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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 June 2008 (12.06.2008)

PCT

(10) International Publication Number
WO 2008/069473 A1

(51) International Patent Classification:
H04L 9/06 (2006.01)

(21) International Application Number:
PCT/KR2007/005844

(22) International Filing Date:
21 November 2007 (21.11.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/872,501 4 December 2006 (04.12.2006) US
10-2007-0029367 26 March 2007 (26.03.2007) KR

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

(72) Inventors: **YOU, Yong-Kuk**; 101-1402 Daewoo Apt., Geumho-dong 4-ga, Seongdong-gu, Seoul 133-094 (KR). **KIM, Seong-Soo**; 101-403 Gwangnam Apt., 518-2 Dunchon 2-dong, Gangdong-gu, Seoul 134-062 (KR). **CHOI, Sang-Su**; 403-1601 Sinyeongtong Hyundai 4-cha Apt., Banwol-dong, Hwaseong-si, Gyeonggi-do 445-984 (KR). **LEE, So-Young**; 103 Bestvill Apt., 1236-4 Maetan 3-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-373 (KR).

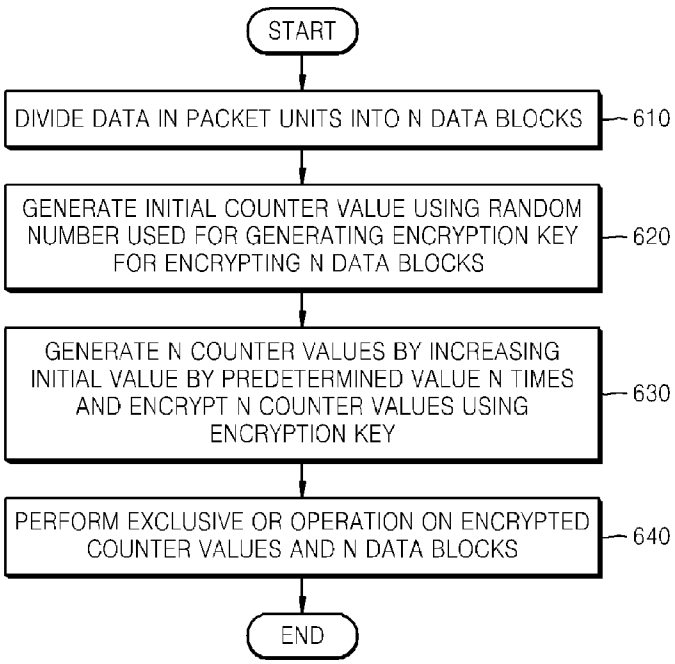
(74) Agent: **Y.P.LEE, MOCK & PARTNERS**; Koryo Building, 1575-1, Seocho-dong, Seocho-gu, Seoul 137-875 (KR).

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

(54) Title: METHOD AND APPARATUS FOR ENCRYPTING DATA



(57) Abstract: A method of encrypting data is provided. The method includes dividing data in packet units into N data blocks; generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks; generating N counter values by increasing the initial value by a predetermined value N times and encrypting the N counter values using the encryption key; and performing an exclusive OR operation on the N encrypted counter values and the N data blocks.

WO 2008/069473 A1

Description

METHOD AND APPARATUS FOR ENCRYPTING DATA

Technical Field

[1] Methods and apparatuses consistent with the present invention relate to encrypting data, and more particularly, to encrypting data in a digital transmission content protection (DTCP) standard .

Background Art

[2] The DTCP standard was developed as a protocol for audio/video (AV) data transmission protection between devices connected in accordance with the Institute of Electrical and Electronics Engineers (IEEE) 1394 standard, and has been extended for protection of AV data transmitted by universal serial bus (USB), media oriented systems transport (MOST), Bluetooth, or Internet protocol (IP). The original purpose of the DTCP standard was to transmit compressed AV data. However, the DTCP standard can also be used for transmitting all types of data regardless of their content format. Algorithms used for encrypting data in accordance with the DTCP standard include M6 and a cipher block chaining (CBC) mode of the advanced encryption standard (AES) using a 128-bit key. The CBC mode of AES is a more stable algorithm.

[3] Currently, demands for communication of non-compressed AV data through a wireless communication system having a transmission rate of several gigabits per second (Gbps) by using a tens of gigahertz (GHz) band have increased, and thus related technologies are being actively developed. The DTCP standard can also be applied to the above-described data communication technologies. In this case, the size of the transmission data is large, requiring a high-speed encryption algorithm.

[4] FIG. 1 is a diagram illustrating a related art encryption algorithm in a CBC mode of the AES, showing encryption and decryption processes.

[5] In the encryption process, data is divided into 128-bit data blocks P1 through Pn, and AES encryption is performed respectively on the data blocks P1 through Pn.

[6] The data block P1 is added to an initial value (IV) and then encrypted using an encryption key Ek, to generate encrypted data C1. The data block P2 is added to the encrypted data C1 and the result is encrypted using the encryption key Ek to generate encrypted data C2 is generated. In the same manner, encrypted data C1 through Cn is generated using the data blocks P1 through Pn.

[7] The decryption process is the inverse process of the encryption process.

[8] In the decryption process, the encrypted data C1 is decrypted using a decryption key Dk and the result is added to an initial value IV to obtain the data block P1. The encrypted data C2 is decrypted using the decryption key Dk and the result is added to

the encrypted data C1 to obtain the data block P2. In the same manner, the data blocks P1 through Pn are obtained.

[9] As described above, the related art encryption algorithm using the CBC mode of the AES requires more time for encryption and decryption. Additionally, each encryption or decryption is affected by the previous encryption or decryption result.

[10] To solve the above-mentioned problem, a counter mode of the AES can be used.

[11] FIG. 2 is a diagram illustrating a related art encryption algorithm in a counter mode of the AES, showing encryption and decryption processes.

[12] In the encryption process, data is divided into 128-bit data blocks P1 through Pm, a number of counters t1 through tm corresponding to the number of the data blocks P1 through Pm are generated, and AES encryption is performed on the data blocks P1 through Pm using the counters t1 through tm.

[13] In this case, the counters t1 through tm are predetermined values regardless of the data blocks P1 through Pm. In general, counters t2 through tm are set by adding 1 to the previous counter. For example, a counter t2 is set by adding 1 to an initial counter t1, and a counter t3 is set by adding 1 to the counter t2.

[14] The counters t1 through tm are encrypted using an encryption key Ek and then an exclusive OR operation is performed on the encrypted counters t1 through tm and the data blocks P1 through Pm, respectively. Thus, encrypted data C1 through Cm are generated.

[15] The decryption process is the inverse process of the encryption process.

[16] In the decryption process, the counter t1 is encrypted using the encryption key Ek and then an exclusive OR operation is performed on the encrypted counter t1 and the encrypted data C1. Thus, the original data block P1 is obtained. Data blocks P2 through Pn may be obtained in the same manner as the data block P1.

[17] The encryption algorithm in the counter mode of the AES does not rely on a previous AES encryption result, enabling parallel encryption and decryption and increasing encryption speed.

[18] However, the counter mode of the AES is not included in the DTCP standard, and has weaknesses. The counters in the counter mode of the AES can be predicted in advance, and a third party can recreate original data from encrypted data if a plurality of data blocks are encrypted using the same encryption key and the same counter.

Disclosure of Invention

Technical Solution

[19] Exemplary embodiments of the present invention overcome the above disadvantages and other disadvantages not described above. Also, the present invention is not required to overcome the disadvantages described above, and an exemplary

embodiment of the present invention may not overcome any of the problems described above.

[20] The present invention provides a method and apparatus for encrypting data quickly and reliably in accordance with a DTCP standard.

Advantageous Effects

[21] The exemplary embodiments of the present invention allow fast and stable data encryption by dividing data in packet units into N data blocks, generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks, generating N counter values by increasing the initial value by a predetermined value N times, encrypting the N counter values using the encryption key, and performing an exclusive OR operation on the encrypted counter values and the data blocks.

Description of Drawings

[22] The above and other aspects of the present invention will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings in which:

[23] FIG. 1 is a diagram illustrating a related art encryption algorithm in a CBC mode of the AES;

[24] FIG. 2 is a diagram illustrating a related art encryption algorithm in a counter mode of the AES;

[25] FIG. 3 is a diagram of an apparatus for encrypting data, according to an exemplary embodiment of the present invention;

[26] FIG. 4 is a diagram showing the structure of a packet in accordance with a DTCP / IEEE 1394 standard;

[27] FIG. 5 is a diagram showing the structure of a packet in accordance with a DTCP / IP standard; and

[28] FIG. 6 is a flowchart illustrating a method of encrypting data, according to an exemplary embodiment of the present invention.

Best Mode

[29] According to an aspect of the present invention, there is provided a method of encrypting data, the method including dividing data in packet units into N data blocks; generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks; generating N counter values by increasing the initial value by a predetermined value N times and encrypting the N counter values using the encryption key; and performing an exclusive OR operation on the N encrypted counter values and the N data blocks.

[30] Each of the counter values may include a bit for representing the random number, a

bit for representing a transferred data block number, and a bit for representing a counter.

[31] Each of the counter values may include a bit for representing the random number, a bit for representing an additional random number which is different from the random number, and a bit for representing a counter.

[32] The method may further include generating a packet formed of a predetermined number of data blocks from among the N data blocks on which an exclusive OR operation is performed with the N encrypted counter values, and each of the counter values may include a bit for representing the random number, and a bit for representing partial information of the packet.

[33] Each of the counter values may further include a bit for representing a counter.

[34] The method may further include generating a packet formed of a predetermined number of data blocks from among the N data blocks on which an exclusive OR operation is performed with the N encrypted counter values, and each of the counter values may include a bit for representing the random number, a bit for representing a number of the packet, and a bit for representing a counter.

[35] The method may further include generating a packet formed of a predetermined number of data blocks from among the N data blocks on which an exclusive OR operation is performed with the N encrypted counter values, and the initial counter value may be changed for each packet.

[36] The initial counter value may be increased by a predetermined value for each packet.

[37] The method may further include generating the encryption key, and the generating of the encryption key may include generating the encryption key based on copy control information of the data, the random number, and an exchange key shared by apparatuses for encrypting and decrypting data.

[38] The random number may be periodically changed, and may be periodically increased by a predetermined value.

[39] Each data block may be 128 bits, each counter value may be 128 bits, and the random number may be equal to or greater than 64 bits.

[40] The packet may include a region which represents the random number, and may include a region which represents whether the random number is an odd number or an even number in order to represent whether the random number has changed.

[41] According to another aspect of the present invention, there is provided an apparatus for encrypting data, the apparatus including a data division unit which divides data in packet units into N data blocks; a random number generation unit which generates a random number used for generating an encryption key for encrypting the data blocks; a counter generation unit which generates an initial counter value using the random number and generates N counter values by increasing the initial value by a pre-

determined value N times; an encryption unit which encrypts the N counter values using the encryption key; and an operation unit which performs an exclusive OR operation on the N encrypted counter values and the N data blocks.

[42] The apparatus may further include a packet generation unit which generates a packet formed of a predetermined number of data blocks from among the N data blocks on which an exclusive OR operation is performed with the N encrypted counter values.

[43] The apparatus may further include an encryption key generation unit which generates the encryption key, wherein the encryption key generation unit generates the encryption key based on copy control information of the data, the random number, and an exchange key shared by apparatuses for encrypting and decrypting data.

[44] According to another aspect of the present invention, there is provided a computer readable recording medium having recorded thereon a computer program for executing a method of encrypting data, the method including dividing data in packet units into N data blocks; generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks; generating N counter values by increasing the initial value by a predetermined value N times and encrypting the N counter values using the encryption key; and performing an exclusive OR operation on the N encrypted counter values and the N data blocks.

Mode for Invention

[45] The present invention will now be described in detail by explaining exemplary embodiments of the invention with reference to the attached drawings.

[46] FIG. 3 is a diagram of an apparatus for encrypting data, according to an exemplary embodiment of the present invention.

[47] Referring to FIG. 3, the apparatus includes a data division unit 310, a random number generation unit 320, a counter generation unit 330, an encryption unit 340, and an operation unit 350.

[48] The data division unit 310 divides data in packet units into N data blocks. N is a natural number equal to or greater than 2.

[49] In this case, the data may be divided into 128-bit data blocks according to the current exemplary embodiment, but the present invention is not limited thereto. The data may also be divided into different sized data blocks.

[50] The random number generation unit 320 generates a random number to be used to generate an encryption key for encrypting the data blocks.

[51] The random number may be periodically increased by a predetermined value, for example, 1. In this case, a plurality of data blocks may be encrypted using the same encryption key generated using the same random number.

[52] Preferably, the apparatus for encrypting data according to an exemplary embodiment of the present invention may further include an encryption key generation unit (not

shown) which generates an encryption key. The encryption unit 340 encrypts a counter value using the encryption key generated by the encryption key generation unit.

[53] The encryption key generation unit generates the encryption key based on copy control information of the data, the random number, and an exchange key shared by the apparatus for encrypting data according to an exemplary embodiment of the present invention and an apparatus for decrypting data which decrypts the data encrypted by the apparatus for encrypting data.

[54] The encryption key generation unit periodically and randomly generates the exchange key, and the random number generation unit also periodically and randomly generates the random number.

[55] In this case, the cycle for generating the random number is shorter than the cycle for generating the exchange key. That is, the random number is generated more frequently than the exchange key.

[56] Based on the exchange key and the random number generated as described above and the copy control information of the data, the encryption key may be generated using a function shared by the apparatuses for encrypting and decrypting data, as in Mathematical Formula 1.

[57] $$K_C = \text{J-AES}(K_X, f[\text{EMI}], N_C) \qquad \text{Where:}$$

$$f[\text{EMI}] \{ \quad f[\text{EMI}]=C_a \text{ when EMI} = \text{Mode A} \quad f[\text{EMI}]=C_b \text{ when EMI} = \text{Mode B} \quad f[\text{EMI}]=C_c \text{ when EMI} = \text{Mode C} \quad \} \qquad \ldots(1)$$

[58] J-AES represents the function shared by the apparatuses for encrypting and decrypting data, Kx represents the exchange key, EMI (encryption mode indicator) represents the copy control information of the data, and Nc represents the random number.

[59] In this case, f[ ] is an operator which converts each EMI into an appropriate constant. For example, f[ ] may convert a 2-bit EMI into a 96-bit constant.

[60] Additionally, the EMI may have a plurality of modes. For example, 'copy-never', 'copy-one-generation', and 'no-more-copy' may be set respectively to Modes A, B and C.

[61] An encryption key Kc is changed in accordance with the mode of EMI, and changes of the exchange key Kx and the random number Nc.

[62] When the encryption key is generated by the apparatus for encrypting data as described above, the apparatus for decrypting data also has to have the encryption key

in order to decrypt the data encrypted using the encryption key.

[63] A method of generating the encryption key, performed by the apparatus for decrypting data, will now be described.

[64] The apparatus for encrypting data periodically and randomly generates the exchange key, encrypts the exchange key using an authentication key shared by the apparatuses for encrypting and decrypting data, and transfers the encrypted exchange key to the apparatus for decrypting data.

[65] The apparatus for decrypting data decrypts the encrypted exchange key using the authentication key and extracts the exchange key.

[66] Then, the apparatus for encrypting data periodically and randomly generates the random number and transfers the random number to the apparatus for decrypting data. However, under certain circumstances, the random number is not separately transferred but is recorded in a header of a packet when the apparatus for encrypting data transfers data in the form of a packet to the apparatus for decrypting data. When the packet is transferred, the EMI, which is the copy control information of the data, is recorded and transferred in the packet.

[67] FIG. 4 is a diagram showing the structure of a packet in accordance with a DTCP / IEEE 1394 standard.

[68] FIG. 4 shows an EMI region 410 and an Odd/Even region 420. The EMI region 410 represents an EMI, which is copy control information of data in a header of the packet, and the Odd/Even region 420 represents whether a random number is an odd number or an even number in order to represent whether the random number has changed.

[69] The above-described packet does not have a region which represents the random number itself, and it is assumed that a counter value is increased by a predetermined value in a counter mode. For example, if the counter value increases by 1, odd and even numbers are represented alternately in the Odd/Even region 420.

[70] FIG. 5 is a diagram showing the structure of a packet in accordance with a DTCP / IP standard

[71] Referring to FIG. 5, a header of the packet includes an extended encryption mode indicator (E-EMI) region 510 which represents an EMI, which is copy control information of data, and a random number region 520 which represents a random number.

[72] Here, the EMI region 410 illustrated in FIG. 4 is 2 bits, while the E-EMI region illustrated in FIG. 5 is 4 bits and may include more modes than the EMI region 410 illustrated in FIG. 4.

[73] The random number region 520 represents the random number Nc generated by the random number generation unit 320 illustrated in FIG. 3. The random number Nc may be 64 bits as in FIG. 5.

[74] Referring back to FIG. 3, the apparatus for decrypting data uses the exchange key, the random number, and the copy control information of the data generated as described above to generate an encryption key which is identical to the encryption key of the apparatus for encrypting data and is also used for decrypting the encrypted data.

[75] The counter generation unit 330 generates an initial counter value using the random number generated by the random number generation unit 320, and generates N counter values by increasing the initial counter value by a predetermined value N times.

[76] According to an exemplary embodiment of the present invention, the random number used for generating the encryption key is reused for generating the counter value. Accordingly, a fewer number of operations are required in comparison with the case when a random number for generating an encryption key and a random number for generating a counter value are generated separately.

[77] The detailed operation of the counter generation unit 330 will be described later with reference to Mathematical Formulae 2 through 6.

[78] The encryption unit 340 encrypts the N counter values into encryption keys.

[79] The operation unit 350 encrypts each of the data blocks by performing an exclusive OR operation on the encrypted counter values and the data blocks.

[80] The operation of the counter generation unit 330 will now be described.

[81] First, the counter generation unit 330 generates the initial counter value which may be formed as in Mathematical Formula 2.

[82] $$N_c | count \quad \ldots\ldots\ldots (2)$$

[83] Here, Nc represents the random number, and count represents a counter.

[84] For example, if the initial counter value is 128 bits, it may be formed of a 64-bit random number and a 64-bit counter. In this case, the counter may be disposed in front of the random number.

[85] The counter count may start at 0 but is not limited thereto.

[86] The counter values are determined by increasing the counter of Mathematical Formula 2 by the predetermined value. For example, if the counter is 4 bits and the counter of the initial counter value is 0000, the counter may be changed and increased by 1 to 0001, 0010, 0011 and so on. However, if the counter is increased to 1111, the next value of the counter 1111 is 0000 again.

[87] The counters may repeat the same values after they return again to 0000 as in the above-described example.

[88] In the encryption algorithm using the counter mode of the AES, a third party can recreate original data from encrypted data if a plurality of data blocks are encrypted

using the same encryption key and the same counter.

[89] Accordingly, if the random number is not changed and only the counter is changed, the same counter value may be reused while the encryption key is not changed. Therefore, the counter generation unit 330 needs to generate the counter values by changing composition forms of the counter values such that the same encryption keys do not have the same counter value.

[90] Examples of the counter values generated by changing values in order to prevent the counter generation unit 330 from reusing the same counter value will now be described.

[91] First, the counter generation unit 330 may generate the counter value to include a bit for representing a random number Nc, a bit for representing a number of transferred data blocks datablockno, and a bit for representing the counter count as in Mathematical Formula 3.

[92] In this case, if the random number Nc is changed, datablockno is recalculated from when the random number Nc is changed. Accordingly, datablockno of a first data block after the random number Nc is changed is set to 0.

[93] $$N_c|datablock_{no}|count$$

..... (3)

[94] For example, the counter value may include a bit for representing a 64-bit random number, a bit for representing a 32-bit transferred data block number, and a bit for representing a 32-bit counter.

[95] In this case, datablockno of a counter for encrypting a data block after 100 data blocks are transferred is 101. Thus, each data block has a different value of datablockno, and the same counter value is not used for the same encryption keys when the data is encrypted.

[96] If the data is formed in packets, datablockno is represented in a header of the packet, transferred to the apparatus for decrypting data, and used for calculating the counter value required for decrypting the packet.

[97] Preferably, but not necessarily, the apparatus for encrypting data according to an exemplary embodiment of the present invention may further include a packet generating unit (not shown) which generates a packet including a predetermined number of data blocks. In this case, each data block is included in the packet after an exclusive OR operation is performed on the data block and the counter value encrypted using the encryption key.

[98] Also, the counter generation unit 330 may generate the counter value to include a bit for representing the random number Nc, a bit for representing an additional random number Nc2 which is different from the random number Nc, and a bit for representing

the counter count as in Mathematical Formula 4.

[99] Here, if the additional random number Nc2 is identical to the random number Nc, the additional random number Nc2 is changed. If the random number Nc is changed, the additional random number Nc2 may not be changed.

[100] $$N_c|N_{c2}|count$$ ..... (4)

[101] For example, the counter value may include a bit for representing a 64-bit random number, a bit for representing a 32-bit additional random number, and a bit for representing a 32-bit counter.

[102] In this case, the random number generation unit 320 has to generate the additional random number Nc2 as well as the random number Nc for generating the encryption key. Accordingly, more operation is required than in the case when only one random number Nc is generated. However, since two random numbers Nc and Nc2 are used, the operation is more stable than when only one random number Nc is used.

[103] If the data is formed in packets, the additional random number Nc2 is represented in the header of the packet, transferred to the apparatus for decrypting data, and used for calculating the counter value required for decrypting the packet.

[104] Alternatively, the counter generation unit 330 may generate the counter value to include a bit for the random number Nc, a bit for representing a packet number packetno, and a bit for representing the counter count as in Mathematical Formula 5.

[105] $$N_c|packet_{no}|count$$ ..... (5)

[106] For example, the counter value may include a bit for representing a 64-bit random number, a bit for representing a 32-bit packet number, and a bit for representing a 32-bit counter.

[107] In this case, the packet number packetno of the counter value to be used for encrypting a data block included in a first packet is 1 and the packet number packetno of the counter value to be used for encrypting a data block included in a second packet is 2.

[108] In this case, if the random number Nc is changed, packetno is recalculated from when the random number Nc is changed. Accordingly, packetno of a first packet after the random number Nc is changed is set to 1.

[109] Thus, the same counter value is not used for the same encryption keys when the data is encrypted.

[110] If the data is formed in packets, packetno is represented in the header of the packet,

transferred to the apparatus for decrypting data, and used for calculating the counter value required for decrypting the packet.

[111] Also, the counter generation unit 330 may generate the counter value to include a bit for the random number Nc and a bit for representing partial information datapart of a packet as in Mathematical Formula 6.

[112]

$$N_c | data_{part}$$

..... (6)

[113] For example, the counter value may include a bit for representing a 64-bit random number, and a bit for representing 64-bit partial information of the packet.

[114] The partial information of the packet can be used as the counter value because information of each packet has randomness and the counter value can be kept different from other counter values using the randomness.

[115] Also, a counter may be further included in the counter value of Mathematical Formula 6. For example, the counter value may include a bit for representing a 64-bit random number, a bit for representing 32-bit partial information of the packet, and a bit for representing a 32-bit counter.

[116] Furthermore, the counter generation unit 330 may determine the initial counter value to be changed for each packet.

[117] That is, the random number Nc of the initial counter value of Mathematical Formula 2 is changed for each packet.

[118] In this case, whenever the random number Nc is changed, the encryption key is newly generated. Accordingly, additional operation for generating the random number Nc and the encryption key is required for each packet.

[119] The random number Nc may be changed by adding a predetermined value for each packet.

[120] Examples of counter values are not limited to Mathematical Formulae 2 through 6.

[121] FIG. 6 is a flowchart illustrating a method of encrypting data, according to an exemplary embodiment of the present invention.

[122] In operation 610, data in packet units is divided into N data blocks.

[123] In operation 620, an initial counter value is generated using a random number used for generating an encryption key for encrypting the data blocks.

[124] In operation 630, N counter values are generated by increasing the initial value by a predetermined value N times, and the N counter values are encrypted using the encryption key.

[125] In operation 640, an exclusive OR operation is performed on the encrypted counter values and the data blocks.

[126] The exemplary embodiments of the present invention can be written as computer programs and can be implemented in general-use digital computers that execute the programs using a computer readable recording medium. Examples of the computer readable recording medium include magnetic storage media (e.g. ROM, floppy disks, hard disks, etc.), and optical recording media (e.g. CD-ROMs, or DVDs).

[127] The exemplary embodiments of the present invention allow fast and stable data encryption by dividing data in packet units into N data blocks, generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks, generating N counter values by increasing the initial value by a predetermined value N times, encrypting the N counter values using the encryption key, and performing an exclusive OR operation on the encrypted counter values and the data blocks.

[128] While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various changes in form and detail 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 invention is defined not by the detailed description of the invention but by the appended claims, and all differences within the scope will be construed as being included in the present invention.

Claims

[1] 1. A method of encrypting data, the method comprising:
dividing data in packet units into N data blocks;
generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks;
generating N counter values by increasing the initial counter value by a predetermined value N times and encrypting the N counter values using the encryption key; and
performing an exclusive OR operation on the N encrypted counter values and the N data blocks.

[2] 2. The method of claim 1, wherein each of the N counter values comprises a bit representing the random number, a bit representing a transferred data block number, and a bit representing a counter.

[3] 3. The method of claim 1, wherein each of the N counter values comprises a bit representing the random number, a bit representing an additional random number which is different from the random number, and a bit representing a counter.

[4] 4. The method of claim 1, further comprising generating a packet formed of a plurality of data blocks from among the N data blocks on which the exclusive OR operation is performed with the N encrypted counter values, wherein each of the N counter values comprises a bit representing the random number, and a bit representing partial information of the packet.

[5] 5. The method of claim 4, wherein each of the N counter values further comprises a bit representing a counter.

[6] 6. The method of claim 1, further comprising generating a packet formed of a plurality of data blocks from among the N data blocks on which the exclusive OR operation is performed with the N encrypted counter values, wherein each of the N counter values comprises a bit representing the random number, a bit representing a number of the packet, and a bit representing a counter.

[7] 7. The method of claim 1, further comprising generating a packet formed of a plurality of data blocks from among the N data blocks on which the exclusive OR operation is performed with the N encrypted counter values, wherein the initial counter value is changed for each packet.

[8] 8. The method of claim 7, wherein the initial counter value is increased by a predetermined value for each packet.

[9] 9. The method of claim 1, further comprising generating the encryption key based on copy control information of the data, the random number, and an exchange key shared by apparatuses for encrypting and decrypting data.

[10] 10. The method of claim 1, wherein the random number is periodically changed.

[11] 11. The method of claim 1, wherein the random number is periodically increased by a predetermined value.

[12] 12. The method of claim 1, wherein each data block is 128 bits, each counter value is 128 bits, and the random number is equal to or greater than 64 bits.

[13] 13. The method of claim 7, wherein the packet comprises a region which represents the random number.

[14] 14. The method of claim 7, wherein the packet comprises a region which represents whether the random number is an odd number or an even number in order to represent whether the random number has changed.

[15] 15. An apparatus for encrypting data, the apparatus comprising:
a data division unit which divides data in packet units into N data blocks;
a random number generation unit which generates a random number used for generating an encryption key for encrypting the data blocks;
a counter generation unit which generates an initial counter value using the random number and generates N counter values by increasing the initial counter value by a predetermined value N times;
an encryption unit which encrypts the N counter values using the encryption key; and
an operation unit which performs an exclusive OR operation on the N encrypted counter values and the N data blocks.

[16] 16. The apparatus of claim 15, wherein each of the N counter values comprises a bit representing the random number, a bit representing a transferred data block number, and a bit representing a counter.

[17] 17. The apparatus of claim 15, wherein each of the N counter values comprises a bit representing the random number, a bit representing an additional random number which is different from the random number, and a bit representing a counter.

[18] 18. The apparatus of claim 15, further comprising a packet generation unit which generates a packet formed of a plurality of data blocks from among the N data blocks on which the exclusive OR operation is performed with the N encrypted counter values.

[19] 19. The apparatus of claim 18, wherein each of the N counter values comprises a bit representing the random number, and a bit representing partial information of the packet.

[20] 20. The apparatus of claim 19, wherein each of the N counter values further comprises a bit representing a counter.

[21] 21. The apparatus of claim 18, wherein each of the N counter values comprises a

bit representing the random number, a bit representing a number of the packet, and a bit representing a counter.

[22] 22. The apparatus of claim 18, wherein the counter generation unit determines the initial counter value to be changed for each packet.

[23] 23. The apparatus of claim 22, wherein the counter generation unit determines the initial counter value to be increased by a predetermined value for each packet.

[24] 24. The apparatus of claim 15, further comprising an encryption key generation unit which generates the encryption key based on copy control information of the data, the random number, and an exchange key shared by apparatuses for encrypting and decrypting data.

[25] 25. The apparatus of claim 15, wherein the random number generation unit periodically changes the random number.

[26] 26. The apparatus of claim 15, wherein the random number generation unit periodically increases the random number by a predetermined value.

[27] 27. The apparatus of claim 15, wherein each data block is 128 bits, each counter value is 128 bits, and the random number is equal to or greater than 64 bits.

[28] 28. The apparatus of claim 18, wherein the packet comprises a region which represents the random number.

[29] 29. The apparatus of claim 18, wherein the packet comprises a region which represents whether the random number is an odd number or an even number in order to represent whether the random number has changed.

[30] 30. A computer readable recording medium having recorded thereon a computer program for executing a method of encrypting data, the computer program comprising:

dividing data in packet units into N data blocks;

generating an initial counter value using a random number used for generating an encryption key for encrypting the data blocks;

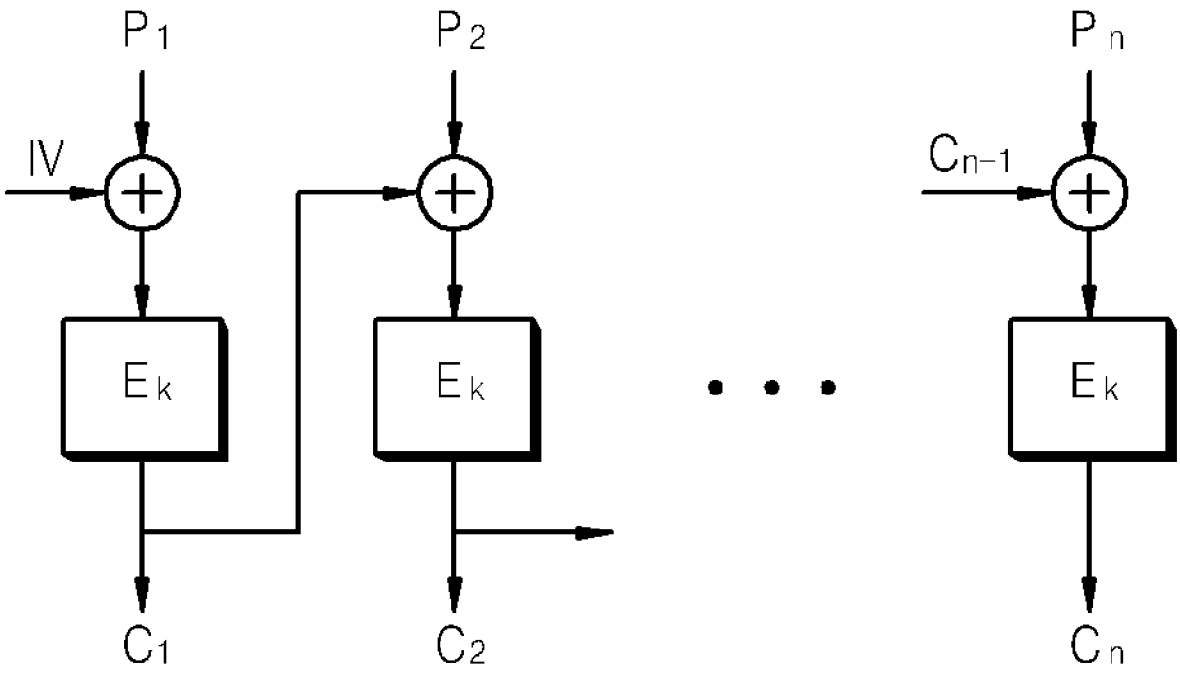
generating N counter values by increasing the initial counter value by a predetermined value N times and encrypting the N counter values using the encryption key; and

performing an exclusive OR operation on the N encrypted counter values and the N data blocks.

WO 2008/069473 PCT/KR2007/005844

FIG. 1

<ENCRYPTION>



<DECRYPTION>

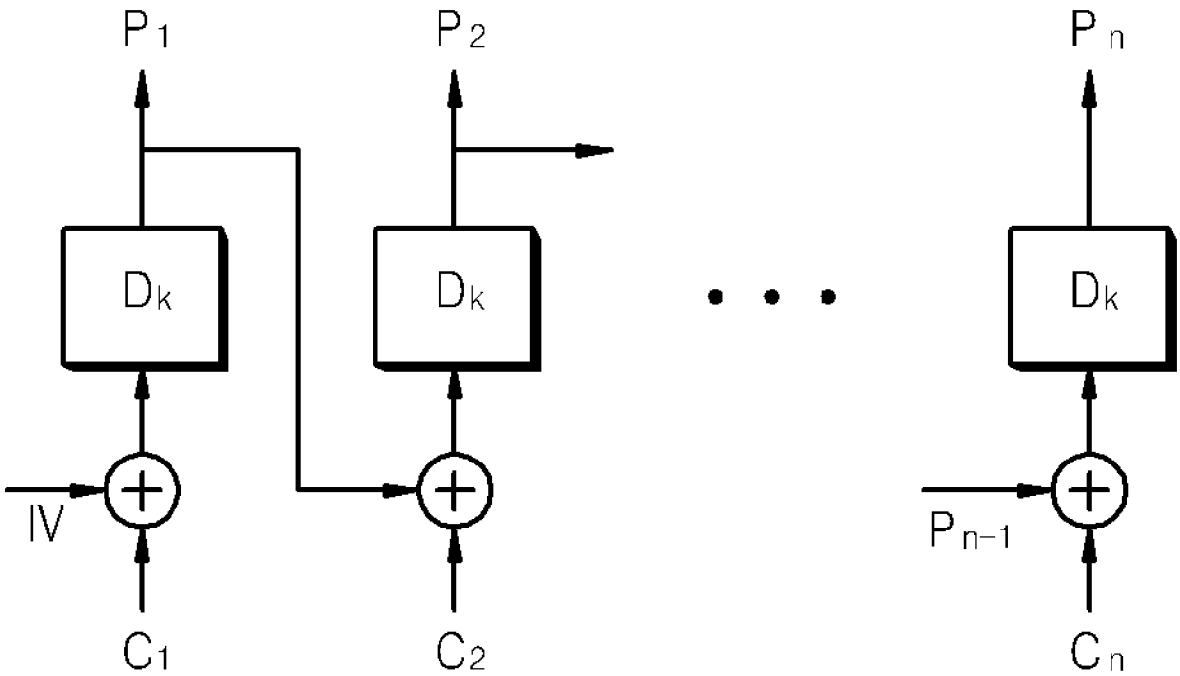


FIG. 2

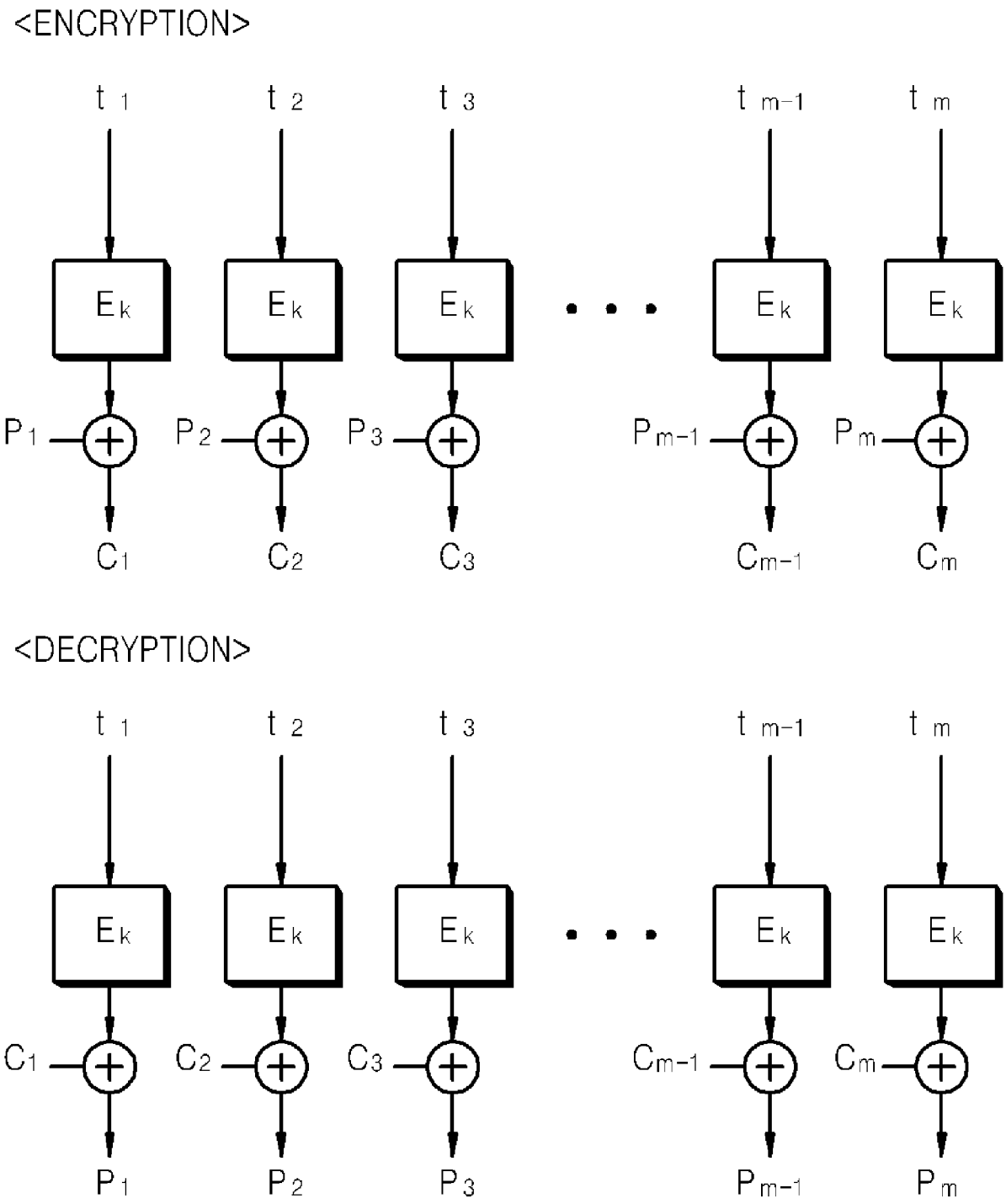

<ENCRYPTION>
t 1
t 2
t 3
t m-1
t m
Ek
P1
P2
P3
Pm-1
Pm
C1
C2
C3
Cm-1
Cm
<DECRYPTION>
t 1
t 2
t 3
t m-1
t m
Ek
C1
C2
C3
Cm-1
Cm
P1
P2
P3
Pm-1
Pm

FIG. 3

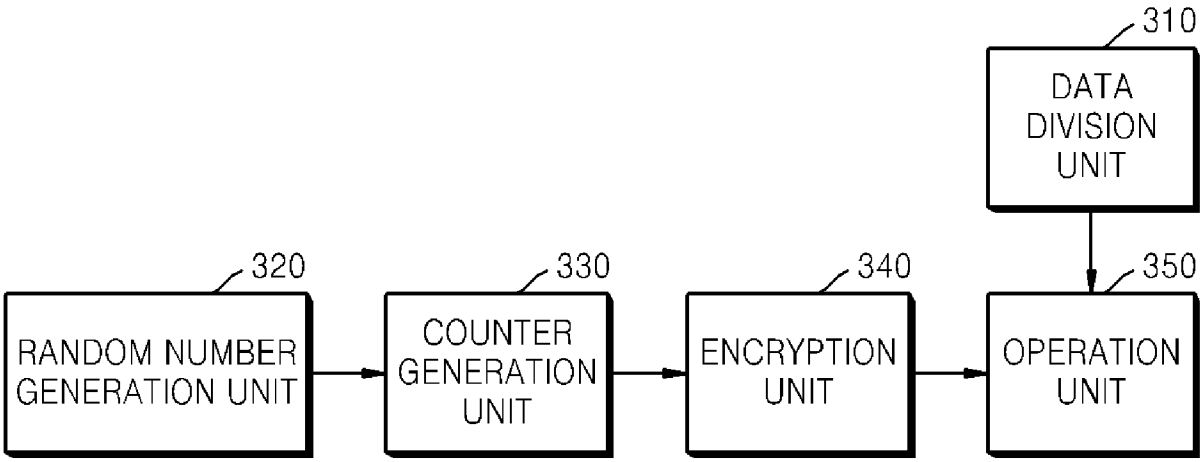

310
DATA DIVISION UNIT
320
RANDOM NUMBER GENERATION UNIT
330
COUNTER GENERATION UNIT
340
ENCRYPTION UNIT
350
OPERATION UNIT

FIG. 4

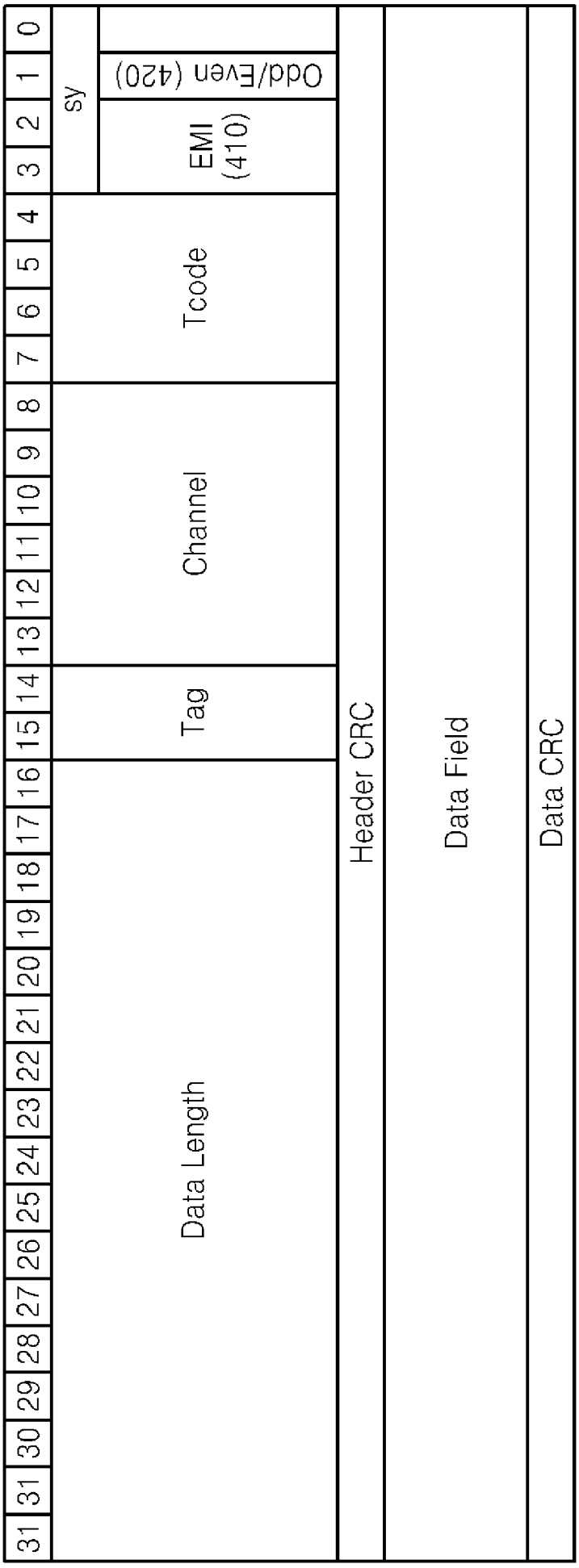

31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
sy
Odd/Even (420)
EMI (410)
Tcode
Channel
Tag
Data Length
Header CRC
Data Field
Data CRC

FIG. 5

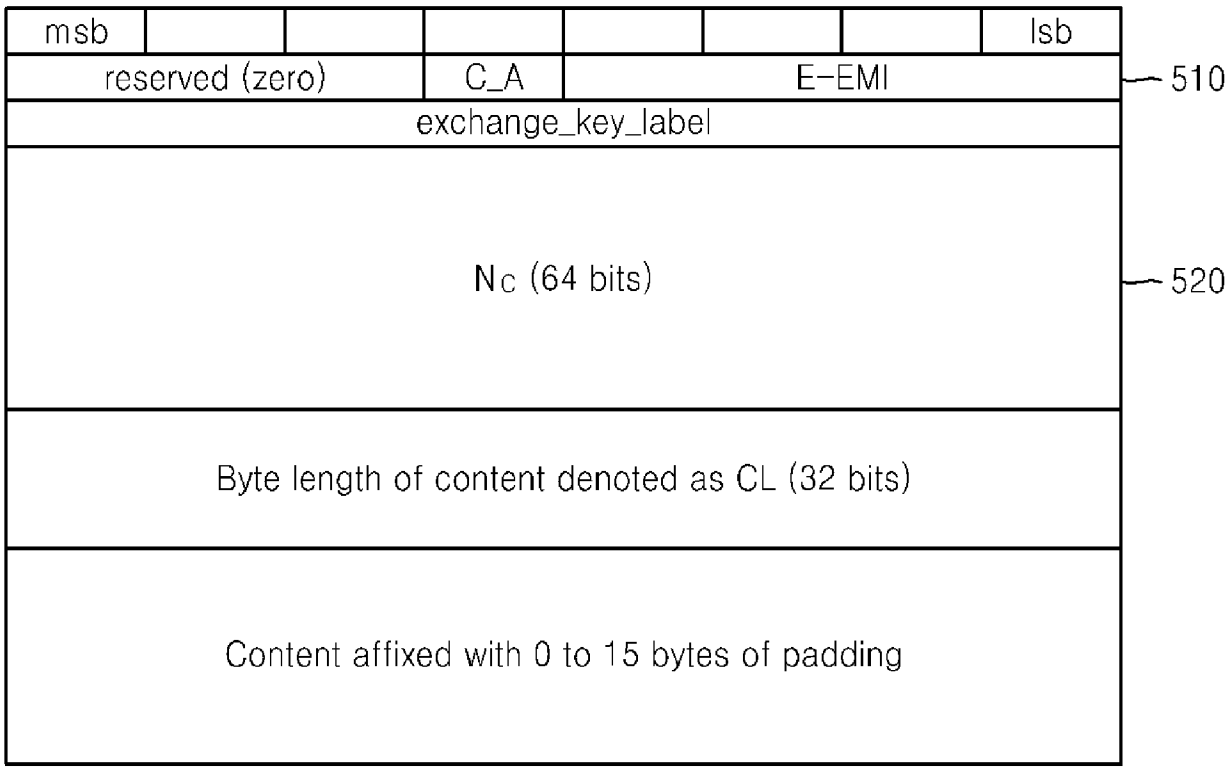
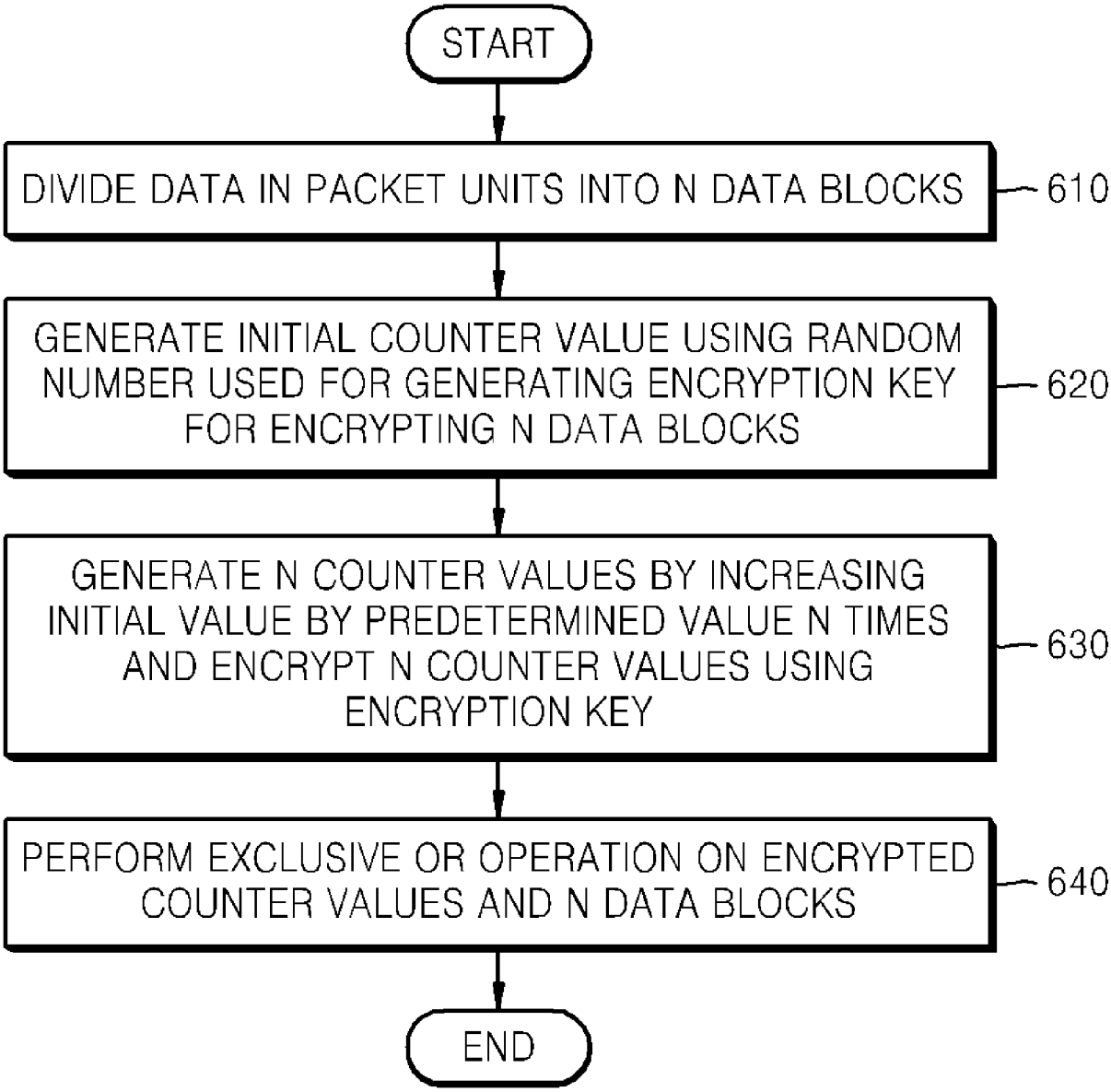

msb
lsb
reserved (zero)
C_A
E-EMI
510
exchange_key_label
Nc (64 bits)
520
Byte length of content denoted as CL (32 bits)
Content affixed with 0 to 15 bytes of padding

FIG. 6


START
DIVIDE DATA IN PACKET UNITS INTO N DATA BLOCKS
610
GENERATE INITIAL COUNTER VALUE USING RANDOM NUMBER USED FOR GENERATING ENCRYPTION KEY FOR ENCRYPTING N DATA BLOCKS
620
GENERATE N COUNTER VALUES BY INCREASING INITIAL VALUE BY PREDETERMINED VALUE N TIMES AND ENCRYPT N COUNTER VALUES USING ENCRYPTION KEY
630
PERFORM EXCLUSIVE OR OPERATION ON ENCRYPTED COUNTER VALUES AND N DATA BLOCKS
640
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/005844

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

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

eKIPASS(KIPO internal), "data encryption", "counter key"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DAVID WAGNER et al., "Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption", September 2000, http://www.cs.ucdavis.edu/~rogaway/papers/ctr.pdf see Review of Counter-Mode Encryption and Figure 1: Encryption and decryption process in counter mode	1-30
A	US 2004/0131182 A1 (PHILLIP W. ORGAWAY) 8 July 2004. see abstract and claims 1-47	1-30

☐ 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	Date of mailing of the international search report
26 FEBRUARY 2008 (26.02.2008)	**26 FEBRUARY 2008 (26.02.2008)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

LEE, Jun Seok

Telephone No. 82-42-481-8199

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/005844

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004/0131182 A1	08.07.2004	None	