

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 April 2006 (13.04.2006)

PCT

(10) International Publication Number
WO 2006/038776 A1

(51) International Patent Classification⁷: G11B 20/10
(21) International Application Number:
PCT/KR2005/003111

(22) International Filing Date:
20 September 2005 (20.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/616,120 6 October 2004 (06.10.2004) US
10-2004-0083240 18 October 2004 (18.10.2004) KR

(71) Applicant: SAMSUNG ELECTRONICS CO., LTD.
[KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si,
Gyeonggi-do 442-742 (KR).

(72) Inventors: KIM, Chi-Hurn; 211-1604 Sinyeongtong
Hyundai 2-cha Apt., 201-216 Banwol-ri, Taean-eup
Hwaseong-si, Gyeonggi-do 445-983 (KR). YOU,
Yong-Kuk; 115-206 Doosan Apt., Geumho-dong 3-ga,
Seongdong-gu, Seoul 133-751 (KR).

(74) Agent: Y.P.LEE, MOCK & PARTNERS; The
Cheonghwa Building, 1571-18, Seocho-dong, Seo-
cho-gu, Seoul 137-874 (KR).

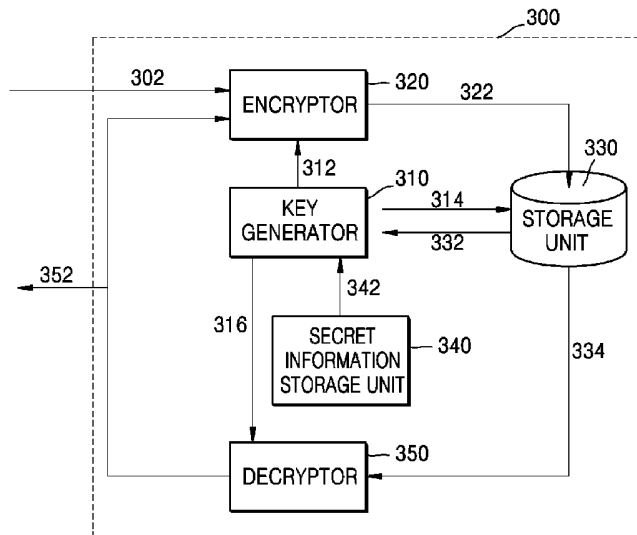
(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KP, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA,
MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ,
OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL,
SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, 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, IS, IT, LT, LU, LV, 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

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR SECURELY STORING DATA



(57) Abstract: An apparatus and method for securely storing data. The apparatus for securely storing data in a predetermined device, includes: a key generator generating a protection key used to encrypt data based on a random number generated by inputting predetermined secret information in a predetermined random number generation function, and generation sequence information, which is information on a generation sequence of the random number, wherein the predetermined secret information is stored in a secure region, and the random number generation function can generate the protection key based on the generation sequence information and the secret information. As described above, the apparatus and method for storing data make it possible to securely store data even if the apparatus for storing data is replaced.

WO 2006/038776 A1



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.

Description

APPARATUS AND METHOD FOR SECURELY STORING DATA

Technical Field

- [1] The present invention relates to an apparatus and method for storing data, and more particularly to an apparatus and method for storing data that make it possible to securely store data even if the apparatus for storing data is replaced, by using the data in an apparatus used as a replacement apparatus .

Background Art

- [2] A household electronic device such as a DVD player includes a hard disk embedded therein and stores contents such as audio/video (AV) data in the hard disk. Due to several reasons including copyright protection, the contents are encrypted using a predetermined encryption key and are stored in the hard disk. The encrypted contents are decrypted using a predetermined decryption key in order to reproduce the contents, and the decrypted contents are encrypted again using a predetermined encryption key and are stored in the hard disk. In order to secure one-time data protection, the contents are encrypted using a different encryption key whenever they are encrypted and stored in the hard disk.
- [3] FIG. 1A is a block diagram of the structure of a conventional data reproducing device such as a DVD player. Referring to FIG. 1A, the data reproducing device 10 comprises an external source 20 that provides contents, an external device 30 that uses the contents, i.e., reproduces the contents, and a data storage unit 40 that stores the contents.
- [4] The external source 20 refers to any device that provides the contents from outside of the data reproducing device 10, and for example, is a video tape, a CD, satellite receiving equipment, cable TV receiving equipment, and the like.
- [5] The external device 30 refers to a device that uses the contents, and for example, is an MPEG decoder, etc.
- [6] The data storage unit 40 encrypts the contents from the external source 20 in order to securely store the contents therein, decrypts the encrypted contents, and provides the external device 30 with the decrypted contents.
- [7] FIG. 1B is a block diagram of the internal structure of a conventional apparatus for storing data 100. The apparatus for storing data 100 comprises an encryptor 110, a key generator 120, a key storage unit 130, a decryptor 140, and a storage unit 150.
- [8] The key generator 120 generates a protection key 122 using random number generation. The protection key 122 is a key used to protect all the data stored in the data storage device 40, i.e. a key used to encrypt and decrypt the data. The protection key is different whenever it is generated due to the use of random number generation.

- [9] The encryptor 110 encrypts contents 102 from the external source 20 using the protection key 122, thereby generating encrypted contents 112 and storing them in the storage unit 150.
- [10] The protection key 122 generated by the key generator 120 is stored in the key storage unit 130. The key storage unit 130 is embodied as a secure region like, for example, a flash memory, etc.
- [11] When the external device 30 uses the contents 102, the decryptor 140 extracts encrypted contents 152 from the storage unit 150, extracts the protection key 122 from the key storage unit 130, and decrypts the encrypted contents 152 using the protection key 122, thereby generating decrypted contents 142 and providing the external device 30 with the decrypted contents 142.
- [12] Contents used in the external device 30 are encrypted in the encryptor 110 and stored in the storage unit 150. A protection key 124 used to encrypt the contents again is generated by the key generator 120. The protection key 124 is different from the protection key 122 used to firstly store the contents.
- [13] FIG. 2 is a flow chart describing a method of storing data using the apparatus for storing data shown in FIG. 1B.
- [14] In Operation 210, the key generator 120 generates the first protection key 122 using random number generation.
- [15] In Operation 220, the encryptor 110 encrypts the contents 102 using the first protection key 122, thereby generating the encrypted contents 112 and storing them in the storage unit 150.
- [16] In Operation 230, the first protection key 122 generated by the key generator 120 is stored in the key storage unit 130.
- [17] In Operation 240, the external device 30 uses the contents, for example, a DVD player reproduces the contents. In Operations 250 to 270, the decryptor 140 extracts the encrypted contents 152 from the storage unit 150, extracts the first protection key 122 from the key storage unit 130, and decrypts the encrypted contents 152 using the first protection key 122, thereby generating the decrypted contents 142 and providing the external device 30 with the decrypted contents 142, which are reproduced by the external device 30.
- [18] The reproduced contents are again encrypted in the encryptor 110 and are stored in the storage unit 150. That is, Operations 210 to 230 are repeated. The second protection key 124 used to encrypt the contents is generated by the key generator 120. The second protection key 124 is different from the first protection key 122 used to firstly store the contents. A different protection key is used to store the contents in order to secure one-time protection of the contents.

Disclosure of Invention

Technical Problem

[19] However, the foregoing apparatus and method for storing data have a problem when the apparatus 100 for storing data is installed in a new device due to after-sales service for the data reproducer 10. Suppose that first device DA includes first storage unit SA, and the first storage unit SA stores encrypted contents E (K1, C1) using a first protection key K1. The first device DA is replaced with the second device DB due to trouble of the first device DA. The first storage unit SA remains unchanged in order to maintain the encrypted contents E (K1, C1). That is, the first storage unit SA is installed in the second device DB.

[20] In this case, the first protection key K1 is neither included in the second device DB nor known to an after-sales service center. Since the first protection key K1 is generated using random number generation, a problem occurs in which the second device DB cannot use, i.e., reproduce, the encrypted contents E (K1, C1) any more.

[21] The problem frequently occurs when a storage medium is upgraded and replaced as well as the device has a defect.

Technical Solution

[22] The present invention provides an apparatus and method for storing data capable of obtaining data stored in the apparatus for storing data, even if a device including the apparatus for storing data is replaced, through after-sales service, etc.

Advantageous Effects

[23] According to the present invention, an apparatus and method for storing data make it possible to obtain data stored in the apparatus for storing data by separately storing information on a random number generation sequence and secret information on random number generation although a device including the apparatus for storing data is replaced through after-sales service, etc.

[24] Also, according to the present invention, An apparatus and method for storing data make it possible to accomplish device binding to allow contents to be used in a single device by allocating intrinsic secret information to each device.

Description of Drawings

[25] FIG. 1A is a block diagram of the structure of a conventional data reproducer such as a DVD player;

[26] FIG. 1B is a block diagram of the internal structure of a conventional apparatus for storing data;

[27] FIG. 2 is a flow chart describing a method of storing data using the apparatus for storing data shown in FIG. 1B;

[28] FIG. 3 is a schematic diagram of an apparatus for storing data according to an

exemplary embodiment of the present invention;

[29] FIG. 4A is a schematic diagram of the general operation of the random number generation function used to encrypt data;

[30] FIG. 4B is schematic diagram of a random number generation function;

[31] FIG. 4C is a schematic diagram of another random number generation function;

[32] FIG. 5A is a schematic diagram of the general operation of the random number generation function used to decrypt data;

[33] FIGS. 5B and 5C are schematic diagrams of the operation of a random number generation function used to decrypt data in view of the random number generation function shown in FIGS. 4B through 4C;

[34] FIG. 6 is a flow chart describing a method of storing data according to an exemplary embodiment of the present invention;

[35] FIG. 7 is a schematic diagram of a method of performing device binding by allocating intrinsic secret information to each device;

[36] FIG. 8 is a flow chart describing a method of extracting data stored in storage before a device is replaced due to a defect in the device;

[37] FIG. 9 is a block diagram of operation relationship between a first device 900 and second device 902;

[38] FIG. 10 is a flow chart describing another method of extracting data stored in storage before a device is replaced due to a defect in the device; and

[39] FIG. 11 is a block diagram of operation relationship between a first device 1100 and second device 1102.

Best Mode

[40] According to an aspect of the present invention, there is provided an apparatus for securely storing data in a predetermined device, including:

[41] a key generator generating a protection key used to encrypt the data based on a random number generated by inputting predetermined secret information to a predetermined random number generation function, and generation sequence information, which is information on a generation sequence of the random number,

[42] wherein the predetermined secret information is stored in a secure region, and the random number generation function can generate the protection key based on the generation sequence information and the secret information.

[43] According to another aspect of the present invention, there is provided a method of securely storing data in a predetermined device, including:

[44] key generating a protection key used to encrypt data based on a random number generated by inputting predetermined secret information in a predetermined random number generation function, and generation sequence information, which is information on a generation sequence of the random number,

[45] wherein the predetermined secret information is stored in a secure region, and the random number generation function can generate the protection key based on the generation sequence information and the secret information.

Mode for Invention

[46] The present invention will now be described more fully with reference to the accompanying drawings.

[47] Hereinafter, the term 'device' means an apparatus for storing data according to an embodiment of the present invention, and refers to devices of any form that use data. For example, the device may be a reproducer such as a DVD player, a game machine that performs game data, a PDA, another mobile device, etc. The apparatus for storing data stores encrypted AV data, game data, etc., decrypts the data when necessary to provide the device with decrypted AV data, game data, etc., and again encrypts the data to securely store encrypted AV data, game data, etc.

[48] FIG. 3 is a schematic diagram of an apparatus for storing data according to an exemplary embodiment of the present invention. Referring to FIG. 3, the apparatus 300 for storing data comprises a key generator 310, an encryptor 320, a storage unit 330, secret information storage unit 340, and a decryptor 350.

[49] Storing of data 302 input from an external source, and extracting of data 352 from the apparatus 300 for storing data, so that an external device can use the data 352, will now be separately described.

[50] When the data 302 is input from an external source, the key generator 310 generates a protection key 312 by inputting secret information 342 into a random number generation function $f()$ that uses a predetermined pseudo-random number generation algorithm. The protection key 312 used to encrypt and decrypt the data 302 is a random number generated by the random number generation function $f()$.

[51] The secret information 342 may be predetermined information used to generate a pseudo-random number like, for example, a seed, and is stored in a secure region of the apparatus 300 for storing data, i.e., the secret information storage unit 340.

[52] The secret information 342 is information uniquely allocated to a device. Different secret information 342 causes a different random number to be generated, even though the random number generation function $f()$ is the same. Therefore, each apparatus for storing data has a different protection key 312, and an object of device binding can be accomplished.

[53] The key generator 310 stores generation sequence information 314 which represents a random number generation sequence, using the random number generation function in the storage unit 330.

[54] The encryptor 320 encrypts the data 302 using the protection key 312, thereby generating the encrypted data 322 and storing it in the storage unit 330.

[55] When the external device uses the data 352, the key generator 310 generates a protection key 316 by extracting the generation sequence information 332 from the storage unit 330, extracting the secret information 342 from the secret information storage unit 340, and inputting the generation sequence information 332 and the secret information 342.

[56] The decryptor 350 extracts encrypted data 334 from the storage unit 330, and decrypts the encrypted data 334 using the protection key 316, thereby generating the decrypted data 352.

[57] The decrypted data 352 is transferred to the external device (not shown). Then, the decrypted data 352 is again encrypted by the encryptor 320 and is stored in the storage unit 330. For example, when the data 302 is AV data, the external device is an AV player that reproduces a video. Also, when the data 302 is information necessary for generating a contents key used to encrypt the contents, an external device may be a device that generates the contents key.

[58] FIGS. 4A through 4C are schematic diagrams of the operation of a random number generation function used to encrypt data according to an exemplary embodiment of the present invention.

[59] FIG. 4A is a schematic diagram of the general operation of the random number generation function used to encrypt data. Referring to FIG. 4A, a random number generation function $f()$ generates random numbers using secret information, and separately outputs a random number generation sequence. The random number generation function $f()$ is a predetermined function in which predetermined random numbers are sequentially generated from predetermined secret information. The generation sequence information and random numbers are linked to each other and are stored in the storage unit 330.

[60] FIG. 4B is schematic diagram of a random number generation function. Referring to FIG. 4B, the random number generation function $f()$ is given as Equation 1,

[61] (1)

$$f() = \text{function w hich satisfies } f(n) = X_k, X_{k+1} = aX_k \pmod{M}, \\ \text{wherein } X_0 = C$$

[62] where X_k is a k^{th} random number, k is generation sequence information, M is a predetermined decimal number, a is a constant, and X_0 is an initial value.

[63] Referring to Equation 1, when the initial value X_0 is obtained, random numbers $X_1, X_2, \dots, X_k, \dots, X_n$ are sequentially generated. The generated random numbers X_1, X_2, \dots are not stored in the apparatus 300 for storing data. Instead, the k and X_k are stored in the storage unit 330.

[64] FIG. 4C is a schematic diagram of another random number generation function. Referring to FIG. 4C, the random number generation function $f()$ is given as Equation 2.

[65]

$$f() = \text{function which satisfies } X_{n+1} = \text{DES}(K_{des}, X_n) \text{ wherein } X_0 = C$$

(2)

[66] The random number generation function is a Data Encryption Standard (DES) encryption algorithm, encrypts a 128-bit input value X_k using DES key K_{des} , and generates a 128-bit output value X_{k+1} . The DES encryption algorithm is well known to a person having skill in the pertinent art.

[67] Like in Equation 1, when the initial value X_0 is obtained, random numbers $X_1, X_2, \dots, X_k, \dots, X_n$ are sequentially generated. The generated random numbers X_1, X_2, \dots , are not stored in the apparatus 300 for storing data. Instead, k and X_k are stored in the storage unit 330.

[68] FIGS. 5A through 5C are schematic diagrams of the operation of a random number generation function used to decrypt data in view of the random number generation function shown in FIGS. 4A through 4C.

[69] FIG. 5A is a schematic diagram of the general operation of the random number generation function used to decrypt data. Referring to FIG. 5A, the random number generation function $f()$ generates random numbers using secret information and generation sequence information. When data is decrypted, the secret information is stored in a secure region of the apparatus 300 for storing data like, for example, a flash memory, and is extracted. When data is decrypted, the generation sequence information is stored in an insecure region of the apparatus 300 for storing data like, for example, a hard disk.

[70] FIGS. 5B and 5C are schematic diagrams of the operation of a random number generation function used to decrypt data in view of the random number generation function shown in FIGS. 4B through 4C.

[71] Referring to FIG. 5B, the key generator 310 generates a k^{th} random number using the initial value X_0 and Equation 1. Referring to FIG. 5C, the key generator 310 generates the k^{th} random number using the initial value X_0 and Equation 2.

[72] Referring to FIGS. 4B and 5B, the secret information may be a coefficient instead of the initial value X_0 . Referring to FIGS. 4C and 5C, the secret information may be the DES key K_{des} instead of the initial value X_0 . In this case, the initial value X_0 may be opened.

[73] FIG. 6 is a flow chart describing a method of storing data according to an embodiment of the present invention.

- [74] In Operation 610, the key generator 310 generates a protection key used to encrypt data to be securely stored in a device and generation sequence information, which is information on a random number generation sequence, using a random number generation function that generates random numbers based on predetermined secret information stored in a secure region of a predetermined device. The random number generation function can generate the protection key based on the generation sequence information and secret information.
- [75] In Operation 620, the encryptor 320 encrypts data using the protection key, thereby generating encrypted data.
- [76] In Operation 630, the encryptor 320 and key generator 310 store the encrypted data and generation sequence information in an insecure region of the device, i.e., the storage unit 330.
- [77] In Operation 640, the key generator 310 generates the protection key by inputting the generation sequence information and secret information in the random number generation function when the device uses data. The protection key generated in Operation 610 is the same as the protection key generated in Operation 640 owing to a characteristic of the random number generation function.
- [78] In Operation 650, the decryptor 350 reads the encrypted data from the storage unit 330 and decrypts it using the protection key generated in Operation 640, thereby generating decrypted data.
- [79] According to the foregoing apparatus and method for storing data, although the storage unit 330 or the device is replaced, the protection key generated before the storage unit 330 or the device is replaced is the same as the protection key generated after the storage unit 330 or the device is replaced. The device DA includes the storage unit SA, and the storage unit SA includes encrypted data $E(K_A, \text{data})$ using protection key K_A . If a part other than the storage unit SA is replaced, i.e., the storage unit SA is installed in a new device DB, the device DB can decrypt the encrypted data $E(K_A, \text{data})$ stored in the storage unit SA, because a new key generator of the device DB can generate the protection key KA from generation sequence information included in the storage unit SA and secret information corresponding to the storage unit SA. The secret information corresponding to the storage unit SA is recorded in the device DB by an after-sales service center.
- [80] According to the foregoing apparatus and method for storing data, device binding can be accomplished since secret information is intrinsic to each device. Device binding means when a device A is authorized to use data, a device B cannot use the data, even if a storage medium having the data is installed in device B. Generally, a data provider, i.e., a contents provider requires device binding to a device provider, i.e., a reproducer manufacturer.

- [81] FIG. 7 is a schematic diagram of a method of performing device binding by allocating intrinsic secret information to each device. Both first and second devices generate random numbers using the random number generation function satisfying $X_{k+1} = aX_k \pmod{M}$ shown in FIGS. 4B and 5B. Both devices use the same random number generation function. However, since the initial value X_0 of the first device is different from the initial value X'_0 of the second device, random numbers generated by the first device, $X_0, X_1, X_2, \dots, X_n$ and random numbers generated by the second device, $X'_0, X'_1, X'_2, \dots, X'_n$ are different from each other.
- [82] For example, the device DA encrypts data using protection key X_2 , stores encrypted data in the storage unit SA, and the storage unit SA is installed in the device DB. Since the device DB includes its secret information sec_B (i.e., initial value X'_0) and excludes secret information sec_A (i.e., the initial value X_0) of the device DA, the device DB cannot generate the protection key X_2 even if both devices use the same random number generation function.
- [83] FIG. 8 is a flow chart describing a method of extracting data stored in storage before a device is replaced due to a defect. FIG. 9 is a block diagram of operation relationship between a first device 900 and second device 902. The method shown in FIG. 8 will now be described with reference to FIG. 9.
- [84] In Operation 810, a key generator 930 of the first device 900 generates a first protection key K_1 using first secret information 954 from secret information storage unit 950 of the first device 900. At this time, generation sequence information 934 of the first protection key K_1 is also generated and stored in storage unit 940 of the first device 900.
- [85] In Operation 820, an encryptor 920 of the first device 900 encrypts data C_1 using the first protection key K_1 , generates encrypted data $E(K_1, C_1)$, and stores the encrypted data $E(K_1, C_1)$ in the storage unit 940 of the first device 900. The first device 900 also includes a decryptor 960.
- [86] In Operation 830, due to a defect of the first device 900, the first device 900 is replaced with the second device 902 while the data $E(K_1, C_1)$ remains unchanged. That is, the storage unit 940 of the first device 900 is installed in the second device 902.
- [87] In Operation 840, the after-sales service center records secret information corresponding to the storage unit 940 of the first device 900, i.e., the first secret information 954 in secret information storage unit 952 of the second device 902. The after-sales service center has tables corresponding to the respective first and second devices and secret information, and confirms a serial number of the storage unit 940 of the first device 900 using the tables in order to determine what the first secret information 954 is.

- [88] In Operation 850, the after-sales service center installs the first storage unit 940 in the second device 902. Therefore, the second device 902 includes the storage unit 940 of the first device 900 in which the encrypted data $E(K_1, C_1)$ and generation sequence information 934 are recorded, and secret information storage unit 952 of the second device 902 in which the first secret information 954 is recorded.
- [89] In Operation 860, a key generator 932 of the second device 902 extracts the first secret information 954 from the secret information storage unit 952 of the second device 902, extracts the generation sequence information 934 from the storage unit 940 of the first device 900, and generates the first protection key K_1 using the first secret information 954, the generation sequence information 934 and a random number generation function. The first device 900 and second device 902 have the same random number generation function.
- [90] In Operation 870, a decryptor 962 of the second device 902 extracts the encrypted data $E(K_1, C_1)$ from the storage unit 940 of the first device 900, decrypts the encrypted data $E(K_1, C_1)$ using the first protection key K_1 generated in Operation 860, and generates decrypted data C_1 . The second device 902 also includes an encryptor 922.
- [91] FIG. 10 is a flow chart describing another method of extracting data stored in storage before a device is replaced due to a defect. FIG. 11 is a block diagram of an operation relationship between a first device 1100 and a second device 1102. The method shown in FIG. 10 will now be described with reference to FIG. 11.
- [92] In Operation 1010, a key generator 1130 of the first device 1100 generates a first protection key K_1 using first secret information 1154 from a secret information storage unit 1150 of the first device 1100. At this time, generation sequence information 1134 of the first protection key K_1 is also generated and is stored in storage unit 1140 of the first device 1100.
- [93] In Operation 1020, an encryptor 1120 of the first device 1100 encrypts data C_1 using the first protection key K_1 , generates encrypted data $E(K_1, C_1)$, and stores the encrypted data $E(K_1, C_1)$ in the storage unit 1140 of the first device 1100. The first device 1100 also includes a decryptor 1160.
- [94] In Operation 1030, due to a defect of the first device 1100, the first device 1100 is replaced with the second device 1102 while the data $E(K_1, C_1)$ remains unchanged. That is, the storage unit 1140 of the first device 1100 is installed in the second device 1102.
- [95] In Operation 1040, the after-sales service center generates the first protection key K_1 using first secret information 1154 corresponding to the storage unit 1140 of the first device 1100 and the generation sequence information 1134 of the first protection key K_1 . The generation sequence information 1134 of the first protection key K_1 can be extracted from the storage unit 1140 of the first device 1100. The after-sales service

center has tables each corresponding to the first and second devices and secret information, and confirms a serial number of the storage unit 1140 of the first device 1100 using the tables in order to determine what the first secret information 1154 is.

[96] In Operation 1050, the after-sales service center decrypts the encrypted data $E(K_1, C_1)$ using the first protection key K_1 to generate decrypted data C_1 . The encrypted data $E(K_1, C_1)$ can be extracted from the storage unit 1140 of the first device 1100.

[97] In Operation 1060, the after-sales service center generates a second protection key K_2 using second secret information 1156 corresponding to a serial number of the second device 1102. At this time, generation sequence information 1146 of the second protection key K_2 is also generated and is stored in storage unit 1140 of the first device 1100.

[98] In Operation 1070, the after-sales service center encrypts data C_1 decrypted in Operation 1050 using the second protection key K_2 , generates encrypted data $E(K_2, C_1)$, and stores the encrypted data $E(K_2, C_1)$ in the storage unit 1140 of the first device 1100.

[99] In Operation 1080, the after-sales service center installs the first storage unit 1140 in the first device 1100 in the second device 1102, and records the second secret information 1156 of Operation 1060 in the secret information storage unit 1152 of the second device 1102.

[100] In Operation 1090, a key generator 1132 of the second device 1102 generates the second protection key K_2 using the generation sequence information 1148 of the second protection key K_2 and secret information 1158. The first device 900 and second device 902 have the same random number generation function.

[101] In Operation 1095, a decryptor 1162 of the second device 1102 extracts the encrypted data $E(K_2, C_1)$ from the storage unit 1140 of the first device 1100 and decrypts the encrypted data $E(K_2, C_1)$ using the second protection key K_2 generated in Operation 109 to generate decrypted data C_1 . The second device 1102 also includes an encryptor 1122.

[102] It is possible for an exemplary embodiment of the present invention to be realized on a computer-readable recording medium as a computer-readable code. Computer-readable recording mediums include every kind of recording device that stores computer system-readable data. ROMs, RAMs, CD-ROMs, magnetic tapes, floppy discs, optical data storage unit, etc. are used as a computer-readable recording medium. Computer-readable recording mediums can also be realized in the form of a carrier wave (e.g., transmission through Internet).

[103] While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing

from the spirit and scope of the invention as defined by the appended claims. The exemplary embodiments should be considered in a descriptive sense only and not for purposes of limitation. Therefore, the scope of the present invention is defined not by the detailed description of the invention but by the appended claims, and all differences within the scope of the present invention will be construed as being included in the present invention

[104]

Claims

- [1] 1. An apparatus for securely storing data in a predetermined device, comprising: a key generator generating a protection key used to encrypt the data, said protection key based on:
a random number generated by inputting predetermined secret information to a predetermined random number generation function, and
generation sequence information, which is information on a generation sequence of the random number,
wherein the predetermined secret information is stored in a secure region, and the random number generation function generates the protection key based on the generation sequence information and the secret information.
- [2] 2. The apparatus of claim 1, further comprising:
an encryptor encrypting the data using the protection key to generate encrypted data;
a storage unit storing the encrypted data and the generation sequence information; and
a secret information storage unit securely storing the secret information with an external access blocked.
- [3] 3. The apparatus of claim 1, wherein the key generator generates the protection key by inputting the generation sequence information and the secret information in the random number generation function when the device uses the data.
- [4] 4. The apparatus of claim 1, further comprising:
a decryptor reading encrypted data from the storage unit and decrypting the encrypted data using the protection key to generate decrypted data when the device uses the data.
- [5] 5. The apparatus of claim 1, wherein the random number generation function generates a different random number when different secret information is input to the random number generation function, even if the generation sequence information is the same.
- [6] 6. The apparatus of claim 5, wherein the secret information is unique information allocated to each device so that device binding can be accomplished.
- [7] 7. The apparatus of claim 1, wherein the key generator generates the random number using a DES algorithm, and the secret information is a Data Encryption Standard (DES) key.
- [8] 8. The apparatus of claim 4, wherein the data is audio/video (AV) contents, and the decryptor reads the encrypted data from the storage unit when the device commands reproduction of the AV contents, and decrypts the encrypted data

using the protection key to generate decrypted data .

- [9] 9. A method of securely storing data in a predetermined device, comprising:
generating a protection key used to encrypt data, said protection key based on:
a random number generated by inputting predetermined secret information in a
predetermined random number generation function, and
generation sequence information, which is information on a generation sequence
of the random number, and
storing the predetermined secret information in a secure region, wherein the
random number generation function generates the protection key based on the
generation sequence information and the secret information.
- [10] 10 The method of claim 9, further comprising:
encrypting the data using the protection key to generate encrypted data;
storing the encrypted data and the generation sequence information in an
insecure region of the device; and
generating a decryption key generating the protection key by inputting the
generation sequence information and the secret information to the random
number generation function when the device uses the data.
- [11] 11. The method of claim 9, further comprising:
decrypting reading encrypted data from the storage unit and decrypting the
encrypted data using the protection key to generate decrypted data when the
device uses the data.
- [12] 12. The method of claim 9, wherein the random number generation function
generates a different random number when different secret information is input
to the random number generation function, even if the generation sequence in-
formation is the same.
- [13] 13. The method of claim 12, wherein the secret information is intrinsic in-
formation allocated to each device so that device binding can be accomplished.
- [14] 14. The method of claim 9, wherein the key generating generates the random
number using a DES algorithm, and the secret information is a DES key.
- [15] 15. The method of claim 9, wherein the data is audio/video (AV) contents, and
the decrypting reads the encrypted data from the storage unit when the device
commands to reproduce the AV contents, and decrypts the encrypted data using
the protection key to generate decrypted data .
- [16] 16. A computer readable medium having embodied thereon a computer program
for executing the method of claim 9.

FIG. 1A

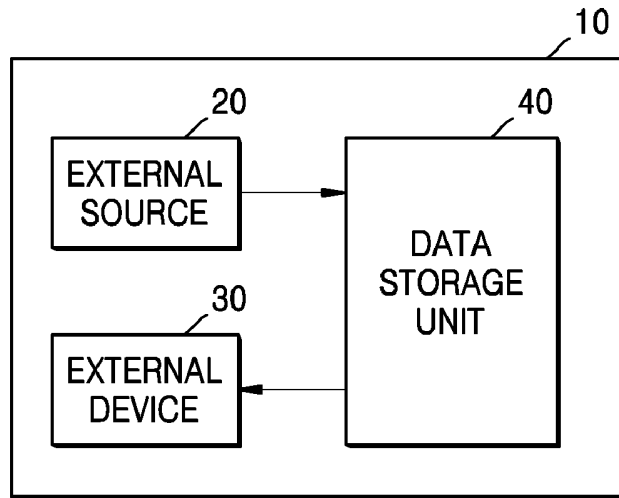


FIG. 1B

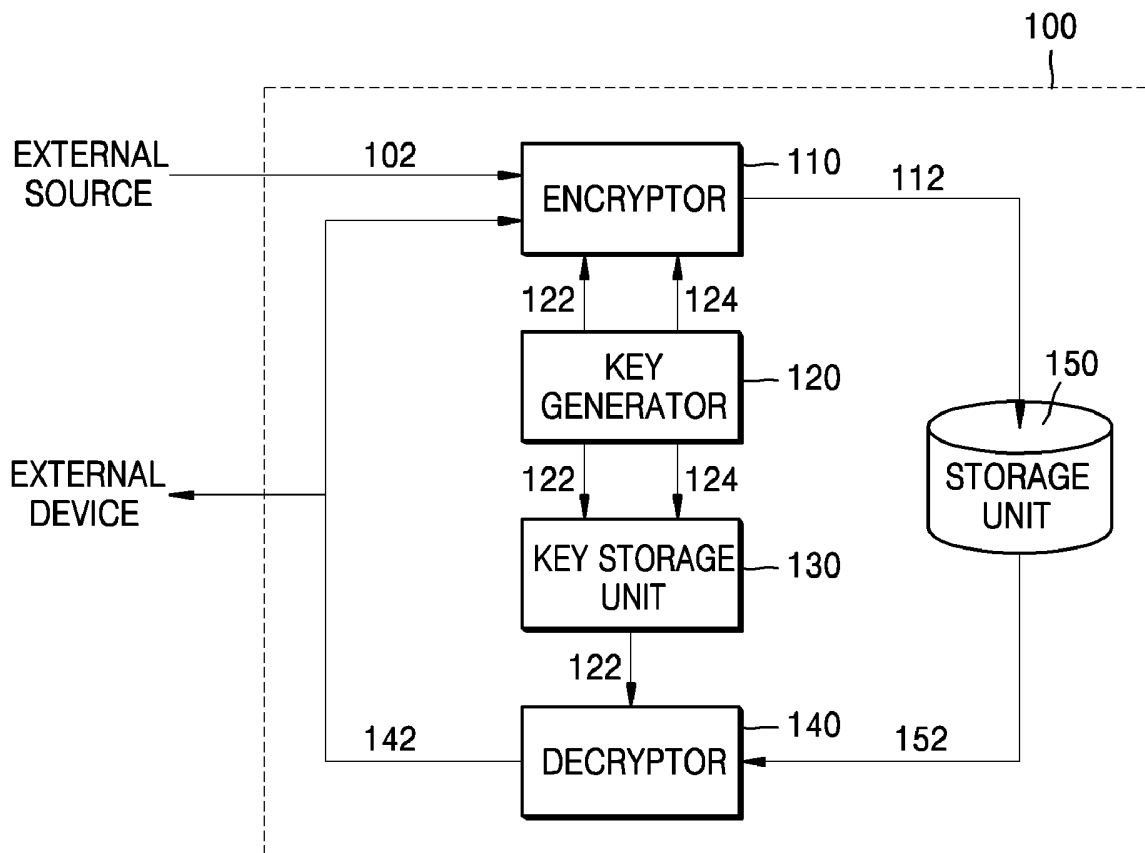


FIG. 2

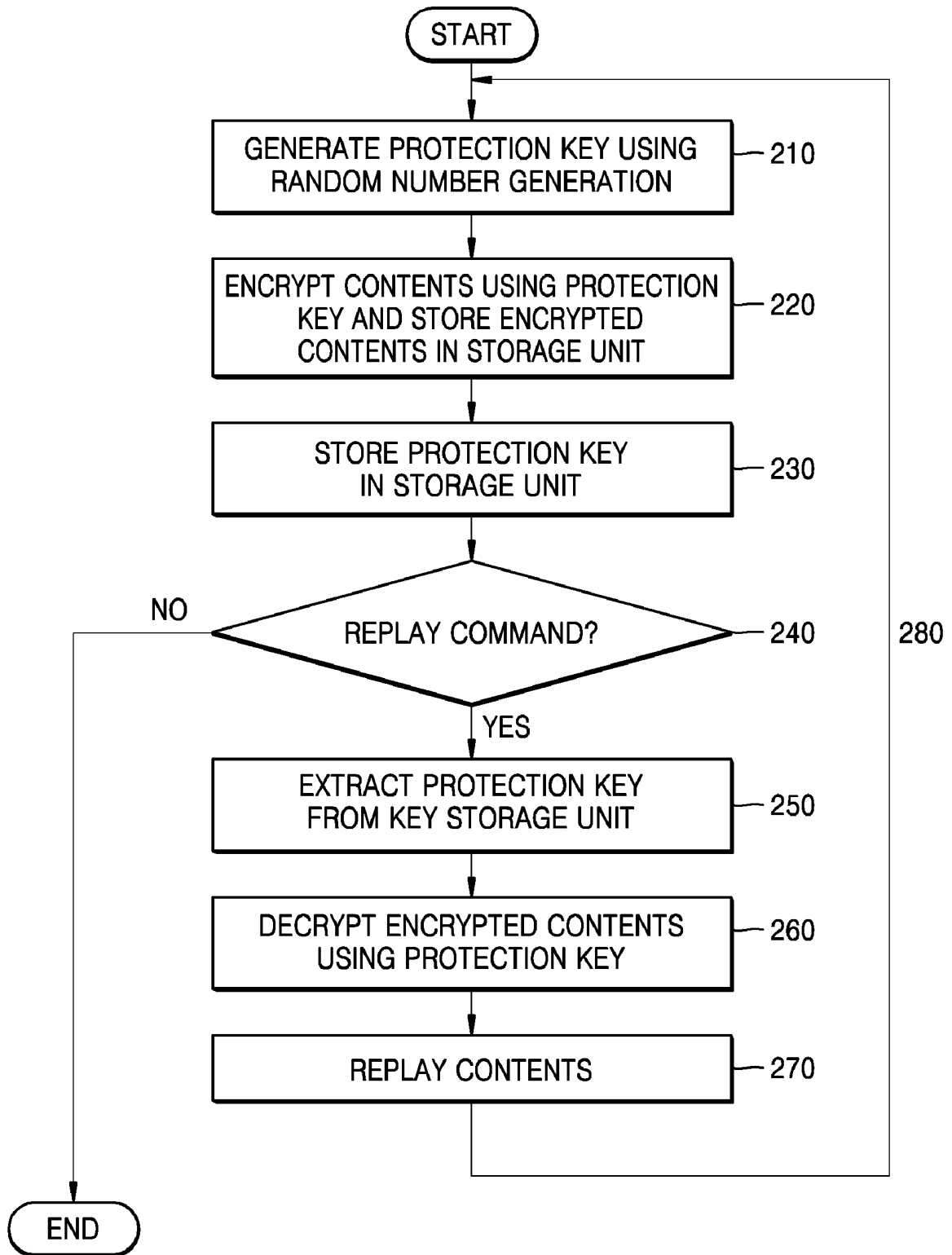


FIG. 3

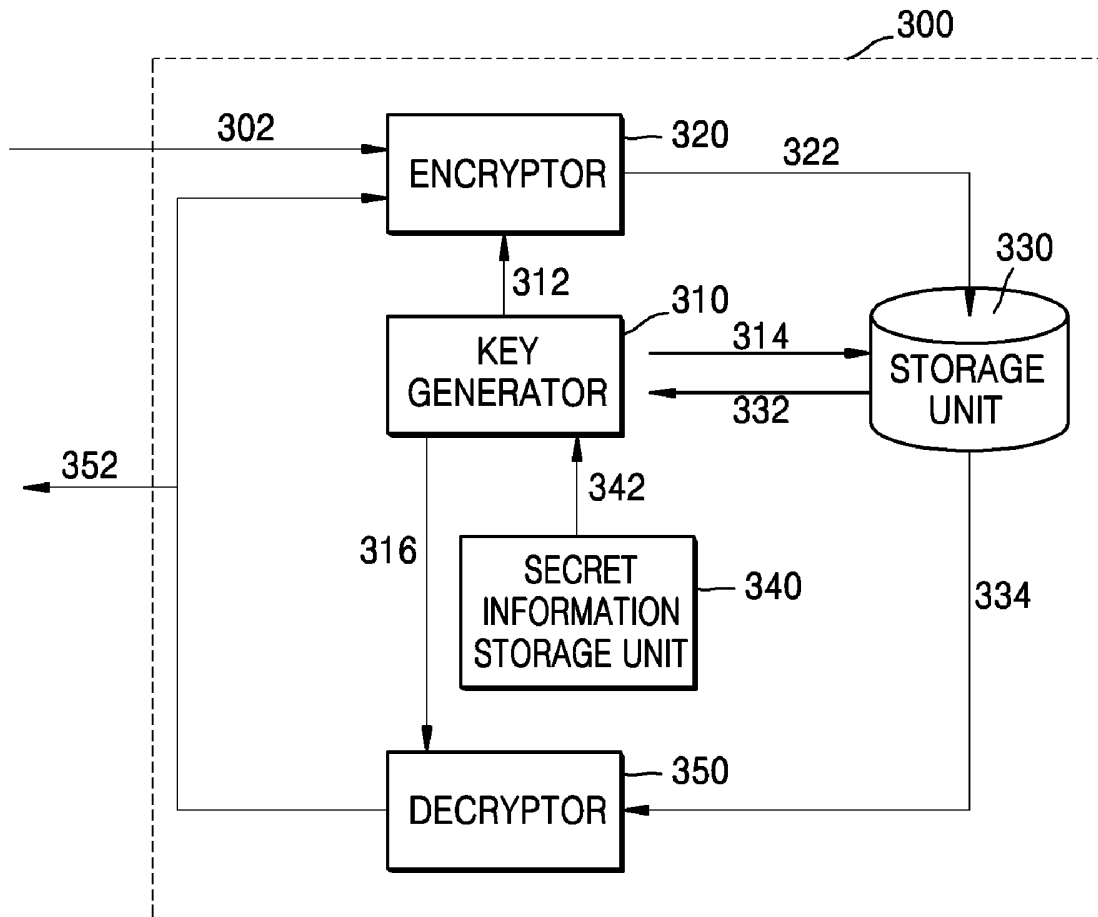


FIG. 4A

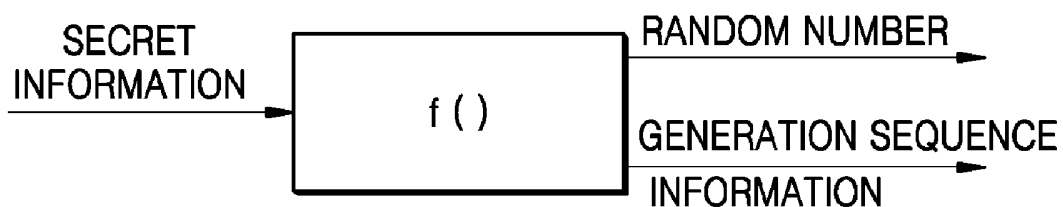


FIG. 4B

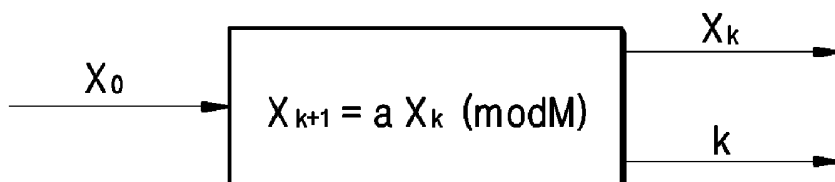


FIG. 4C



FIG. 5A

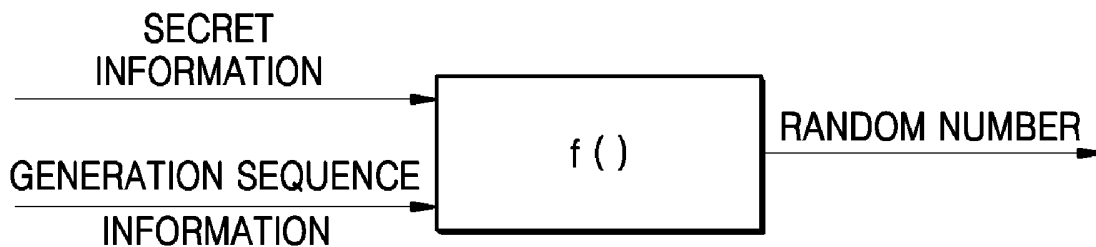


FIG. 5B

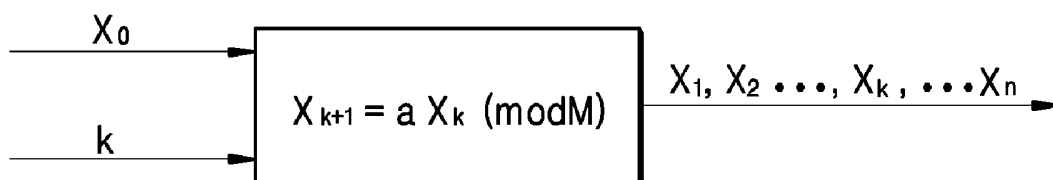


FIG. 5C



FIG. 6

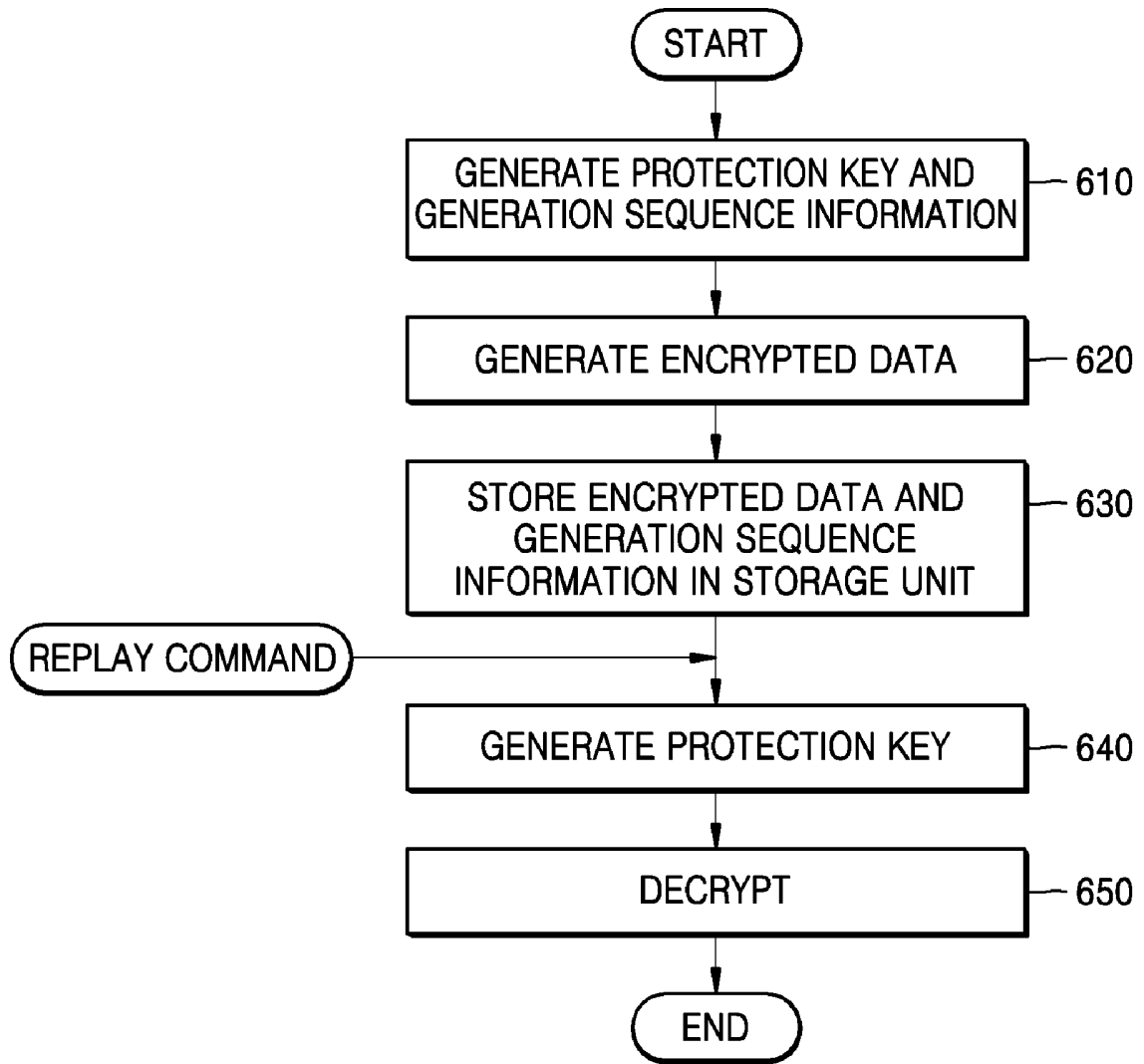


FIG. 7

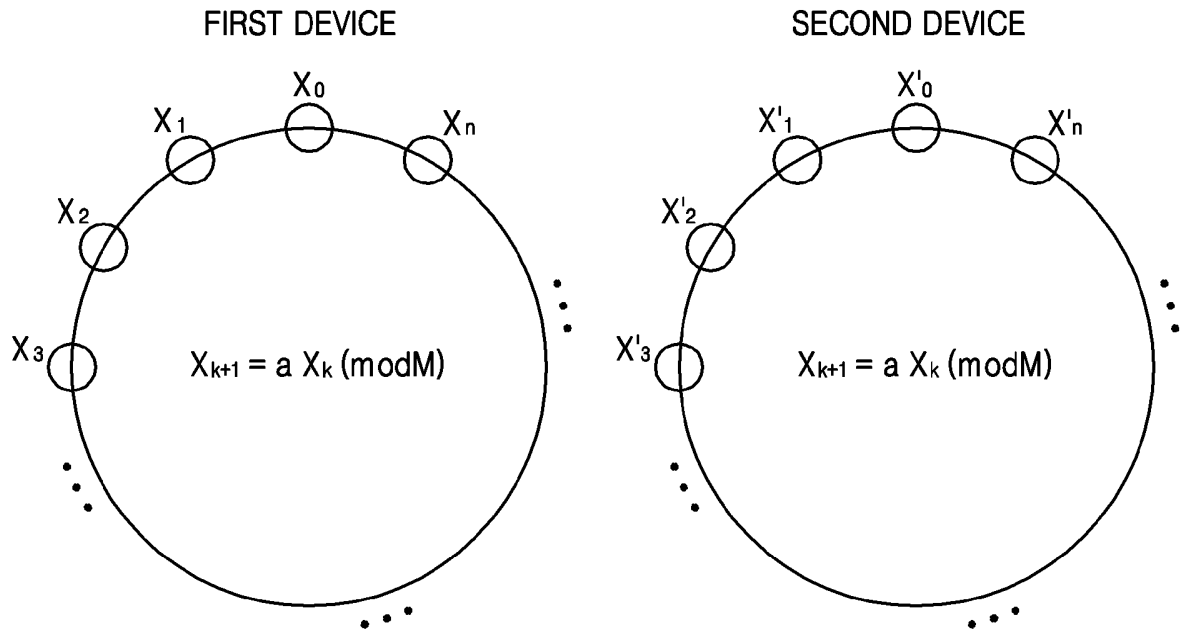


FIG. 8

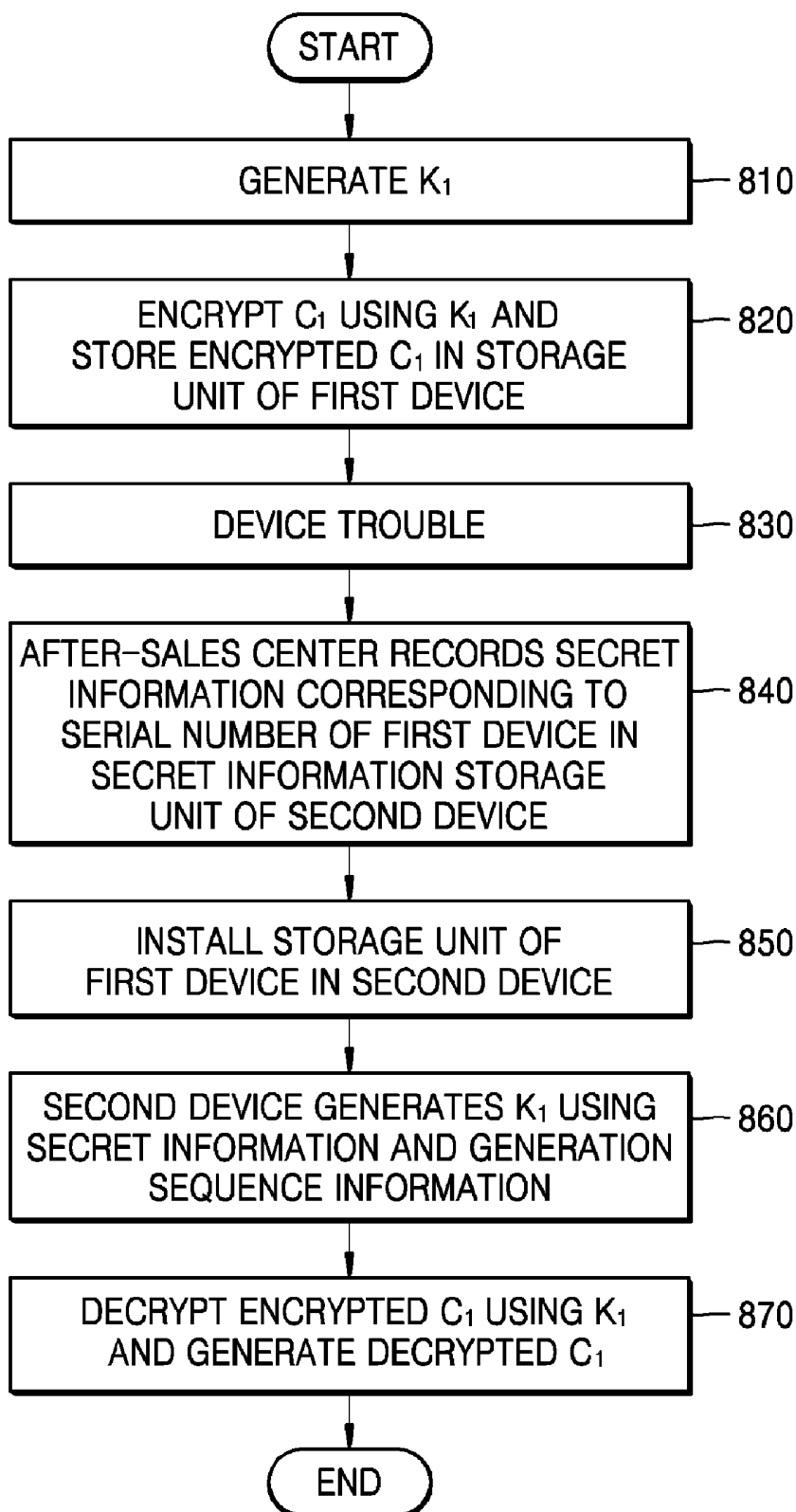


FIG. 9

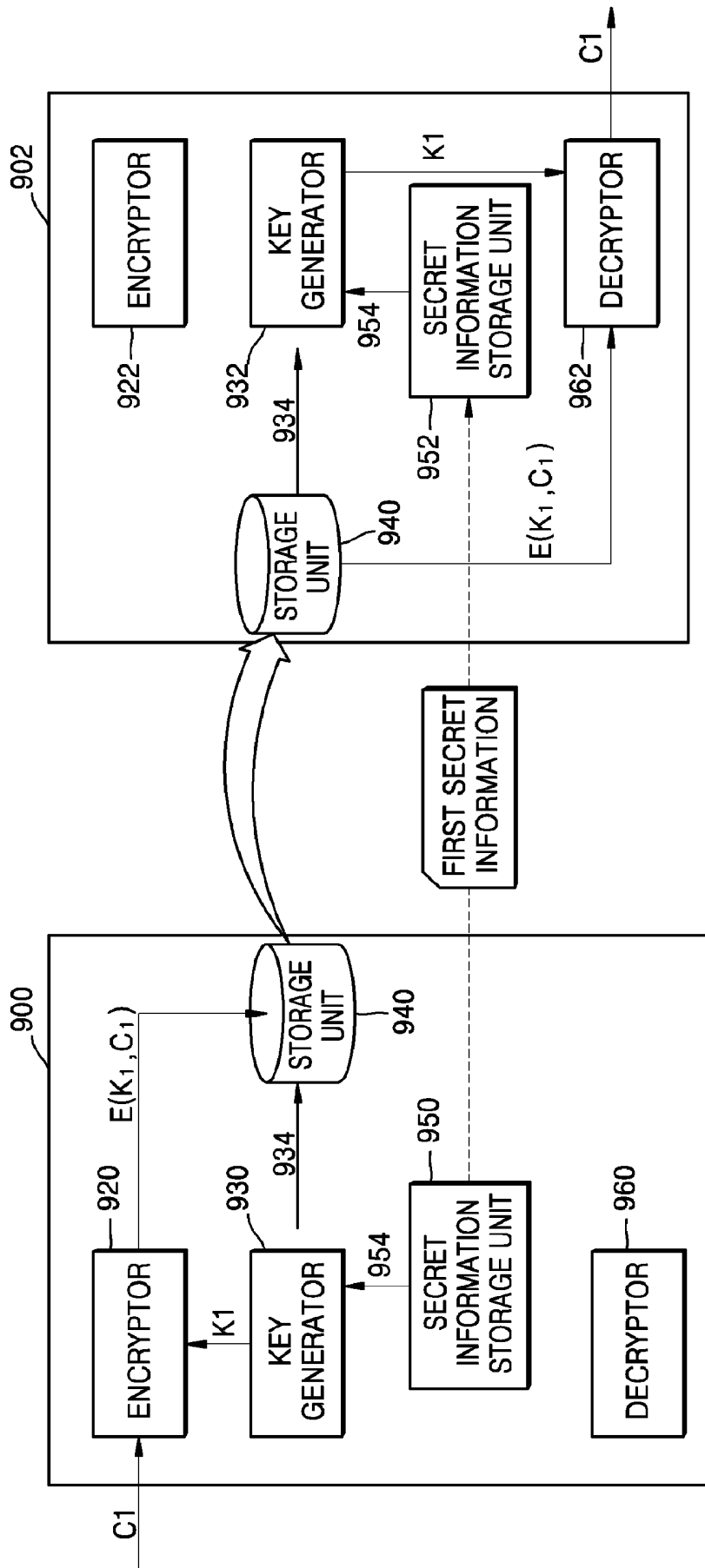


FIG. 10

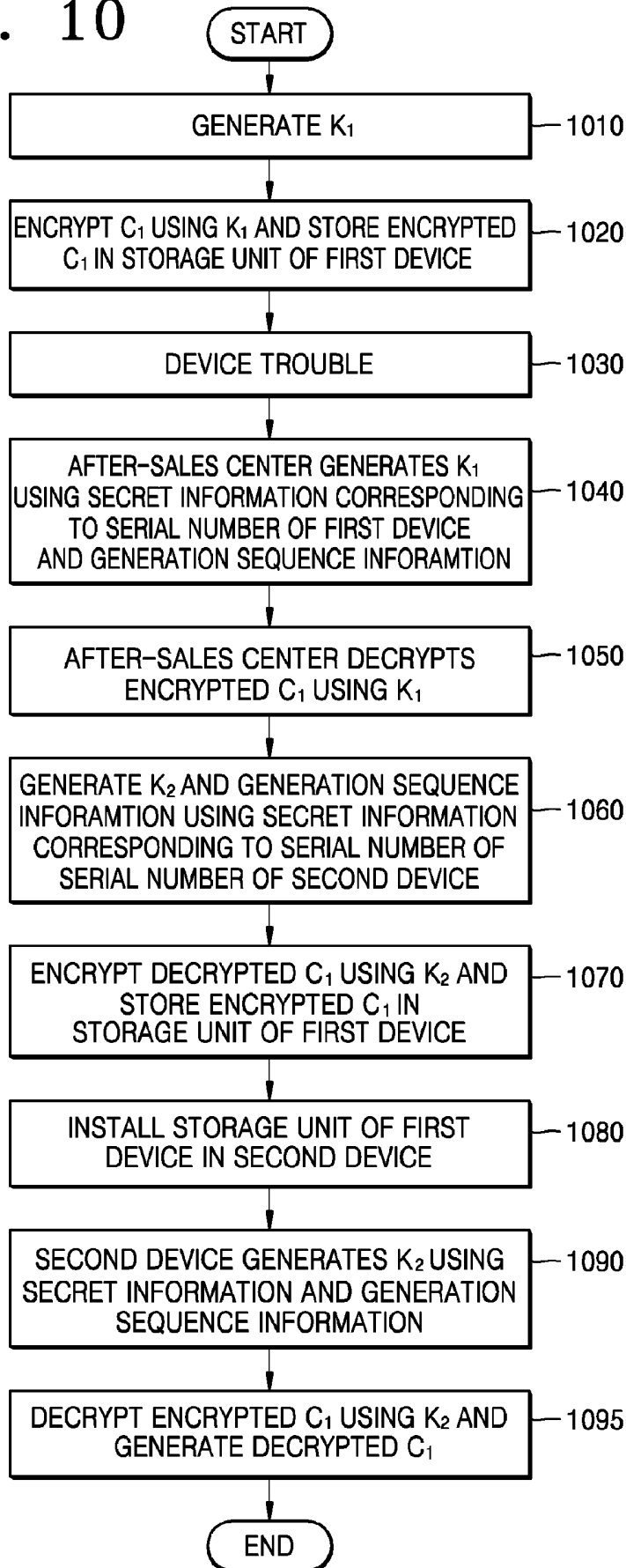
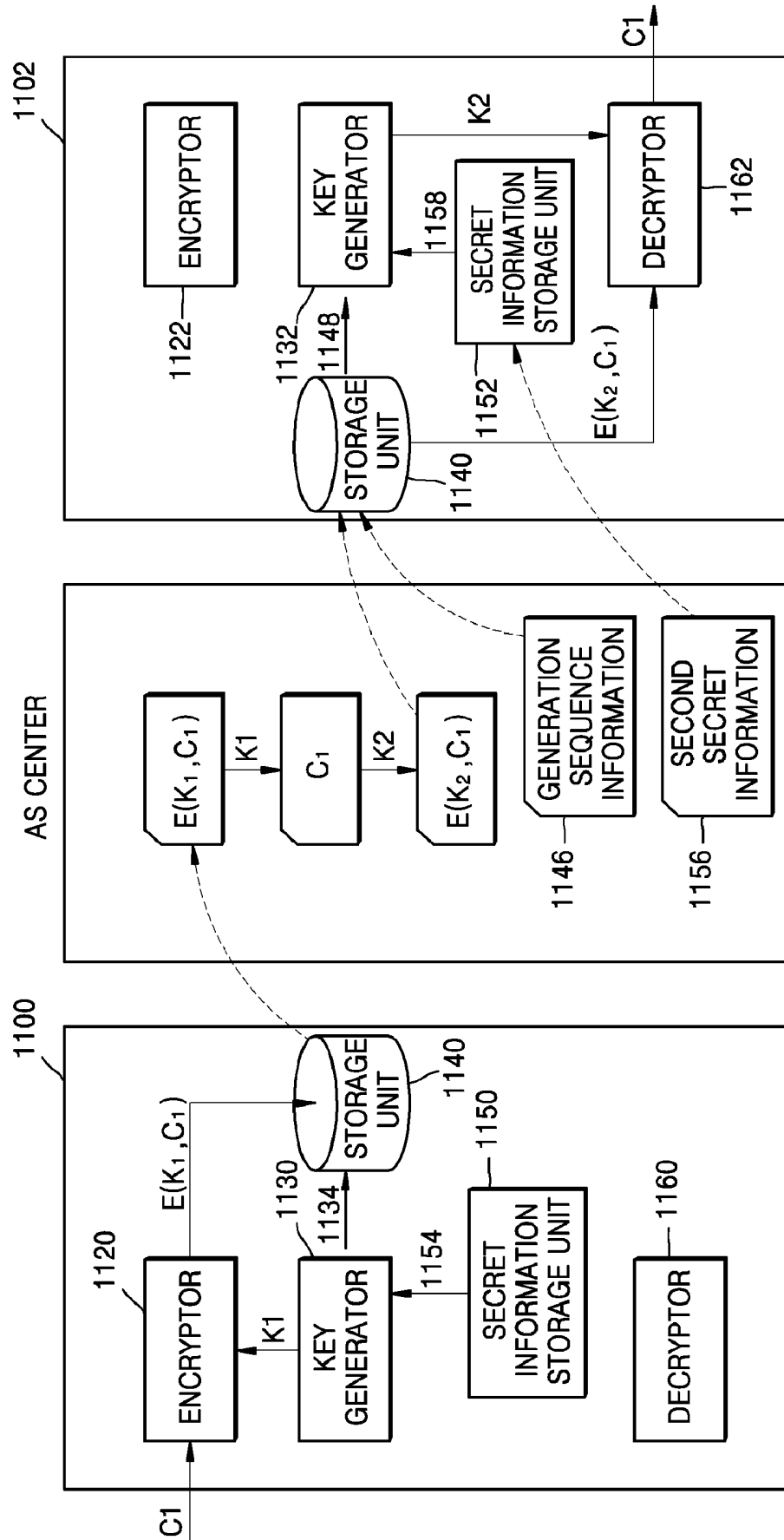


FIG. 11



PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference SH-23190-PCT	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/KR2005/003111	International filing date (<i>day/month/year</i>) 20 SEPTEMBER 2005 (20.09.2005)	(Earliest) Priority Date (<i>day/month/year</i>) 06 OCTOBER 2004 (06.10.2004)
Applicant SAMSUNG ELECTRONICS CO., LTD.		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (See Box No. II)

3. **Unity of invention is lacking** (See Box No. III)

4. With regard to the **title**,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 3

as suggested by the applicant.

because the applicant failed to suggest a figure.

because this figure better characterizes the invention.

b. none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/003111**A. CLASSIFICATION OF SUBJECT MATTER****IPC7 G11B 20/10**

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)

G11B 20/10 H04L 9/08 G06F 12/14

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)

WPI, PAJ "storage, key, protection, security, random, DES(Data Encryption Standard), encrypt, decrypt, sequence"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-286832 A (RICOH CO., LTD.) 13 October 2000 See the whole document	1, 9
A	JP 2002-260326 A (SONY CORP.) 13 September 2002 See the whole document	1, 9
A	JP 2000-228060A (OLYMPUS OPTICAL CO.,LTD.) 15 August 2000 See the whole document	1, 9
A	JP 2002-304807 A (SONY CORP.) 18 October 2002 See the whole document	1, 9

 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 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

30 NOVEMBER 2005 (30.11.2005)

Date of mailing of the international search report

30 NOVEMBER 2005 (30.11.2005)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 920 Dunsan-dong, Seo-gu, Daejeon 302-701,
 Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Yong Woong

Telephone No. 82-42-481-5698

