



US007194090B2

(12) **United States Patent**
Muratani et al.

(10) **Patent No.:** **US 7,194,090 B2**
(45) **Date of Patent:** **Mar. 20, 2007**

(54) **ENCRYPTION APPARATUS, DECRYPTION APPARATUS, EXPANDED KEY GENERATING APPARATUS AND METHOD THEREFOR, AND RECORDING MEDIUM**

(75) Inventors: **Hirofumi Muratani**, Kawasaki (JP);
Masahiko Motoyama, Yokohama (JP);
Kenji Ohkuma, Yokohama (JP);
Fumihiko Sano, Fuchu (JP); **Shinichi Kawamura**, Kodaira (JP)

(73) Assignee: **Kabushiki Kaisha Toshiba**, Kawasaki (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 756 days.

(21) Appl. No.: **09/902,696**

(22) Filed: **Jul. 12, 2001**

(65) **Prior Publication Data**
US 2002/0021802 A1 Feb. 21, 2002

(30) **Foreign Application Priority Data**
Jul. 12, 2000 (JP) 2000-211686

(51) **Int. Cl.**
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **380/29**; 380/21; 380/42;
380/44; 380/45

(58) **Field of Classification Search** 380/29,
380/21, 42, 44, 45
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,202,922 A 4/1993 Iijima

5,432,848 A * 7/1995 Butter et al. 380/2
5,745,577 A * 4/1998 Leech 380/28
5,796,837 A * 8/1998 Kim et al. 380/28
5,825,886 A * 10/1998 Adams et al. 380/28
5,933,501 A * 8/1999 Leppek 380/259
6,185,679 B1 * 2/2001 Coppersmith et al. 713/150
6,189,095 B1 * 2/2001 Coppersmith et al. 713/150
6,243,470 B1 * 6/2001 Coppersmith et al. 380/259

FOREIGN PATENT DOCUMENTS

EP 0982895 A2 * 1/2000
EP 0 982 895 3/2000
WO WO 99/14889 3/1999
WO WO 00/22777 4/2000

OTHER PUBLICATIONS

B. Schneier, Applied Cryptography, Second Edition, pp. 270-277, XP-002237575, 1996.

Alfred J. Menezes, et al., Handbook of Applied Cryptography, Chapter 7 Block Ciphers, pp. 250-259.

* cited by examiner

Primary Examiner—Ayaz Sheikh

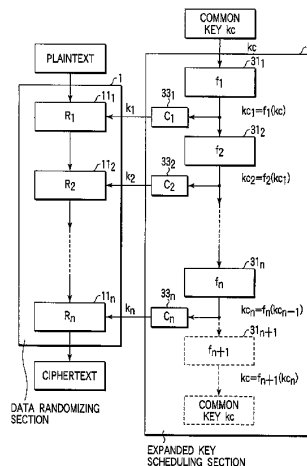
Assistant Examiner—Kaveh Abrishamkar

(74) *Attorney, Agent, or Firm*—Oblon, Spivak, McClelland, Maier & Neustadt, P.C.

(57) **ABSTRACT**

Expanded key schedule circuit for common key encryption system in which expanded keys are used in a predetermined order in data randomizing process for encryption and in a reversed order in data randomizing process for decryption, comprises round processing circuits connected in series. The round processing circuits subject the common key or sub key of a previous stage to a round function to output a sub key. The sub key of the last stage is equal to the common key. The expanded keys are generated from the sub keys.

24 Claims, 32 Drawing Sheets



1

ENCRYPTION APPARATUS, DECRYPTION APPARATUS, EXPANDED KEY GENERATING APPARATUS AND METHOD THEREFOR, AND RECORDING MEDIUM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims the benefit of priority from the prior Japanese Patent Application No. 2000-211686, filed Jul. 12, 2000, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an encryption apparatus and decryption apparatus which employ a plurality of expanded keys in reverse order for encryption and for decryption, and expanded key scheduling apparatus and method therefor, and recording medium storing a computer program therefor.

2. Description of the Related Art

The importance of an encryption technique becomes very high for the purpose of security control of computerized information, in particular, such as information on copyright or information on privacy. Such encryption technique is actually utilized in a variety of forms in a variety of fields.

There are various encryption systems, one of which is a common key encryption system. In the common key encryption system, decryption is carried out by employing a key (common key or secret key) that is identical to a key employed for encryption.

There are various common key encryption systems, one of which is a system employing an expanded key. This system generates a plurality of expanded keys whose total number of bits is greater than the number of bits that it has based on a common key.

In one of the expanded key scheduling systems, a round function (stage function) is acted with respect to a common key, and expanded key is generated based on its output value. Further, a round function is acted with the output value, and a next expanded key is generated based on its output value. Furthermore, a round function is acted with the output value. In this way, round functions are acted one after another, and expanded keys are sequentially generated. Such system is called a round system here.

A common key encryption system employing such expanded key scheduling system includes a common key block encryption system, for example. The common key block encryption system has a structure in which round functions are acted with block data with a predetermined bit length that is a processing unit one after another, with respect to a data randomizing section as well, thereby carrying out encryption or decryption. A typical basic structure of the above encryption system includes a SPN type and Feistel type or the like.

If a round system is employed for generating an expanded key, for example, as in block encryption, it is required to employ an expanded key in an order reversed from an order employed for encryption.

Now, problems with such system will be described here.

FIG. 48 shows an exemplary configuration of an expanded key scheduling section of a conventional encryption apparatus. The generating section comprises round processors **1001₁** to **1001_n**, connected in series and expanded

2

key converters **1005₁** to **1005_n**, respectively connected to outputs of the expanded key processors **1005₁** to **1005_n**.

At a data randomizing section, an expanded key (1) is required for an encryption process. Because of this, a round function (1) is acted with a common key, and its output value is obtained. Then, an expanded key conversion (1) is acted with the output value, and an expanded key (1) is obtained. A data randomizing section carries out an encryption process by employing this expanded key (1).

At the data randomizing section, an expanded key (2) is required for an encryption process. Because of this, a round function (2) is acted with an output value of the round function (1), and its output value is obtained. Then, an expanded key conversion (2) is acted with the output value, and an expanded key (2) is obtained. The data randomizing section carries out an encryption process by employing this expanded key (2).

Subsequently, an expanded key is generated by an expanded key scheduling section, and an encryption process is carried out by the data randomizing section in the same way.

Now, processing for decryption will be described here.

For decryption, it is required to employ an expanded key in an order reversed from that for encryption, i.e., in order from expanded key (n) to expanded key (1). However, in a conventional decryption apparatus having an expanded key scheduling section with its configuration similar to that shown in FIG. 48, expanded keys are generated in order from expanded key (1) to expanded key (n). Because of this, for example, prior to processing of the data randomizing section, there has been a need to generate all the expanded keys and store them in a memory.

However, there has been a problem that a device having only poor hardware environment such as IC card, for example, does not have a sufficient storage space for storing all the expanded keys required for decryption.

To overcome this problem, there is proposed an expanded key scheduling section shown in FIG. 49. The generating section comprises the round processors **1001₁** to **1001_n**, connected in series, round processors **1021₁** to **1021₂** connected in series, the round processor **1021_n** being connected to the round processor **1001_n**, the expanded key converters **1005₁** to **1005_n**, respectively connected to outputs of the expanded key processors **1021₂** to **1021_n**, and **1001₁**.

An expanded key scheduling process identical to that for encryption is temporarily carried out, and a round function is acted at the last stage, thereby obtaining an output value R_n . Then, the inverse function of each round function is acted with the output value R_n in a stage direction reversed from that for encryption, and expanded keys are generated in order from expanded key (n) to expanded key (1), i.e., in an on-the-fly manner.

However, there has been a problem that a delay time occurs until decryption has been started because of unnecessary time for first generating the same expanded key R_n as that for encryption.

As has been described above, in the conventional technique, expanded keys cannot be generated in reverse order, thus making it necessary to generate and store all the expanded keys prior to a decryption process. Because of this, there has been a problem that there is no sufficient storage space for storing all the expanded keys required for decryption in poor hardware environment such as IC card, for example.

In addition, in order to avoid this problem by generating keys in the on-the-fly manner, it is required to temporarily carry out an expanded key scheduling process identical to