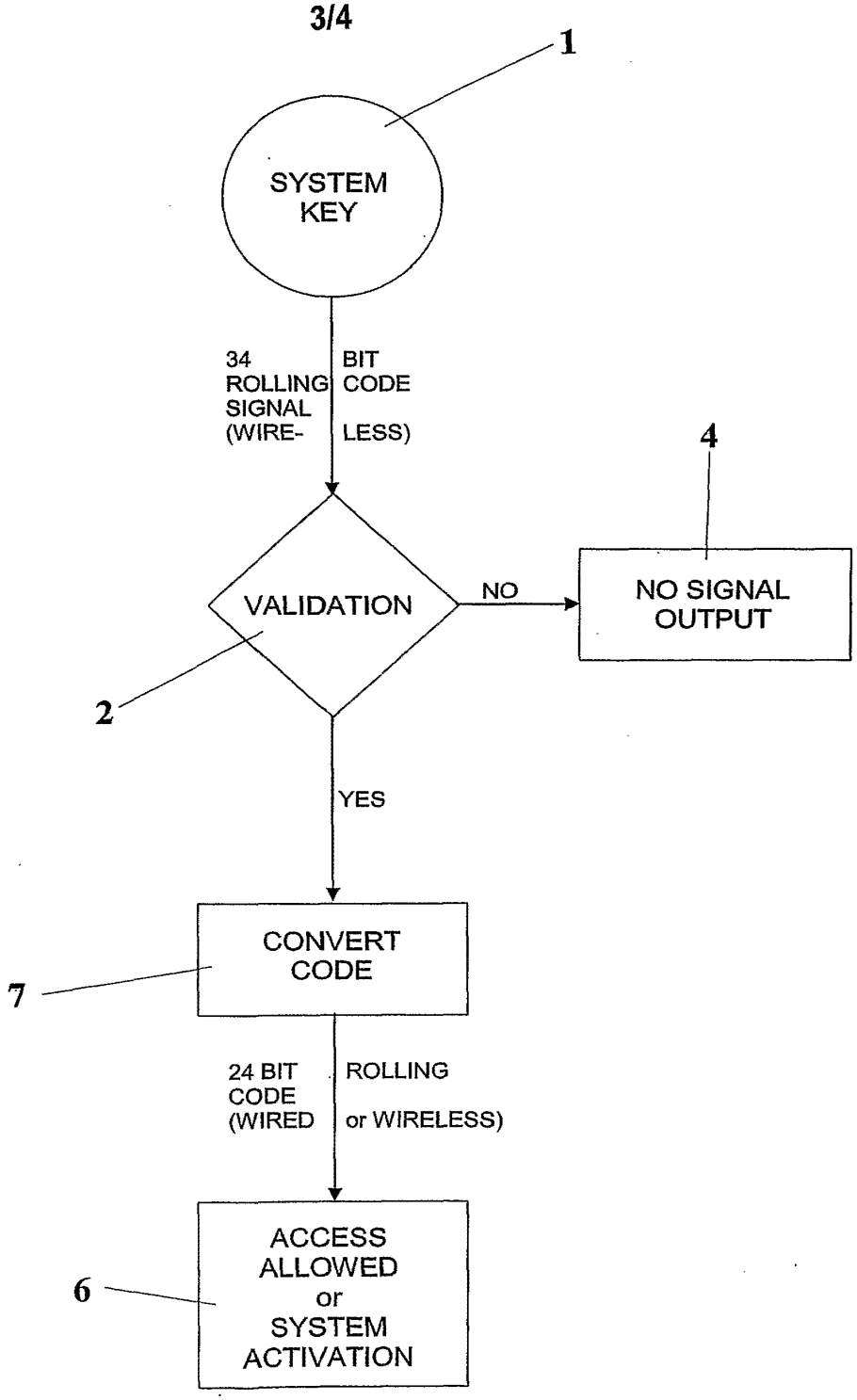

1
SYSTEM KEY
34 ROLLING SIGNAL (WIRE-
BIT CODE
LESS)
4
VALIDATION
NO
NO SIGNAL OUTPUT
2
YES
CONVERT CODE
7
24 BIT CODE (WIRED
ROLLING
or WIRELESS)
ACCESS ALLOWED or SYSTEM ACTIVATION
6

FIGURE 3

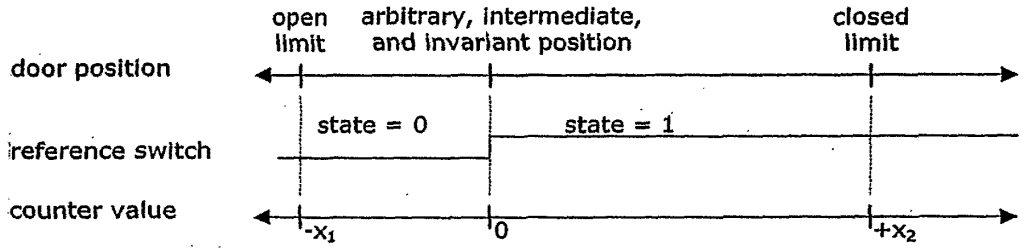


FIGURE 4

WAVELYNX EX. 1003, Pg. 385
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ03/00211

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: H04Q 9/00, H04J 13/00

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)

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)
WPAT, USPTO (code, rolling, access)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6411199 B1 (Geiszler et al) 25 June 2002 Whole Document	
A	US 5949349 A (Farris et al) 7 September 1999 Whole Document	
A	GB 2275552 A (Rover Group Limited) 31 August 1994 Whole Document	

☐ 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
27 November 2003	- 4 DEC 2003
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **R.H. STOPFORD** Telephone No : (02) 6283 2177

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/NZ03/00211

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member
US	6411199	NONE
US	5949349	NONE
GB	2275552	NONE

END OF ANNEX

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 February 2005 (24.02.2005)

PCT

(10) International Publication Number
WO 2005/018137 A1

(51) International Patent Classification[7]: H04L 9/32, G06K 9/00

(21) International Application Number: PCT/AU2004/001083

(22) International Filing Date: 13 August 2004 (13.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003904317 13 August 2003 (13.08.2003) AU

(71) Applicant *(for all designated States except US)*: **SECURICOM (NSW) PTY LTD** [AU/AU]; 48 Margate Street, Ramsgate, NSW 2217 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BURKE, Christopher, John** [AU/AU]; 48 Margate Street, Ramsgate, NSW 2217 (AU).

(74) Agent: **SPRUSON & FERGUSON**; GPO Box 3898, Sydney, NSW 2001 (AU).

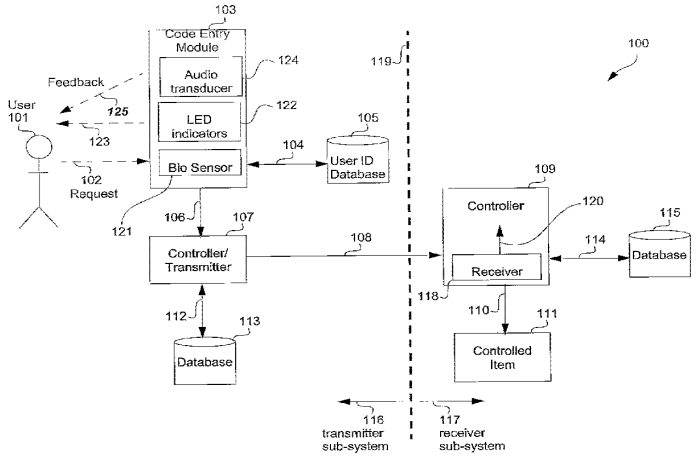
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *with amended claims*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: REMOTE ENTRY SYSTEM



(57) Abstract: A system (100) is disclosed for providing secure access to a controlled item (111), the system comprising a database (105) of biometric signatures, a transmitter subsystem (116) comprising a biometric sensor (121) for receiving a biometric signal (102), means for matching the biometric signal against members of the database of biometric signatures (105) to thereby output an accessibility attribute, and means (107) for emitting a secure access signal (106) conveying information dependent upon said accessibility attribute, wherein the secure access signal (108) comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, and a receiver sub-system (117) comprising means (109) for receiving the transmitted secure access signal (108) and means for providing conditional access to the controlled item (111) dependent upon said information.

WO 2005/018137 A1

REMOTE ENTRY SYSTEM

Field of the Invention

The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

Background

Fig. 1 shows a prior art arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 403. Thus, for example, the request 402 can be a sequence of secret numbers directed to a keypad 403. Alternately, the request 402 can be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

The code entry module 403 conveys the request 402 by sending a corresponding signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access.

A proximity card can also be used to emit the request 402, in which case the code entry module 403 has appropriate functionality.

WAVELYNX EX. 1003, Pg. 389
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Although the request 402 can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in **Fig. 1** is typically less secure. The infrastructure 400 is generally hardwired, with the code entry module 403 generally being mounted on the outside jamb of a secured door. In such a situation, the signal path 404 can be over a significant distance in order to reach the controller 405. The path 404 represents one weak point in the security system 400, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module 403 and the controller 405. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module 403 and the controller 405. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user 401, or to enable modification for other subversive purposes.

Current systems as depicted in **Fig. 1** utilise a communication protocol called "Wiegand" for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405.

More advanced protocols such as RS 485 have been used in order to overcome the vulnerability of the Wiegand protocol over the long distance route 404. RS 485 is a duplex protocol offering encryption capabilities at both the transmitting and receiving ends, ie. the code entry module 403 and the controller 405 respectively in the present case. The length of the path 404 nonetheless provides an attack point for the unauthorised person.

WAVELYNX EX. 1003, Pg. 390
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Due to the cost and complexity of re-wiring buildings and facilities, security companies often make use of existing communication cabling when installing and/or upgraded security systems, thereby maintaining the vulnerability described above.

Summary

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

According to a first aspect of the present invention, there is provided a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the

transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; wherein the receiver sub-system comprises;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a method for providing secure access to a controlled item, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction.

According to another aspect of the present invention, there is provided a method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving the secure access signal transmitted by a transmitter sub-system, and means for providing conditional access to the controlled item

dependent upon information conveyed in the secure access signal, said method comprising the steps of:

receiving a biometric sensor by biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided a method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, said method comprising the steps of:

receiving the transmitted secure access signal; and

providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

code for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

code for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to populate a database of biometric signatures in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a series of entries of the biometric signal;

code for determining at least one of the number of said entries and a duration of each said entry;

code for mapping said series into an instruction; and

code for populating the database according to the instruction.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a biometric sensor by biometric signal;

code for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

code for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to receive a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving the transmitted secure access signal; and

code for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a system for providing secure access, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

a control panel for receiving the information and for providing the secure access requested.

Other aspects of the invention are also disclosed.

Brief Description of the Drawings

Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

Fig. 1 shows a prior art arrangement for providing secure access;

Fig. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

Fig. 3 shows an example of a method of operation of the remote control module of **Fig. 2**;

Fig. 4 shows an example of a method of operation of the (fixed) control device of **Fig. 2**;

Fig. 5 shows incorporation of a protocol converter into the arrangement of **Fig. 2**; and

Fig. 6 shows another example of how the remote access system operates;

Fig. 7 shows an access process relating to the example of **Fig. 6**;

Fig. 8 shows one enrolment process relating to the example of **Fig. 6**;

Fig. 9 shows another enrolment process relating to the example of **Fig. 6**; and

Fig. 10 is a schematic block diagram of the system in **Fig. 2**.

Detailed Description including Best Mode

It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

Fig. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure. A user 101 makes a request, as depicted by an arrow 102, to a code entry module 103. The code entry module 103 includes a biometric sensor 121 and the request 102 takes a form which corresponds to the nature of the sensor

121 in the module 103. Thus, for example, if the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module 103.

The code entry module 103 interrogates, as depicted by an arrow 104, a user identity database 105. Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 then the user database 105 contains biometric signatures for authorised users against which the request 102 can be authenticated. If the identity of the user 101 is authenticated successfully, then the code entry module 103 sends a signal 106 to a controller/transmitter 107. The controller/transmitter 107 checks, as depicted by an arrow 112, the current rolling code in a database 113. The controller 107 then updates the code and sends the updated code, this being referred to as an access signal, as depicted by an arrow 108 to a controller 109. The rolling code protocol offers non-replay encrypted communication.

The controller 109 tests the rolling code received in the access signal 108 against the most recent rolling code which has been stored in a database 115, this testing being depicted by an arrow 114. If the incoming rolling code forming the access signal 108 is found to be legitimate, then the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101. It is noted that the controller 109 contains a receiver 118 that receives the transmitted access signal 108 and converts it into a form that is provided, as depicted by an arrow 120, into a form that the controller 109 can use.

The code entry module 103 also incorporates at least one mechanism for providing feedback to the user 101. This mechanism can, for example, take the form or one or more Light Emitting Diodes (LEDs) 122 which can provide visual feedback,

depicted by an arrow 123 to the user 101. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125.

The arrangement in **Fig. 2** has been described for the case in which the secure code in the access signal 108 used between the sub-systems 116 and 117 is based upon the rolling code. It is noted that this is merely one arrangement, and other secure codes can equally be used. Thus, for example, either of the Bluetooth™ protocol, or the Wi Fi™ protocols can be used.

Rolling codes provide a substantially non-replayable non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system 116 and the receiver/controller 118/109.

Rolling codes use a different code variant each time the transmission of the access signal 108 occurs. This is achieved by encrypting the data from the controller 107 with a mathematical algorithm, and ensuring that successive transmissions of the access signal 108 are modified using a code and/or a look-up table known to both the transmitter sub-system 116 and the receiver sub-system 117. Using this approach successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller 107 remains the same. The modification of the code in the access signal 108 for each transmission significantly reduces the likelihood that an intruder can access the information replay the information to thereby gain entry at some later time.

The sub-system in **Fig. 2** falling to the left hand side, as depicted by an arrow 116, of a dashed line 119 can be implemented in a number of different forms. The sub-

system 116 can for example be incorporated into a remote fob (which is a small portable device carried by the user 101), or alternately can be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system 116 communicates with the sub-system 117 on the right hand side of the dashed line 119 via the wireless communication channel used by the access signal 108. The sub-system 117 is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. The location of the sub-system 117 must of course be consistent with reliable reception of the wireless access signal 108.

Although typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 can use a wired medium. This is particularly the case when the transmitter sub-system 116 is mounted in an enclosure on the door jamb rather than in a portable key fob.

The biometric signature database 105 is shown in **Fig. 2** to be part of the transmitter sub-system 116. However, in an alternate arrangement, the biometric signature database 105 can be located in the receiver sub-system 117, in which case the communication 104 between the code entry module 103 and the signature database 105 can also be performed over a secure wireless communication channel such as the one used by the access signal 108. In the event that the secure access system is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC can be integrated into the receiver sub-system 117 of **Fig. 1**.

In the event that the sub-system 116 is implemented as a remote fob, the combination of the biometric verification and the strongly encrypted wireless communication provides a particularly significant advantage over current systems. The remote key fob arrangement allows easy installation, since the wired communication path

404 (see **Fig. 1**) is avoided. Other existing wiring elements of the present systems 400 can be used where appropriate. When the sub-system 116 is implemented as a remote fob, the fob incorporates the biometric (eg fingerprint) authentication arrangement, in which case only one biometric signature is stored in the fob. This arrangement reduces the requirements on the central database 115. Once the key fob authenticates the user through biometric signature (eg fingerprint) verification, the rolling code in the access signal 108 is transmitted to the controller 109 for authorisation of the user for that location at that time.

In addition to authenticating the user 101 the biometric sensor 121 in the code entry module 103 in conjunction with the controller 107 can also check other access privileges of the user 101. These access privileges can be contained in the database 105 which can be located either locally in the remote key fob, or in the receiver sub-system 117 as previously described. In one example, Tom Smith can firstly be authenticated as Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the transmitter sub-system 116 can check if Tom Smith is in fact allowed to use the particular door secured by the device 111 on weekends. Thus the security screening offered by the described arrangement can range from simple authentication of the user's identity, to more comprehensive access privilege screening.

The incorporation of the biometric sensor 121 into the code entry module 103 in the form of a remote key fob also means that if the user 101 loses the remote key fob, the user need not be concerned that someone else can use it. Since the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor 121 in the code entry module 103, the lost key fob is useless to anyone apart from the rightful user 101.

The transmitter sub-system 116 is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the biometric sensor 121 in the code entry module 103 and directly forcing the controller 107 to emit the rolling code access signal 108.

Fig. 3 shows the method of operation of the remote control module (ie the sub-system 116) of **Fig. 2**. The method 200 commences with a testing step 201 in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 200 is directed in accordance with an NO arrow back to the step 201 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 200 is directed in accordance with a YES arrow to a step 202. The step 202 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101 of the sub-system 116.

A subsequent testing step 203 checks whether the comparison in the step 202 yields the desired authentication. If the biometric signature matching is authenticated, then the process 200 is directed in accordance with a YES arrow to a step 204. The authentication of the biometric signature matching produces an accessibility attribute for the biometric signal 102 in question. The accessibility attribute establishes whether and under which conditions access to the controlled item 111 should be granted to a user. Thus, for example, the accessibility attribute may comprise one or more of an access attribute (granting unconditional access), a duress attribute (granting access but with activation of an alert tone to advise authorities of the duress situation), an alert attribute (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a telemetry attribute, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-

WAVELYNX EX. 1003, Pg. 402
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

system such as a "low battery" condition. The step 204 enables the user 101 to select a control option by providing one or more additional signals (not shown) to the controller 107. Thus for example the control option could enable the user 101 to access one of a number of secure doors after his or her identity has been authenticated in the step 203. In the subsequent step 205 the controller 107 sends the appropriate access signal 108 to the controller 109. The process 200 is then directed in accordance with an arrow 206 back to the step 201.

Thus for example the sub-system 116 can be provided with a single biometric sensor 121 in the code entry module 103 which enables the user 101 to select one of four door entry control signals by means of separate buttons on the controller 107 (not shown). This would enable the user 101, after authentication by the biometric sensor 121 in the code entry module 103 and the controller 107 to obtain access to any one of the aforementioned for secure doors.

Returning to the testing step 203, if the signature comparison indicates that the biometric signal 102 is not authentic, and has thus not been received from the proper user, then the process 200 is directed in accordance with a NO arrow back to the step 201. In an alternate arrangement, the NO arrow from the step 203 could lead to a disabling step which would disable further operation of the sub-system 116, either immediately upon receipt of the incorrect biometric signal 102, or after a number of attempts to provide the correct biometric signal 102.

Fig. 4 shows the method of operation of the control sub-system 117 of **Fig. 2**. The method 300 commences with a testing step 301 which continuously checks whether the access signal 108 has been received from 107. The step 301 is performed by the controller 109. As long as the access signal 108 is not received the process 300 is directed in accordance with a NO arrow in a looping manner back to the step 301. When

the access signal 108 is received, the process 300 is directed from the step 301 by means of a YES arrow to a step 302. In the step 302, the controller 109 compares the rolling code received by means of the access signal 108 with a reference code in the database 115. A subsequent testing step 303 is performed by the controller 109. In the step 303 if the code received on the access signal 108 is successfully matched against the reference code in the database 115 then the process 300 is directed in accordance with a YES arrow to a step 304.

In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door). The process 300 is then directed from the step 304 as depicted by an arrow 305 back to the step 301. Returning to the testing step 303 if the code received on the access signal 108 is not successfully matched against the reference code in the database 115 by the controller 109 then the process 300 is directed from the step 303 in accordance with a NO arrow back to the step 301.

As was described in regard to **Fig. 3**, in an alternate arrangement, the process 300 could be directed, if the code match is negative, from the step 303 to a disabling step which would disable the sub-system 117 if the incorrect code where received once or a number of times.

Fig. 5 shows incorporation of a protocol converter into the arrangement of **Fig. 2**. In the arrangement of **Fig. 2** the receiver 118 in the controller 109 is able to directly receive and process the rolling code in the access signal 108 in a manner as to provide, as depicted by the arrow 120, the necessary information to the controller 109. **Fig. 5** shows how an existing controller depicted by a reference numeral 109' that uses Wiegand input signalling can be used in the disclosed arrangement when alarm systems are upgraded. **Fig. 5** shows how the incoming access signal 108 is received by a receiver 118' as is the case in **Fig. 2**. In **Fig. 5** however the receiver 118' provides, as depicted by an arrow 503,

the received rolling code from the access signal 108 to a rolling code/Wiegand protocol converter 501. The converter 501 converts, as depicted by an arrow 504, the incoming rolling code 503 to a form that can be used by the controller 109' that is designed to handle Wiegand protocol incoming signals. Therefore, the converted incoming signal 504 is in the Wiegand format.

The converter 501 uses a microprocessor-based arrangement running software code to process the incoming rolling code information 503 and decode this information 503 to clear text form. The converter 501 converts this clear text to a Wiegand variable bit-length data stream. In **Fig. 2**, the receiver 118 performs the conversion of the incoming rolling code access signal 108 to clear text which enables the controller 109 to identify the serial number of the originating key fob sub-system 116 to enable the access rights of the user to be verified.

Further to the Wiegand conversion arrangement, the protocol converter 501 approach can be adapted to convert between the incoming rolling code 503 (or any other appropriate secure code) to any other convenient protocol used by the controller 109'.

The advantage of the rolling code/Wiegand converter 501 is that security system upgrades can be made without replacing Wiegand compatible controller 109'. Accordingly, existing systems as are described in **Fig. 1** can be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (ie., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor modifications might however be necessary. When upgrading systems in this manner, the sub-system 116 can either be used in a remote fob configuration, or can be placed in a secure housing on an external door jamb.

From a practical perspective, incorporating the protocol converter 501 into an existing controller 109' would require direct wiring of the converter 501 into the housing of the secure controller 109'.

Fig. 6 shows another process 700 of operation of the remote access system. The process 700 commences with a step 701 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module in **Fig. 2**. If not, then the process 700 follows a NO arrow back to the step 701. If however a biometric signal has been received, then the process 700 follows a YES arrow to a step 702 that determines if the user ID database 105 in **Fig. 2** is empty. This would be the case, for example, if the code entry module is new and has never been used, or if the user 101 has erased all the information in the database 105.

If the database 105 is empty, then the process 700 is directed by an arrow 703 to 706 in **Fig. 8** which depicts a process 800 dealing with the enrolment or the administration function for loading relevant signatures into the database 105. If on the other hand the database 105 is not empty, then the process 700 is directed to a step 704 that determines if the biometric signal that has been received is an administrator's biometric signal.

The disclosed remote entry system can accommodate at least three classes of user, namely administrators, (ordinary) users, and duress users. The administrators have the ability to amend data stored, for example, in the database 105, while the ordinary users do not have this capability. The first user of the code entry module 103, whether this is the user who purchases the module, or the user who programs the module 103 after all data has been erased from the database 105, is automatically categorised as an administrator. This first administrator can direct the system 100 to either accept further administrators, or alternately to only accept further ordinary users.

Although the present description refers to "users", in fact it is "fingers" which are the operative entities in system operation when the biometric sensor 121 (see **Fig. 2**) is a fingerprint sensor. In this event, a single user can enrol two or more of his or her own fingers as separate administrators or (ordinary) users of the system, by storing corresponding fingerprints for corresponding fingers in the database 105 via the enrolment process 800 (see **Fig. 8**).

Some class overlap is possible. Thus a stored signature can belong to an administrator in the duress class.

The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

One example of a legal control signal can be expressed as follows:

"Enrol an ordinary user" -> dit, dit, dit, dah

where "dit" is a finger press of one second's duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration.

In the event that a legitimate sequence of finger presses are not delivered within the predetermined time, then the presses are considered not to be control information and merely to be presses intended to provide access to the controlled item 111. Legitimate control sequences are defined in Read Only Memory (ROM) in the controller 107.

WAVELYNX EX. 1003, Pg. 407
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The code entry module 103 has feedback signalling mechanisms 122, implemented for example by a number of LEDs, and 124, implemented by an audio transducer. The LEDs 122 and the audio transducer 124 are used by the controller to signal the state of the code entry module 103 to the user 101, and to direct the administration process. Thus, in one example, three LEDs, being Red, Amber and Green are provided.

When the Amber LED is flashing, it means "Press the sensor". When the Amber LED is steady ON, it means "Maintain finger pressure". When the Amber LED is OFF, it means "Remove finger pressure". When the system enters the enrolment state (depicted by the process 800 in **Fig. 8**), then the audio transducer 124 emits the "begin enrolment" signal (*dit dit dit dit*) and the Red LED flashes. Enrolment of a normal user (according to the step 807 in **Fig. 8**) is signalled by the OK audio signal (*dit dit*) and a single blink of the Green LED.

Returning to the step 704, if the step determines that the biometric signal received is an administrator's signal, then the process 700 is directed by a YES arrow to 706 in **Fig. 8** as depicted by the arrow 703. If on the other hand, the step 704 indicates that the received biometric signal does not belong to an administrator then the process 700 is directed by a NO arrow to 707 in **Fig. 7**.

Fig. 7 shows the access process 600 by which a biometric signal 102 (see **Fig. 2**) is processed in order to provide access to the controlled item 111, or to take other action. Entering the process at 707 from **Fig. 6**, the process 600 proceeds to a step 602 that compares the received biometric signature to signatures stored in the database 105. A following step 603 determines if the received signal falls into the "duress" category. Signatures in this category indicate that the user 101 is in a coercive situation where, for example, an armed criminal is forcing the user 101 to access the secure facility (such as a

bank door). If the step 603 determines that the signature is in the duress class, then a following step 604 prepares a "duress" bit for incorporation into the code access signal 108. The aforementioned duress bit is an access attribute of the biometric signal 102. Thereafter the process 600 proceeds to a step 605.

Modules used in the code entry module for producing the rolling code enable a number of user defined bits to be inserted into the access signal 108, and these bits can be used to effect desired control functions in the receiver sub-system 117. The disclosed system 100 utilises four such user bits, namely (a) to indicate that the user belongs to the duress category, (b) to indicate a "battery low" condition, or other desired system state or "telemetry" variable, for the code entry module 103, (c) to indicate that the biometric signal represents a legitimate user in which case the secure access to the controlled item 111 is to be granted, or (d) to indicate that the biometric signal is unknown, in which case the controller 109 in the receiver sub-system 117 sounds an alert tone using a bell (not shown) or the like.

Returning to **Fig. 7**, if the step 603 determines that the biometric signal is not in the duress class, then the process 600 proceeds according to a NO arrow to the step 605. The step 605 determines if the code entry module 103 has a low battery condition, in which event the process 600 proceeds according to a YES arrow to a step 606 that prepares a telemetry bit for insertion into the access signal 108. The aforementioned telemetry bit is an access attribute of the biometric signal 102. Thereafter, the process proceeds to a step 607.

If the step 605 determines that telemetry signalling is not required, then the process 600 proceeds according to a NO arrow to the step 607. The step 607 checks the biometric signal against the signatures in the database 105. If the received biometric signal matches a legitimate signature in the database 105, then the process is directed to a

step 608 that prepares an "access" bit for insertion into the access signal 108. This access bit directs the controller 109 in the receiver sub-system 117 to provide access to the controlled item 111. The aforementioned access bit is an access attribute of the biometric signal 102. The process 600 then proceeds to a step 610.

If the step 607 determines that the biometric input signal does not match any legitimate signatures in the database 105, then the process 600 proceeds according to a NO arrow to a step 609 that prepares an "alert" bit for insertion into the access signal 108. The aforementioned alert bit is an access attribute of the biometric signal 102. This alert bit directs the controller 109 (a) not to provide access to the controlled item 111, and (b) to provide an alert tone, like ringing a chime or a bell (not shown), to alert personnel in the vicinity of the receiver sub-system 117 that an unauthorised user is attempting to gain access to the controlled item 111. The alert bit can also cause a camera mounted near the controlled item 111 to photograph the unauthorised user for later identification of that person. The camera can be activated if the person attempting to gain access is unauthorised, and also if the person attempting to gain access is authorised but uses a duress signature.

An optional additional step (not shown) can prepare an identification field for insertion into the access signal 108. This sends, to the receiver sub-system 117, ID information that the receiver sub-system can use to construct an audit trail listing which users, having signatures in the database 105, have been provided with access to the controlled item 111.

The process 600 is then directed to the step 610 which inserts the various user defined bits into the access signal 108 and sends the signal 108 to the receiver sub-system 117. Thereafter, the process 600 is directed by an arrow 611 to 705 in **Fig. 6**.

Fig. 8 shows a process 800 for implementing various enrolment procedures. The process 800 commences at 706 from **Fig. 6** after which a step 801 determines if the biometric signal is a first administrators input (which is the case if the database 105 is empty). If this is the case, then the process 800 is directed to a step 802 that stores the administrator's signature in the database 105. From a terminology perspective, this first administrator, or rather the first administrator's first finger (in the event that the biometric sensor 121 in **Fig. 2** is a fingerprint sensor), is referred to as the "superfinger". Further administrator's fingers are referred to as admin-fingers, and ordinary users fingers are referred to merely as "fingers". The reason that someone would enrol more than one of their own fingers into the system is to ensure that even in the event that one of their enrolled fingers is injured, the person can still operate the system using another enrolled finger.

It is noted that the step 802, as well as the steps 805, 807 and 809 involve sequences of finger presses on the biometric sensor 121 in conjunction with feedback signals from the LEDs 122 and/or the audio speaker 124. The process 800 then proceeds to a step 810 that determines if further enrolment procedures are required. If this is the case, then the process 800 proceeds by a YES arrow back to the step 801. If no further enrolment procedures are required, then the process 800 proceeds by a NO arrow to 705 in **Fig. 6**.

Returning to the step 801, if the biometric signal is not a first administrator's signal, then the process 800 proceeds by a NO arrow to a step 803. The step 803 determines if a further administrator signature is to be stored. It is noted that all signatures stored in the database are tagged as belonging to one or more of the classes of administrator, ordinary user, and duress users. If a further administrator signature is to be

stored, then the process 800 proceeds by a YES arrow to the step 802 that stores the biometric signal as a further administrator's signature.

If a further administrator's signature is not required, then the process 800 proceeds according to a NO arrow to a step 804 that determines if a duress signature is to be stored. If this is the case then the process 800 follows a YES arrow to a step 805 that stores a duress signature. The process 800 then proceeds to the step 810. If however the step 804 determines that a duress signature is not required, then the process 800 proceeds by a NO arrow to s step 806.

The step 806 determines if a further simple signature (ie belonging to an ordinary user) is to be stored. If a further simple signature is to be stored, then the process 800 proceeds by a YES arrow to the step 807 that stores the biometric signal as a further ordinary signature.

If a further simple signature is not required, then the process 800 proceeds according to a NO arrow to a step 808 that determines if any or all signatures are to be erased from the database 105. If this is the case then the process 800 follows a YES arrow to a step 809 that erases the desired signatures. The process 800 then proceeds to the step 810. If however the step 804 determines that no signatures are to be erased, then the process 800 proceeds by a NO arrow to the step 810.

Fig. 9 shows another enrolment process relating to the example of **Fig. 6**. The process 900 commences at 706 from **Fig. 6** after which a step 901 determines if the received biometric signal comes from the first administrator. If this is the case, then the process 900 proceeds according to a YES arrow to a step 902. The step 902 emits an "Enrolment" tone and flashes the green LED once only. Thereafter, a step 905 reads the incoming biometric signal which is provided by the user as directed by the Amber LED. When the Amber LED flashes continuously, this directs the user to "Apply Finger".

When the Amber LED is in a steady illuminated state, this directs the user to "Maintain Finger Pressure". Finally, when the amber LED is off, this directs the user to "Remove Finger".

Returning to the step 901, if the incoming biometric signal does not belong to the first administrator, then the process 900 proceeds according to a NO arrow to a step 903. The step 903 emits an "Enrolment" tone, and flashes the Red LED in an on-going fashion. Thereafter, the process 900 proceeds according to an arrow 904 to the step 905.

Following the step 905, a step 906 determines whether the incoming biometric signal is legible. If this is not the case, then the process 900 proceeds according to a NO arrow to a step 907. The step 907 emits a "Rejection" tone, after which the process 900 is directed, according to an arrow 908 to 705 in **Fig. 6**. Returning to the step 906, if the incoming biometric signal is legible, then the process 900 follows a YES arrow to a step 909. The step 909 determines whether the finger press exceeds a predetermined time. If this is not the case, then the process 900 follows a NO arrow to a step 910 which stores the biometric signal, which in the present case is a fingerprint signature. Thereafter the process 900 follows an arrow 911 to 705 in **Fig. 6**.

Returning to the step 909 if the finger press does exceed the predetermined period, then the process follows a YES arrow to a step 912. The step 912 erases relevant signatures depending upon the attributes of the incoming biometric signal. Thus, for example, if the incoming biometric signal belongs to an ordinary user, then the ordinary user's signature in the database 105 is erased by the step 912. If, on the other hand, the incoming biometric signal belongs to the first administrator, then all the signatures in the database 105 are erased. Administrators who are not the first administrator can be granted either the same powers as the first administrator in regard to erasure of signatures, or can be granted the same powers as ordinary user in this respect.

Once the step 912 has completed erasure of the relevant signatures, then the process 900 follows an arrow 913 to 705 in **Fig. 6**.

Fig. 10 is a schematic block diagram of the system in **Fig. 2**. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in **Fig. 10** wherein the processes of **Figs. 3-4**, and **6-9** may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems 116 and 117 from the computer readable medium, and then executed under direction of the respective processor modules 107 and 109. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

The following description is directed primarily to the transmitter sub-system 116, however the description applies in general to the operation of the receiver sub-system 117. The computer system 100' is formed, having regard to the transmitter sub-system 116, by the controller module 107, input devices such as the bio sensor 121, output devices including the LED display 122 and the audio device 124. A communication

interface/transceiver 1008 is used by the controller module 107 for communicating to and from a communications network 1020. Although **Fig. 2** shows the transmitter sub-system 116 communicating with the receiver sub-system 117 using a direct wireless link for the access signal 108, this link used by the access signal 108 can be effected over the network 1020 forming a tandem link comprising 108-1020-108'. The aforementioned communications capability can be used to effect communications between the transmitter sub-system 116 and the receiver sub-system 117 either directly or via the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The controller module 107 typically includes at least one processor unit 1005, and a memory unit 1006, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module 107 also includes an number of input/output (I/O) interfaces including an audio-video interface 1007 that couples to the LED display 122 and audio speaker 124, an I/O interface 1013 for the bio-sensor 121, and the interface 1008 for communications. The components 1007, 1008, 1005, 1013 and 1006 the controller module 107 typically communicate via an interconnected bus 1004 and in a manner which results in a conventional mode of operation of the controller 107 known to those in the relevant art.

Typically, the application program modules for the transmitter sub-system 116 are resident in the memory 1006 iROM, and are read and controlled in their execution by the processor 1005. Intermediate storage of the program and any data fetched from the bio sensor 121 and the network 1020 may be accomplished using the RAM in the semiconductor memory 1006. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory 1006. Still further, the software modules can also be loaded into the transmitter sub-system 116 from other

computer readable media, say over the network 1020. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system 116 for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the transmitter sub-system 116. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

The system 100 can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

Claims

1. A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

2. A system according to claim 1, wherein the transmitter sub-system further comprises means for populating the database of biometric signatures.

3. A system according to claim 2, wherein the means for populating the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction.

4. A system according to claim 3 further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

5. A system according to claim 4, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

6. A system according to claim 5, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

7. A system according to claim 6, wherein the controlled item is one of:

a locking mechanism of a door; and

an electronic lock on a Personal Computer (PC).

8. A system according to claim 6, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

9. A system according to claim 6, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

10. A system according to claim 6, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

11. A transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item

dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

12. A transmitter sub-system according to claim 11, further comprising means for populating the database of biometric signatures.

13. A transmitter sub-system according to claim 12, wherein the means for populating the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction.

14. A transmitter sub-system according to claim 13 further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal; and

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database, said

identification field for use in constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

15. A transmitter sub-system according to claim 14, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

16. A transmitter sub-system according to claim 15, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

17. A transmitter sub-system according to claim 16, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class.

18. A transmitter sub-system according to claim 16, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

19. A transmitter sub-system according to claim 16, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

20. A receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; wherein the receiver sub-system comprises;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

21. A receiver sub-system according to claim 20, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class.

22. A receiver sub-system according to claim 21, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

23. A receiver sub-system according to claim 22, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

24. A receive sub-system according to claim 23, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

25. A receiver sub-system according to claim 23, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

26. A method for providing secure access to a controlled item, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

providing conditional access to the controlled item dependent upon said information.

27. A method according to claim 26, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

28. A method according to claim 27, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures, and wherein the step of providing said conditional access comprises the steps of:

providing access to the controlled item if the accessibility attribute comprises an access attribute;

providing access to the controlled item and sounding an alert if the accessibility attribute comprises a duress attribute; and

denying access to the controlled item and sounding an alert if the accessibility attribute comprises an alert attribute.

29. A method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction.

30. A method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving the secure access signal transmitted by a transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, said method comprising the steps of:

receiving a biometric sensor by biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

31. A method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, said method comprising the steps of:

receiving the transmitted secure access signal; and

providing conditional access to the controlled item dependent upon said information.

32. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

code for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

code for providing conditional access to the controlled item dependent upon said information.

33. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to populate a database of biometric signatures in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a series of entries of the biometric signal;

code for determining at least one of the number of said entries and a duration of each said entry;

code for mapping said series into an instruction; and

code for populating the database according to the instruction.

34. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a biometric sensor by biometric signal;

code for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

code for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

35. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to receive a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving the transmitted secure access signal; and

code for providing conditional access to the controlled item dependent upon said information.

36. A system for providing secure access, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

a control panel for receiving the information and for providing the secure access requested.

37. A system according to claim 36 wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information.

38. A system according to claim 36, wherein the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database.

39. A system according to claim 38, wherein the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

40. A system according to claim 36, wherein the secure wireless signal comprises an RF carrier and a rolling code.

41. A system according to claim 37, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter converts the rolling code to the Wiegand protocol.

AMENDED CLAIMS

[received by the International Bureau on 13 December 2004 (13.12.04);
Claims 1, 11, 20, 26 and 29-36 amended; claims 42-44 added;
(14 pages)]

1. A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

2. A system according to claim 1, wherein the transmitter sub-system further comprises means for populating the database of biometric signatures.

3. A system according to claim 2, wherein the means for populating the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

WAVELYNX EX. 1003, Pg. 430
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

means for mapping said series into an instruction; and

means for populating the database according to the instruction.

4. A system according to claim 3 further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

5. A system according to claim 4, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

6. A system according to claim 5, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

7. A system according to claim 6, wherein the controlled item is one of:

a locking mechanism of a door; and

WAVELYNX EX. 1003, Pg. 431
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

an electronic lock on a Personal Computer (PC).

8. A system according to claim 6, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

9. A system according to claim 6, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

10. A system according to claim 6, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

11. A transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises:

a biometric sensor for receiving a biometric signal;

WAVELYNX EX. 1003, Pg. 432
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item; and

means for emitting the secure access signal conveying said information dependent upon said accessibility attribute.

12. A transmitter sub-system according to claim 11, further comprising means for populating the database of biometric signatures.

13. A transmitter sub-system according to claim 12, wherein the means for populating the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction.

14. A transmitter sub-system according to claim 13 further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal; and

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database, said identification field for use in constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

WAVELYNX EX. 1003, Pg. 433
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

15. A transmitter sub-system according to claim 14, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

16. A transmitter sub-system according to claim 15, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

17. A transmitter sub-system according to claim 16, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class.

18. A transmitter sub-system according to claim 16, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

19. A transmitter sub-system according to claim 16, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

WAVELYNX EX. 1003, Pg. 434
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

20. A receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute; wherein the receiver sub-system comprises;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

21. A receiver sub-system according to claim 20, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class.

22. A receiver sub-system according to claim 21, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

WAVELYNX EX. 1003, Pg. 435
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

23. A receiver sub-system according to claim 22, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

24. A receive sub-system according to claim 23, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

25. A receiver sub-system according to claim 23, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

26. A method for providing secure access to a controlled item, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item;

WAVELYNX EX. 1003, Pg. 436
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information.

27. A method according to claim 26, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

28. A method according to claim 27, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures, and wherein the step of providing said conditional access comprises the steps of:

providing access to the controlled item if the accessibility attribute comprises an access attribute;

providing access to the controlled item and sounding an alert if the accessibility attribute comprises a duress attribute; and

denying access to the controlled item and sounding an alert if the accessibility attribute comprises an alert attribute.

WAVELYNX EX. 1003, Pg. 437
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

29. A method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction.

30. A method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving the secure access signal transmitted by a transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, said method comprising the steps of:

receiving a biometric sensor by biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item; and

WAVELYNX EX. 1003, Pg. 438
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

emitting the secure access signal conveying said information dependent upon said accessibility attribute.

31. A method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, said method comprising the steps of:

receiving the transmitted secure access signal; and

providing conditional access to the controlled item dependent upon said information.

32. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item;

code for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

WAVELYNX EX. 1003, Pg. 439
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

code for providing conditional access to the controlled item dependent upon said information.

33. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to execute a method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said program comprising:

code for receiving a series of entries of the biometric signal;

code for determining at least one of the number of said entries and a duration of each said entry;

code for mapping said series into an instruction; and

code for populating the database according to the instruction.

34. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a biometric sensor by biometric signal;

WAVELYNX EX. 1003, Pg. 440
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

code for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item; and

code for emitting the secure access signal conveying said information dependent upon said accessibility attribute.

35. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to receive a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute capable of granting more than two types of access to the controlled item, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, said computer program product comprising:

code for receiving the transmitted secure access signal; and

code for providing conditional access to the controlled item dependent upon said information.

36. A system for providing secure access to a controlled item, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

WAVELYNX EX. 1003, Pg. 441
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

a control panel for receiving the information and for providing the secure access requested.

37. A system according to claim 36 wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information.

38. A system according to claim 36, wherein the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database.

39. A system according to claim 38, wherein the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

40. A system according to claim 36, wherein the secure wireless signal comprises an RF carrier and a rolling code.

41. A system according to claim 37, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter converts the rolling code to the Wiegand protocol.

42. A method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a

WAVELYNX EX. 1003, Pg. 442
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

receiving a biometric signal; and

enrolling the biometric as an administrator if the database of biometric signatures is empty.

43. A method according to claim 42 wherein the enrolling step comprises receiving another biometric signal to confirm the enrolling of the biometric as an administrator.

44. A method according to claim 43 wherein the enrolling step is performed dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

WAVELYNX EX. 1003, Pg. 443
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

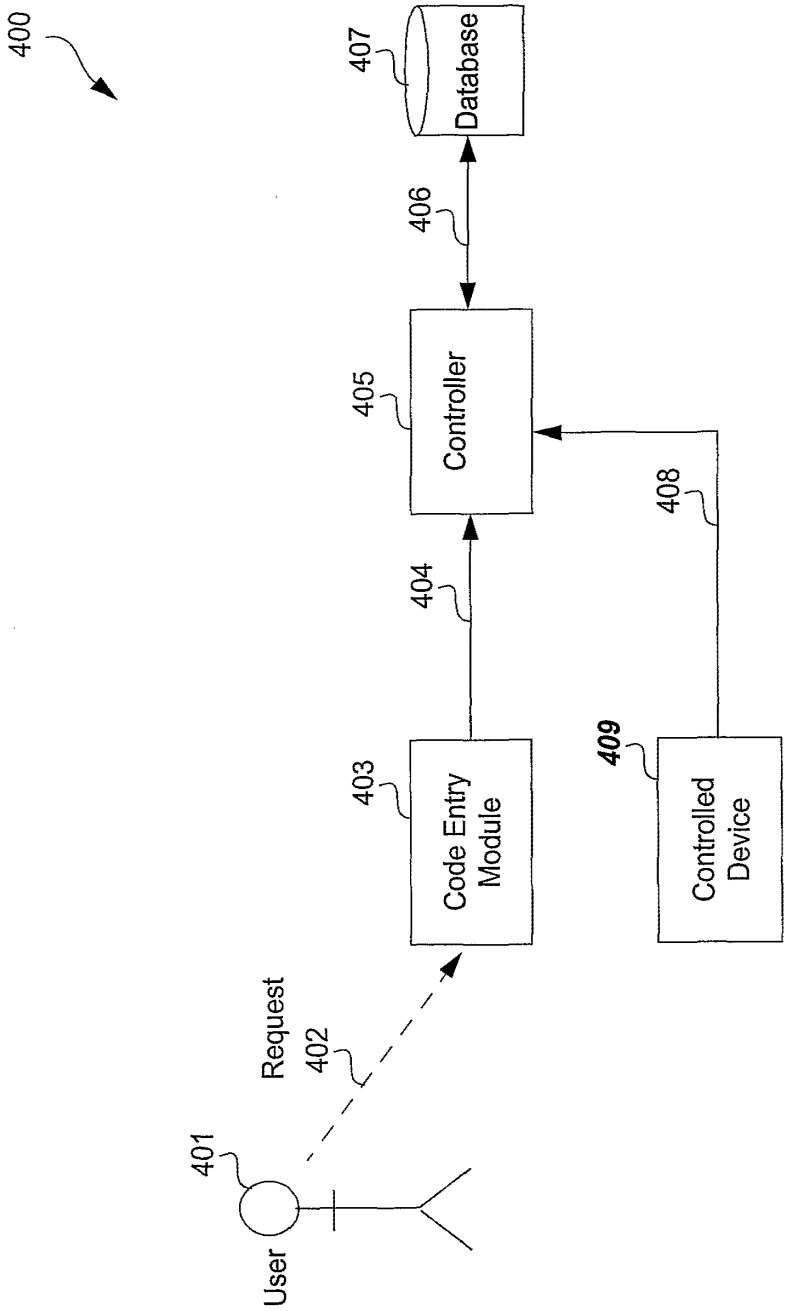


Fig. 1
(prior art)

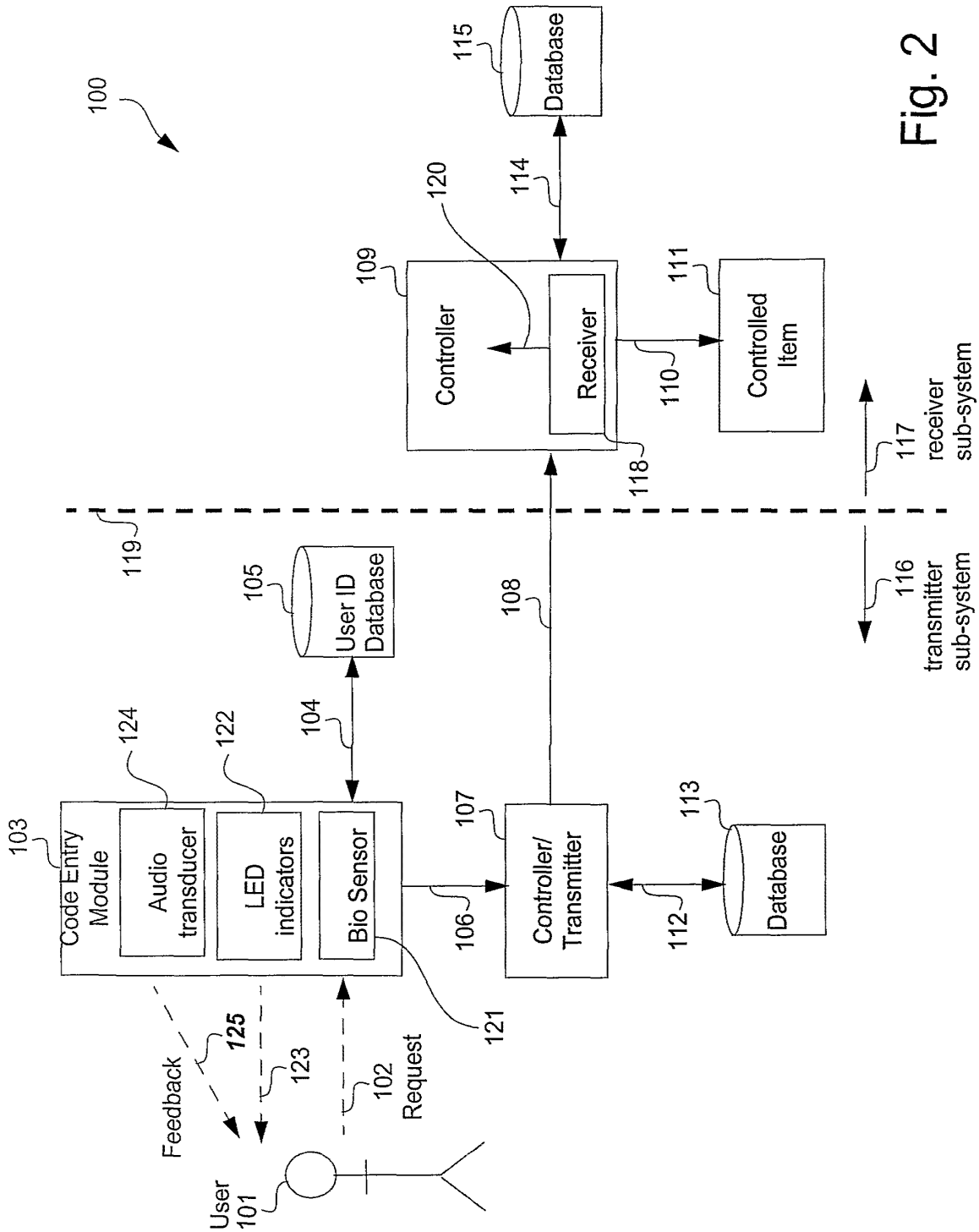

100
115
Database
114
120
109
Controller
Receiver
111
Controlled Item
110
118
117
receiver sub-system
119
116
transmitter sub-system
105
User ID Database
108
104
124
122
103
Code Entry Module
Audio transducer
LED indicators
Bio Sensor
107
Controller/ Transmitter
113
Database
106
112
121
Feedback
125
123
102
Request
User
101

Fig. 2

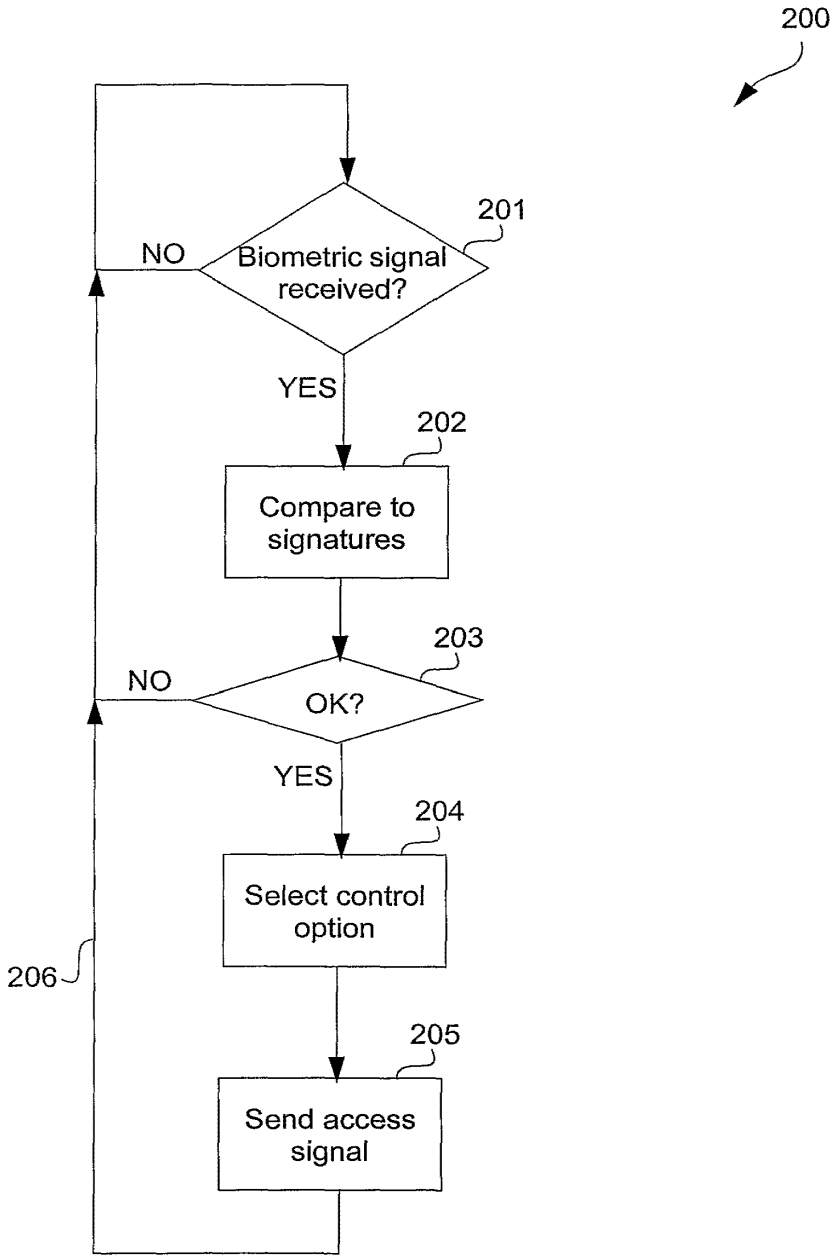

200
201
Biometric signal received?
NO
YES
202
Compare to signatures
203
OK?
NO
YES
204
Select control option
205
Send access signal
206

Fig. 3

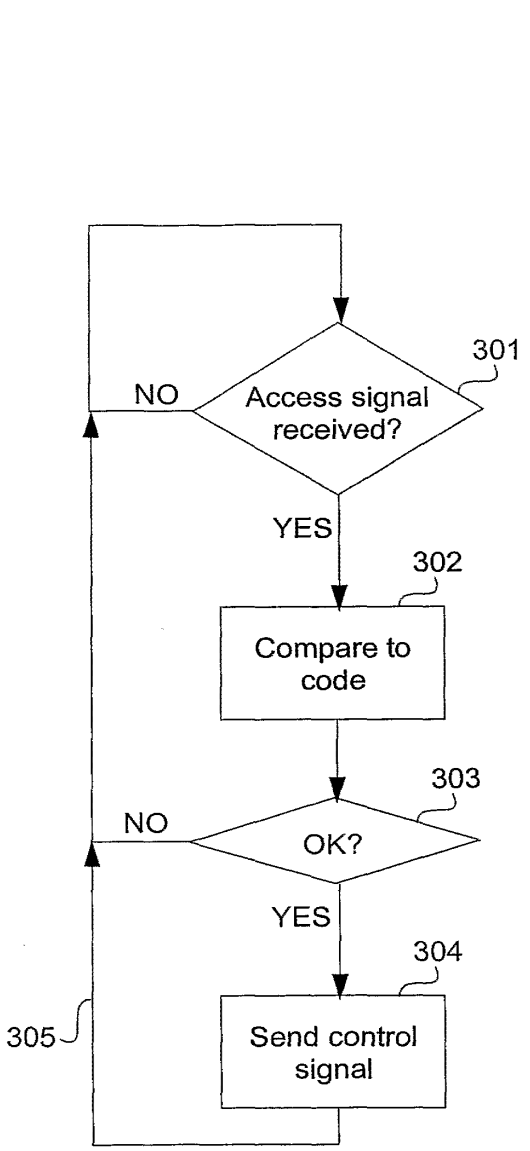
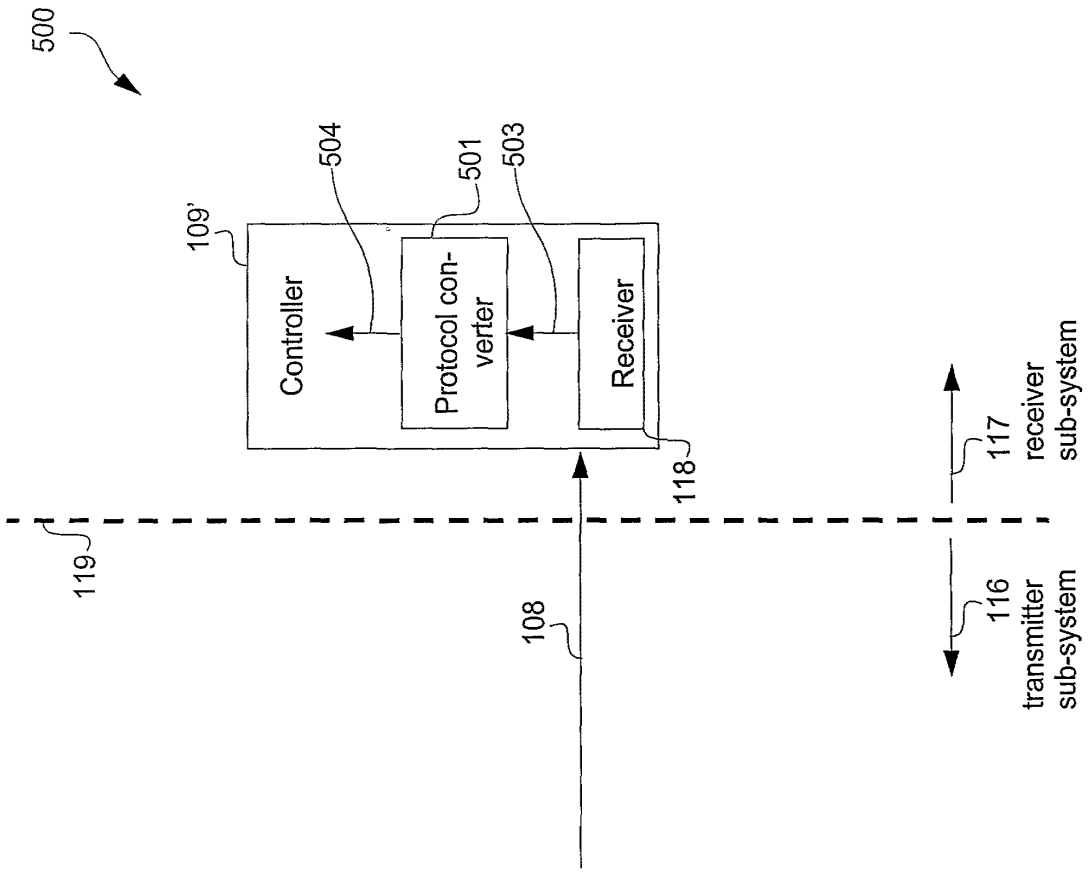

300
301
Access signal received?
NO
YES
302
Compare to code
303
OK?
NO
YES
304
Send control signal
305

Fig. 4

Fig. 5


500
109'
504
501
503
Controller
Protocol con-
verter
Receiver
118
119
108
117
receiver
sub-system
116
transmitter
sub-system

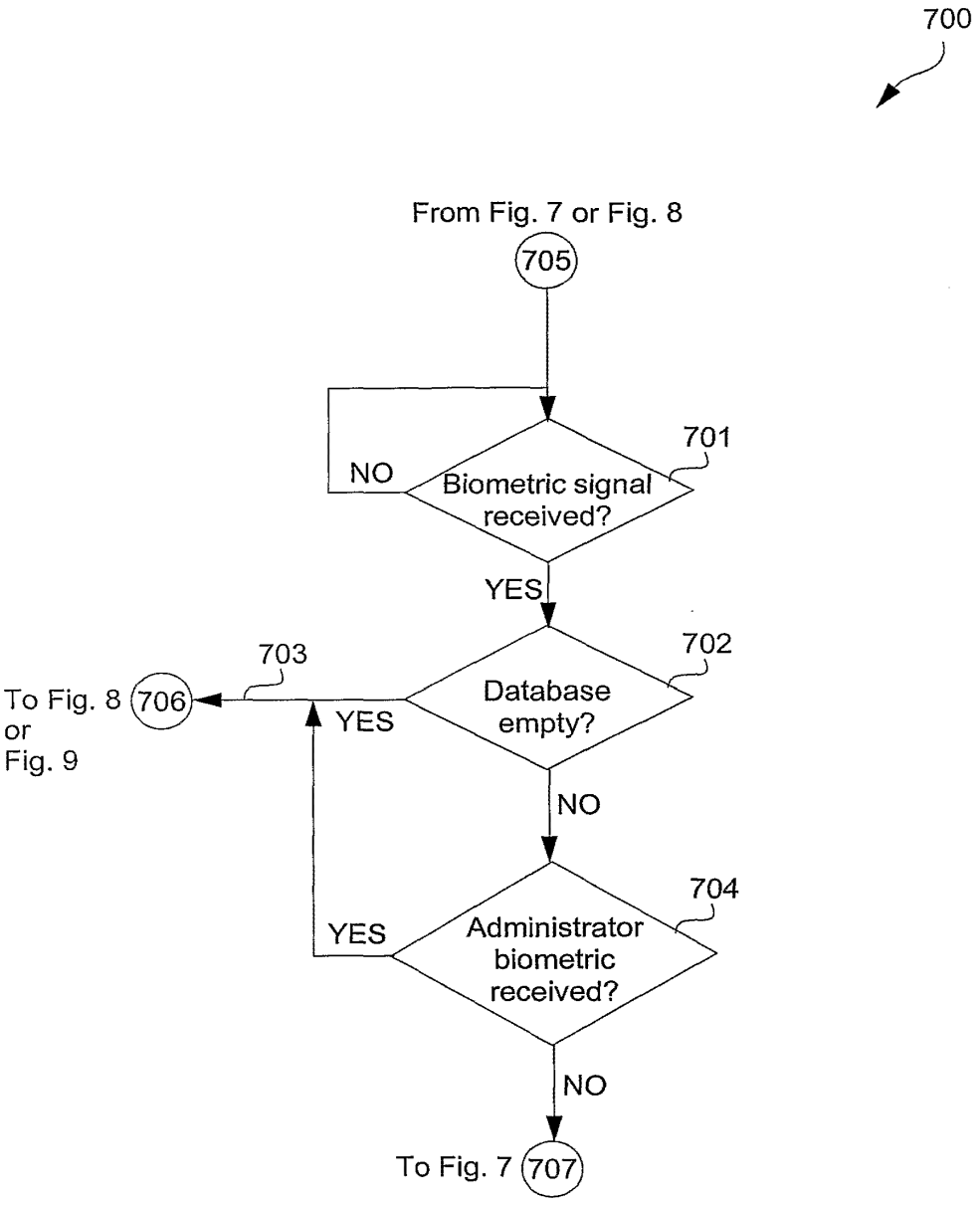

700
From Fig. 7 or Fig. 8
705
701
NO
Biometric signal received?
YES
703
702
To Fig. 8 or Fig. 9
706
YES
Database empty?
NO
704
YES
Administrator biometric received?
NO
To Fig. 7
707

Fig. 6

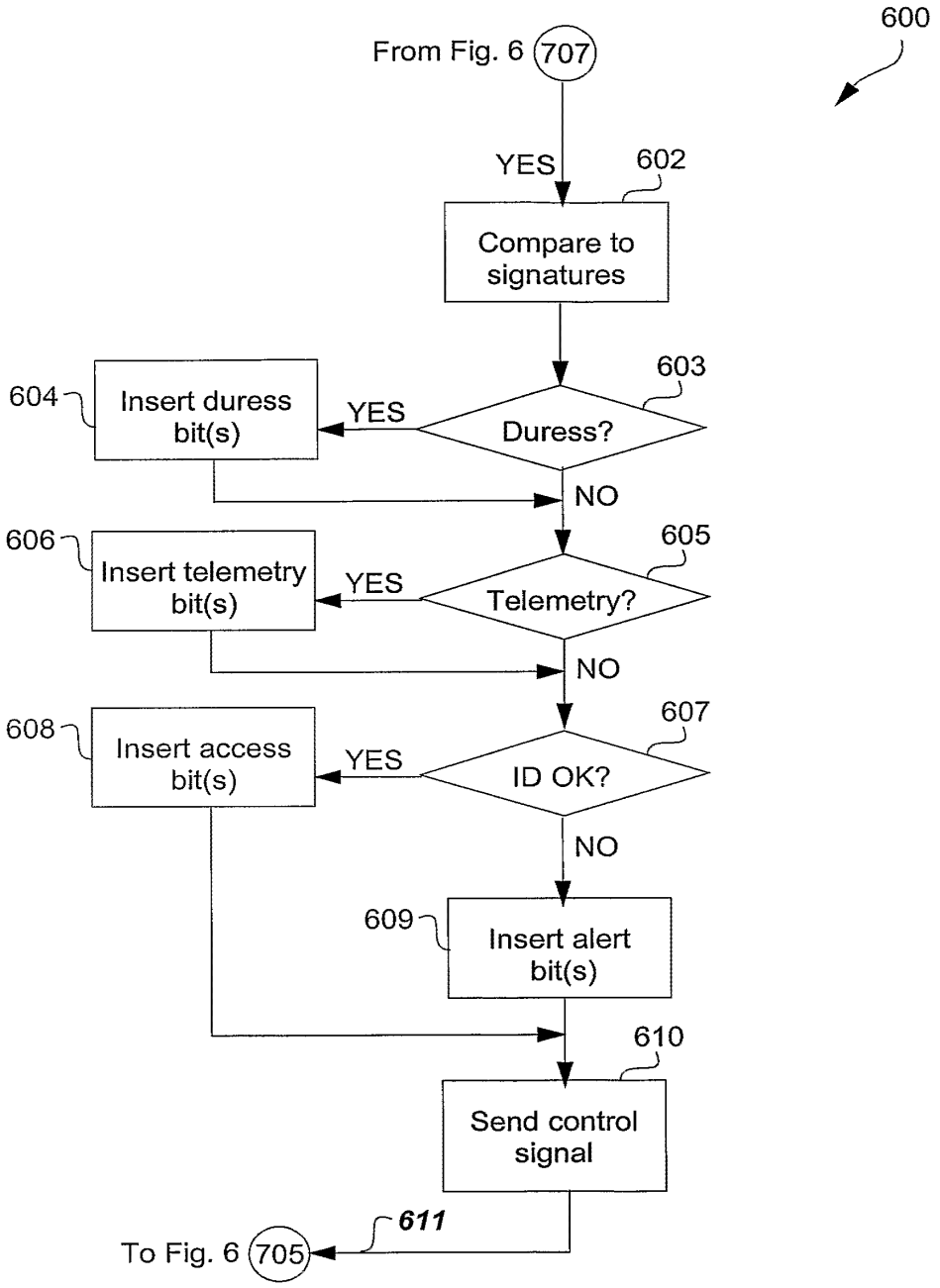

600
From Fig. 6
707
YES
602
Compare to signatures
603
604
Insert duress bit(s)
YES
Duress?
NO
606
Insert telemetry bit(s)
YES
605
Telemetry?
NO
608
Insert access bit(s)
YES
607
ID OK?
NO
609
Insert alert bit(s)
610
Send control signal
611
To Fig. 6
705

Fig. 7

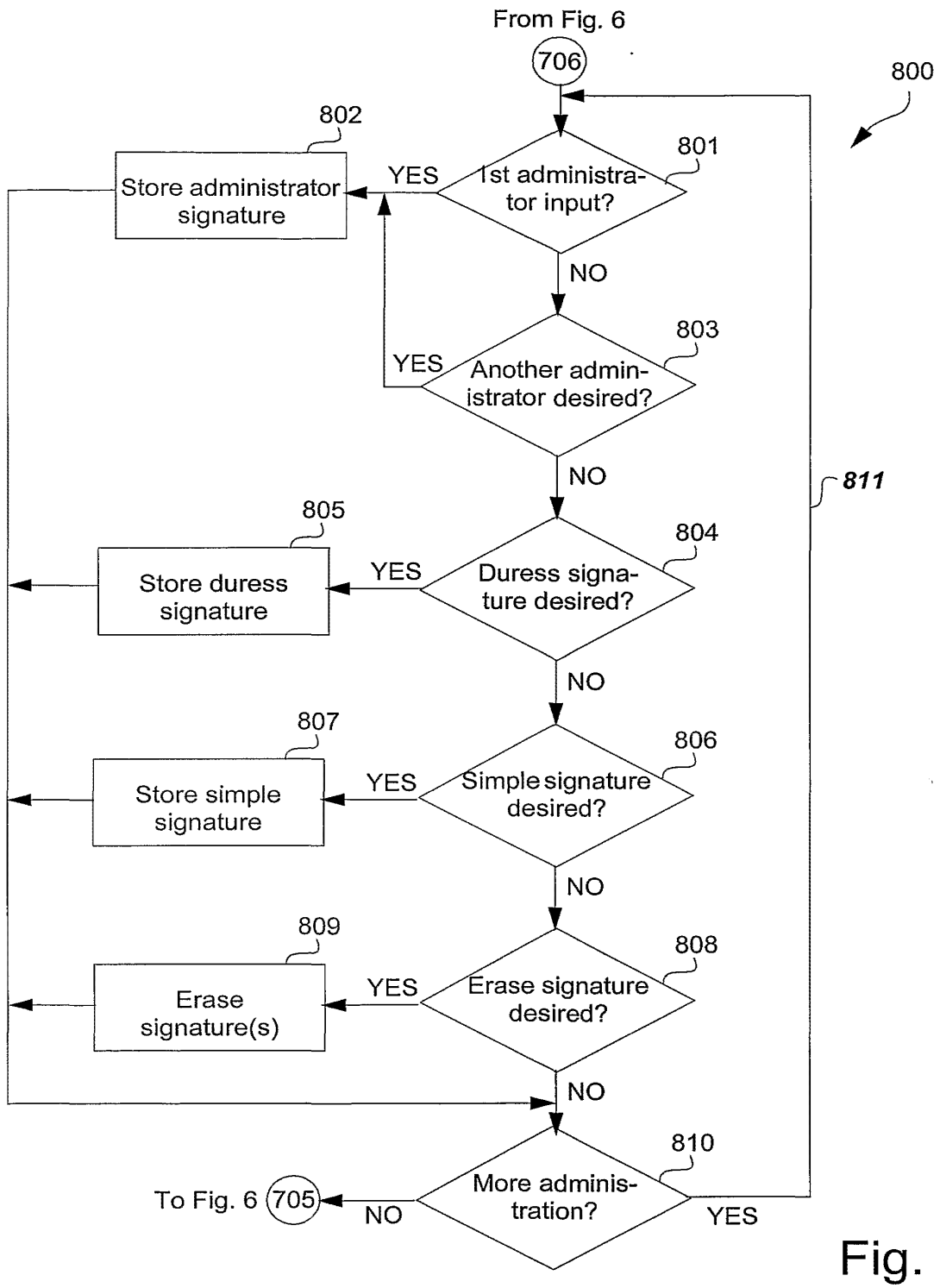

From Fig. 6
706
800
802
801
Store administrator signature
YES
1st administrator input?
NO
803
YES
Another administrator desired?
NO
811
805
804
Store duress signature
YES
Duress signature desired?
NO
807
806
Store simple signature
YES
Simple signature desired?
NO
809
808
Erase signature(s)
YES
Erase signature desired?
NO
810
To Fig. 6
705
NO
More administration?
YES

Fig. 8

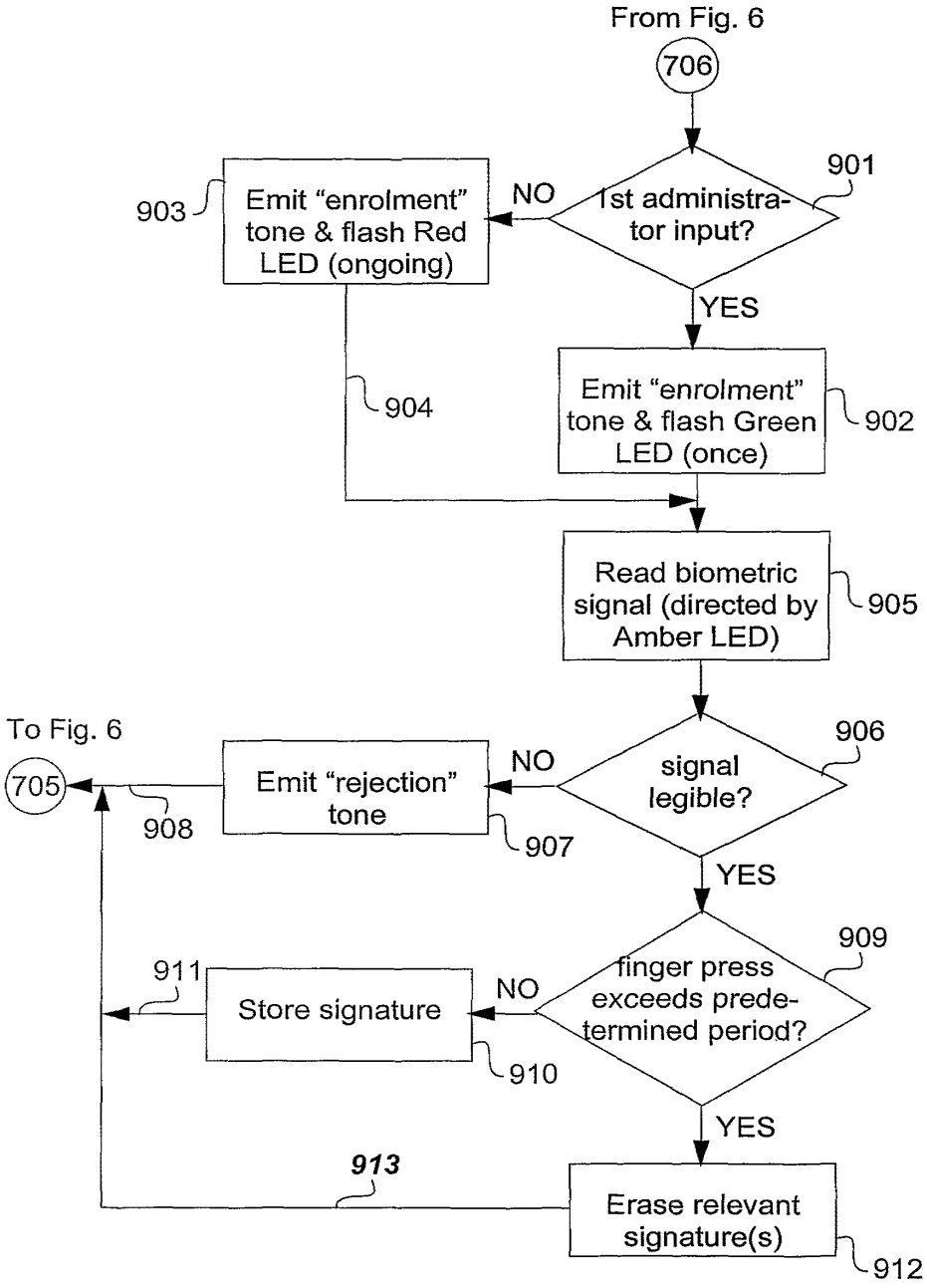

From Fig. 6
706
900
901
1st administrator input?
NO
903
Emit "enrolment" tone & flash Red LED (ongoing)
YES
904
Emit "enrolment" tone & flash Green LED (once)
902
Read biometric signal (directed by Amber LED)
905
To Fig. 6
705
906
signal legible?
NO
Emit "rejection" tone
908
907
YES
909
finger press exceeds predetermined period?
911
NO
Store signature
910
YES
913
Erase relevant signature(s)
912

Fig. 9

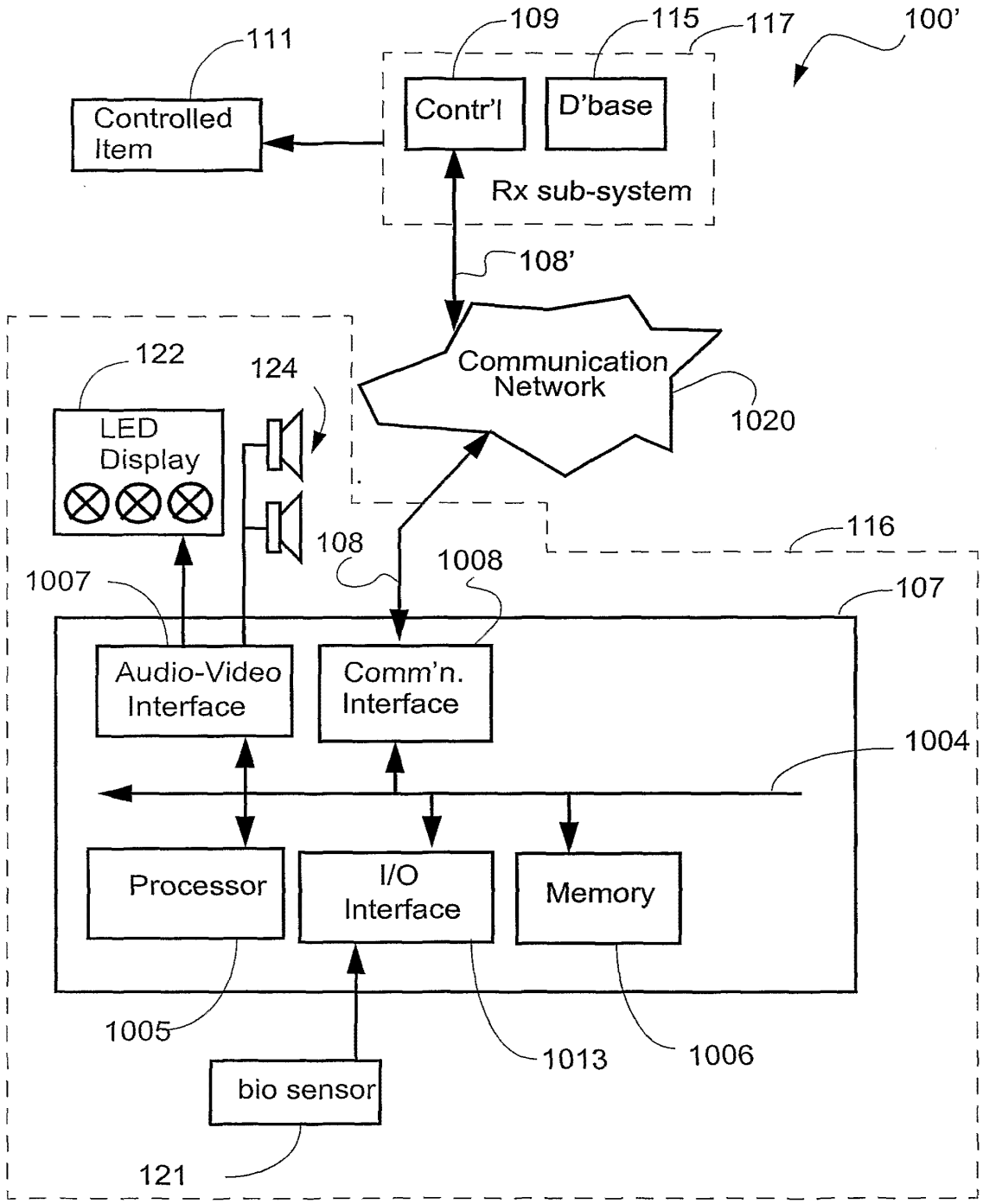

111
109
115
117
100'
Controlled Item
Contr'l
D'base
Rx sub-system
108'
Communication Network
1020
122
124
LED Display
108
116
1008
1007
107
Audio-Video Interface
Comm'n. Interface
1004
Processor
I/O Interface
Memory
1005
1013
1006
bio sensor
121

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2004/001083

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: H04L 9/32, G06K 9/00

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)

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)
WPAT, USPTO: BIOMETRIC, SECURE, ACCESS, DATABASE, MATCH, TRANSMIT AND SIMILAR TERMS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/0051173 A1 (KRUEGER) 13 March 2003 Whole document	1-41
X	WO 2001/071462 A2 (WIDCOMM, INC.) 27 September 2001 Whole document	1-41
X	US 6219439 B1 (BURGER) 17 April 2001 Whole document	35
A		1-34, 36-41

☐ 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
3 September 2004	17 SEP 2004
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **SUSHIL AGGARWAL** Telephone No : (02) 6283 2192

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2004/001083

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:
As reasoned on the 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 an additional fee, this Authority did not invite payment of any additional fee.
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.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

WAVELYNX EX. 1003, Pg. 455
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Supplemental Box
(To be used when the space in any of Boxes I to VIII is not sufficient)

Continuation of Box No: III

The international application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked to form a single general inventive concept. In coming to this conclusion, the International Searching Authority has found that there are different inventions as follows:

1. Claims 1-32, and 34 relate to providing secure access to a controlled item wherein a transmitter subsystem receives a biometric signal from a biometric sensor, matches it against members of a database of biometric signatures and emits a secures access signal comprising at least one of a rolling code, an encrypted Bluetooth protocol, and a WiFi protocol, which is received by a receiver subsystem to provide conditional access to the controlled item.
2. Claim 33 relates to a computer program product having a code for populating a database of biometric signatures.
3. Claim 35 relates to a computer program product having a code for receiving a transmitted secure access signal and providing conditional access to a controlled item dependent upon said signal.
4. Claims 36-41 relate to providing secure access wherein a transmitter transmits information using a secure wireless signal dependent upon a request from a user and the authentication of the user identity by a biometric sensor and a control panel for receiving the information and for providing the secure access.

The above groups of inventions are not so linked as to form a single general inventive concept, that is, a 'technical relationship' between the inventions, as defined in PCT Rule 13.2 does not exist. Hence, the application does not relate to one invention or to a single inventive concept.

WAVELYNX EX. 1003, Pg. 456
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2004/001083

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	20030051173	NONE					
WO	2001/071462	CA	2369675	CA	2369676	EP	1196896
		WO	0171671				
US	6219439	NONE					

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

WAVELYNX EX. 1003, Pg. 457
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 March 2005 (31.03.2005)

PCT

(10) International Publication Number
WO 2005/029315 A1

(51) International Patent Classification[7]: G06F 7/58

(21) International Application Number:
PCT/US2003/021422

(22) International Filing Date: 9 July 2003 (09.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **GLOBESPANVIRATA INCORPORATED** [US/US]; 100 Schultz Drive, Red Bank, NJ 07701 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NOWSHADI, Farshid** [GB/GB]; 45 Montrose Avenue, Luton, Beds (GB). **MOORE, Mark** [GB/GB]; 7 George Street, Cambridge, (GB).

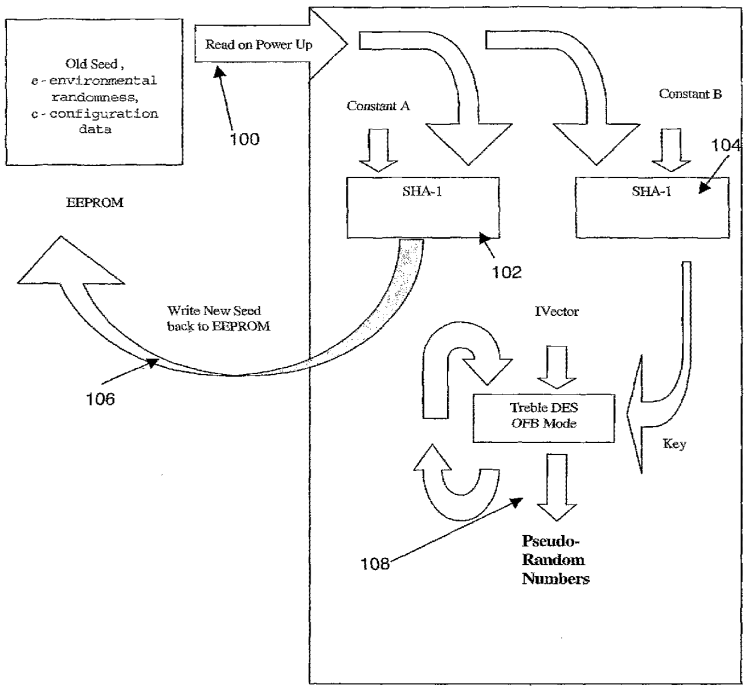
(74) Agents: **DUNCAN, Kevin, T.** et al.; Intellectual Property Dept., Hunton & Williams_LLP, 1900 K Street, N.W. Suite 200, Washington, DC 20006-1109 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR GENERATING PSEUDO-RANDOM NUMBERS



(57) Abstract: A method and system is provided for generating pseudo-random numbers utilizing techniques of both the SHA-1 and DES encryption standards, wherein a pseudo-random number generator is re-keyed periodically using an external input of physical randomness. In accordance with one embodiment of the present invention, a current seed value S_j is loaded from a non-volatile storage. Next, values E, representative of environmental randomness, and Cm representative of configuration data are likewise loaded. A new seed value S_{j+1}, is generated in accordance with the equation $S_{j+1}=f(S_j; A;C;E)$, wherein f represents a selected encryption algorithm, and B is a second constant, and wherein S_j is concatenated with A, which is concatenated with S which is concatenated with E. The new seed is then written to the non-volatile storage. Next, a key, K, is generated in accordance with the equation $K=f(S_j; B; C; E)$, wherein B is a second constant. Lastly, a pseudo-random number putout, P_n, is generated in accordance with equation $P_n=f_{3DES}(K, P_{n-1})$ where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

WO 2005/029315 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR GENERATING PSEUDO-RANDOM NUMBERS

Cross-Reference to Related Applications

The present applications claims priority to co-pending United States Provisional Patent Application No. 60/393,733 entitled "System and Method for Generating Pseudo-Random Numbers, filed on July 8, 2003, the entirety of which is incorporated by reference herein.

Background of the Invention

The present invention relates generally to the field of computer systems and, more particularly, to systems and methods for generating random or pseudo-random numbers within such systems, for the purpose of maintaining system security.

Many chips have the means to generate random numbers. These may be true random number generators, in which the randomness comes from some physical source such as shot noise or oscillator drift; or pseudorandom number generators, in which a key is used to generate a long sequence of bits that are hard to predict if the key is not known. Each has its advantages.

True random number generators produce outputs that are statistically independent of each other. Thus the compromise of some set of outputs, or of the state of the device at some given time, does not impair the security of random numbers generated in either the past or the future. On the other hand, true random number generators are tricky to design (many designs being dependent on the precise fabrication process); they are hard to test; they may be vulnerable to an opponent who can manipulate chip inputs (such as Vcc); and the rate at which random numbers are generated is usually fairly low.

Pseudorandom number generators can provide deterministic output at high rates; they can use thoroughly studied and well-understood building blocks; and can be made just as testable and resilient as the rest of the device. However their unpredictability depends on some cryptographic key remaining unknown to an opponent. While appropriate use of a one-way cryptographic function can prevent a key compromise being used to deduce previous inputs, there is no obvious way to recover security following a compromise. Unfortunately, known methods for generating such pseudo-random numbers such as encryption using the SHA-1 or DES algorithms do not afford the level of protection required to ensure that the cryptographic key remains secure.

Accordingly, there is a need in the art of computer systems for a system and method for generating pseudo-random numbers which overcome the security limitations of known systems.

Summary of the Invention

The present invention overcomes the problems noted above, and realizes additional advantages, by providing for methods and systems for generating pseudo-random numbers utilizing techniques of both the SHA-1 and DES encryption standards.

In accordance with one embodiment of the present invention a current seed value S_j is loaded from a non-volatile storage. Next, values E, representative of environmental randomness, and C, representative of configuration data are likewise loaded. A new seed value, S_{j+1}, is generated in accordance with the equation $S_{j+1} = f(S_j; A; C; E)$, wherein f represents a selected encryption algorithm , and B is a second constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E. The

WAVELYNX EX. 1003, Pg. 461
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

new seed is then written to the non-volatile storage. Next, a key, K, is generated in accordance with the equation $K = f(S_j; B; C; E)$, wherein B is a second constant. A pseudo-random number output, P_n, is then generated in accordance with the equation $P_n = f_{3DES}(K, P_{n-1})$, where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

Brief Description Of The Drawings

The present invention can be understood more completely by reading the following Detailed Description of the Preferred Embodiments, in conjunction with the accompanying drawings.

FIG. 1 is a simplified flow diagram illustrating one embodiment of a method for generating pseudo-random numbers in accordance with the present invention.

Detailed Description of the Invention

Referring now to the Figures and, in particular, to FIG. 1, there is shown a simplified flow diagram illustrating one embodiment of a method and system for generating pseudo-random numbers in accordance with the present invention. In particular, the present invention utilizes key features of both of the above-identified methodologies. This combination of the two approaches results in a pseudo-random number generator that is re-keyed periodically using an external input of physical randomness.

The pseudo-random number output will be computed in step 108 using the 3DES (triple DES) encryption hardware, operated in output feedback mode. Writing $f_{3DES}(K, P)$ for the encryption of P using the key K, we have

WAVELYNX EX. 1003, Pg. 462
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$P_n = f_{3DES}(K, P_{n-1})$$

Where, the initial value P_0 can be set to any fixed value such as 0. This will provide a source of pseudorandom numbers with a rate of about 15 Mbit/sec. The key K will be derived from a seed S kept externally in non-volatile memory. Initially, on power-up, the device loads the current value S_j of the seed, plus configuration data C and environmental randomness E in step 100. The device will compute the key K in step 102 and the next value S_{j+1} of the seed in step 104 as follows, using, in one embodiment, the FIPS 180 secure hash standard algorithm (SHA). The seed S_j will preferably be 160 bits in length if the current secure hash standard algorithm SHA-1 is used, and 256 bits if the proposed new standard SHA-256 algorithm is used:

$$S_{j+1} = f_{SHA}(S_j; A; C; E)$$

$$K = f_{SHA}(S_j; B; C; E)$$

Here A and B are two different fixed constants whose value is not otherwise critical (for example, A = 1 and B = 2). Furthermore, the phrase (X; Y) denotes X concatenated with Y. The configuration data C may be any length, and the environmental randomness E should have at least 80 bits of entropy.

Following this updating computation, the new seed value S_j is written back to non-volatile storage in step 106. The function of the environmental randomness E (which may be derived from whatever sources are available) is security recovery. If, at some time, the seed is compromised by an adversary who manages to read the off-chip non-volatile storage, the use of fresh randomness should deny him knowledge of subsequent seeds and the pseudorandom numbers derived from them.

WAVELYNX EX. 1003, Pg. 463
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

In an additional embodiment, if it is desired to make it harder for a competitor to produce a compatible chip, then one or more of the components of the updating computation may be protected. A simple way to do this is to make A and B into secrets that are read from a ROM address that is not externally readable. A more thorough way to obscure the computation is to replace SHA with an algorithm that is proprietary. In the former case, A and B may be compromised by an opponent who mounts an invasive attack (such as microprobing the bus, or using a scanning capacitance microscope to read out the ROM). In the latter case, an opponent who performs this reverse engineering is further hindered by proprietary algorithm. If the threat of litigation is reckoned to be enough in itself, then, the constants A and B might contain as substrings the customer's copyright notice.

Further, if it is desired that a key compromised occurring during a session should not expose keys used earlier in that session, then the second equation of the key updating computation may be carried out more frequently than once per power cycle. In the limit, all the random numbers could be computed using SHA as successive values of the key K. In this case, as no use would be made of the 3DES hardware provided, there would be a noticeable performance penalty. Whether this mattered would depend on the application.

If it becomes a requirement at some future time to have a true random source on-chip, then this can be input to an on-the-fly update. Some care is needed though to ensure that enough random bits are input to each update that an opponent cannot work forwards by exhaustive search.

WAVELYNX EX. 1003, Pg. 464
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

It should be understood that the 160-bit SHA-1 algorithm is in the process of being supplemented by the 256-bit SHA-256 and the 512-bit SHA-512 algorithms. Similarly, the existing standard DES modes of operation are in the process of being supplemented by the new dual counter mode. The practical consequences of these upgrades for technical security are few, but it may be decided to support them anyway in case they become a checkbox item for customers. For example, it might be objected that the output of SHA is only 160 bits, while 3DES uses a 168-bit key. In practice, the remaining eight key bits may be set to an arbitrary or zero value; but the objection is removed by the use of SHA-256 from whose output 168 distinct key bits may be drawn. Similarly, it may be objected that 3DES in output feedback mode will cycle after about 2^{32} pseudorandom values have been drawn; this is unlikely to be an issue in the envisaged applications, but the objection is removed by the use of the new dual-counter mode of operation, for which a further 64 bits of key is required to initialize the counters. In that case, one should use SHA-256 to provide the 232 bits required in total.

The pseudo-random number generation system of the present invention makes a number of assumptions about the physical protection of the equipment being protected. In particular, the present invention assumes that the protected device contains no on-chip non-volatile memory, thus requiring that any encryption key material must be stored off-chip. It follows that potential adversaries must not have unsupervised access to the equipment. In particular, the off-chip non-volatile memory is to be kept secure & inaccessible by unauthorised personnel. Further, it is assumed that the attacker does not

WAVELYNX EX. 1003, Pg. 465
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

have unsupervised access to the electrical interface of the device or of associated chips, with which timing attacks might be possible.

While the foregoing description includes many details and specifities, it is to be understood that these have been included for the purposes of explanation only, and are not to be interpreted as limitations of the present invention. Many modifications to the embodiments described above can be made without departing from the spirit and scope of the invention, as is intended.

WAVELYNX EX. 1003, Pg. 466
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

WHAT IS CLAIMED IS:

1. A method for generating pseudo-random numbers, comprising the steps of:

loading a current seed value S_j from a non-volatile storage;

loading a value, E, representative of environmental randomness;

loading a value, C, representative of configuration data;

generating a new seed value, S_{j+1}, in accordance with the following equation:

$$S_{j+1} = f(S_j; A; C; E),$$

wherein f represents a selected encryption algorithm , and B is a second constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E;

writing the new seed value S_{j+1} to the non-volatile storage;

generating a key, K, in accordance with the following equation:

$$K = f(S_j; B; C; E),$$

wherein B is a second constant; and

generating a pseudo-random number output, P_n, in accordance with the following equation:

$$P_n = f_{3DES}(K, P_{n-1}),$$

where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

2. The method of claim 1, wherein the function f comprises the FIPS 180 secure hash standard algorithm (SHA).

3. The method of claim 1, wherein the value E includes at least 80 bits of entropy.

WAVELYNX EX. 1003, Pg. 467
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

4. The method of claim 1, wherein the seed S_j is 160 bits in length.

5. The method of claim 1, wherein the seed S_j is 256 bits in length.

6. The method of claim 1, wherein the seed S_j is 512 bits in length.

7. The method of claim 1, wherein an initial value of P_0 is 0.

8. The method of claim 1, further comprising the steps of loading values for the first and second constants A and B from a protected ROM address.

9. The method of claim 8, wherein the first and second constants A and B further incorporate a copyright notice embedded therein.

10. The method of claim 1, wherein the f_{3DES} hardware is operated in output feedback mode.

11. The method of claim 1, wherein the f_{3DES} hardware is operated in dual counter mode.

12. A computer-readable medium incorporating one or more instructions for generating pseudo-random numbers, the instructions comprising:

one or more instructions for loading a current seed value S_j from a non-volatile storage;

one or more instructions for loading a value, E, representative of environmental randomness;

one or more instructions for loading a value, C, representative of configuration data;

one or more instructions for generating a new seed value, S_{j+1}, in accordance with the following equation:

WAVELYNX EX. 1003, Pg. 468
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$S_{j+1} = f(S_j; A; C; E),$$

wherein f represents a selected encryption algorithm , and B is a second constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E;

one or more instructions for writing the new seed value S_{j+1} to the non-volatile storage;

one or more instructions for generating a key, K, in accordance with the following equation:

$$K = f(S_j; B; C; E),$$

wherein B is a second constant; and

one or more instructions for generating a pseudo-random number output, P_n, in accordance with the following equation:

$$P_n = f_{3DES}(K, P_{n-1}),$$

wherein f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

13. The computer-readable medium of claim 12, wherein the function f comprises the FIPS 180 secure hash standard algorithm (SHA).

14. The computer-readable medium of claim 12, wherein the value E includes at least 80 bits of entropy.

15. The computer-readable medium of claim 12, wherein the seed S_j is 160 bits in length.

WAVELYNX EX. 1003, Pg. 469
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

16. The computer-readable medium of claim 12, wherein the seed S_j is 256 bits in length.

17. The computer-readable medium of claim 12, wherein the seed S_j is 512 bits in length.

18. The computer-readable medium of claim 12, wherein an initial value of P_0 is 0.

19. The computer-readable medium of claim 12, further comprising one or more instructions for loading values for the first and second constants A and B from a protected ROM address.

20. The computer-readable medium of claim 19, wherein the first and second constants A and B further incorporate a copyright notice embedded therein.

21. The computer-readable medium of claim 12, wherein the f_{3DES} hardware is operated in output feedback mode.

22. The computer-readable medium of claim 12, wherein the f_{3DES} hardware is operated in dual counter mode.

WAVELYNX EX. 1003, Pg. 470
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

1/1

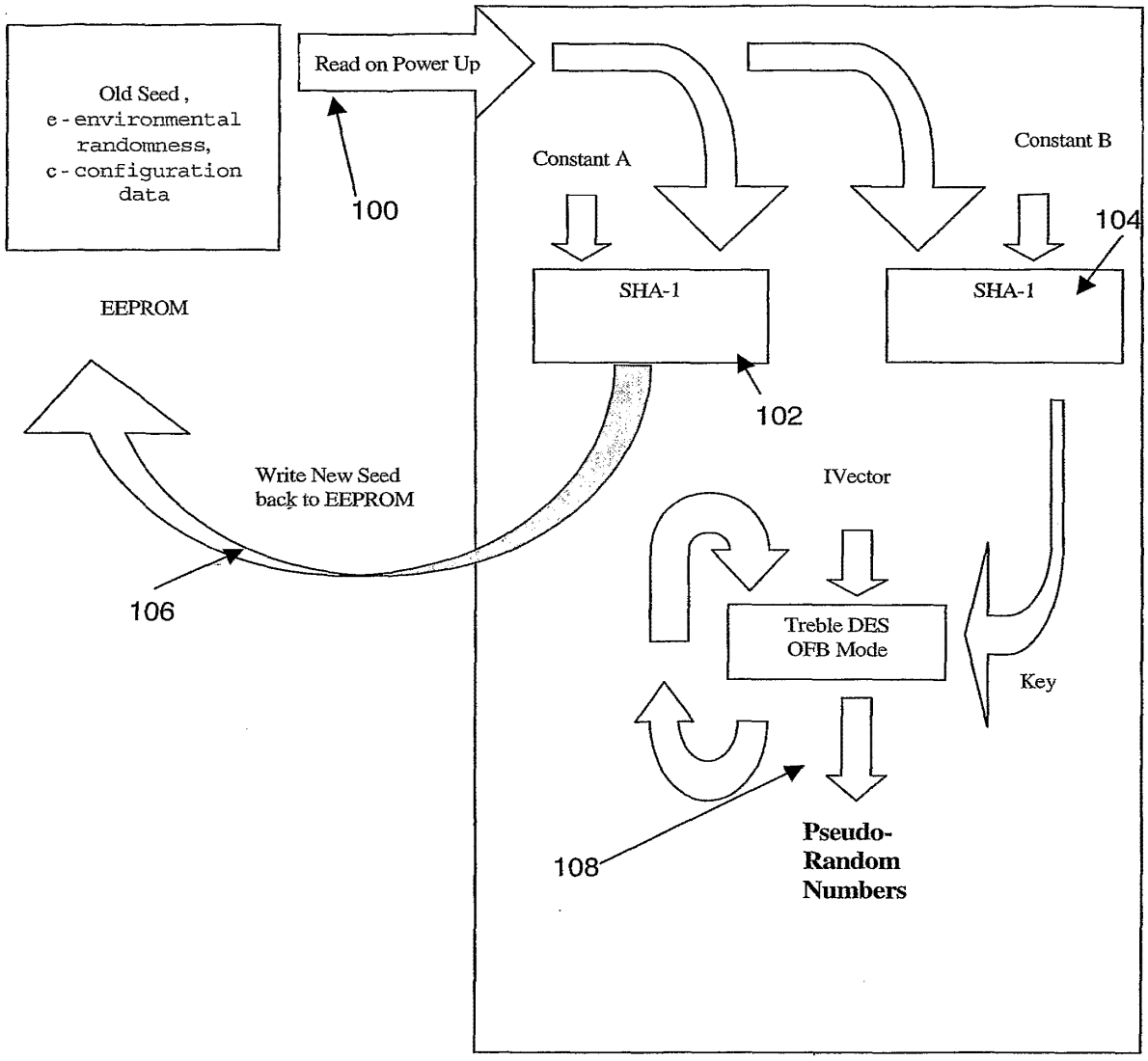

Old Seed,
e - environmental randomness,
c - configuration data
Read on Power Up
100
Constant A
Constant B
104
SHA-1
SHA-1
EEPROM
102
Write New Seed back to EEPROM
IVector
106
Treble DES OFB Mode
Key
108
Pseudo-Random Numbers

FIG. 1

INTERNATIONAL SEARCH REPORT

Inte al Application No
PCT/US 03/21422

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58

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 7 G06F

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 practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 778 069 A (SIMON DANIEL R ET AL) 7 July 1998 (1998-07-07) column 3, line 1 - column 6, line 45; table 1	1-22
Y	PETER GUTMANN: "Software Generation of Practically Strong Random Numbers" 7TH USENIX SECURITY SYMPOSIUM, 26 January 1998 (1998-01-26), - 29 January 1998 (1998-01-29) pages 1-17, XP002306325 SAN ANTONIO, TEXAS page 5, right-hand column, last paragraph - page 7, right-hand column, paragraph 2	1-22
A	US 6 272 223 B1 (CARLSON ROLF E) 7 August 2001 (2001-08-07) column 6, line 32 - column 7, line 28	1-22

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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
18 November 2004	02/12/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Prins, L

INTERNATIONAL SEARCH REPORT

Inte al Application No
PCT/US 03/21422

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PRENEEL B: "State-of-the-art Ciphers for Commercial Applications" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 18, no. 1, 1999, pages 67-74, XP004154866 ISSN: 0167-4048 Chapter 1 up to and including section 1.2	1-22
A	A.J. MENEZES, P.C. VAN OORSCHOT, S.A. VANSTONE: "Handbook of Applied Cryptography" 1997, CRC PRESS , BOCA RATON, FLORIDA , XP002306328 pages 169-175 Section 5.3 up to and including section 5.3.1	1-22
A	JOHN KELSEY, BRUCE SCHNEIER, DAVID WAGNER, CHRIS HALL: "Cryptanalytic Attacks on Pseudorandom Number Generators" FAST SOFTWARE ENCRYPTION, FIFTH INTERNATIONAL WORKSHOP PROCEEDINGS, PARIS, FRANCE, March 1998 (1998-03), pages 1-22, XP002306326 SPRINGER-VERLAG Section 4.1	1-22
A	POMPILIU DONESCU, VIRGIL D. GLIGOR, DAVID WAGNER: "A Note on NSA's Dual Counter Mode of Encryption"'Online! 5 August 2001 (2001-08-05), XP002306327 Retrieved from the Internet: URL:http://www.cs.berkeley.edu/{daw/papers /dcm-prelim.ps> 'retrieved on 2004-11-18! abstract	11,22
A	WO 99/10858 A (LEIGHTON F THOMSON) 4 March 1999 (1999-03-04) page 9, line 22 - line 24	9,20

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte al Application No
PCT/US 03/21422

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5778069 A	07-07-1998	NONE	
US 6272223 B1	07-08-2001	US 2003028567 A1	06-02-2003
		US 6428413 B1	06-08-2002
		US 6210274 B1	03-04-2001
		US 2004209660 A1	21-10-2004
WO 9910858 A	04-03-1999	US 5949885 A	07-09-1999
		AU 9208298 A	16-03-1999
		EP 1019889 A2	19-07-2000
		WO 9910858 A2	04-03-1999

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2005 (28.04.2005)

PCT

(10) International Publication Number
WO 2005/038729 A1

(51) International Patent Classification[7]: G07C 9/00

(21) International Application Number:
PCT/US2004/033926

(22) International Filing Date: 15 October 2004 (15.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/512,461 16 October 2003 (16.10.2003) US
10/870,475 16 June 2004 (16.06.2004) US

(71) Applicant *(for all designated States except US)*: **SCM MICROSYSTEMS, INC.** [US/US]; 47211 Bayside Parkway, Fremont, CA 94538 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **MERKERT, Robert, J., Sr.** [US/US]; 21 Chippenham Drive, Voorhees, NJ 08043 (US).

(74) Agent: **GARRETT, ARTHUR, S.**; Finnegan, Henderson, Farabow, Garrett, & DunneR, L.L.P., 901 New York Avenue, NW, Washington, D.C. 20001-4413 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ACCESS CONTROL SYSTEM

(57) Abstract: An access system is disclosed that provides secured access to a security area. In some embodiments of the present invention, the access system includes an input device that is accessible to a user and capable of reading an authentication and/or identification information provided by the user; a standard signal control panel coupled to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device; and a signal processor coupled between the input device and the standard signal control panel, the signal processor being located in the secure area, wherein the input device provides data in a secured communication channel to the signal processor and the signal processor, in response to the data provided by the input device, provides the data to the standard signal control panel utilizing a standard signal. In some embodiments, the standard signal control panel may be a Wiegand or Magnetic-strip control panel. In some embodiments, the secured communications channel may be an RS422, RS485 or a TCP/IP protocol channel.

WO 2005/038729 A1

ACCESS CONTROL SYSTEM

DESCRIPTION

Related Applications

[001] This application claims priority to U.S. Provisional Application No. 60/512,461 filed Oct. 16, 2003, entitled "Access System" and U.S. Application No.10/870,475 filed June 16, 2004, entitled "Access System," which claims priority to Germany Application DE 20309254.6, filed on June 16, 2003 in Germany, all of which are herein incorporated by reference in their entirety.

Field of the Invention

[002] The present invention is related to access devices to provide physical access to a secured area and, in particular, to access devices compatible with current access control systems while providing higher levels of security.

Background of the Invention

[003] Secured access to sensitive areas has become an important issue, especially after the events of 11 September 2001. As such, there is a current focus on technological systems for controlling access to security areas in both the private and public arenas. Such systems must be made highly impervious to attack by those wishing to gain unauthorized access to the secured area.

[004] Security systems using, for example, Wiegand readers and control panels adapted to evaluate the data read from a Wiegand card are well known and widely employed in various applications like systems for unlocking doors or parking garage gates, etc. Usually, the Wiegand reader is located to be accessible to the user (Wiegand card holder) while the control panel, which after a positive evaluation of the

WAVELYNX EX. 1003, Pg. 476
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

data, performs a security relevant operation (e.g. unlocking a door) is located in an area which is not accessible to the user, e.g. in a secure room, to guarantee a certain level of security.

[005] U.S. Patent 5,679,945 discloses an access system that provides an "intelligent" card reader in order to replace existing magnetic stripe readers, bar code readers and Wiegand readers without the need for retrofitting of existing computer systems, which are coupled to the existing readers. However, readers that utilize a standard signal for communication into a secured area are easily attacked by those seeking unauthorized access to the secured area. Therefore, access systems utilizing readers that provide standard signals (e.g., Wiegand, Mag Stripe, or bar-code standard signals) do not provide a high level of security because those signals are more susceptible to, for example, replay attacks. Replay attacks in a conventional access control system can be accomplished by an intruder gaining access to the communication wires. By capturing the data sent on a valid data transfer, the attacker can later replay the same data and gain unauthorized entrance.

[006] Therefore, there is a strong need, especially in a highly security conscious environment, to provide access systems with high levels of security against unauthorized access.

SUMMARY

[007] In accordance with the present invention, an access system is provided that includes an input device accessible to a user and capable of reading authentication and/or identification information provided by the user, and a standard control panel coupled to the input device for evaluation of the information provided by the user. The standard control panel can be located in a secure area remote from

WAVELYNX EX. 1003, Pg. 477
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the input device and can accept input signals compatible with those from standard signal readers that read traditional access cards, such as, for example, magnetic strip (Mag Stripe) cards, Wiegand cards, bar-code cards, etc. The input device can, for example, be a device that reads smart cards or memory cards, either contact or contactless. In some embodiments, the input device can also read inputted information from the user (user information) or data regarding the user (e.g., biometric data such as fingerprints).

An access system according to the present invention can include an input device that is accessible to a user and capable of reading authentication and/or identification information provided by the user; a standard signal control panel coupled to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device; and a signal processor coupled between the input device and the standard signal control panel, the signal processor being located in the secure area, wherein the input device provides data in a secured communication channel to the signal processor; and the signal processor, in response to the data provided by the input device, provides the data to the standard signal control panel utilizing a standard signal.

[008] These and other embodiments are further discussed below with respect to the following figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] Figure 1 shows a block diagram illustrating an access system according to the prior art.

[010] Figure 2 shows a block diagram of an embodiment of an access system according to the present invention.

WAVELYNX EX. 1003, Pg. 478
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[011] Figure 3 is shows a block diagram of embodiment of an access system according to the present invention.

[012] Figure 4 shows a block diagram of an embodiment of an access system according to the present invention.

[013] Figure 5 shows a block diagram of an embodiment of an access system according to the present invention that utilizes encrypted or signed, self-clocked data transmission.

[014] Figures 6A and 6B illustrate uni-directional and bi-directional data transmission, respectively.

[015] Figure 7 illustrates sample wave shapes for Wiegand signals, Mag-Stripe signals, and self-clocked di-phase signals.

[016] Figure 8 illustrates sample timing diagrams for self-clocked di-phase communication on Transmit and Receive data.

[017] Figure 9 shows a block diagram of a signal processor according to the present invention.

[018] Figure 10 shows a security system according to the present invention.

[019] Figure 11 illustrates relative security level based on combinations of various inputs requested of a user attempting to gain access.

[020] Figure 12 illustrates a three-factor card reader.

[021] Figure 13 illustrates other card readers.

[022] In the figures, elements having the same designation have the same or similar functions.

WAVELYNX EX. 1003, Pg. 479
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

DESCRIPTION OF THE EMBODIMENTS

[023] Embodiments of the present invention provide an access system with an extremely high level of security. Embodiments of the invention include a signal processor coupled between the input device and the control device. The input devices in some embodiments can include encryption to encrypt information obtained from the user (i.e., from a memory or smart card, from input to a keypad, and/or from user data -- for example fingerprints). The signal processor, which can be placed in a secured location, can convert the encrypted information into a standard signal that can be sent to the standard control device, for example a standard Wiegand signal, magnetic strip signal, or strip-chart signal. Embodiments of the present invention, then, can be highly versatile because they can, for example, be utilized with Wiegand control panels without being restricted to Wiegand readers as input devices and without transmitting insecure Wiegand signals from the reader to a secured area.

[024] With the signal processor located in a secured location, for example at or near the control panel, the risk of interference with the data by those attempting to gain unauthorized access can be significantly reduced. A higher level of security can be guaranteed with regard to the data transfer from the input device to the control panel because it is not possible to intercept and abuse the authentication/identification information provided by the user if it is encrypted until it reaches the signal processor, especially if the signal processor and the control panel are located in a secure area which is not accessible from an unsecured area, and if a dynamic element is used in the data transfer. A second communication channel between the input device and the securely located signal processor can be provided. The input device can include a smart card reader into which a secure output can be implemented, for example an

WAVELYNX EX. 1003, Pg. 480
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

RS422, an RS485 or a TCP/IP output protocol can be implemented in some embodiments.

[025] An access system according to some embodiments of the present invention may further include a host computer coupled to the input device and located remotely from the input device. The host computer may also be coupled to the control panel and the signal processor. Data may be transmitted between the input device and the host computer utilizing, for example, an RS485 or a TCP/IP protocol

[026] Figure 1 shows a block diagram of a prior art access system that includes a standard Wiegand reader 10 and a Wiegand control panel 12 adapted to retrieve data from standard Wiegand reader 10. The Control panel 12 is located in a secure area 14 remote from Wiegand reader 10, which is accessible to a user attempting to obtain access to a secure area. In order to gain access, the user inserts his Wiegand card (not shown), which contains authentication and, if required, identification information, into the Wiegand reader 10. The information is transmitted from the reader 10 to the control panel 12 where the information is evaluated. Depending on the result of the evaluation, the control panel 12 either performs a security relevant operation, e.g. unlocking a door or the like, to grant the user the requested access, or it denies access.

[027] The weak point in an access system such as that illustrated in Figure 1 is the link between Wiegand reader 10 and control panel 12. The Wiegand data lines are susceptible to replay attacks, i.e. data can be intercepted at the wiring going into secured area 14 and replayed to gain unauthorized entrance.

[028] Figure 2 shows an embodiment of an access system according to the present invention. A reader 16 is coupled to a signal processor 18. Signal processor

WAVELYNX EX. 1003, Pg. 481
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

18 receives signals from reader 18 and converts these signals to standard signals that can be transmitted to control panel 12. In some embodiments, signal processor 18 and control panel 12 are physically located in a secured area 14. In some embodiments, control panel 12 can be a Wiegand control panel. It should be understood that the term "Wiegand control panel" is not restricted to a particular hardware configuration but rather includes any suitable control panel, which is capable of processing data signals in a Wiegand format by using corresponding signal processing or software. Additionally, although an embodiment utilizing a Wiegand control signal is described here, other control signal formats can also be utilized, for example magnetic strip (Mag Stripe) formats or bar-code formats.

[029] In the embodiment shown in Figure 2, the standard Wiegand reader 10 shown in Figure 1 is replaced by another input device, for example a smart card reader 16 into which a smart card (not shown) containing authentication/identification information can be inserted (for contact reading) or otherwise interfaced with (for example for contactless reading). Reader 16 can include an encryption circuit that encrypts the information read from the smart card and an output port, for example an RS422, an RS485 or a TCP/IP output port, for outputting data to signal processor 18. The embodiment of the access system shown in Figure 2 includes a signal processor 18 coupled between reader 16 and control panel 12. Signal processor 18 and control panel 12 can be co-located in secure area 14, which is remote from card reader 16.

[030] In some embodiments, card reader 16 can include a contactless reader for reading a contactless smart card. In general, embodiments of card reader 16 can include contactless smart card readers, contact smart card readers, memory card readers, a user input device such as a keypad on which a user can input

WAVELYNX EX. 1003, Pg. 482
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

authentication/identification data, biometric devices such as a fingerprint or retinal scan reader for directly evaluating the identity of the user, and other signaling devices for communicating with the user.

[031] To begin operation of the embodiment of the access system shown in Figure 2, the user inserts a smart card into smart card reader 16, or in the case of a contactless smart card brings the smart card in close proximity to reader 16. The information on the smart card is read by reader 16. In some embodiments, the information from the smart card can be encrypted in reader 16. The information can then be transmitted to signal processor 18 using a secured, for example RS422, RS485 or TCP/IP protocol, output port. Data transfer between smart card reader 16 and signal processor 18, then, can be regarded as a "secure channel." Signal processor 18 converts the information received from reader 16 into a standard signal (e.g., a Wiegand signal, a bar code signal, or a magnetic stripe signal) that can be received by control panel 12. Control panel 12 is able to evaluate the standard signal and, based on access protocols, decides whether to allow or to deny access to the user.

[032] Figure 3 shows another embodiment of access system according to the present invention. The embodiment shown in Figure 3 includes reader 16, signal processor 18 and control panel 12 as was previously discussed with Figure 2. Further, a host computer 20 can be coupled to one or more of control panel 12, signal processor 18, and reader 16. Remote host computer 20 can be located outside secure area 14 and is coupled to reader 16 and to control panel 12. Communication between host computer 20 and reader 16 can be provided by a further secure channel, for example data can be transferred using an RS485 or a TCP/IP protocol.

WAVELYNX EX. 1003, Pg. 483
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[033] The operation of the embodiment of the access system of Figure 3 to gain access is similar to that described above with respect to Figure 2. However, the embodiment of access system shown in Figure 3 can easily be adapted to various requirements. For example, the secure channel between remote host computer 20 and reader 16 can be used to change the configuration of reader 16 on command from host computer 20 in a comfortable and secure manner. For example, differing levels of security can be implemented by sending commands to reader 16 and control panel 12 from host computer 20. Additionally, host computer 20 can be used to define the type of input devices from which correct identification data is obtained that are required to gain access. Suitable input devices that can be included in reader 16 include a contactless smart card reader, a contact smart card reader, PIN pads (or keypads), biometric devices (for example fingerprint or retinal readers), and combinations thereof. The input devices from which data is required in order to gain access can be changed as a function of security threat level, day of week, time of day, or other conditions. The coupling between host computer 20 and control panel 12 allows checking as to whether a control panel operation has been successfully executed. Further, host computer 20 can be used to identify a possible malfunction of control panel 12 by utilizing test signals.

[034] Additionally, reader 16 may include user-interface (for example a data screen or set of LED displays) for communicating information to a user. The LED signals may originate from control panel 12 and be transmitted through the secured channel between signal processor 18 and reader 16 as is indicated in Figure 3. Further, the secured channel between signal processor 18 and reader 16 may be bi-directional as is shown in Figure 3. In that case, control panel 12 may transmit data

WAVELYNX EX. 1003, Pg. 484
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

and instructions to reader 16, for example regarding security levels and such, over a bi-directional secured line. Additionally, LED display data may be transmitted between control panel 12 and reader 16 over separate lines or through the bi-direction secured line. Control panel 12 may also communicate system status to reader 16 for display to a user directly without communicating through signal processor 18.

[035] Figure 4 illustrates an access system similar to that illustrated in Figure 3, except that the secured channel between reader 16 and signal processor 18 is a uni-directional line. Reader 16, then, cannot receive data from control panel 12 through the secured channel. In some embodiments, status information can be communicated between control panel 12 and reader 16 using a separate line. Status information can be displayed in reader 16 through LCD displays, LED lights, or audible tones, for example. As further shown in Figure 4, setup information can be transmitted to reader 16 separately. Setup information can include for example, which of the various input devices of reader 16 are activated in order to collect the appropriate information from the user to meet the current level of security.

[036] Figure 5 illustrates another embodiment of an access system according to the present invention. As has been discussed above, reader 16 is typically located in a non-secure area on the outside of a locked entranceway. Reader 16 can include interfaces for smart cards, contactless smart cards, biometric readers (e.g. fingerprint readers), PIN pads, and/or other user interface devices. Reader 16 transmits data which may be encrypted and/or digitally signed, extracted from a smart card or other input device to signal processor 18, which is located in secure area 14. In some embodiments, signal processor 18 can be located near or possibly in standard signal control panel 12.

WAVELYNX EX. 1003, Pg. 485
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[037] Digital signatures may be used to authenticate the information being sent to the control panel to ensure that it originated with the card or device that actually sent the information, and to ensure that the transmitted information was not altered after the information being transmitted was digitally signed.

[038] There exist many well-known processes for creating and validating digital signatures. One example is the Digital Signature Algorithm, which may be used by a *signatory* to generate a digital signature on data and by a *verifier* to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process.

[039] To generate the correct digital signature for a signatory, knowledge of the private key of the signatory is needed. In other words, signatures cannot be forged, without knowledge of a signatory's private key. However, by using the signatory's public key, anyone can verify a correctly signed message.

[040] The Digital Signature Algorithm uses parameters denoted by p, q, g, and x, which are defined below:

p is an L-bit prime p, where $512 \leq L \geq 1024$, and L is divisible by 64;

q *is* a 160-bit prime q, such that q is a factor of $p - 1$, i.e. $(p - 1) = qz$, where z is any natural number;

h is chosen such that, $1 < h < p - 1$ and $g = h^z \bmod p > 1$;

x is chosen randomly such that $0 < x < q$ and $y = g^x \bmod p$.

The Public Key is y and the Private Key is x.

[041] To generate a digital signature, the algorithm also makes use of a one-way hash function, *SHA(m)*, such as, for example, the Secure Hash Algorithm,

WAVELYNX EX. 1003, Pg. 486
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

and a randomly generated number k, where $0 < k < q$. Parameter k is regenerated for each time a signature is generated. Parameters x and k are used for signature generation and are kept secret.

[042] The Digital Signature (r,s) of a message M is the pair of numbers r and s computed according to the equations below:

$$r = (g^k \bmod p) \bmod q \quad \text{and}$$

$$s = (k^{-1} SHA(M) + xr)) \bmod q.$$

[043] Prior to verifying the signature in a signed message, p, q, g and the sender's public key y and identity are made available to verifiers. These parameters may be publicly distributed. Additionally, the Digital Signature (r, s) is also made available along with its associated message M to potential verifiers.

[044] To verify the signature, the verifier first checks to see that $0 < r < q$ and $0 < s < q$; if either condition is violated, the signature is invalid.

[045] If these two conditions are satisfied, the verifier computes:

$$w = s^{-1} \bmod q;$$

$$u_1 = ((SHA(M)) * w) \bmod q;$$

$$u_2 = (rw) \bmod q; \text{ and}$$

$$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q.$$

[046] If $v = r$, then the signature is verified. On the other hand, if $v \neq r$, then the message may have been modified and the signature should be considered invalid.

[047] In some embodiments, data sent from reader 16 to signal processor 18 can be clocked data or self-clocked data. As has been described above, signal

WAVELYNX EX. 1003, Pg. 487
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

processor 18 converts the data received from reader 16 into a standard format signal, such as, for example, Wiegand, Mag Stripe, or bar code that is recognizable by standard signal control panel 12.

[048] In some embodiments, a host computer 20 can communicate with signal processor 18 and with reader 16 through signal processor 18. As discussed above, host computer 20 can, for example, vary the level of security or alter the action or display setup of reader 16.

[049] In some embodiments, a security module or processor is located in each of reader 16 and signal processor 18 to allow for the secure transfer of data between reader 16 and signal processor 18, either through encryption or digitally signing the data. In some embodiments, a dynamic element can be used in the data transmission process to ensure that a replay attack cannot be used to gain unauthorized access to an entrance portal through reader 16. Replay attacks in a conventional access control system can be accomplished by an intruder gaining access to the communication wires, between the output terminal of reader 10 (Figure 1) and the control panel 12. By capturing the data sent on a valid data transfer, the attacker can later replay the same data and gain unauthorized entrance. In some embodiments consistent with the present invention, the dynamic element could include date and time information corresponding to the date and time when the reader was accessed. The date and time information can be sent to the signal processor, which can then check the received information with the current date and time to ensure that the information sent is not a replay attack.

[050] In some embodiments, the secured communication channel between reader 16 and signal processor 18 can utilize the wiring that may be in place when

WAVELYNX EX. 1003, Pg. 488
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

replacing a conventional access system, for example the Wiegand wiring. The existing two wires can be used for data and clock for one-way communication between reader 16 and signal processor 18 or bi-directional communication can be established using self-clocked data, for example non-return to zero (NRZ) or Di-phase communications. There are many advantages to using a bi-directional communication path between reader 16 and signal processor 18. Some of these include error retransmission capability, the ability to transmit status level information between control panel 12 to reader 16 via data signal processor 18, and general two-way communications for various other functions.

[051] Utilizing self-clocked NRZ or Di-phase communication between reader 16 and signal processor 18 allows for improved data detection and immunity to sporadic 'noise' signals generated by external sources on the data lines between reader 16 and signal processor 18. The technique employs the use of a sampling clock that is at a frequency of 8, 16, 32 or higher times that of the data transmission frequency. Multiple samples can be taken of the data line in each bit transmission in order to ascertain the data bit's true state. A plurality of clock signals indicating the same data status during the given bit time can be used to ascertain the state of the data bit. In some embodiments, both reader 16 and signal processor 18 can have independent sampling clocks running at the same higher frequency as that of the data bit frequency. In some embodiments, the data between reader 16 and signal processor 18 may be out of synchronization by only a few, for example one, clock cycle of the higher frequency clock.

[052] Di-phase communication can be used to further improve communication between reader 16 and signal processor 18. The state of the data is

WAVELYNX EX. 1003, Pg. 489
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

changed on every data bit time period. If the data were in a high state it would be changed to a low state, and vice versa. A data 'one' is in the same state for the entire bit period. A data 'zero' changes state at the half-bit time. The value of the data bit is determined by comparing the state of the data bit during the first half of the data bit period and the second half of the data bit period. If the data state is the same in both half-bit times, the value of the data bit is a 'one'; if the data state is different in both halves of the bit time the data bit is a 'zero'.

[053] In some embodiments, reader 16 can change configuration on request from a host computer via a communications channel or from control panel 12 through status lines. In some embodiments, data signal processor 18 can receive configuration information from host computer 20 or from standard signal control panel 12 and can transmit the configuration data to reader 16 via the bi-directional data lines between signal processor 18 and reader 16. An example of configuration information being sent to reader 16 is a requirement for additional user inputs, such as card and PIN pad data; card, PIN pad and biometric data; or other combinations. Such security level changes may be sent as required based on time of day, day of the month, or National Security levels.

[054] Figures 6A and 6B illustrate uni-directional and self-clocked bi-directional data lines, respectively. Figure 6A shows how the Data out-0 line from the reader, such as from exemplary reader 16, is sent to the Signal Processor across the data channel interface. A signal arriving on the Data out-0 or D0 lines, at the Signal Processor is always interpreted as a "0". Figure 6B shows transmission of data using a self-clocked bi-directional line for the Data in-1 signal, across the data channel interface. Data transmitted by the Reader is buffered and sent to the Signal

WAVELYNX EX. 1003, Pg. 490
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Processor. Similarly, data transmitted by the Signal Processor is buffered and sent to the Reader. A signal arriving on the Data out-1, Data in-1 or D1 line at the Signal Processor is always interpreted as a "1".

[055] Figure 7 illustrates sample wave shapes for Wiegand (D0, D1), Mag Stripe (Clock and Data), and self-clocked Di-phase. The data being transmitted, shown in the Data row of Figure 7 is the 9-bit binary stream "110100101". As shown in Fig. 7, transmission of this data using Wiegand (D0, D1) depicted as W-D0 and W-D1 uses 9 clock cycles. Whenever a "0" is being transmitted during a clock cycle, the W-D0 line is asserted. If a "1" is being transmitted during a clock cycle, the W-D1 line is asserted. Thus, the W-D1 line is asserted during the first two clock cycles corresponding to the first two binary digits "11" of the 9-bit stream being transmitted. On the third clock cycle, the W-D0 line is asserted corresponding to the third digit ("0") of the binary stream. In the Mag Stripe (Clock and Data), as shown in Fig. 7, the Data line is asserted for "1's" and negated for "0's". Thus, the Data line is asserted for the first two clock cycles and then negated during the third clock cycle corresponding to the initial "110" data sequence of the 9-bit stream.

[056] In the Self-Clocked Di-phase scheme, if the line is held to a constant value over the entire clock period, then the data being transmitted is a "1". On the other hand, if the line value changes in the middle of the clock period the data being transmitted is a "0". Thus, the line is high for the entire first clock period, low for all of the second clock period, and changes in the middle of third clock period corresponding to the "110" data sequence. Figure 8 illustrates an example of self-clocked Di-phase communication, on transmit and receive data. Fig. 8 shows changes in the "Data Out" and "Data In" signals over 16 cycles of the base input clock, which

WAVELYNX EX. 1003, Pg. 491
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

corresponds to the Bit Time or Bit Period. Changes in Data Out or Data In during the bit period indicate that a "0" is being transmitted whereas a constant value (0 or 1) for the entire period indicates that the data on the line is a "1".

[057] Figure 9 shows an embodiment of signal processor 18. The embodiment of signal processor 18 shown in Figure 9 includes a microprocessor 21 coupled to a reader communications switch 20 and a control panel data line switch 22. Further, microprocessor 21 may be coupled to a communications channel interface 23 for communications with host computer 20 and to a security access module (SAM) 24.

[058] Reader communications switch 20 can be coupled to one or more readers 16 of differing types through, for example, a bi-directional data communications channel. Further, data regarding each of the readers can be communicated to control panel 12 through control panel line switch 22. In some embodiments, data regarding the readers could include data regarding the status of the readers, such as whether they are active, inactive or malfunctioning.

[059] Conversion of data from reader 16 to a standard signal for standard signal control panel 12 can be accomplished in software operating on microprocessor 21 and stored in memory. In some embodiments, software operating on microprocessor 21 and stored in memory could implement portions of a digital signature verification and authentication algorithm. SAM 24 stores and implements encryption codes and, in some embodiments, can be removable using a "SAM lock".

[060] Figure 10 shows an example of a security system according to the present invention. A security system according to the present invention includes one or more access systems according to the present invention. Further, host computer 20

WAVELYNX EX. 1003, Pg. 492
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

may include one or more workstations, such as an access control station, badging station, and guard workstation. As shown, control panel 12 communicates, through signal processor 18, with reader 16 and can open an appropriate door 30 once access is approved.

[061] In some embodiments of the invention, various levels of security may be programmed into control panel 12 and reader 16. For example, security levels may be classified with regard to threat level, for example low, guarded, significant, high, and severe. The level of authentication/identification required for each threat level may be different. For example, in a low threat security environment access may be gained with a contactless card. With a guarded level, the access system may be set to require both a contactless card and that the user input a personal identification number (PIN) into a keypad. With a significant threat, a contact card and a PIN may be required. In a high threat security level, a contact card and some biometric input (e.g., fingerprint) may be required to gain access. In a severe threat security level, three inputs -- a contact card, a PIN, and a biometric input -- may be requested of a user attempting to gain access. Figure 11 illustrates the relative security level with respect to various inputs and combinations of inputs requested of the user in a security system. In some embodiments, a single smart card may be configured to provide both contactless and contact connection with reader 16.

[062] Figure 12 illustrates a card reader that can be utilized in embodiments of the present invention. The embodiment of card reader shown in Figure 12 includes an LCD display, a keypad for accepting PIN information, a smart card reader, a contactless reader, and a fingerprint sensor. A series of LEDs can indicate security level. Further, an acoustic alarm may be included.

WAVELYNX EX. 1003, Pg. 493
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[063] Figure 13 illustrates other types of card readers that may be utilized with embodiments of the present invention.

[064] Although any standard formats may be utilized in embodiments of the present invention, in some embodiments, the contact card readers may be ISO 7816 card readers and the contactless cards may be ISO 14443, parts 1-4 with a FIPS 140-2 approved algorithm. Further, the card reader can be programmable, for example in order to extract SEIWG-12 data strings or other ID strings from a smart card.

[065] Several standards and working groups have been established in the area of access control. For example, the Security Equipment Integration Working Group has issued a specification on September 30, 2002: "Development of a specification for SEIWG-compliant Access Control Components; a study by the Security Equipment Integration Working Group," September 30, 2002, which is herein incorporated by reference in its entirety and made a part of this disclosure. Further, the Physical Access Interoperability Working Group has implemented a "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 1.0," July 2, 2003, which is herein incorporated by reference in its entirety and made a part of this disclosure. Additionally, the Security Industry Association has issued an "Access Control Standard Protocol for the 26-Bit Wiegand Reader Interfaces," October 17, 1996, which is herein incorporated by reference in its entirety and made a part of this disclosure. The later document provides information regarding the Wiegand standard.

[066] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. For example, embodiments utilizing standards other than the Wiegand

WAVELYNX EX. 1003, Pg. 494
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

standard for signaling between signal processor 18 and control panel 12 can be utilized. Additionally, other protocols may be utilized for secure transmission channels other than the RS422, RS485 or TCP/IP protocols described as examples here. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

WAVELYNX EX. 1003, Pg. 495
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

WHAT IS CLAIMED IS:

1. An access system, comprising:

an input device that is accessible to a user and capable of reading authentication and/or identification information provided by the user;

a standard signal control panel coupled to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device; and

a signal processor coupled between the input device and the standard signal control panel, the signal processor being located in the secure area,

wherein the input device provides data in a secured communication channel to the signal processor and the signal processor, in response to the data provided by the input device, provides the data to the standard signal control panel utilizing a standard signal.

2. The system of claim 1, wherein the data provided by the input device in the secured communication channel includes a dynamic element.

3. The method of claim 2, wherein the dynamic element is used to ensure that a replay attack cannot be used to gain unauthorized access to an entrance portal.

4. The system of claim 1, wherein the standard signal is chosen from a set consisting of Wiegand signals, Mag Stripe signals, and Bar Code signals.

5. The system of claim 1, wherein the signal processor is co-located with the control panel in the secure area.

6. The system of claim 1, wherein the input device includes a smart card reader.

7. The system of claim 1, wherein the input device includes a PIN pad.

WAVELYNX EX. 1003, Pg. 496
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

8. The system of claim 1, wherein the input device includes a biometric device.

9. The system of claim 1, further including a host computer coupled to the input device and the standard signal control panel, the host computer communicating parameters to the input device and the standard signal control panel through secured channels.

10. The system of claim 1, wherein the communications channel is secured using at least one of the following methods:

encryption of the transmitted information; and/or

authentication of the transmitted information using a digital signature; and/or

the use of a dynamic element, shared by input device and the signal processor to protect against replay attacks.

11. The system of claim 1, wherein the input device communicates with the signal processor in a self-clocked non return to zero or Di-phase communication.

12. An access system comprising:

means for receiving authentication and/or identification information provided by a user;

means for securely transmitting the authentication and/or identification information provided by the user;

means for receiving the securely transmitted information; and

means for providing the received information to a standard control panel using standard signals; and

WAVELYNX EX. 1003, Pg. 497
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

means for controlling access to a secured area based on the information received by the standard control panel.

13. The system of claim 12, wherein the authentication and/or identification information provided by a user includes at least one of smart card information, biometric information, or PIN information.

14. The system of claim 12, wherein means for receiving authentication and/or identification information provided by a user further includes means for combining additional dynamic information with the authentication and/or identification information.

15. The method of claim 14, wherein the additional dynamic information is based on temporal information generated contemporaneously with the authentication and/or identification information provided by the user.

16. The system of claim 12, wherein means for securely transmitting the authentication and/or identification information provided by the user further includes means for digitally signing and/or encrypting the information.

17. The system of claim 12, wherein means for receiving the securely transmitted information further includes means for decrypting and/or authenticating the received information.

18. The system of claim 12, wherein means for means for providing the received information to a standard control panel using standard signals further includes means for translating the received information to a format compatible with standard control panel inputs.

WAVELYNX EX. 1003, Pg. 498
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

19. The method of claim 18, wherein the standard control panel inputs are chosen from chosen from a set consisting of Wiegand signals, Mag Stripe signals, and Bar Code signals.

20. An access method comprising:

receiving authentication and/or identification information provided by a user through an input device;

securely transmitting the authentication and/or identification information provided by the user;

receiving the securely transmitted information;

providing the received information to a standard control panel using standard signals; and

controlling access to a secured area based on the information received by the standard control panel.

21. The method of claim 20, wherein the authentication and/or identification information provided by a user through an input device includes at least one of smart card information, biometric information, or PIN information.

22. The method of claim 20, wherein receiving authentication and/or identification information provided by a user through an input device further includes combining additional dynamic information with the authentication and/or identification information.

23. The method of claim 22, wherein the additional information is generated by the input device.

WAVELYNX EX. 1003, Pg. 499
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

24. The method of claim 22 wherein the additional dynamic information is based on temporal information generated contemporaneously with the authentication and/or identification information provided by the user.

25. The method of claim 20 wherein securely transmitting the authentication and/or identification information provided by the user further includes digitally signing and/or encrypting the information.

26. The method of claim 25, wherein the digital signing and/or encryption of the information is performed by the input device.

27. The method of claim 20, wherein the steps of receiving the securely transmitted information and providing the received information to a standard control panel using standard signals are performed by a signal processor.

28. The method of claim 20, wherein receiving the securely transmitted information further includes decrypting and/or authenticating the received information.

29. The method of claim 20 wherein providing the received information to a standard control panel using standard signals further includes translating the received information to a format compatible with standard control panel inputs.

30. The method of claim 29, wherein the standard control panel inputs are chosen from chosen from a set consisting of Wiegand signals, Mag Stripe signals, and Bar Code signals.

31. The method of claim 27, wherein the input device communicates with the signal processor using self-clocked non return to zero or Di-phase communication.

WAVELYNX EX. 1003, Pg. 500
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 2

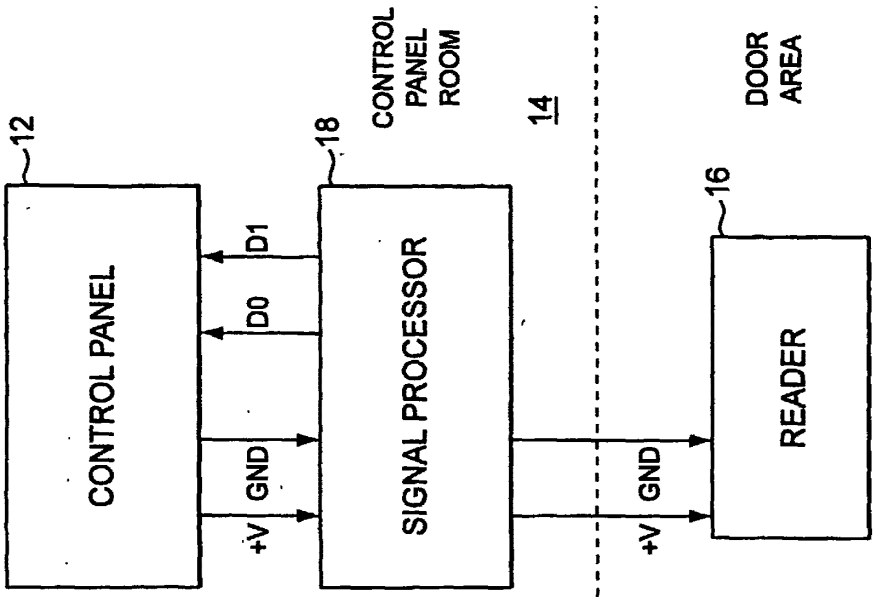
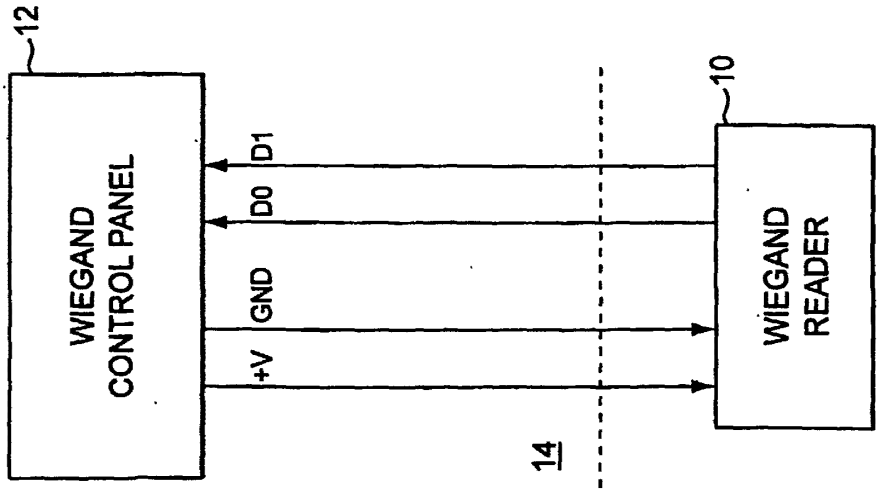


FIG. 1



WAVELYNX EX. 1003, Pg. 501
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

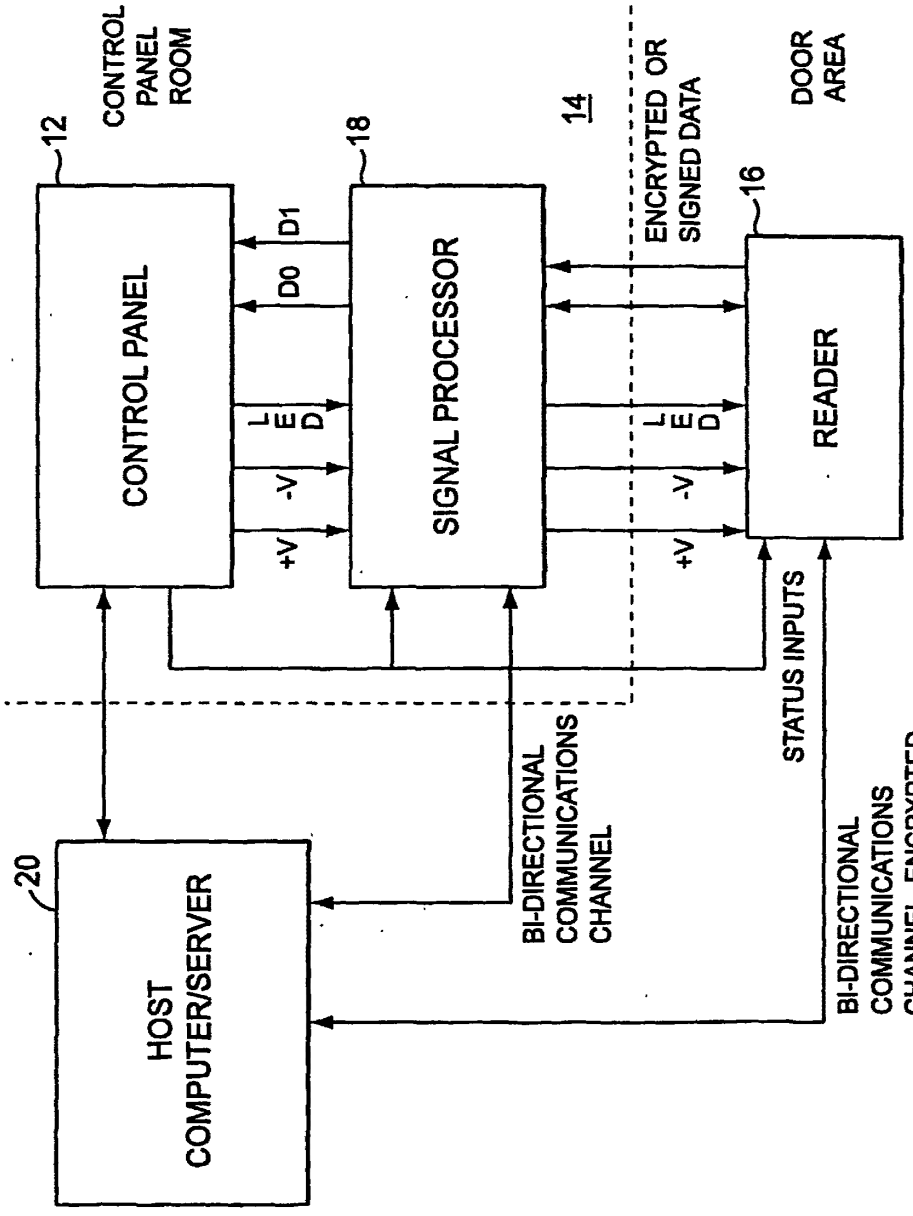


FIG. 3

WAVELYNX EX. 1003, Pg. 502
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

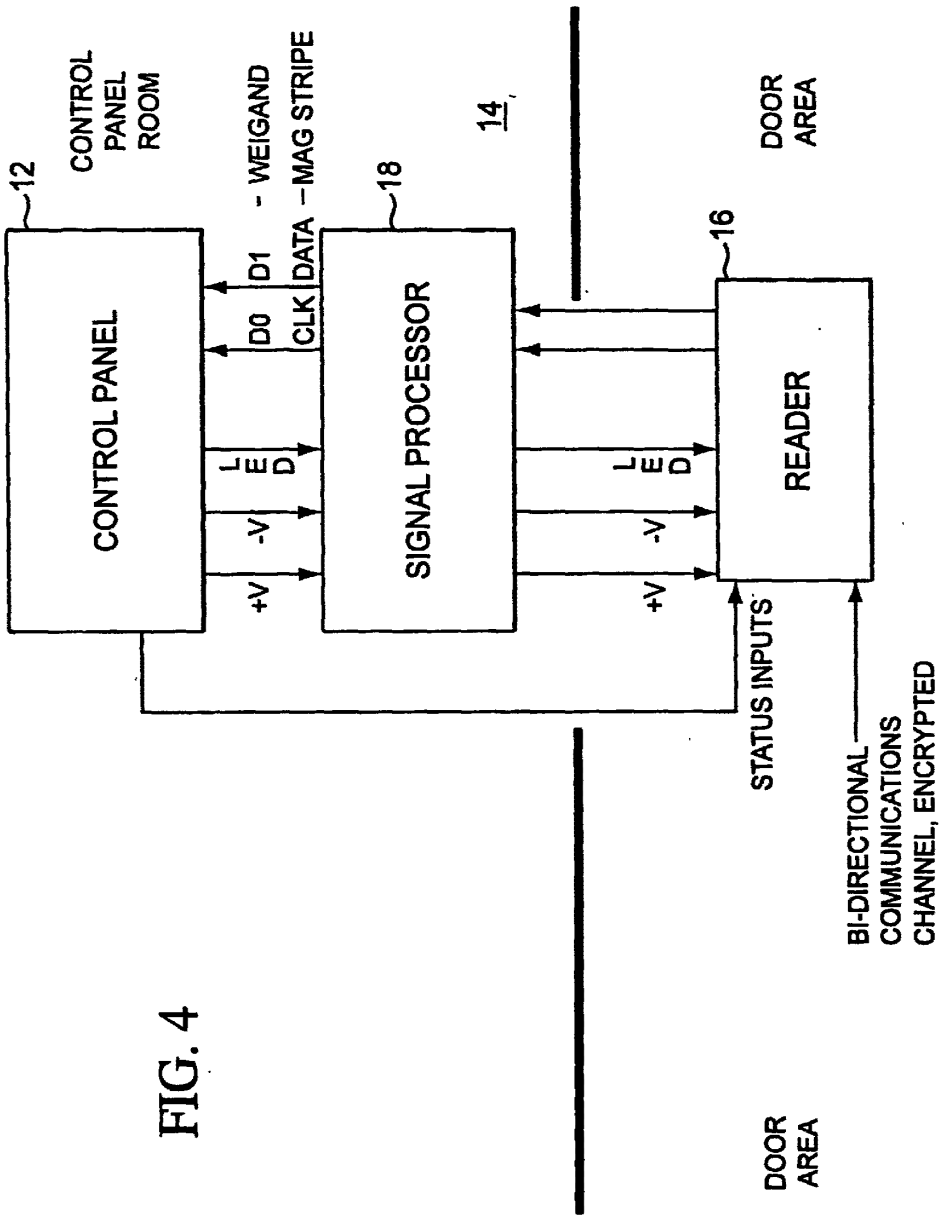


FIG. 4

WAVELYNX EX. 1003, Pg. 503
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

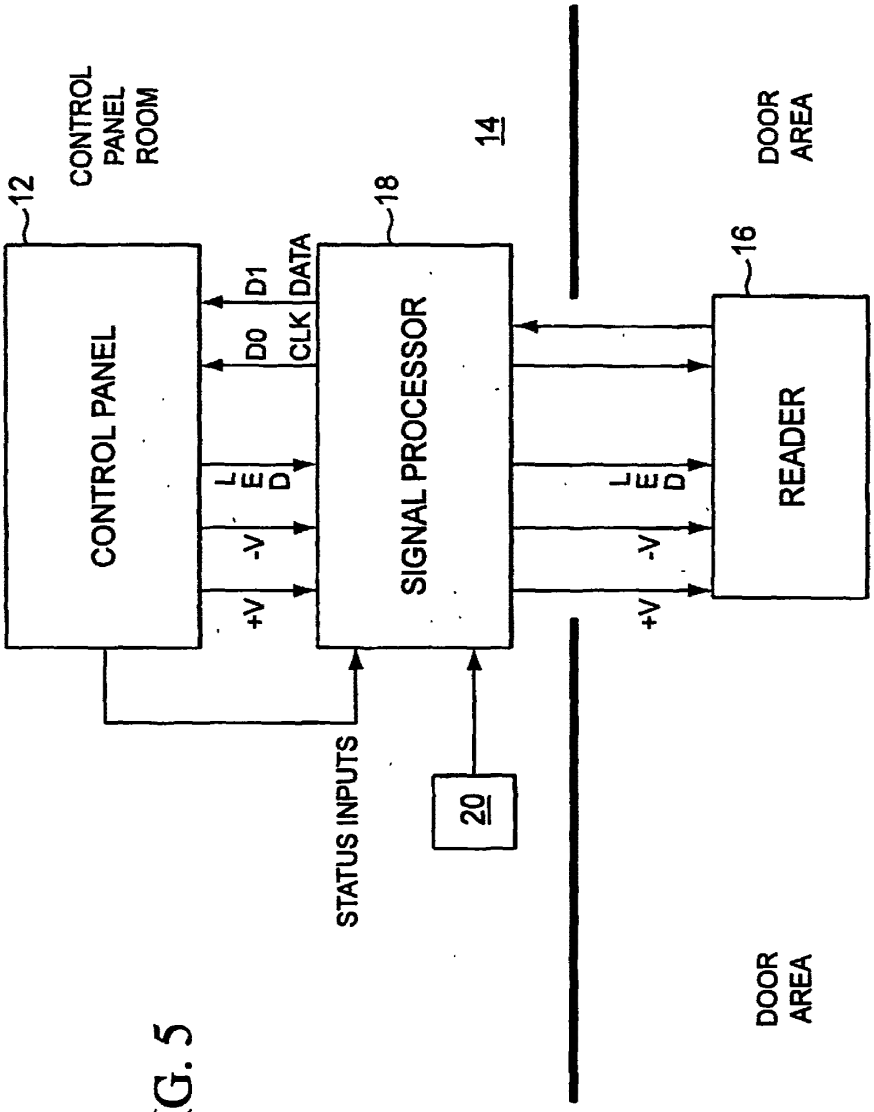


FIG. 5

WAVELYNX EX. 1003, Pg. 504
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

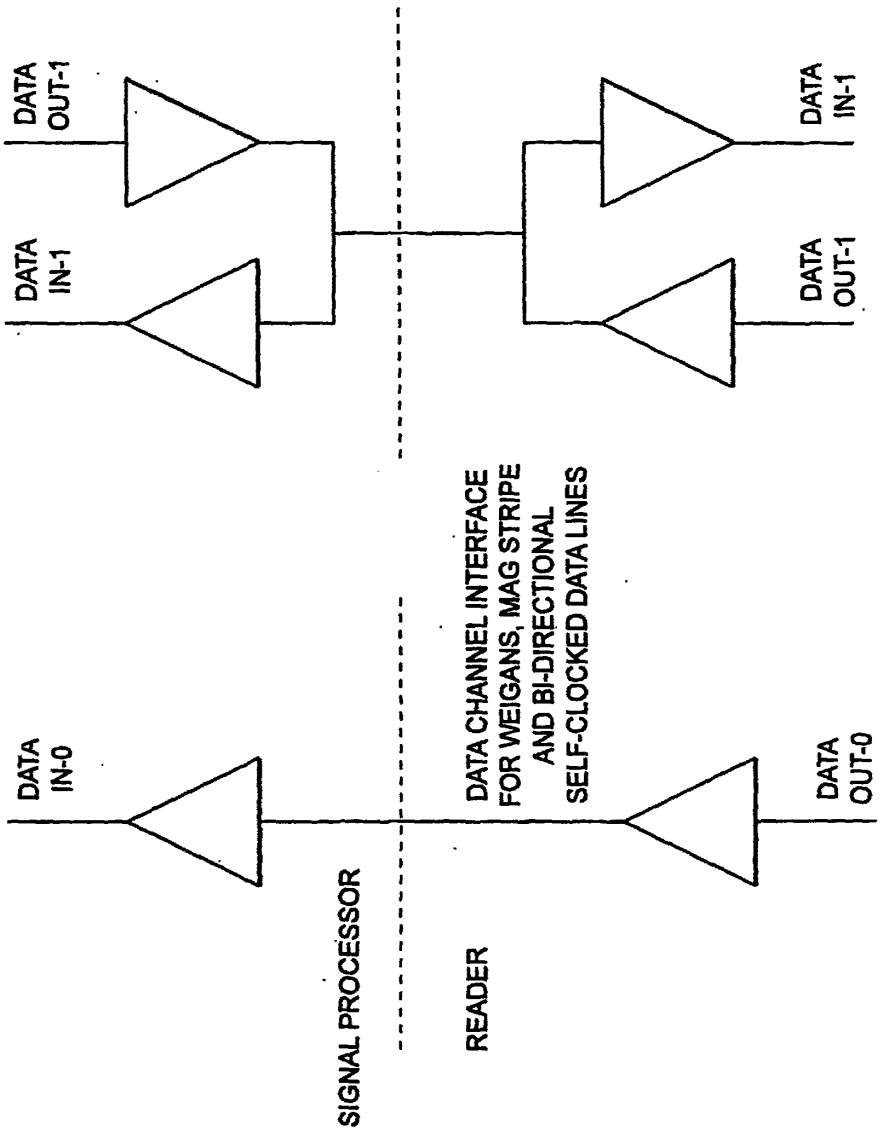


FIG. 6B

FIG. 6A

WAVELYNX EX. 1003, Pg. 505
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

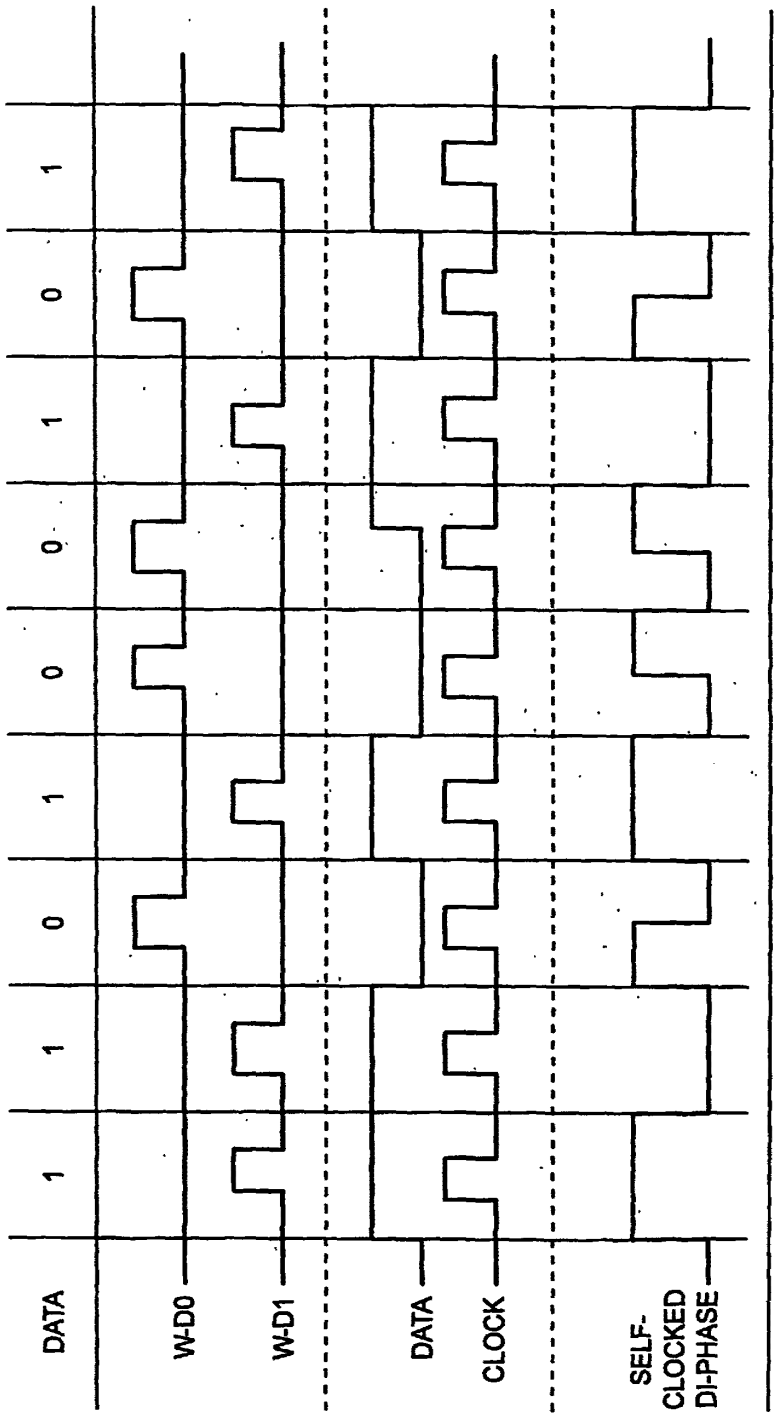


FIG. 7

WAVELYNX EX. 1003, Pg. 506
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

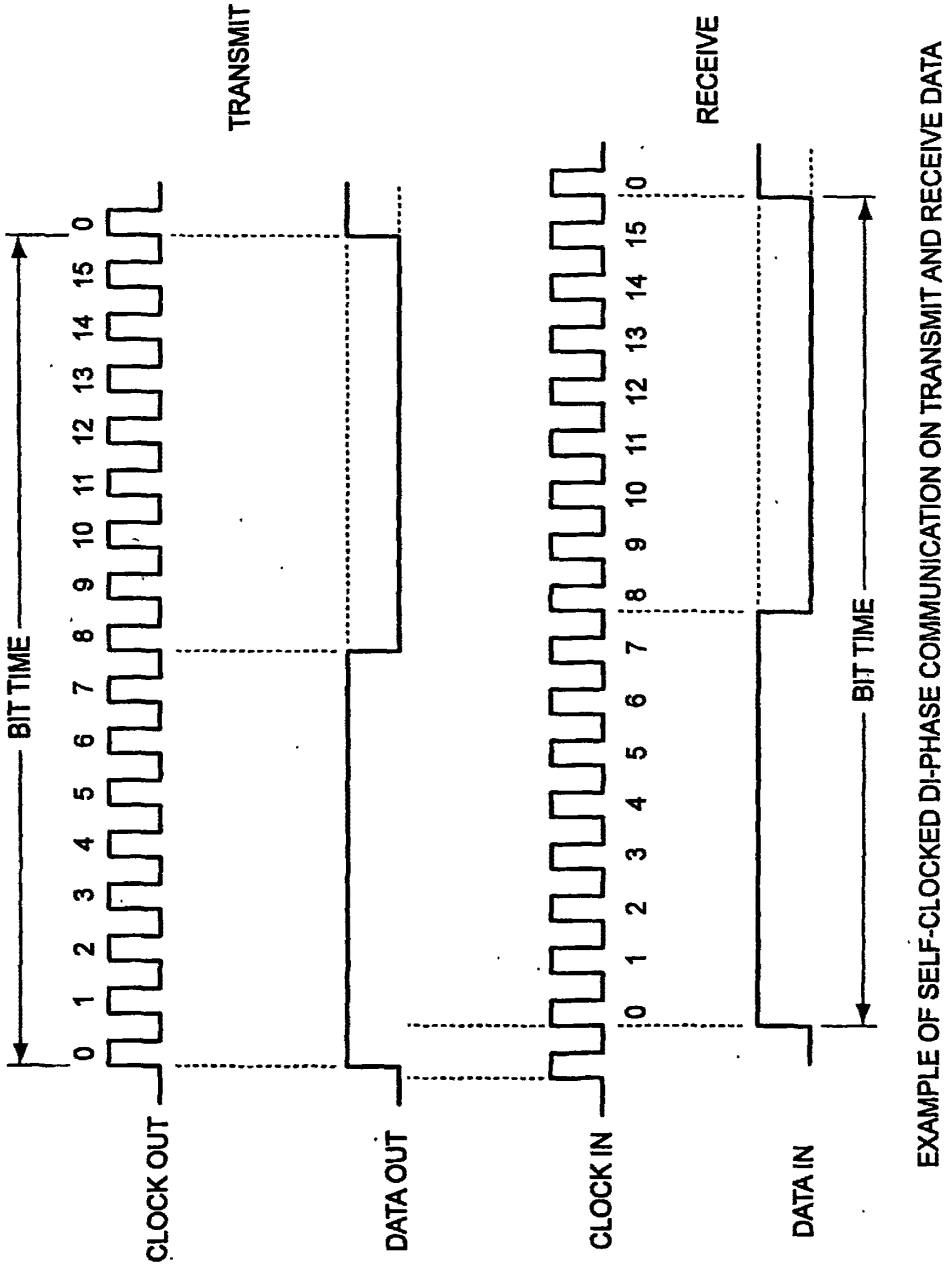


FIG. 8

WAVELYNX EX. 1003, Pg. 507
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

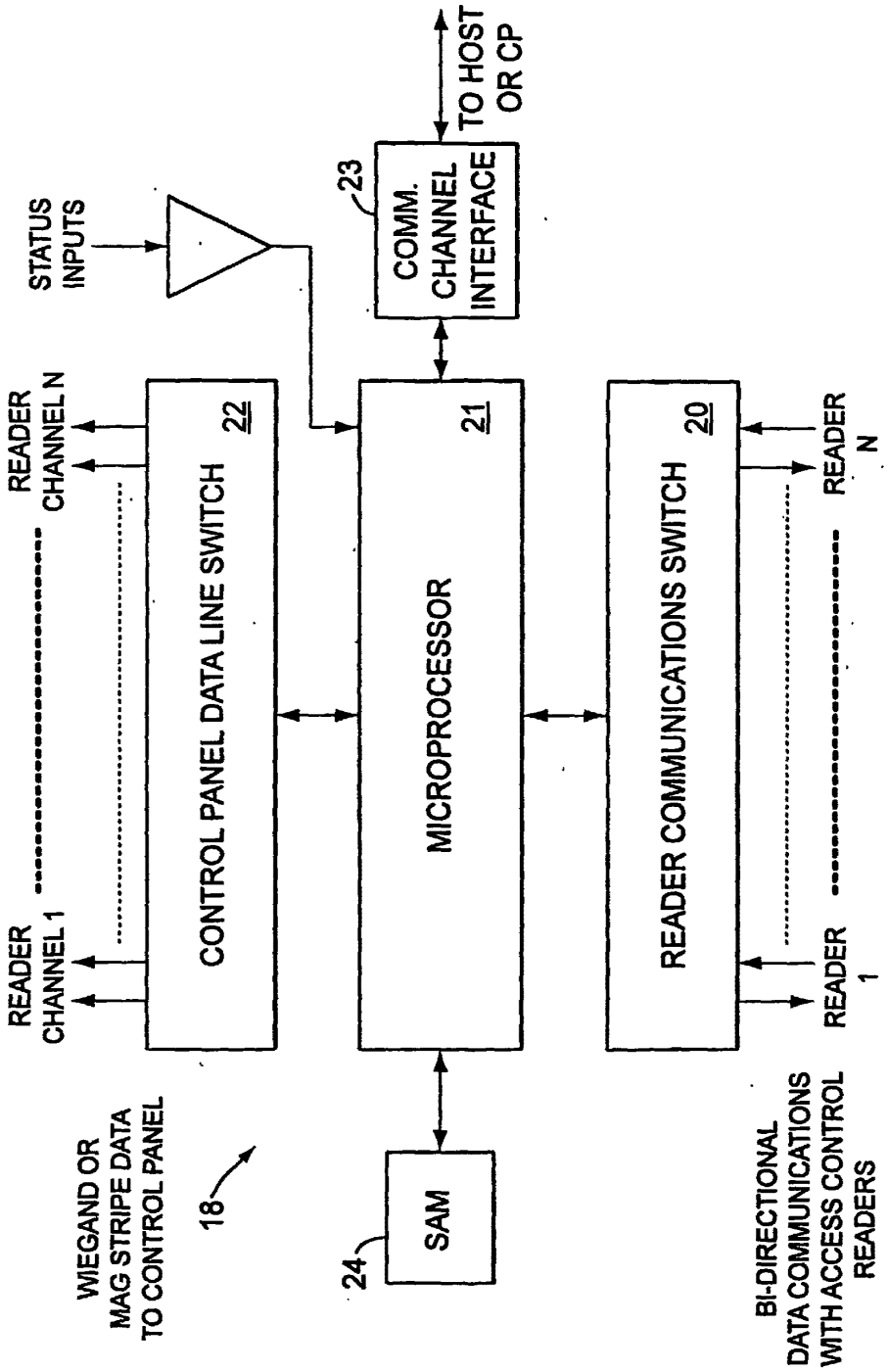


FIG. 9

WAVELYNX EX. 1003, Pg. 508
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

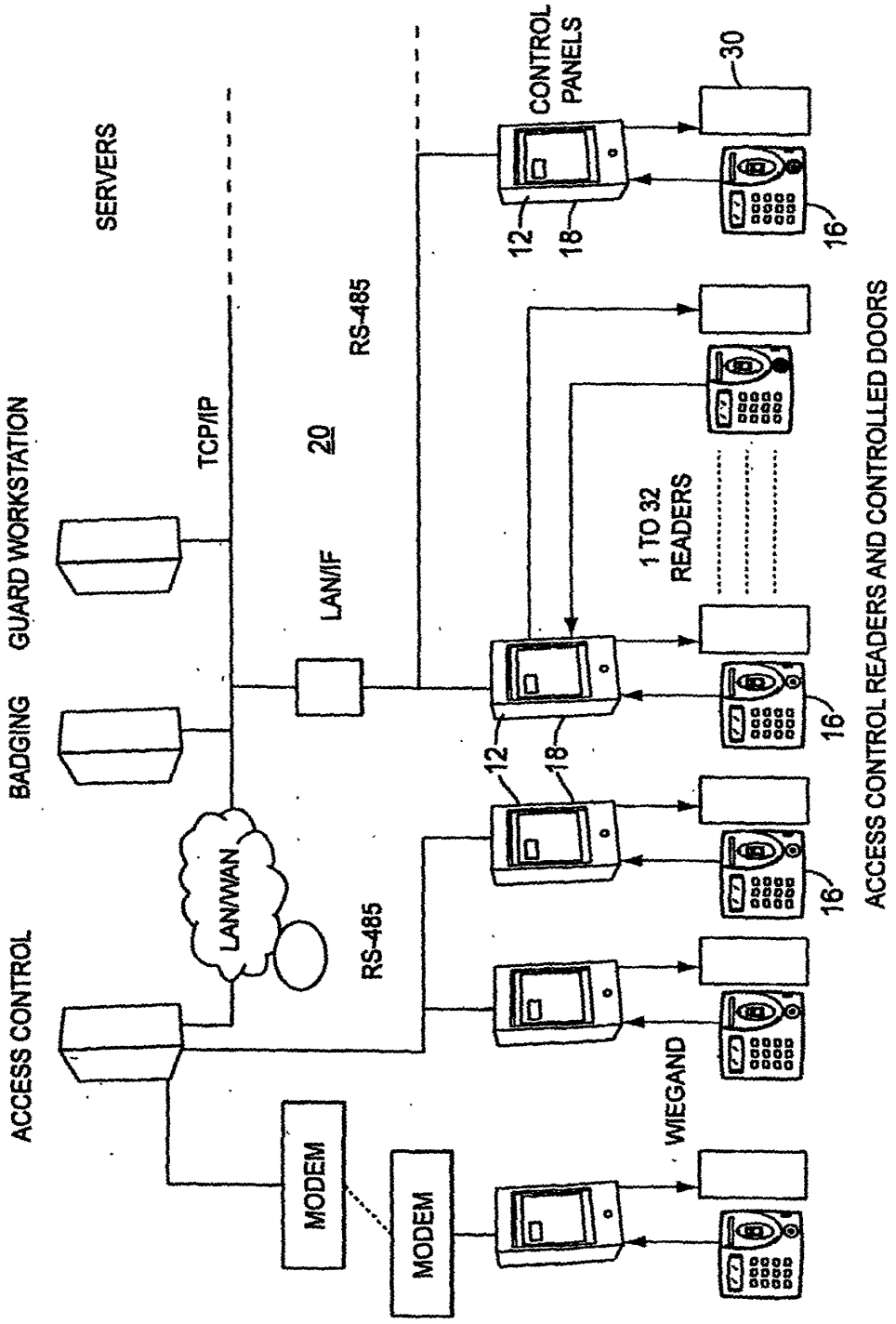


FIG. 10

WAVELYNX EX. 1003, Pg. 509
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

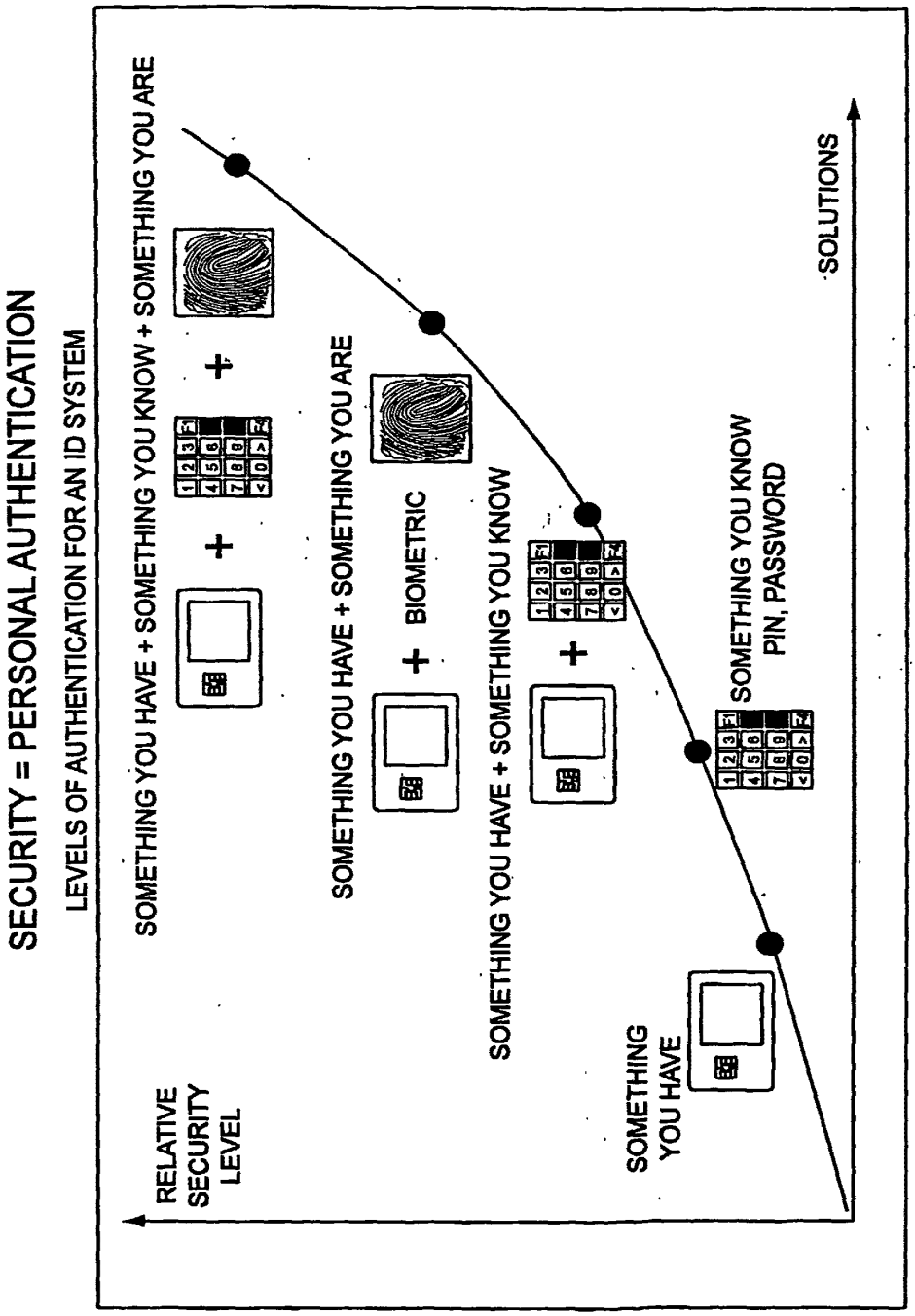


FIG. 11

WAVELYNX EX. 1003, Pg. 510
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

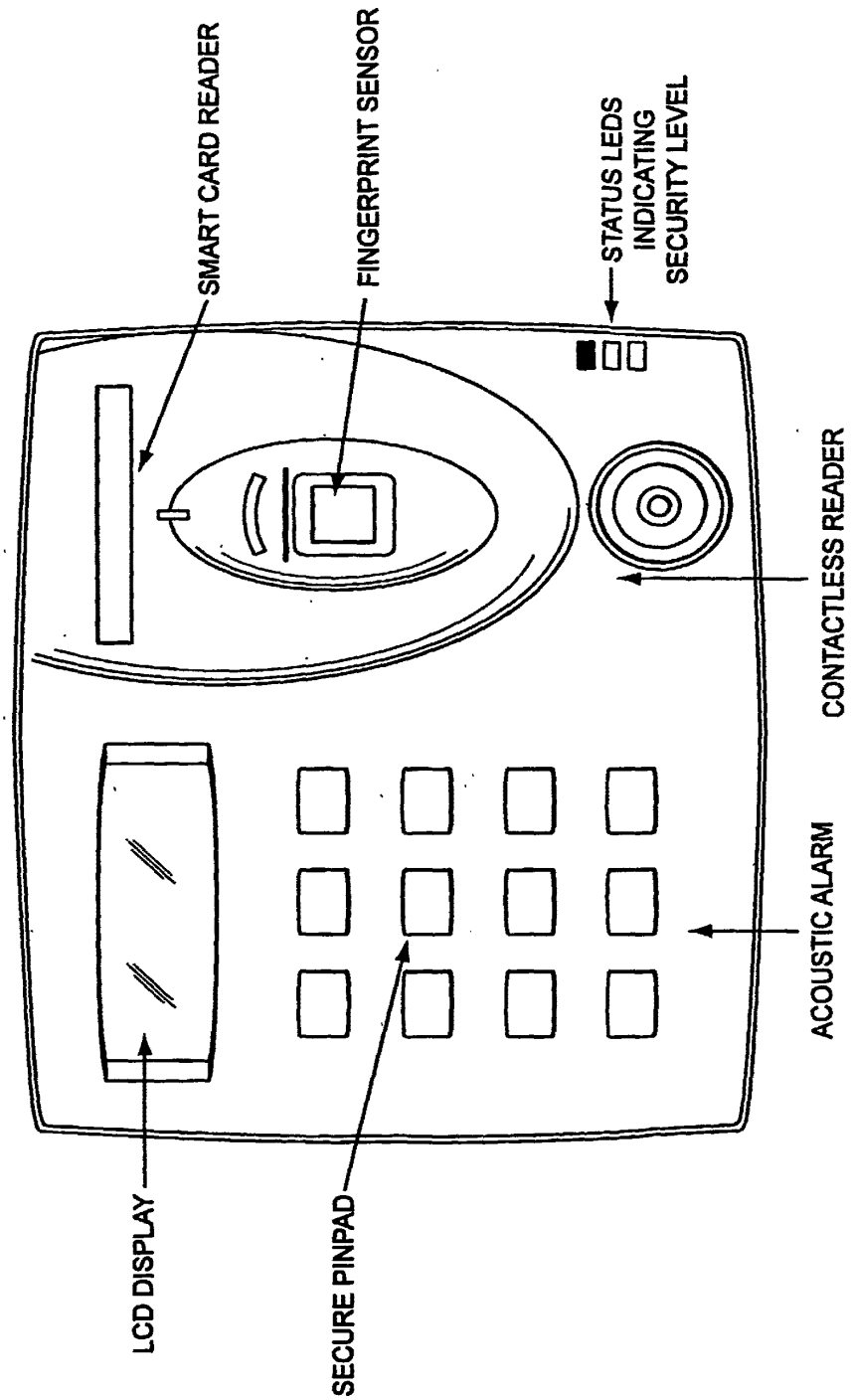


FIG. 12

WAVELYNX EX. 1003, Pg. 511
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

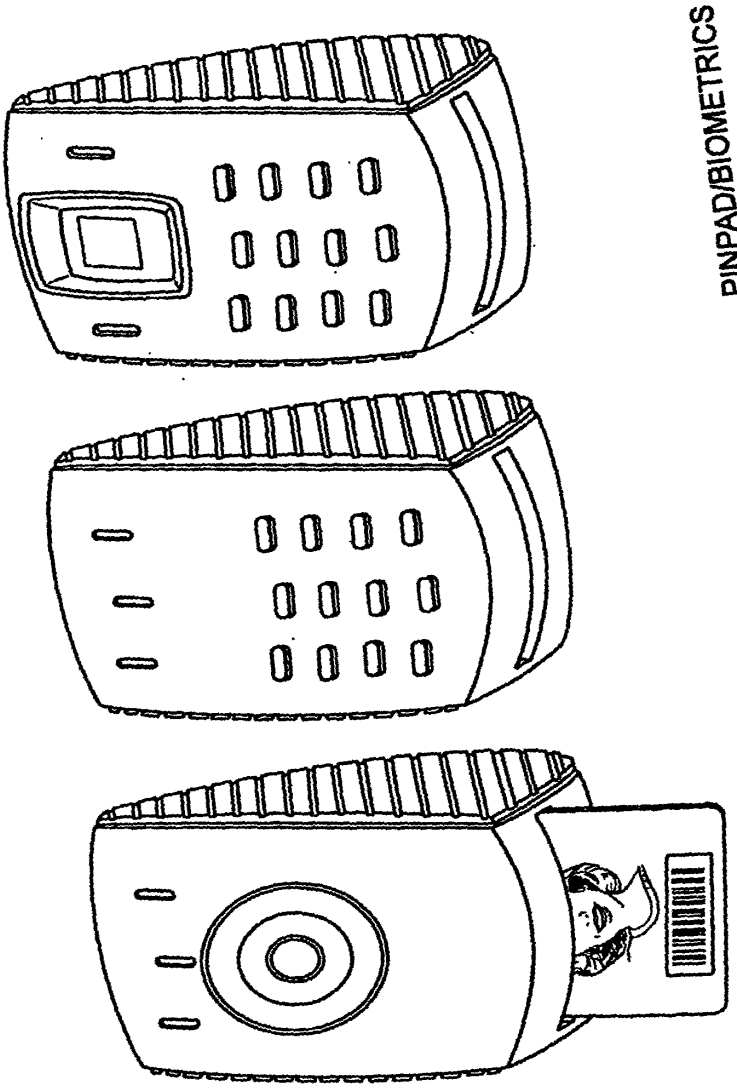


FIG. 13

WAVELYNX EX. 1003, Pg. 512
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

PCT/US2004/033926

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

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 7 G07C

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 practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 679 945 A (RENNER ET AL) 21 October 1997 (1997-10-21) cited in the application figures 2,6	1-11, 20-31
A	US 2002/110242 A1 (BRUWER FREDERICK JOHANNES) 15 August 2002 (2002-08-15) paragraph '0008!	1-11, 20-31
A	US 6 532 298 B1 (CAMBIER JAMES L ET AL) 11 March 2003 (2003-03-11) column 16, line 56 - column 17, line 21	1-11, 20-31
A	US 5 995 630 A (BORZA ET AL) 30 November 1999 (1999-11-30) column 11, line 12 - line 24	1-11, 20-31

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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
16 February 2005	24/02/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kemény, M

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/014642 A1 (MARTINSSON ROY ET AL) 16 January 2003 (2003-01-16) paragraph '0010!	1-11, 20-31
A	EP 1 237 091 A (FUJITSU LIMITED) 4 September 2002 (2002-09-04) paragraph '0028!	1-11, 20-31
A	WO 01/27723 A (HEWLETT-PACKARD COMPANY; VAMVAKAS, ATHANASIOS; PEARSON, SIANI; CHEN, L) 19 April 2001 (2001-04-19) page 2, line 1 - line 6 page 11, line 22 - page 12, line 26	1-11, 20-31

WAVELYNX EX. 1003, Pg. 514
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

PCT/US2004/033926

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5679945 A	21-10-1997	AU 5313896 A	16-10-1996
		CA 2217052 A1	03-10-1996
		WO 9630857 A1	03-10-1996
		US 6223984 B1	01-05-2001
US 2002110242 A1	15-08-2002	AU 2028602 A	01-07-2002
		EP 1354300 A2	22-10-2003
		WO 0250782 A2	27-06-2002
		ZA 200303622 A	21-06-2004
US 6532298 B1	11-03-2003	US 6483930 B1	19-11-2002
		US 6377699 B1	23-04-2002
		AU 6774200 A	17-04-2001
		WO 0120561 A1	22-03-2001
		AU 1615300 A	13-06-2000
		BR 9916864 A	21-08-2001
		CA 2350309 A1	02-06-2000
		EP 1153361 A1	14-11-2001
		JP 2002530976 T	17-09-2002
		NO 20012510 A	19-07-2001
		WO 0031679 A1	02-06-2000
		US 6424727 B1	23-07-2002
		US 2002131623 A1	19-09-2002
		ZA 200103797 A	10-05-2002
US 5995630 A	30-11-1999	WO 9838567 A1	03-09-1998
		EP 1012689 A1	28-06-2000
		CA 2198993 A1	07-09-1997
US 2003014642 A1	16-01-2003	AU 7695400 A	17-04-2001
		CN 1378667 T	06-11-2002
		EP 1228433 A1	07-08-2002
		JP 2003509771 T	11-03-2003
		WO 0120463 A1	22-03-2001
		EP 1480099 A2	24-11-2004
		SE 0001687 A	18-03-2001
EP 1237091 A	04-09-2002	WO 0142938 A1	14-06-2001
		EP 1237091 A1	04-09-2002
		US 2003005310 A1	02-01-2003
WO 0127723 A	19-04-2001	EP 1224518 A1	24-07-2002
		WO 0127723 A1	19-04-2001
		JP 2003511784 T	25-03-2003

Form PCT/ISA/210 (patent family annex) (January 2004)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 February 2006 (16.02.2006)

PCT

(10) International Publication Number
WO 2006/015625 A1

(51) International Patent Classification[7]: G06F 7/58

(21) International Application Number:
PCT/EP2004/051747

(22) International Filing Date: 9 August 2004 (09.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELECOM ITALIA S.P.A.** [IT/IT]; Piazza degli Affari, 2, I-20123 Milano (IT).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GOLIC, Jovan** [YU/IT]; c/o Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT).

(74) Agents: **MACCALLI, Marco** et al.; Maccalli & Pezzoli S.r.l., Via Settembrini, 40, I-20124 Milano (IT).

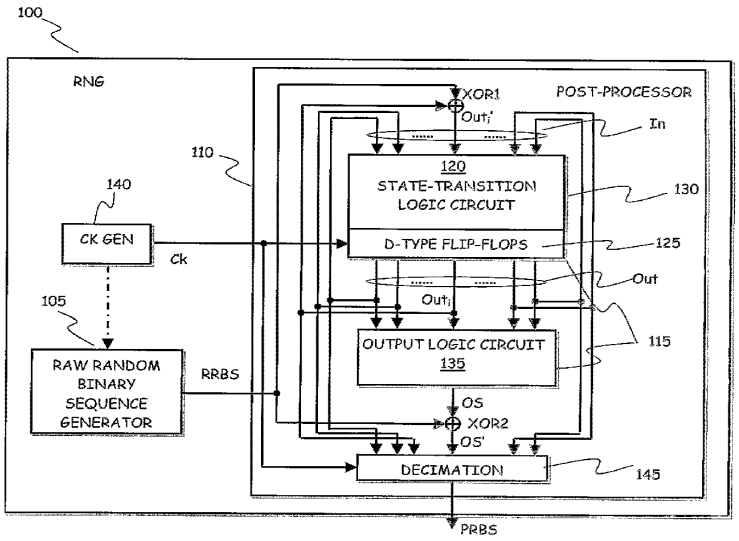
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR GENERATING RANDOM DATA



(57) Abstract: An apparatus for generating random data, comprising a raw random sequence source (105) adapted to generate a raw random sequence (RRBS) and a digital post processor (110) adapted to process said raw random sequence to generate said random data (PRBS), wherein said digital post-processor (110) comprises a synchronous fmite state machine (115) having at least one input adapted to repeatedly receive a current value of said raw random sequence and at least one output to provide a current output value (OS) depending on previous values of said raw random sequence.

WO 2006/015625 A1

METHOD AND APPARATUS FOR GENERATING RANDOM DATA

* * * * * * *

DESCRIPTION

Field of the invention

The present invention generally relates to a method and an apparatus for generating random data, in particular to a method and an apparatus for post-processing raw random binary sequences to obtain purely random and/or pseudo-random numbers.

Background of the invention

In many applications in the field of computers and other electronic devices there is a need for a physical source of true random numbers. Such applications include computer simulations of various probabilistic algorithms and processes, such as Monte Carlo numerical analysis, computer games, cryptographic algorithms and protocols whose security relies on the ability to generate unpredictable secret keys. High-speed truly random sequences are also needed for setting up countermeasures against so-called side-channel attacks against specific electronic devices, particularly microelectronic devices, implementing security schemes, such as integrated chip cards; such countermeasures include for example random masking of cryptographic functions, as well as generation of secret keys for the encryption of internal links and memories in such devices.

The output of a Random Number Generator (RNG) is typically a binary sequence that, in principle, has to be unpredictable in the sense of the information theory. Equivalently stated, it should be possible to statistically model the RNG output as a purely random sequence, *i.e.*, a sequence of mutually independent, uniformly distributed binary random variables (bits), with maximal possible entropy *per* bit. In particular, it should be computationally infeasible to distinguish the RNG output sequence from a purely random sequence or, equivalently, it should be computationally infeasible to predict the RNG output sequence.

Several techniques are known in the art for generating true random numbers. For practical reasons, RNGs implemented in the solid-state, semiconductor technology are preferable, because they can more easily be incorporated in Integrated Circuits (ICs), particularly digital ICs. A conventional type of hardware-based RNGs exploit thermal noise in resistors and/or shot noise in PN-junctions; regretfully, these RNGs include

WAVELYNX EX. 1003, Pg. 517
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

analog elements, and are therefore difficult to be incorporated in digital ICs. RNGs that can be implemented by digital integrated circuits only are therefore preferred; such RNGs are usually based on the phase jitter of free-running oscillators, implemented as ring oscillators (a structure consisting of an odd number of inverter logic gates connected in a circular cascade to form a ring). Another class of digital RNGs exploit the meta-stability of SR (Set-Reset) latches and edge-triggered flip-flops based on SR latches such as D-type flip-flops.

Typically, an RNG can be represented as essentially consisting of two parts, namely, a physical source of randomness, which produces a raw random binary sequence which is random, but not purely random, and a post-processing part, which produces the final output sequence by processing elements of the raw random binary sequence. This is disclosed for example in US 2003/0014452, and such an architecture is for example also recognizable in the circuits described in US 4,641,102, US 5,570,307, US 6,240,432, US 2002/0156819, and US 2002/0186086.

The raw binary sequence may have a high speed, but it typically has statistical weaknesses: individual bits in the sequence show a slight bias, *i.e.*, the probabilities of occurrence of the two binary output values, "0" and "1" are not equal, and/or bits in the sequence that are relatively close to each other in time are correlated to a certain degree.

The main objective of the post-processing part is to eliminate such statistical weaknesses from the raw random binary sequence, in the information-theoretic or at least in the computational sense. Eliminating statistical weaknesses in the information-theoretic sense means that each output bit should approximately convey one bit of information or entropy, a result possible to be achieved only by reducing the speed of the raw random binary sequence. Such post-processing is sometimes referred to as randomness extraction. Eliminating statistical weaknesses in the computational sense means that the output sequence need not be purely random, but it should be computationally infeasible or at least difficult to distinguish the output sequence from a purely random sequence. In this case, the speed need not be reduced.

Another important objective of post-processing is to provide robustness of the statistical properties of the RNG output sequence with respect to changes in operating conditions, such as voltage, temperature, and other environmental conditions, and also with respect to physical attacks against the physical source of randomness, particularly in case the raw random binary sequence is heavily biased.

WAVELYNX EX. 1003, Pg. 518
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Most of the techniques proposed so far for post-processing of raw random binary sequences are essentially linear in one way or the other. More precisely, the known techniques are typically based on sequential linear transformations implemented by synchronously clocked Linear Feedback Shift Registers (LFSRs) with additive inputs (which means that some of the LSFR internal signals are combined in XOR - eXclusive OR - with the raw binary sequence as an input signal), or on block linear transformations applied to the input raw random binary sequence to be post-processed. The Applicant observes that if the speeds of the LFSR clock signal and the input signal are the same, then this method is essentially known in digital communications as data scrambling and serves to improve the statistics of the input signal. A basic block transformation known in the art is the so-called Von Neyman extractor, which is capable of removing the bias from a raw random binary sequence, provided that the bits in the input raw random binary sequence are statistically independent. More precisely, the input bits are divided into non-overlapping pairs, and for each pair, the output bit is produced only if the two input bits in the pair are not equal and is equal to the first (or the second) input bit. Equivalently, the XOR operation is applied to individual input bit pairs: if the result is equal to zero, then the pair is discarded, and if it is equal to one, then the first (or the second) input bit is taken to the output. Consequently, even if the raw random binary sequence is purely random, the speed is reduced four times on average.

Randomness extraction techniques can be based on linear transformations only. However, these techniques may become insecure if the speed reduction is not sufficiently large.

The usage of general block linear transformations is suggested and analyzed in B. Barak *et al.*, "True Random Number Generators Secure in a Changing Environment," Cryptographic Hardware and Embedded Systems - CHES 2003, Lecture Notes in Computer Science, vol. 2779, pp. 166-180, 2003, which proposes a technique for digital post-processing of random data called randomness extraction that is based on a randomly chosen and fixed linear function, applied to blocks of input data, taken from any random number generator, to produce reduced-size blocks of output data. By using some known results on the so-called universal hash functions, it is proven that under certain conditions almost all such functions give rise to nearly uniform distributions of the corresponding blocks of output data. However, the Applicant argues that these mathematical results are not very meaningful for a fixed linear function, as there may exist families of linear

WAVELYNX EX. 1003, Pg. 519
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

functions that do not yield nearly uniform distributions of output blocks. Further, a nearly uniform distribution of output blocks does not imply a nearly uniform distribution of each (linear) transformation of output blocks. In addition, this sort of randomness extraction is not sufficiently robust, namely, it does not provide computational unpredictability of output data if the entropy of input data is significantly reduced by the adversary's action on the underlying random number generator. As the blocks have to be long, the implementation cost in terms of the gate count is considerable.

Most physical randomness sources are capable of generating raw random binary sequences that possibly have a high speed, but whose entropy rate (entropy content *per* bit) is not high. A general, well-known technique for producing a high-speed, but pseudo-random sequence calls for applying a randomness extractor to the raw random binary sequence, thereby reducing its speed, and then to use the obtained sequence to produce a random seed for a PRNG; an example of this general technique is provided in the already cited reference US 2003/0014452. The PRNG is clocked at a high speed to produce the final output sequence. The resulting output sequence is thus a pseudo-random sequence, generated from a truly random seed. Such a PRNG should be computationally secure (*i.e.*, its output sequence should be computationally unpredictable), and this makes the PRNG relatively complex to be implemented. For example, it can be based on cryptographic hash functions.

In US 6,581,078, a physical noise source produces digital signals that are combined with signals produced by a PRNG, through an additional memory and using an XOR gate. The combined signals are sent to the input of the PRNG. The resulting signals are allegedly unpredictable while exhibiting the intended statistical characteristics.

The Applicant observes that the speed of the PRNG is not specified, and that the requirements for the PRNG, except for the output statistics, are not specified in that document, and a linear, and hence insecure, PRNG based on a linear congruence is suggested to be used.

Summary of the invention

The Applicant is of the opinion that, in spite of the known solutions, a need remains for a new method and device for digital post-processing of random data that can be efficiently implemented by using only logic gates in digital semiconductor technology.

In particular, the Applicant has observed that in order to achieve computational

WAVELYNX EX. 1003, Pg. 520
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

security, the post-processing technique should not merely be a linear one, but should also incorporate non-linear transformations.

The Applicant has found that instead of using a randomness extractor to obtain a truly random sequence from a raw random binary sequence, and then a PRNG producing a pseudo-random sequence from a random seed periodically provided thereto by the randomness extractor, it is possible to avoid such a randomness extraction by directly applying the raw random binary sequence to a PRNG.

In particular, the Applicant has found that an efficient post-processing of a raw random binary sequence generated by a (physical) source of randomness can be carried out by operating a PRNG in a non-autonomous mode, *i.e.*, by continuously feeding the PRNG with the raw random binary sequence, in such a way that the output binary sequence is a purely random binary sequence if the input binary sequence is a purely random binary sequence. This condition ensures that the PRNG itself cannot introduce statistical weaknesses in the raw random binary sequence. For example, the feeding can be implemented *via* one or more additive inputs to PRNG through which the raw random binary sequence is supplied by means of XOR logic gate(s).

For the purposes of the present invention, by "non-autonomous" it is intended that at least one of the inputs to the device is received from a different device.

The PRNG may be a synchronous sequential circuit implementing a Finite-State Machine (FSM).

The proposed PRNG is structurally simple and fast, in order to be relatively easily implemented in hardware, and at the same time practically secure, in the sense that its output sequence is not easily predictable even if the raw random binary sequence is assumed to be known. In particular, this should be true if the PRNG is assumed to be operated in the autonomous mode, without the continuous feeding of the raw random binary sequence, which can typically be implemented by assuming that the raw random binary sequence consists of all zeros.

According to a first aspect of the present invention, an apparatus for generating random data is provided as set forth in appended claim 1, comprising a raw random sequence source adapted to generate a raw random sequence and a digital post-processor adapted to process said raw random sequence to generate said random data, wherein said digital post-processor comprises a synchronous finite-state machine having at least one input adapted to repeatedly receive a current value of said raw random sequence and at

WAVELYNX EX. 1003, Pg. 521
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

least one output to provide a current output value depending on previous values of said raw random sequence.

In an embodiment of the present invention, said digital post-processor further comprises a logic circuit suitable to receive said current output value and said current value of said raw random sequence and to provide a current output data as a function of said current output value and said current value of said raw random sequence, the random data being related to the sequence of said current output data.

Preferably, the apparatus further comprises a decimation circuit suitable to receive said output data and to generate said random data, said finite state machine being suitable to be clocked by a first clock signal, said decimation circuit operating according to a second clock signal that has a period that is k times the period of the first clock signal, k having a value variable in time, said value being calculated each time a random data is generated. In particular, said value of k at a given time depends on the current state of the finite-state machine.

Said logic circuit may comprise a latin-square type logic circuit. said latin-square type logic circuit may comprise an XOR gate.

In particular, said finite-state machine implements a state-transition function and comprises a state-transition sequential circuit having a set of inputs and a set of outputs, said set of outputs being suitable to provide current state values of said state-transition function, said set of inputs including said at least one input of said finite-state machine, said apparatus comprising a further logic circuit suitable to receive at least one of said current state values and said current value of said raw random sequence and to provide an input value for said state-transition sequential circuit.

Preferably, the finite-state machine is such that the output binary sequence is purely random if the input raw random sequence is purely random.

In a preferred embodiment of the present invention, the finite-state machine is such that the output binary sequence is computationally unpredictable even if the raw random sequence is known.

Even more preferably, the finite-state machine is such that a change in the first input bit of the input binary sequence induces a computationally unpredictable change in the subsequent output binary sequence.

In particular, said finite-state machine includes a plurality of synchronous delay logic units connected in a cascade one to another and clocked by the first clock signal, the

WAVELYNX EX. 1003, Pg. 522
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

plurality of synchronous delay logic units comprising a first and a last synchronous delay logic units in the cascade, said set of outputs comprising an output of the last synchronous delay logic unit and said set of inputs comprising an input of the first synchronous delay logic unit, said finite-state machine comprising a first feedback path from the output of the last synchronous delay logic unit to the input of the first synchronous delay logic unit, said plurality of synchronous delay logic units further comprising at least one intermediate synchronous delay logic unit in the cascade.

In an embodiment of the present invention, said finite-state machine comprises at least one second feedback path from said output of the last synchronous delay logic unit to an input of a respective synchronous delay logic unit in the cascade, said respective synchronous delay logic unit being chosen in the group consisting of the at least one intermediate synchronous delay logic unit and the last synchronous delay logic unit in the cascade.

In particular, the finite-state machine further comprises an XOR logic combination of said at least one second feedback path and the output of a preceding synchronous delay logic unit that precedes said respective synchronous delay logic unit where said at least one second feedback path terminates.

In an embodiment of the present invention, said at lest one second feedback path includes a plurality of feedback paths.

The finite-state machine has an output signal, said output signal is preferably extracted from a first internal state signal of the finite-state machine according to an irregular clocking. In particular, the irregular clocking is controlled by a clocking control signal, said clocking control signal being a logic combination of at least a second and a third internal state signals of the finite-state machine.

In an embodiment of the present invention, the output signal is a logic combination of the first internal state signal with at least a fourth and a fifth internal state values of the finite-state machine.

In an embodiment of the present invention, said raw random sequence source may comprise at least one further logic circuit corresponding to an associated finite-state machine having a state-transition function including states arranged to form cycles of states,

wherein:

the at least one further logic circuit has a set of logic circuit inputs and a set of

WAVELYNX EX. 1003, Pg. 523
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

logic circuit outputs fed back to said logic circuit inputs;

the associated finite-state machine is autonomous and asynchronous;

the state-transition function is void of loops; and

any of said cycles of states has either a minimum length equal to three states, in case the cycle is stable, or a minimum length of two states, in case the cycle is meta-stable.

In particular, said finite-state machine associated with the at least one further logic circuit has an output function, and the random binary sequence generator further comprises at least one further output logic circuit operatively connected to at least one of said logic circuit outputs of the at least one further logic circuit, the further output logic circuit having an output for providing an output signal by implementing said output function. The at least one of said logic circuit outputs has a value that cannot get stuck at a constant value.

The raw random sequence source may further comprise a sampling circuit for sampling said output signal.

In particular, the at least one further logic circuit comprises a plurality of asynchronous logic inversion units connected in cascade one to another, respectively.

Said plurality of asynchronous logic inversion units may comprise a first and a last asynchronous logic inversion units in the cascade, said set of logic circuit outputs comprising an output of the last asynchronous logic inversion unit and said set of logic circuit inputs comprising an input of the first asynchronous logic inversion unit, said at least one further logic circuit comprising a first feedback path from the output of the last asynchronous logic inversion unit to the input of the first asynchronous logic inversion unit.

Said plurality of asynchronous logic inversion units may further comprise at least one intermediate asynchronous logic inversion unit in the cascade, wherein said at least one logic circuit comprises at least one second feedback path from an output of a respective asynchronous logic inversion unit in the cascade to the input of the first asynchronous logic inversion unit, and wherein said respective asynchronous logic inversion unit is chosen in the group consisting of the first asynchronous logic inversion unit and the at least one intermediate asynchronous logic inversion unit.

In an embodiment of the present invention, the at least one further logic circuit further comprises an XOR logic combination of the first and the at least one second

WAVELYNX EX. 1003, Pg. 524
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

feedback paths.

In particular, said at least one second feedback path in the further logic circuit includes a plurality of second feedback paths.

The at least one further logic circuit may have an associated binary polynomial $f(x)$ defined as:

$$f(x) = \sum_{i=0}^{r} f_i x^i$$

wherein x^i corresponds to the output of the ith asynchronous logic inversion unit in the cascade, f_i is a feedback coefficient associated with the ith asynchronous logic inversion unit and indicative of the presence of the ith of said plurality of second feedback paths from said output of the ith inversion unit to the input of the first inversion unit, the summation being a binary addition, and the binary polynomial $f(x)$ satisfying the conditions:

$$f(x) = (1+x)h(x)$$

and

$$h(1)=1.$$

In another embodiment of the present invention, said plurality of asynchronous logic inversion units comprises at least one intermediate asynchronous logic inversion unit in the cascade, and said at least one further logic circuit comprises at least one second feedback path from said output of the last asynchronous logic inversion unit to an input of a respective asynchronous logic inversion unit, said respective asynchronous logic inversion unit being chosen in the group consisting of the at least one intermediate asynchronous logic inversion unit and the last asynchronous logic inversion unit in the cascade.

In particular, the at least one further logic circuit may further comprise an XOR logic combination of said at least one second feedback path and the output of a preceding asynchronous logic inversion unit that precedes said respective asynchronous logic inversion unit where said at least one second feedback path terminates.

Said at lest one second feedback path in the further logic circuit may include a plurality of feedback paths, and the logic circuit with feedback may have an associated binary polynomial $g(x)$ defined as:

WAVELYNX EX. 1003, Pg. 525
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$g(x) = \sum_{i=0}^{s} g_i x^i$$

wherein x^i corresponds to the output of the ith asynchronous logic inversion unit in the cascade, g_i is a feedback coefficient associated with the ith asynchronous logic inversion unit and indicative of the presence of the ith of said plurality of second feedback paths from said output of the last inversion unit to the input of the ith inversion unit, the summation being a binary addition, and the binary polynomial $g(x)$ satisfying the conditions:

$$g(x) = (1+x)k(x)$$

with s being odd.

In an embodiment of the present invention, the binary polynomial $g(x)$ satisfies the further condition:

$$k(1)=1.$$

Each of said asynchronous logic inversion units may comprises a given odd number of logic inverters.

In an embodiment of the present invention, the state-transition function associated with the at least one further logic circuit is an affine transformation, affine with respect to the binary field.

In particular, the generic element of the at least one logic circuit is selected from the group consisting of binary complement elements, binary identity elements and binary addition elements.

The sampling circuit may operate according to a timing signal, and may comprise a D-type flip-flop.

The at least one further logic circuit may comprise at least a first and a second further logic circuits, having respective output logic circuits operatively connected thereto and implementing the output function of the finite-state machine associated with the respective further logic circuit, the output logic circuits having each a respective output for providing an output signal by implementing said output function.

The raw random sequence source may further comprise a combination of the output signals of the output logic circuits for producing a combined output signal.

According to another aspect of the present invention, a method for generating random data as set forth in claim 19 is provided, comprising generating a raw random sequence and post-processing the raw random sequence so as to obtain said random data,

WAVELYNX EX. 1003, Pg. 526
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

wherein said post-processing the raw random binary sequence comprises continuously feeding the raw random binary sequence as an input to a synchronous state-transition sequential circuit.

Said feeding the raw random binary sequence may comprise:

feeding a current value of the raw random binary sequence to the state-transition sequential circuit of a finite-state machine by using a combination logic and

clocking the state-transition logic circuit to produce a next internal state value, said next internal state value depending on the current raw random binary sequence value and on the internal state value at a current time.

The method may further comprise obtaining a combined output value by combining a value related to said current internal state value with said current value of the raw random binary sequence.

The method may further comprise obtaining said random data by taking the combined output values at irregular time intervals.

Brief description of the drawings

The features and advantages of the present invention will be made apparent by the following detailed description of some preferred embodiments thereof, provided merely by way of non-limiting examples, description that will be conducted making reference to the attached drawings, wherein:

Figure 1 schematically shows, in terms of the relevant functional blocks, the general structure of a RNG including a post-processing circuit according to an embodiment of the present invention;

Figure 2 shows, still schematically but in greater detail, a possible implementation of the post-processing circuit of **Figure 1**, in an embodiment of the present invention;

Figure 3 schematically shows, in terms of the relevant functional blocks, the general structure of a raw random binary sequence generator according to an embodiment of the present invention;

Figure 4 shows a first possible implementation of the raw random binary sequence generator of **Figure 3**;

Figure 5 shows a second possible implementation of the raw random binary sequence generator of **Figure 3**; and

Figure 6 shows a third possible implementation of the raw random binary

WAVELYNX EX. 1003, Pg. 527
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

sequence generator of **Figure 3**.

Detailed description of the preferred invention embodiments

Referring to the drawings, in **Figure 1** the general structure of an RNG according to an embodiment of the present invention is schematically shown, in terms of the relevant functional blocks. The RNG, globally identified by **100**, includes a raw random sequence source **105**, particularly a raw random binary sequence generator, generating a raw random binary sequence **RRBS** that is supplied to a post-processing circuit **110** for being post-processed so as to generate a purely random binary sequence **PRBS**.

According to an embodiment of the present invention, the post-processing circuit **110** includes a Pseudo-Random Number Generator (PRNG, implemented by means of a Finite-State Machine - FSM -) **115**.

In an embodiment of the present invention, the FSM **115** includes a cascade of a logic (combinational) circuit **120** that implements a state-transition function, and is thus referred to as the state-transition logic circuit, and a plurality of delay units **125** connected in parallel, particularly D-type flip-flops. The cascade formed by the logic circuit **120** and the flip-flops **125** is called the state-transition sequential circuit **130**. In particular, the FSM **115** is synchronous, and receives, as a timing signal, a clock signal **Ck**, generated by a clock signal generator **140**. The clock signal **Ck** acts in particular as a trigger signal for the D-type flip-flops **125**.

The state-transition sequential circuit **130** has inputs **In** adapted to receive input signals carrying input values to the state-transition sequential circuit **130** and outputs **Out** adapted to provide output signals carrying output values of the state-transition sequential circuit **130** (In the following, reference symbols **In** and **Out** will be indifferently used for indicating both the inputs and outputs as well as the input and output signals, respectively.) Particularly, the output signals **Out** correspond to the outputs of the D-type flip-flops **125**. The values of the output signals **Out** vary according to the transition of states defined by the state-transition function, and such values, at a generic time, represent the current state of the FSM **115**; due to feedback, these values are also used as the values of the input signals **In** to determine the next state of the FSM **115** at the outputs of the logic circuit **120**. This next state is taken to the outputs of the state-transition sequential circuit **130** at the next time, that is, at the next edge of the clock signal **Ck**, to effectively become the next state of the FSM **115**.

WAVELYNX EX. 1003, Pg. 528
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The FSM **115** further includes an output logic circuit **135** connected to the output signals **Out** of the state-transition sequential circuit **130** and suitable to apply an output logic function to said output signals so as to produce an output signal **OS** of the FSM **115**.

According to an embodiment of the present invention, the raw random binary sequence **RRBS** generated by the raw random binary sequence generator **105** is continuously fed into the input to the FSM **115**. In particular, according to an embodiment of the present invention, the output value of the state-transition sequential circuit **130** is continuously combined with the value of the raw random binary sequence **RRBS**, and the value resulting from such a combination is fed back to the state-transition logic circuit **120** as an input thereto. Even more in particular, according to an embodiment of the present invention, assuming by way of non-limitative example that the raw random binary sequence **RRBS** is represented by an one-bit signal (*i.e.*, it is an one-bit stream), the raw random binary sequence **RRBS** is combined, for example by an XOR operation (implemented for example by a two-input XOR gate **XOR1**) with at least one, denoted as $\mathbf{Out_i}$ in the drawing, of the output signals **Out** of the state-transition sequential circuit **130**, thus obtaining a combined signal $\mathbf{Out_i'}$. The combined signal $\mathbf{Out_i'}$ is fed back, together with the other output signals **Out** of the state-transition sequential circuit **130**, to the inputs **In** thereof.

The input, raw random binary sequence **RRBS** is thus continuously introduced into the post-processing circuit **110**, in the example through an XOR operation, which, at each time, combines a current input bit (*i.e.*, one bit of the input raw random binary sequence **RRBS**) with at least one ($\mathbf{Out_i}$) bit selected from the bits representing the current internal state of the FSM **115**, and the result of the combination is fed back into the FSM **115** together with the other current internal state bits, so as to determine the value of the next internal state of the FSM **115**, at the next time (*i.e.*, at the next edge of the clock signal **Ck**).

It is observed that the adoption of an XOR operation (gate **XOR1** in the drawing) for combining the input raw random binary sequence **RRBS** with at least one selected output $\mathbf{Out_i}$ of the state-transition sequential circuit **130** is not to be considered limitative to the present invention: other types of combination are in fact possible. In particular, the input raw random binary sequence **RRBS** may be a multi-bit signal, and/or it might be combined with more than one of the outputs **Out** of the state-transition sequential circuit **130**.

WAVELYNX EX. 1003, Pg. 529
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The output signal OS obtained from the output logic circuit **135** has a current value that is thus derived from the current internal state of the FSM **115** and is hence related to the previous values of the input raw random binary sequence RRBS, but the current value of the output signal OS is not related to the current value of the input raw random binary sequence RRBS. The current value of the output signal OS is further combined again with the current value of the raw random binary sequence RRBS; in particular, the combination is an XOR operation, implemented for example by a two-input XOR gate **XOR2**. As a result of the combination, a modified output signal OS' is obtained, whose value is related to the current internal state of the FSM **115** (and thus to the previous values of the input raw random binary sequence **RRBS**) and also to the current value of the input raw random binary sequence **RRBS**.

More generally, when the raw random binary sequence **RRBS** and the output signal **OS** of the output function include more than one bit at a time, the combination of the output signal **OS** with the input raw random binary sequence **RRBS** may be accomplished by an operation of the so-called "latin square" type (a class of operations to which the XOR operation belongs), which, as already known to those skilled in the art, is defined in a such a way that each operand can be recovered from the result of the operation given the value of the other operand.

Preferably, according to an embodiment of the present invention, the state-transition function implemented by the state-transition logic circuit **120** and the output function implemented by the output logic circuit **135** are chosen so as to satisfy the so-called "computational unpredictability" criterion: it is difficult, ideally computationally infeasible, to predict the sequence of values of the modified output signal **OS'** when the input raw random binary sequence **RRBS** is a fixed and known sequence, such as the "all-zeros" sequence, the "all-ones" sequence or, more generally, any predefined known sequence of "0"s and "1"s. In other words, the state-transition and output functions are such that, when the PRNG is operated in the autonomous mode (without being fed with an input raw random binary sequence) or is fed with an input binary sequence that is fixed and known, then it produces, as the modified output signal **OS'**, an output sequence that is not easily predictable.

Preferably, according to an embodiment of the present invention, the at least one output signal $\mathbf{Out_i}$, *i.e.*, the corresponding internal state bit of the FSM **115** selected to be combined with the input raw random binary sequence **RRBS**, is chosen in such a way to

WAVELYNX EX. 1003, Pg. 530
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

satisfy the "propagation" criterion: for an arbitrarily chosen initial state of the FSM **115**, a change of the first bit in the input raw random binary sequence RRBS gives rise to a pseudo-random (*i.e.*, computationally unpredictable) change of the output bits in the output sequence OS' subsequent to the first output bit, that is, to a change difficult (ideally, computationally infeasible) to be predicted.

Moreover, the post-processing circuit **110** should satisfy the "randomness" criterion: the output sequence is purely random if the input sequence RRBS is assumed to be purely random. This condition is mathematically defined and can be controlled theoretically. In particular, a possible way to satisfy this criterion, as shown in **Figure 1**, calls for combining the output signal **OS** of the output logic circuit **135** with the input **RRBS** sequence by means of an XOR operation (implemented in the shown example by the XOR gate **XOR2**). The randomness criterion is then satisfied due to the fact that the current value of the modified output signal **OS'** is obtained by XOR-ing the current value of the input sequence **RRBS** with the current value of the output signal **OS**, which itself depends on the previous values of the input sequence **RRBS**, but not on the said current value of the input sequence **RRBS**. More generally, when the raw random binary sequence **RRBS** and the output signal **OS** include more than one bit at a time, their combination may be performed by using a "latin square".

In order to eliminate or substantially reduce the statistical weaknesses exhibited by the raw random binary sequence **RRBS**, as discussed in the introductory part of the present description, the post-processing circuit **110** needs to carry out a reduction in speed, *i.e.*, the output, purely random binary sequence **PRBS** should have a lower speed than the raw random binary sequence **RRBS**.

For this purpose, according to an embodiment of the present invention, the purely random binary sequence **PRBS** is obtained after applying the modified output signal **OS'** to a speed reduction circuit implemented as a decimation circuit **145**, which takes to the output only some values of the modified output signal **OS'** while discarding the other values, depending on the internal state sequence of the FSM **115**. In particular, the decimation circuit can be implemented by means of irregular clocking described below.

According to an embodiment of the present invention, the clock signal **Ck** that triggers the D-type flip-flops **125** of the FSM **115** may thus have a frequency that is the same as or even higher than the speed of the input sequence **RRBS** (expressed in bits *per* second). In particular, the clock signal **Ck** may be synchronous, or even coincide, with a

WAVELYNX EX. 1003, Pg. 531
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

timing (clock) signal used in the raw random binary sequence generator **105** to produce the raw random binary sequence **RRBS**. The reduction in speed needed for eliminating or substantially reducing the statistical weaknesses exhibited by the raw binary sequence **RRBS** is preferably achieved by means of an irregular clocking scheme: instead of taking the value of the modified output signal **OS'** at regular times (i.e., every period, or a fixed multiple of the period, of the clock signal **Ck**), the FSM **115** is each time clocked a variable number of times chosen from a set of at least two different numbers of times, *i.e.*, it is clocked a number of times that is either a first number of times or a second number of times, before each new value of the modified output signal **OS'** is made available as a value of the output sequence **PRBS**. In other words, the decimation circuit **145** implements an irregular clocking scheme according to which each new value of the output sequence **PRBS** is made available after a time which is a variable multiple k of the period of the clock signal **Ck** that clocks the FSM **115**, wherein said variable multiple k may take at least two different values. Such a decimation circuit is equivalent to a D-type flip-flop receiving at its input the output signal **OS'** and being clocked by an irregular clock signal, say **Ck'**, having a time-varying period, which at each time is a multiple k of the period of the clock signal **Ck**.

In particular, according to an embodiment of the present invention, the irregular clocking scheme is a self-clock-controlled scheme, implemented according to a clock-control sequence that is obtained by applying a specified function (preferably chosen in such a way so as not to violate the above-mentioned "computational unpredictability" and "randomness" criteria) to the internal state sequence; in other words, the decimation circuit **145** implements an irregular clocking scheme such that, at current time, the next value of said variable multiple k depends on the current internal state of the FSM **115**.

It is observed that a clock frequency higher than the speed of the input sequence **RRBS** means that each bit in the raw random binary sequence **RRBS** is actually repeatedly used at the input of the PRNG (*i.e.*, it is presented twice or more at the input of the PRNG), whereas a lower clock frequency would mean that some of the bits in the raw random binary sequence **RRBS** are discarded. Instead, irregular clocking of the PRNG means that some of its output bits are discarded. Altogether, the output speed (*i.e.*, the speed of the purely random binary sequence **PRBS**) can be higher than the input speed (the speed of the input raw random binary sequence **RRBS**) if the frequency of the clock signal **Ck** is sufficiently high.

WAVELYNX EX. 1003, Pg. 532
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

In an embodiment of the present invention, if the clock-control sequence is a two-valued, binary sequence, *i.e.*, if it includes only two different values, denoted as δ1 and δ2, then, each time an output bit is produced, the value of a clock-control bit (obtained by applying the specified function to the current FSM internal state) determines the number of times, δ1 or δ2, the D-type flip-flops should be clocked before the next output bit is produced. In this case, if the clock-control bit is not biased, then the expected reduction in speed due to the irregular clocking is (δ1 + δ2)/2 times.

Figure 2 shows, still schematically but in greater detail, a possible implementation of the post-processing circuit of **Figure 1**, in an embodiment of the present invention. In this invention embodiment, the PRNG comprises an LFSR, particularly a self-clock-controlled LFSR and, even more particularly, a self-clock-controlled LFSR in the so-called Galois configuration. Generally speaking, an LFSR is a cascade of a plurality of delay elements **D1**, ..., **Dr** (concisely, **Di**, with **i** = **1** to **r**), where **D1** is the last element and **Dr** the first element in the cascade (by convention, in the Galois configuration, the index identifying the generic delay element decreases from **r** to **1** in going from the first delay element to the last one in the cascade); the delay elements are typically formed by D-type flip-flops and are operated synchronously, being in particular clocked by a same clock signal, such as the clock signal **Ck**.

In a conventional Galois LFSR, the output **O1** of the last flip-flop **D1** forms a feedback signal, the signal **FB** depicted in **Figure 2**, that is fed as an input **Ir** to the first flip-flop **Dr**. In the circuit of **Figure 2**, the signal **FB** is also fed back to the input of at least another flip-flop in the cascade. In particular, feedback paths are provided that allow combining the feedback signal **FB**, preferably by means of two-input XOR gates $\mathbf{X_i}$ (with i= 1 to **r-1**, $\mathbf{X_{r-1}}$ being the first XOR gate in the cascade), with the output signal of the generic flip-flop **Di**, so as to produce the input signal to the subsequent flip-flop in the cascade. In particular, which ones of the output signals of the flip-flops **Di** in the cascade are combined in XOR with the feedback signal **FB** to obtain the input signal to the subsequent flip-flop is determined by an open/closed state of a plurality of switches $\mathbf{S_i}$ (with i= 1 to **r-1**, $\mathbf{S_{r-1}}$ being the first switch in the cascade); said open/closed state is specified by the assertion/deassertion of respective open/closed state control signals $\mathbf{t_i}$ (with i= 1 to **r-1**): when the generic control signal $\mathbf{t_i}$ is deasserted, *e.g.*, at a logic "0", the corresponding switch $\mathbf{S_i}$ is open and the output signal of the preceding flip-flop **D(i+1)** in the cascade is not XOR-ed with the feedback signal **FB**, being instead directly fed as an

WAVELYNX EX. 1003, Pg. 533
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

input to the subsequent flip-flop Di in the cascade; on the contrary, when the control signal t_i is asserted, *e.g.*, at a logic "1", the corresponding switch S_i is closed and the output signal of the preceding flip-flop D(i+1) in the cascade is XOR-ed with the feedback signal FB, and the resulting combination is fed as an input to the subsequent flip-flop Di in the cascade. In other words, the open/closed state of the generic switch S_i, as specified by the corresponding open/closed state control signal t_i, determines the effective number of feedback paths from the output of the last flip-flop D1 to the input of the other flip-flops (but the first) in the cascade.

It is observed that it is not necessary to materially implement (r-1) selectively activatable feedback paths, the activation of which is individually determined by the open/closed state of the respective switch: the open/closed state control signals t_i may in fact be regarded as binary-valued coefficients, each coefficient specifying, depending on the respective value ("1" or "0"), if the associated feedback path is materially provided or not, that is, whether or not there is provided the two-input XOR gate X_i. However, if all the possible feedback paths are provided for, selectively activatable by controlling the respective switches, the circuit is configurable, and greater flexibility is ensured.

According to an embodiment of the present invention, the Galois-like LFSR is made to operate in a non-autonomous manner, *i.e.*, it is fed with an input signal from the outside. In particular, in the exemplary invention embodiment of **Figure 2**, the output **O1** of the last flip-flop **D1** is combined, in particular XOR-ed, by the XOR gate **XOR1**, with the input raw random binary sequence **RRBS**, so as to produce the feedback signal **FB**. Thus, according to this embodiment of the present invention, the feedback signal **FB** carries not only information on the current state of the LFSR, but also depends on the input raw random binary sequence. It is observed that the specific flip-flop output chosen to be combined with the input raw random binary sequence **RRBS** is not *per-se* limitative to the present invention.

The output signal **OS** of the LFSR is obtained by combining, particularly XOR-ing (by means of a two-input XOR gate **X1**), a first signal $O'_{\gamma-1}$ taken from the output of the XOR gate $X_{\gamma-1}$ that is connected to the output of the γ-th flip-flop $D\gamma$, where $t_{\gamma-1} = 1$, with a second signal O_{jk} obtained as a combination of the further signals O_j and O_k taken from the outputs of two further flip-flops **Dj** and **Dk** in the cascade, respectively, particularly an OR combination performed by means of an OR gate **OR**. It is observed that nothing prevents from choosing, as the first signal, the output **O1** of the last flip-flop

WAVELYNX EX. 1003, Pg. 534
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

D1 XOR-ed with the input signal RRBS (*i.e.*, taking $\gamma = 1$), in which case the LFSR output signal OS is formed by XOR-ing the feedback signal FB with the output of the OR gate OR.

Comparing the structure of **Figure 2** with that of **Figure 1**, it is observed that the outputs of the flip-flops Dr,..., D1 in the cascade form the output signals Out of the state-transition sequential circuit **130**. The output logic circuit **135** is comprised of the OR gate OR and two XOR gates $X_{\gamma-1}$ and XOR1, and the XOR gate XOR2 functionally corresponds to the XOR gate X1.

The Galois-like LFSR of **Figure 2**, when clocked regularly (*i.e.*, when the output bits are taken at regular intervals, corresponding in particular to the period of the clock signal **Ck**), is a linear sequential circuit governed by linear equations, and whose output (*e.g.*, the output **O1** of the last flip-flop **D1**) is relatively easily predictable by solving the corresponding linear equations.

According to an embodiment of the present invention, in order to eliminate the linear predictability of the LFSR, the decimation circuit **145** is provided, adapted to implement an irregular clocking; in other words, the decimation circuit **145** is such that not all the bits in the output sequence **OS'** of the LFSR are taken in consideration: some of the bits in the LFSR output sequence **OS'** are instead discarded, but not regularly, rather according to an irregular clock-control scheme, particularly a self-clock-control scheme, determined by a clock-control signal.

In particular, according to an embodiment of the present invention, the decimation circuit **145** is adapted to implement the clock-control scheme in hardware, by means of a counting logic circuit, for example a multi-modulus (*e.g.*, a two-modulus) counter **205**, clocked by the clock signal **Ck**, and receiving a modulus selection signal **CkC**, that determines the modulus ($\delta 1$ or $\delta 2$) of the counter, in the example herein considered generated by combining, particularly XOR-ing in a XOR gate **X2**, the outputs $\mathbf{O}_{\tau 1}$ and $\mathbf{O}_{\tau 2}$ taken from the outputs of two flip-flops **Dτ1** and **Dτ2** in the cascade, respectively. More generally, the clock-control signal depends, according to a specified logic function, on the internal state of the LFSR, *i.e.*, on the values of the outputs of the different flip-flops. Preferably, the flip-flops **Dτ1** and **Dτ2** are chosen so that $\min(i,j,\gamma) > \max(\tau 1,\tau 2)$. The counter **205** has an output signal **C** that controls an enable input **E** of a D-type flip-flop **210**, which receives at a data input **D** the output signal **O** of the LFSR, and is clocked by the clock signal **Ck**, so that the output is produced only when the enable input **E** is

WAVELYNX EX. 1003, Pg. 535
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

active. The operation of the decimation circuit is thus equivalent to that of a D-type flip-flop with an always active enable input, but irregularly clocked by another clock signal Ck' with a time-varying period, which at each time is a multiple of the period of the clock signal Ck, the multiple taking values δ1 or δ2 in this particular example. The output Q of the flip-flop **210** forms the output **PRBS** of the post-processing circuit **110**.

The clock-control signal CkC takes the form of a binary sequence, so that, each time an output bit is produced in the output sequence **PRBS**, the values, at that time, of the two outputs $O_{\tau 1}$ and $O_{\tau 2}$ taken from the outputs of two flip-flops $D\tau 1$ and $D\tau 2$ in the cascade determine the value of the clock-control signal **CkC**, which in turn determines the number of times, δ1 or δ2 in the example herein considered, the LFSR should be clocked in order to produce the next output bit (by accordingly setting the two-modulus counter so as to count up to δ1 or δ2 before the signal C controlling the enable input E is asserted).

Since the clock-control signal **CkC** bit is not biased, the expected speed of the output sequence **PRBS** is (δ1 + δ2)/2 times smaller than the frequency of the clock signal **Ck**.

The number r of flip-flops in the cascade, *i.e.*, the length of the LFSR, and the feedback paths from the output of the last flip-flop in the cascade to the input of the other flip-flops, affect the period of the binary sequence, *e.g.*, of the sequence appearing at the output **O1** of the flip-flop **D1** (however, any other flip-flop output may be considered), as well as the statistical properties thereof, when the input **RRBS** sequence is assumed to consist of all zeros. A convenient way to analyze the circuit of **Figure 2** is to represent the feedback coefficients by means of a binary "feedback" polynomial *t(x)*:

$$t(x) = \sum_{i=0}^{r} t_i x^i$$

wherein x^i corresponds to the generic flip-flop output, **i** varies from 0 to r, the summation is binary (*i.e.*, it is a modulo-2 addition), and $\mathbf{t_0} = \mathbf{t_r} = 1$. A condition ensuring that an LFSR is capable of generating binary sequences with maximal period (equal to $2^r - 1$) and good statistical properties is that the feedback coefficients are chosen in such a way that the feedback polynomial is a primitive polynomial.

Merely by way of example, a practical implementation of the solution presented in **Figure 2** may provide for having an oscillator structure having the following binary polynomial *t(x)* (the number of flip-flops **r** = 64):

WAVELYNX EX. 1003, Pg. 536
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$$t(x) = 1 + x + x^2 + x^4 + x^6 + x^{11} + x^{13} + x^{14} + x^{16} + x^{23} + x^{24} + x^{27} + x^{33} + x^{41} + x^{48} + x^{51} + x^{54} + x^{56} + x^{57} + x^{58} + x^{59} + x^{60} + x^{64}$$

with $j = 58$, $k = 51$, $\gamma = 42$, $\tau 1 = 30$, $\tau 2 = 17$, $\delta 1 = 3$, and $\delta 2 = 5$.

In the following, a possible implementation of the raw random binary sequence generator **105** is described, making reference to **Figures 3** to **5**; however, it is pointed out that the specific structure of the raw random binary sequence generator is not limitative to the present invention, and the post-processing implemented by the post-processing circuit **110** can be applied to any raw random binary sequence **RRBS**, irrespective of the way it is generated in.

Referring now to **Figure 1**, the general structure of the raw random binary sequence generator **105** according to an embodiment of the present invention is schematically shown, in terms of the relevant functional blocks. The raw random binary sequence generator **105** includes a logic (*i.e.*, combinatorial) circuit with feedback **315**, having a set of logic circuit inputs, for receiving input signals **InS** to the logic circuit, and a set of logic circuit outputs, for providing output signals **OutS**, which are fed back to the logic circuit inputs. The logic circuit with feedback **315** corresponds to an associated Finite-State Machine (FSM) having a state-transition function. In particular, the logic circuit with feedback **315** implements the state-transition function of an autonomous FSM, *i.e.*, an FSM that receives no external inputs: all the inputs of the logic circuit **315** receive in feedback input signals, whose values represent the current state of the FSM, respective output signals of the logic circuit **315**, whose values represent the next state of the FSM.

The logic circuit with feedback **315** is asynchronous, *i.e.*, it is operated without a timing or clock signal, and it evolves through the succession of states in a manner that is not synchronous with a specific timing signal, but rather according to the delays of the constituent logic gates.

In particular, the state-transition function implemented by the logic circuit with feedback **315** is, in the mathematical sense, an affine transformation with respect to the binary field. As is generally known, an affine transformation or affine map between two vector spaces consists of a linear transformation followed by a translation. In the binary case, a linear transformation is composed of binary linear functions, where a binary linear function is a binary (XOR) sum of a subset of input variables, whereas an affine transformation is a linear transformation whose output variables are allowed to be

WAVELYNX EX. 1003, Pg. 537
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

complemented. Note that a binary complement of a binary variable is equal to the binary sum of this variable and the constant 1.

The logic circuit with feedback **315** is then composed of combinatorial logic elements; preferably, the generic combinatorial logic element of the logic circuit with feedback **315** is either a binary complement element (*e.g.*, an inverter), or a binary identity element, or a binary addition element (*e.g.*, an XOR logic gate).

In particular, to avoid feedback loops not involving any logic gate, the binary identity element is implemented by delay units, for example, composed of an even number of logic inverters.

The values of the logic circuit output signals **OutS** vary following the evolution of the logic circuit with feedback **315** through the corresponding sequence of states. The output signals **OutS** are fed to an output logic circuit **320**, that implements an output logic function to be applied to the output signals **OutS** of the logic circuit with feedback **315**, so as to produce an oscillating output signal **OutSig**. The logic circuit with feedback **315** and the output logic circuit **320** implement together an autonomous FSM operated asynchronously.

The oscillating output signal **OutSig** is fed to a sampling unit **325**, operated by the timing or clock signal **Ck** generated for example by the clock signal generator **140** (although a different clock signal might be used); the sampling unit **325** is adapted to sample the oscillating output signal **OutSig** at a rate determined by the frequency of the clock signal **Ck**. The sampling unit **325** may for example comprise a D-type flip-flop, receiving at a data input thereof the oscillating output signal **OutSig** and being clocked by the clock signal **Ck**. In particular, the clock signal **Ck** may, for example, be the system clock of an Integrated Circuit (IC – not shown in the drawing) in which the RNG **100** is incorporated, for example, an IC for a smart card; alternatively, the clock signal **Ck** may be generated by means of an independent, free-running ring oscillator.

At the output of the sampling unit **325**, the raw random binary sequence **RRBS** is obtained.

In particular, according to an embodiment of the present invention, the logic circuit with feedback **315** is such that no fixed points exist in its state-transition function. As known in the art, a state-transition function can be represented by a state-transition diagram, in which each state is connected by a directed branch to its corresponding next state, which is uniquely determined by the state-transition function. Adopting such a

WAVELYNX EX. 1003, Pg. 538
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

representation, the condition of the absence of fixed points in the state-transition function translates into the absence of loops in the state-transition diagram, wherein by loop there is intended a single state together with a single directed branch leaving from and re-entering into that state. If a fixed point exists in the state-transition function, the logic circuit with feedback **315** may, and in fact is likely to, get stuck in the corresponding state, in which case the output signals **OutS** would no more oscillate, having instead a constant value, thus producing a constant raw binary sequence. The condition of the absence of fixed points guarantees instead that the logic circuit with feedback **315** never gets stuck in a fixed state and thus oscillates among a number of states, so that the produced raw binary sequence does not have a constant value.

It is observed that the above-mentioned condition of the absence of fixed points in the state-transition function reflects on the internal structure of the logic circuit with feedback **315**: for example, a logic circuit with feedback **315** having a structure similar to that of an LFSR, but operated asynchronously, with delay elements instead of synchronous D-type flip-flops, is not suitable, because the corresponding state-transition function has a fixed point, being a state composed of all zeros.

Also, still in order to avoid that the output signal **OutSig** remains constant, the output logic circuit **320** should be such that the output function it implements effectively depends on the parts of the internal state (*i.e.*, on subsets of the output signals **OutS**) that do not get stuck at a fixed value, as the condition of the absence of fixed points does not imply that there are not parts of the internal state that can get stuck at a fixed value.

The described arrangement allows obtaining an output signal **OutSig** that is guaranteed to oscillate, and that not only exhibits digital pseudo-randomness properties similar to those of the output sequence of the same FSM when assumed to be operated synchronously, clocked by a clock signal, but, thanks to the asynchronicity, the output signal **OutSig** also exhibits randomness properties, due to unpredictable variations in the delay of logic gates in the logic circuit with feedback **315**, delay variations being further propagated and enhanced through feedback, and, possibly, also to internal meta-stability events due to feedback as well. For example, delay variations may derive from fluctuations in operating voltage and temperature, because of various internal and external noise factors.

Advantageously, in addition to the pseudo-randomness and randomness properties of the output signal **OutSig**, additional randomness is introduced in the raw random

WAVELYNX EX. 1003, Pg. 539
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

binary sequence RRBS thanks to meta-stability that is induced within the sampling unit 325. For example, such meta-stability events are frequent if the following two conditions are met.

Firstly, the delay-to-rise time ratio of the oscillating output signal OutSig should be relatively small, which means that the delays of the internal logic gates of the logic circuit with feedback 315 are relatively short, which further means that the basic oscillating frequency of the output signal OutSig is relatively high. The basic oscillating frequency is reciprocal to the total logic delay in the shortest feedback loop present in the logic circuit with feedback 315. If such a condition is met, it is likely that many transitions in the oscillating output signal **OutSig** cannot be completed to the digital, binary level, so that this signal is likely to exhibit unpredictable variations on the analog as well as digital level; in other words, the oscillating output signal **OutSig** is not just a sequence of pure (full value) high and low voltage values corresponding to the digital values of 1 and 0, but rather it is more like a sort of analog noise.

Secondly, unlike the known solutions exploiting ring oscillators, the sampling rate of the oscillating output signal **OutSig**, corresponding to the frequency sampling clock signal **Ck**, instead of being much smaller than the basic oscillating frequency of the oscillating output signal **OutSig** to be sampled, is preferably similar to this frequency. Therefore, if the output signal **OutSig** has a relatively small delay-to-rise time ratio, then so does the clock signal **Ck**.

As a consequence of the two conditions defined above, the characteristic setup and/or hold times for the sampling D-type flip-flop are frequently violated. This in turn introduces additional randomness into the raw random binary sequence, due to frequent meta-stability events occurring in the sampling D-type flip-flop, maintaining the high speed of the oscillating output signal **OutSig**. As a result, a high-speed raw random binary sequence **RRBS** that contains a high amount of entropy *per* bit is thus obtained at the output of the sampling unit **325**. In other words, the entropy rate (*i.e.*, the amount of entropy *per* second) of the raw random binary sequence **RRBS** is high, as desired.

The degree of pseudo-randomness existing in the raw random binary sequence **RRBS** depends on the particular state-transition function of the FSM implemented by the logic circuit with feedback **315**. In particular, for obtaining an oscillating output signal **OutSig** having a long period and good statistical properties, in synchronous operation, an additional requirement for the FSM is that the corresponding state-transition diagram

WAVELYNX EX. 1003, Pg. 540
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

contains only relatively long cycles. However, it is observed that also short cycles may be allowed, even cycles of length 2, composed of only 2 states, provided that such short cycles are meta-stable in the asynchronous operation, which means that it is practically impossible that the state sequence gets stuck in one of them by oscillating among the corresponding states. By way of comparison, a conventional ring oscillator, irrespective of the number of cascaded inverters, can always be equivalently reduced to a logic circuit with feedback containing only one logic inverter with an appropriate delay, so that the underlying state-transition diagram then has only one cycle of length 2, which is stable.

The good pseudo-randomness properties expected for the synchronous operation are translated into the corresponding pseudo-randomness properties corresponding to the asynchronous operation of the FSM, which, together with the introduced randomness properties described above, provide an increased degree of robustness, *i.e.*, insensitivity to changes in the statistics of the underlying random variations in the delay of internal logic gates, in comparison with conventional ring oscillators.

Hereinafter, three possible practical implementations of the random binary sequence generator **105** will be presented, being intended that the three implementations that will be discussed are to be intended as merely exemplary, not at all limitative, and that other implementations are possible.

Referring firstly to **Figure 4**, a plurality of, *e.g.*, *r*, logic inversion units $\mathbf{400_1}$, $\mathbf{400_2}$, ..., $\mathbf{400_{(r-1)}}$, $\mathbf{400_r}$ are connected in cascade one to another. Except for the last inversion unit $\mathbf{400_r}$ in the cascade, the output of each inversion unit $\mathbf{400_1}$, $\mathbf{400_2}$, ..., $\mathbf{400_{(r-1)}}$ is directly used as the input to the next inversion unit.

A plurality of feedback paths from the outputs of the inversion units to the input of the first inversion unit $\mathbf{400_1}$ in the cascade are provided. In particular, the output signal $\mathbf{405_r}$ of the last inversion unit $\mathbf{400_r}$ in the inversion units cascade, said output signal $\mathbf{405_r}$ corresponding to the oscillating output signal **OutSig** of the raw random binary sequence generator **105**, is fed back as an input signal $\mathbf{I_1}$ to the first inversion unit $\mathbf{400_1}$ of the inversion unit cascade; along the feedback path, said output signal $\mathbf{405_r}$ is combined, particularly according to XOR operations (performed, for example, by two-input XOR gates $\mathbf{410_1}$, $\mathbf{410_2}$, ..., $\mathbf{410_{(r-1)}}$), with one or more of the output signals $\mathbf{405_1}$, $\mathbf{405_2}$, ..., $\mathbf{405_{(r-1)}}$; which ones of the output signals $\mathbf{405_1}$, $\mathbf{405_2}$, ..., $\mathbf{405_{(r-1)}}$ are combined in XOR operation with the output signal $\mathbf{405_r}$ to obtain the input signal $\mathbf{I_1}$ to the first inversion unit $\mathbf{400_1}$ is determined by the open/closed state of one or more of a plurality of switches $\mathbf{415_1}$, $\mathbf{415_2}$,

WAVELYNX EX. 1003, Pg. 541
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

..., $415_{(r-1)}$; said open/closed state is specified by the assertion/deassertion of open/closed state control signals f_1, f_2, ..., f_{r-1}: when the generic control signal f_i ($i = 1, 2, ..., r-1$) is deasserted at a logic "0", the corresponding switch 415_i is open and the output signal 405_i is not XOR-ed with the output signal 405_r of the last inversion unit 400_r; on the contrary, when the control signal f_i is asserted at a logic "1", the corresponding switch 415_i is closed and the output signal 405_i is XOR-ed with the output signal 405_r of the last inversion unit 400_1. In other words, the open/closed state of the switches 415_1, 415_2, ..., $415_{(r-1)}$, as specified by the logic state of the open/closed state control signals f_1, f_2, ..., f_{r-1}, determines the feedback paths from the outputs of the inversion units to the input of the first inversion unit of the cascade.

In a practical implementation, the generic inversion unit 400_i is, for example, formed by an elementary inverter, *e.g.*, a CMOS inverter, or, alternatively, by an odd number of elementary inverters in a series; this latter construction may be in some circumstances preferable, because in this way the designer may individually adjust the transmission delay of the single inversion unit in the cascade. However, it is pointed out that the specific construction of the inversion units is not limitative to the present invention: in general, any logic circuit acting as a logic inverting delay unit can be exploited.

It is observed that, in practice, it is not necessary to materially implement (r-1) selectively activatable feedback paths, the activation of which is individually determined by the open/closed state of the respective switch: the open/closed state control signals f_1, f_2, ..., f_{r-1} may in fact be regarded as binary-valued coefficients, each coefficient specifying, depending on the respective value, if the associated feedback path is materially provided or not. In other words, the output of the last inversion unit 400_r, together with the outputs of the preceding inverters as specified by the coefficients f_i being equal to "1" are XOR-ed together to form the feedback signal defining the input I_1 to the first inverter 400_i in the cascade; the outputs of those inversion units in the cascade corresponding to the coefficients f_i equal to "0" are instead not used to form the feedback signal.

However, if all the possible feedback paths are provided for, selectively activatable by controlling the respective switches, the circuit results to be configurable, and greater flexibility is ensured.

It is also observed that although in the exemplary implementation herein described

WAVELYNX EX. 1003, Pg. 542
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018