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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 May 2006 (26.05.2006)

PCT

(10) International Publication Number
WO 2006/054843 A1

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

(21) International Application Number:
PCT/KR2005/003762

(22) International Filing Date:
8 November 2005 (08.11.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/628,386 17 November 2004 (17.11.2004) US
10-2004-0099434 30 November 2004 (30.11.2004) KR

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

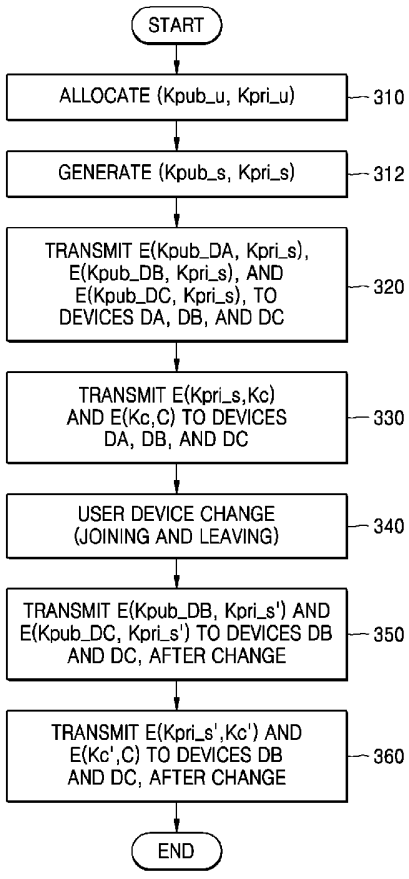
(72) Inventors: **KIM, Myung-Sun**; 105-104 Daewoo Apt., Sam-dong, Uiwang-si, Gyeonggi-do 437-751 (KR). **HAN, Sung-Hyu**; 102-1006 Family Apt., Munjeong 2-dong, Songpa-gu, Seoul 138-767 (KR). **YOU, Yong-Kuk**; 115-206 Doosan Apt., Geumho-dong 3-ga, Seongdong-gu, Seoul 133-751 (KR). **YOON, Young-Sun**; 511-704 Sangrok Apt., 341-515, Gwonseon-dong, Gwonseon-gu, Suwon-si, Gyeonggi-do 441-742 (KR). **LEE, Jae-Heung**; (206), 1250-8 Maetan 3-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-848 (KR). **KIM, Bong-Seon**; 903-411 Jugong Apt., 901-906 Geumgok-dong, Bundang-gu, Seongnam-si, Gyeonggi-do 463-724 (KR).

(74) Agent: **Y.P. LEE, MOCK & PARTNERS**; The Cheonghwa Building, 1571-18 Seocho-dong, Seocho-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, KN, 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.

[Continued on next page]

(54) Title: METHOD FOR TRANSMITTING CONTENT IN HOME NETWORK USING USER-BINDING



(57) Abstract: A method for transmitting content to a user device from a home server in a home network is provided. The method includes: receiving an allocated user public key and a user private key of a user to whom the home server belongs; generating an arbitrary session public key and a session private key, generating an encrypted session private key by encrypting the session private key using a device public key that is a public key of the user device, and transmitting the encrypted session private key to the user device; and transmitting the content encrypted using a predetermined content key and a content key encrypted using the session private key to the user device. According to the method, by binding the content to each user, instead of to each device, the content can be safely and conveniently shared.

WO 2006/054843 A1

(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*

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

METHOD FOR TRANSMITTING CONTENT IN HOME NETWORK USING USER-BINDING

Technical Field

[1] The present invention relates to a content transmission method, and more particularly, to a content transmission method enabling user devices in a home network to share content more conveniently and safely.

Background Art

[2] Digital content is transmitted to a user by a content provider. The content should be protected such that only after the user obtains a proper right by paying a fee for the content, the user can use the digital content and if the proper right is not obtained, the user cannot use the content.

[3] In order to prevent an unauthorized user from obtaining the content, the content should be encrypted with a content key and the content key should be distributed only to an authorized user.

[4] Meanwhile, with the latest development of home network technologies, one user can own more than one user device, and also, the movement of content between devices becomes possible. Sometimes, a user wants to use content in all devices owned by the user, with one payment. However, if the content can be moved freely in a reproducible way between devices, an unauthorized user can obtain and use the content. Accordingly, in home networking, a technology which permits a movement of content between user devices in a home network of an authorized user while preventing an unauthorized user from obtaining the content or using the content even if the content obtained, is needed.

[5] In particular, Federal Communications Commission (FCC) of the U.S. requires from July, 2005, a technology by which a 1-bit broadcast flag (BF) should be inserted into a high density (HD) level content broadcast through digital broadcasting in the U.S. so that if the BF of the content is 1, the content can be protected such that an unauthorized user cannot use the content.

[6] FIG. 1 is a diagram showing the structure of a home network.

[7] A content provider CP transmits content to a home server HS through a transmission channel 10.

[8] The home server HS is connected to user devices DA, DB, and DC, and manages joining and secession of an authorized user device, and transmits the content only to an authorized user device, that is, a device currently registered.

[9] Here, a domain refers to a set of user devices connected to one home server. The

devices in a domain will vary due to user devices joining or leaving the home network. Accordingly, a process for preventing a user device that has left and is no longer registered with the home network from obtaining content is needed.

[10] Content is encrypted by using a content key and the content key is encrypted by using a common key, and the content and the content key are transmitted to each of the user devices DA, DB, and DC. The common key can be obtained only by a user device that is currently registered in the home network.

[11] FIG. 2 is a flowchart of the operations performed by the conventional method for transmitting content.

[12] In operation 210, the home server HS receives content C from the transmission channel 10, and by encrypting the content C using a content key Kc, the home server HS generates an encrypted content E(Kc, C). The transmission channel 10 can be any of a variety of channels, such as the Internet, ground wave, and satellite broadcasting.

[13] In operation 220, the user device DA transmits its unique information Xa' to the home server HS.

[14] In operation 230, the home server HS generates a common key Ks by using the unique information Xa', and then transmits it to the user device DA.

[15] In operation 240, the home server HS transmits the encrypted content E(Kc, C), an encrypted content key E(Ks, Kc), and a license L_A to user device DA.

[16] The license L_A includes usage rule UR on the content C and the unique information Xa' of the user device DA.

[17] In operation 250, the user device DA extracts the unique information Xa' from the license L_A received in operation 240, and then compares this with DA's own unique information Xa.

[18] In operation 260, the user device DA determines if Xa'=Xa and whether or not it is possible to generate the content key Kc by decoding the encrypted content key E(Ks, Kc) received in operation 240 by using the common key Ks received in operation 230. If these two conditions are met, the user device DA in operation 220 is the same as the user device DA in operation 240, and therefore the user device DA can reproduce the content C.

[19] However, the conventional method has the following drawbacks.

[20] First, since the content C is bound to a user device, sharing the content in two or more user devices belonging to the same user is inconvenient. All these devices, that is, even devices belonging to the same user, must receive newly issued licenses based on their respective unique information. For example, when the device DB tries to reproduce the content received from the device DA, operations for transmitting unique information Xb' of the device DB, generating content Kc', generating common key Ks', and generating license L_B for the device DB must all be performed again.

[21] Secondly, unique information of a user device is exposed to external devices.

[22] Since most of the unique information Xa', Xb', ..., of user devices play important roles in the security aspect, it is preferable to avoid leakage of this information.

[23] Thirdly, sharing content between user devices should be performed through the home server HS.

[24] Generally, since authorization of use of the content C relies, in most cases, on a fee payment by a user and one user wants to use freely content in two or more user devices belonging to the domain of the user, the drawbacks described above become more serious obstacles to the development of home networks, the demand for which is currently increasing.

Disclosure of Invention

Technical Problem

[25]

Technical Solution

[26] The present invention provides a method for transmitting content in a home network by binding the content to each user instead of to each device so that the content can be safely and conveniently shared.

Advantageous Effects

[27] According to aspects of the present invention as described above, in a home network, by binding content to each user with using a common key structure, not to each device, the content can be safely and conveniently shared.

Description of Drawings

[28] 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:

[29] FIG. 1 is a diagram showing the structure of a home network;

[30] FIG. 2 is a flowchart of the operations performed by the conventional method for transmitting content;

[31] FIG. 3 is a flowchart of the operations performed by a method for transmitting content from a home server to a user device according to an exemplary embodiment of the present invention;

[32] FIG. 4 illustrates an example of a home network according to an exemplary embodiment of the present invention;

[33] FIG. 5 illustrates a method for transmitting content between user devices according to an exemplary embodiment of the present invention;

[34] FIG. 6 illustrates a method for transmitting content between user devices according to another exemplary embodiment of the present invention; and

[35] FIG. 7 illustrates a process for examining whether or not session keys are identical when session keys are updated, in the content transmission method of FIG. 5.

Best Mode

[36] According to an aspect of the present invention, there is provided a method for transmitting content to a user device from a home server in a home network, the method including: the home server receiving an allocated user public key and user private key of the user to whom the home server belongs; generating an arbitrary session public key and session private key, generating an encrypted session private key by encrypting the session private key using a device public key that is a public key of the user device, and transmitting the encrypted session private key that is generated to the user device; and transmitting content that is encrypted using a predetermined content key and content key encrypted using the session private key to the user device. The session public key and session private key may be updated whenever the user device joins or a change in registration of the user device with the home network occurs.

[37] According to another aspect of the present invention, there is provided a method for transmitting content from a second user device to a first user device in a home network, the method including: the second user device receiving a user public key of a second user to whom the second user device belongs; generating a device certificate value by using a predetermined device value and the public key of the second user, and then transmitting the device certificate value to the home server of the first user device by using the device certificate value and the user private key of the first user to whom the first user device belongs, and determining whether or not the first user and the second user are identical based on the server certificate value generated by the home server and the device value; and receiving content encrypted by using a predetermined content key, and a content key encrypted by using a predetermined session public key, the content and content key being transmitted by the second user device if the first user and the second user are determined to be identical, wherein, the session private key corresponding to the session public key is transmitted to the user device by using a pair of the public key and private key of the user device if registration of the user device with the home network changes.

[38] The device certificate value may be generated by the following equation:

[39] $C\_A=m^{Kpub\_u1'}$

[40] where C_A is the device certificate value, m is a device value, and Kpub_u1' is a user public key transmitted by the second user device.

[41] The server certificate value may be generated by the following equation:

[42] $C\_A'=C\_A^{Kpri\_u1}$

[43] where C_A' is the server certificate value, and Kpri_u1 is the user public key of the

first user.

[44] The determination of whether or not the first user and the second user are identical may be performed by examining whether or not the server certificate value C_A' is the same as the device value m.

[45] The device certificate value may be generated by the following equation:

[46] $C\_A=m*r^{Kpub\_u1'}$

[47] where C_A is the device certificate value, m is a device value, Kpri_u1' is the user public key transmitted by the second device, and r is an arbitrary random number.

[48] The server certificate value may be generated by the following equation:

[49] $C\_A'=C\_A^{Kpri\_u1}$

[50] where C_A' is the server certificate value, and Kpri_u1 is the user public key of the first user.

[51] The determining whether the first user and the second user are identical may comprise determining whether a value that is obtained by dividing the server certificate value C_A' by arbitrary random number r is the same as device value m.

[52] The method may further include determining whether a session private key of the first device is identical to a session private key of the second user device by using an electronic signature if the first user and the second user are determined to be identical.

[53] The determining of whether the session private key of the first user device is identical to the session private key of the second user device may include: the first user device generating a first electronic signature value by encrypting an arbitrary first random number with using the session private key of the first user device; the first user device transmitting the first electronic signature value and the first random number to the second user device; and the second user device decoding the first signature value by using the session public key of the second user device, and determining whether or not a result value that is generated by decoding the first electronic signature is identical to the first random number.

[54] The determining of whether the session private key of the first user device is identical to the session private key of the second user device may further include: the second user device generating a second electronic signature value by encrypting an arbitrary second random number with using the session private key of the second user device; the second user device transmitting the second electronic signature value and the second random number to the first user device; and the first user device decoding the second signature value by using the session public key of the first user device, and determining whether a result value that is generated by decoding the second electronic signature is identical to the second random number.

Mode for Invention

[55] Aspects of the present invention will now be described more fully with reference to

the accompanying drawings, in which exemplary embodiments of the invention are shown.

[56] Referring to FIG. 3, it is assumed that at present user devices DA, DB, and DC are connected to a home server HS, a home network HN is formed with the home server HS and user devices DA, DB, and DC which belong to user U.

[57] In operation 310, the home server HS receives a user common key Kpub_u and a user private key Kpri_u that are allocated to the user U to whom the home server HS belongs. According to the characteristics of a common key structure, the user common key Kpub_u is public and the user private key Kpri_u is owned only by the home server HS.

[58] In operation 312, the home server HS generates a pair of arbitrary session keys (Kpub_s, Kpri_s), that is, a session common key Kpub_s and a session private key Kpri_s. Likewise, according to the characteristics of a common key structure, a common key Kpub_s is public and private key Kpri_s can be obtained only by user devices connected to the current home server HS, that is, user devices belonging to the domain of the home server HS.

[59] In operation 320, the home server HS encrypts the session private key Kpri_s by using device common keys Kpub_DA, Kpub_DB, and Kpub_DC to generate encrypted session private keys E(Kpub_DA, Kpri_s), E(Kpub_DB, Kpri_s), and E(Kpub_DC, Kpri_s) and the home server HS then transmits the encrypted session private keys E(Kpub_DA, Kpri_s), E(Kpub_DB, Kpri_s), and E(Kpub_DC, Kpri_s) to the user devices DA, DB, and DC, respectively.

[60] In operation 330, in response to requests of the user devices DA, DB, and DC, the home server HS transmits the encrypted content E(Kc, C) and the encrypted content key E(Kpri_s, Kc) to the user devices DA, DB, and DC. Here, Kc indicates the content key.

[61] In operation 340, a change in user devices occurs. For example, the user device DA may leave the home network HN. Selling a user device to another user can be an example of this change of user devices.

[62] In operation 350, the home server HS generates a pair of new session keys (Kpub_s', Kpri_s') and then, transmits the new session private key Kpri_s' in an encrypted state to user devices that belongs to home network HN after the change, that is, the user devices DB and DC.

[63] That is, by encrypting the new session private key Kpri_s' by using the device common keys Kpub_DB and Kpub_DC, the home server HS generates encrypted session private keys E(Kpub_DB, Kpri_s') and E(Kpub_DC, Kpri_s'), and transmits the encrypted session private keys to the user devices DB and DC, respectively.

[64] In operation 360, in response to requests from the user devices DB and DC, the

home server HS transmits the encrypted content E(Kc', C) and the encrypted content key E(Kpri_s, Kc') to the user devices DB and DC. Here, Kc' indicates the new content key.

[65] According to the method of FIG. 3, all of the user devices DA, DB, and DC belonging to the user U can obtain the session private key Kpri_s before the user device DA leaves the home network, and therefore can reproduce the content C. Accordingly, the inconvenience of requiring each user device to separately obtain an individual license can be reduced.

[66] Also, since a user device does not need to transmit unique information to the home server, unnecessary leakage of unique information can be prevented.

[67] FIG. 4 illustrates an example of a home network according to an exemplary embodiment of the present invention.

[68] In FIG. 4, it is assumed that at present user devices DA, DB, and DC are connected to a home server HS1, and a home network HN is formed with the home server HS1 and the user devices DA, DB, and DC, which belong to the user U. At this time, the user device DA is going to leave the home network HN.

[69] According to the method for transmitting content of FIG. 3, after the user device DA leaves the home network HN, a pair of session keys (Kpub_s, Kpri_s) is updated with a new pair of session keys (Kpub_s', Kpri_s) such that after leaving, the user device DA cannot reproduce content transmitted to the user devices DB and DC after the user device DA leaves. However, since the user device DA still has session private key Kpri_s, if an encrypted content E(Kc, C) and an encrypted content key E(Kpri_s, Kc) transmitted by the user device DB are received, the user device DA can obtain and reproduce the content C, that is, the content that was transmitted to the user device DA before the user device DA left the home network HN.

[70] Due to digital content policies, a case where content transmitted by the user device DB and received by the user device DA before the user device DA left the home network and then reproducing the content by the user device DA after the user device DA has left the home network should be prevented. For example, the user device DA may register in a home network HN2 of another user U2. In this case, the use of the content C of user U by the user U2 should be prevented. A method for transmitting content between user devices of FIG. 5 should be suggested in this case.

[71] FIG. 5 illustrates a method for transmitting content between user devices according to an exemplary embodiment of the present invention.

[72] It is assumed that at present a home server HS1 and user devices DA, DB, and DC belong to a home network HN1 of user U1, and a home server HS2 and user devices DD, and DE belong to a home network HN2 of user U2.

[73] In operation 510, the user device DA requests the user device DB to send content C.

[74] In operation 520, the user device DB transmits a user common key Kpub_u1' of the user to whom the user device DB belongs to the user device DA.

[75] In operations 530 and 535, the user device DA generates a device certificate value C_A by using a predetermined device value m and the user common key Kpub_u1' received in operation 520, and then, the user device DA transmits the certificate value C_A to the home server HS1 to which the user device DA belongs. The device certificate value C_A is generated, for example, as in the following Equation 1:

[76] $C\_A=m^{Kpub\_u1'}$ (Equation 1)

[77] In operations 540 and 545, the home server HS1 generates a server certificate value C_A' by using the device certificate value C_A received in operation 535 and the user private key Kpri_u1 of the user U1 to whom the home server HS1 belongs, and then transmits the server certificate value C_A' to the user device DA. The server certificate value C_A' is generated, for example, as in following Equation 2:

[78] $C\_A'=C\_A^{Kpri\_u1}$ (Equation 2)

[79] In operation 550, based on the device certificate value C_A and the device value m, the user device DA examines whether or not the user U1 of the user device DA is the same as the user of the user device DB. If the users are identical, operation 560 is performed and if not, operation 580 is performed.

[80] When the device certificate value C_A and the server certificate value C_A' are defined as in Equation 1 and Equation 2, if the user of the user device DB is U1 (i.e., the user common key Kpub_u1' transmitted in operation 520 of the user (not confirmed) to whom the user device DB belongs is the user common key Kpub_u1 of the user U1) the server certificate value C_A' and device value m are identical as shown in the following Equation 3:

[81] $C\_A'=C\_A^{Kpri\_u1}$

[82] $=(m^{Kpub\_u1'})^{Kpri\_u1}$

[83] $=m^{Kpub\_u1'*Kpri\_u1}$

[84] $=m^{Kpub\_u1'*Kpri\_u1}$

[85] $=m$ (Equation 3)

[86] In operation 560, the user device DA transmits a success message (SUCCESS) to the user device DB.

[87] In operation 570, if the user device DB receives the success message (SUCCESS), the user device DB transmits the encrypted content key E(Kpub_s, Kc) and the encrypted content E(Kc, C) to the user device DA.

[88] In operation 580, since the user of user device DA is not the same as the user of the user device DB, the user device DA determines that content C cannot be received by transmission and stops the process.

[89] In the above exemplary embodiment, since the user device DA receives the server

certificate value C_A', including information on the user, from the home server HS1, the user device DA cannot pretend that the user to whom the user device DA belongs to is another user. That is, if the user device DA comes to belong to a home network of another user U2, the user device DA will receive a server certificate value from the home server HS2 and therefore, Equation 3 is not satisfied.

[90] Accordingly, only when the user of user device DB is the same as the user of the user device DA, the user device DA can transmit a success message (SUCCESS) to the user device DB. That is, only when the user device DA proves that the user of the user device DB is the same as the user of the user device DA, user device DA can receive content transmitted by the user device DB.

[91] FIG. 6 illustrates a method for transmitting content between user devices according to another exemplary embodiment of the present invention.

[92] As in FIG. 5, it is assumed that a home server HS1 and user devices DA, DB, and DC belong to a home network HN1 of a user U1, and a home server HS2 and user devices DD, and DE belong to a home network HN2 of user U2.

[93] In operation 610, the user device DA requests the user device DB to send content C.

[94] In operation 620, user device DB transmits a user common key Kpub_u1' of the user to whom the user device DB belongs to the user device DA.

[95] In operations 630 and 635, the user device DA generates a certificate value C_A by using an arbitrary random number r, a predetermined device value m and the user common key Kpub_u1' that is received in operation 620, and then, transmits the certificate value C_A to the home server HS1 to which the user device DA belongs. The device certificate value C_A is generated, for example, as in the following Equation 4:

[96] $C\_A=m*r^{Kpub\_u1'}$ (Equation 4)

[97] In operations 640 and 645, the home server HS1 generates a server certificate value C_A' by using the device certificate value C_A received in operation 635 and the user private key Kpri_u1 of user U1 to whom the home server HS1 belongs, and then transmits the server certificate value C_A to the user device DA. The server certificate value C_A' is generated, for example, as in the following Equation 5:

[98] $C\_A'=C\_A^{Kpri\_u1}$ (Equation 5)

[99] In operation 650, based on the arbitrary random number r, the device certificate value C_A and the device value m used in operation 630, the user device DA examines whether or not the user U1 of the user device DA is the same as the user of the user device DB. If the users are identical, operation 660 is performed. However, if the users are not identical, operation 680 is performed.

[100] When the device certificate value C_A and the server certificate value C_A' are defined as in Equation 4 and Equation 5, if the user of the user device DB is U1 (i.e.,

the user common key Kpub_u1' transmitted in operation 620, of the user (not confirmed) to whom the user device DB belongs is the user common key Kpub_u1 of the user U1) then C_A'r-1 obtained by dividing the server certificate value C_A' by the random number r is the same as the device value m. This is shown in the following Equation 6:

[101] $C\_A'*r^{-1}=^{C\_AKpri\_u1}*r^{-1}$

[102] $=(m*r^{Kpub\_u1'})^{Kpri\_u1}*r^{-1}$

[103] $= m^{Kpri\_u1}*r^{Kpub\_u1'*Kpri\_u1}*r^{-1}$

[104] $= m^{Kpri\_u1}*r^{Kpub\_u1*Kpri\_u1}*r^{-1}$

[105] $=m*r*r^{-1}$

[106] $=m$ (Equation 6)

[107] In operation 660, the user device DA transmits a success message (SUCCESS) to the user device DB.

[108] In operation 670, if the user device DB receives the success message (SUCCESS), the user device DB transmits the encrypted content key E(Kpub_s, Kc) and the encrypted content E(Kc, C) to the user device DA.

[109] In operation 680, since the user of the user device DA is not the same as the user of the user device DB, the user device DA determines that content C cannot be received by transmission and the process is stopped.

[110] As in FIG. 5, since the user device DA receives the server certificate value C_A' including information on the user from the home server HS1, the user device DA cannot pretend that the user to whom the user device DA belongs to is another user. That is, if the user device DA comes to belong to a home network of another user U2, the user device DA will receive a server certificate value from the home server HS2 and therefore, Equation 6 is satisfied. Accordingly, only when the user of the user device DB is the same as the user of the user device DA can the user device DA transmit a success message (SUCCESS) to the user device DB. That is, only when the user device DA proves that the user of the user device DB is the same as the user of the user device DA can the user device DA receive content transmitted by the user device DB.

[111] In the exemplary embodiments of FIGS. 5 and 6, it is possible to define a device value m as m=h(Xa), obtained by hashing unique information Xa of the user device DA.

[112] Since the unique information Xa is hashed and then transmitted to the home server HS1, the unique information Xa is not exposed to the outside.

[113] FIG. 7 illustrates a process for examining whether session keys are identical when session keys are updated, in the content transmission method of FIG. 5.

[114] Even when the user devices DA and DB belong to the same user U1, if the time

when the user device DA joins the home network HN1 is different from the time when user device DB joins the home network HN1, the session key Kpri_s held by the user device DB is different from the session key Kpri_s' held by the user device DA. For example, there can be a case where the user devices DB and DC are in the home network HN1 before time t1, and the user device DB joins the home network HN1 at time t1.

[115] Since a session key used for encrypting a content key is updated if there is a change in elements of a home network, even though the user device DA receives the encrypted content key E(Kpub_s, Kc) transmitted by the user device DB, newly joined user device DA does not have the session key Kpri_s (i.e., the session key before joining the home network) and therefore user device DA cannot obtain content key Kc. Accordingly, when content is transmitted between the user devices DA and DB, a process for examining whether or not versions of session keys are identical is additionally required.

[116] Assuming that the situation is shown as in Table 1, a process for examining the version of a session key will now be explained. Here, the user device DA wants to receive content C from the user device DB.

[117] <Table 1>

[118]

	Before t1	After t1
User devices of HN1	DB, DC	DA, DB, DC
Pair of session keys	Kpri_s, Kpub_s	Kpri_s', Kpub_s'
Encrypted content key	E(Kpub_s, Kc)	E(Kpub_s', Kc)

[119] In operation 710, the user device DA electronically signs using an electronic signature function S( ) with a first random number r, which is an arbitrary random number, and the session private key Kpri_s'. That is, the user device DA generates the electronic signature value S_A=S(Kpri_s', r) by encrypting the first random number r using the session private key Kpri_s' held by the user device DA.

[120] In operation 720, the user device DA transmits the electronic signature value S_A generated in operation 710 and the first random number r to the user device DB.

[121] In operation 730, the user device DB verifies the electronic signature value S_A that is transmitted in operation 720, by using a verification function V( ). That is, the user device DB decodes the electronic signature value S_A transmitted in operation 720 by using the session common key Kpub_s held by the user device DB, and examines whether or not the generated result value, V(Kpub_s, S_A) is the same as the first random number r transmitted in operation 720.

[122] If the session private key Kpri_s' used for electronically signing by the user device DA is the same as the session private key Kpri_s paired with the session public key Kpub_s held by the user device DB, result value V(Kpub_s, S_A) is the same as first random number r. Thus, the version of a session key pair held by the user device DA is the same as that of a session key pair held by the user device DB.

[123] In operation 740, the user device DB electronically signs by using electronic signature function S( ) with a second random number related to the first random number r in operation 730, for example, r+1, and session private key Kpri_s. That is, the user device DB generates an electronic signature value S_B=S(Kpri_s, r+1) by encrypting the related random number (r+1) with the session private key Kpri_s, which is held by the user device DB.

[124] In operation 750, the user device DB transmits the electronic signature value S_B generated in operation 740 and the related random number (r+1) to the user device DA.

[125] In operation 760, the user device DA verifies the electronic signature value S_B transmitted in operation 750 by using the verification function V( ). That is, the user device DA decodes the electronic signature value S_B transmitted in operation 750 by using the session public key Kpub_s' held by user device DA, and examines whether or not the generated result value V(Kpub_s', S_B) is the same as the second random number (r+1) that is obtained by adding 1 to the first random number in operation 710.

[126] In the same manner as in operations 710 through 730, if the session private key Kpri_s used for electronically signing by the user device DB is the same as the session private key Kpri_s' that is paired with the session public key Kpub_s' held by the user device DA, the result value V(Kpub_s', S_B) is the same as the second random number (r+1). This means that the version of the session key pair held by user device DB is the same as that of session key pair held by the user device DA.

[127] The process for examining the version of session keys in operations 710 through 760 is added between operations 660 and 670 in FIG. 5. That is, the process for examining whether or not the versions of session key pairs of the user devices DA and DB are identical is added after the process for confirming whether or not the user devices DA and DB belong to an identical user.

[128] Meanwhile, the method for transmitting content according to an exemplary embodiment of the present invention described above can be implemented as a computer program. Codes and code segments forming the program can be easily inferred by the programmers in the technology field of the present invention. Also, the program is stored in computer readable media, and read and executed by a computer to implement the filtering method. The computer readable media includes magnetic recording media, optical recording media and carrier wave media.

[129] While aspects of 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 details may be made therein without departing from the spirit and scope of the present invention as defined by the following claims. The exemplary embodiments should be considered in 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.

Industrial Applicability

[130]

Sequence List Text

[131]

Claims

[1] 1. A method of transmitting content to a user device from a home server in a home network, the method comprising:
transmitting the content, which is encrypted by using a predetermined content key, and transmitting the predetermined content key, which is encrypted by using a pair of a predetermined session public key and a session private key, to the user device, wherein the content that is transmitted is bound to a user by using a user public key and a user private key of the user to whom the home server belongs.

[2] 2. The method of claim 1, wherein the transmitting comprises:
receiving the user public key and the user private key, which are allocated, of the user to whom the home server belongs;
generating an arbitrary session public key and a session private key, generating an encrypted session private key by encrypting the session private key using a device public key, which is a public key of the user device, and transmitting the encrypted session private key to the user device; and
transmitting, to the user device, the content, which is encrypted by using a predetermined content key, and a content key, which is encrypted by using the session private key.

[3] 3. The method of claim 2, wherein the session public key and the session private key are updated if the user device joins a new home network or a change in registration of the user device with the home network occurs.

[4] 4. The method of claim 2, wherein the user device obtains the session private key by decoding the encrypted session private key using a device private key and the user device obtains the predetermined content key by decoding the encrypted content key using the session private key.

[5] 5. A method of transmitting content from a second user device to a first user device in a home network, the method comprising:
determining whether a user of the first user device is identical to a user of the second device based on pairs of user public keys and user private keys of the first user device and the second user device, and transmitting the content from the second user device to the first user device only if the user of the first device and the user of the second device are determined to be identical, wherein the content is bound to a user by a user public key and a user private key of the user to whom each of the user devices belongs.

[6] 6. The method of claim 5, wherein the determining comprises:
receiving, from the second user device, a user public key of a second user to whom the second user device belongs;

generating a device certificate value by using a predetermined device value and the public key of the second user, and transmitting the device certificate value that is generated to the home server of the first user device;

determining whether the first user and the second user are identical based on the server certificate value that is generated by the home server by using the device certificate value and the user private key of the first user to whom the first user device belongs and the predetermined device value; and

receiving the content that is encrypted by using a predetermined content key, and a content key that is encrypted by using a predetermined session public key, wherein the content and the content key are transmitted by the second user device if the first user and the second user are determined to be identical,

wherein the session private key that corresponds to the session public key is transmitted to the user device by using a pair of the public key and private key of the user device if registration of the user device with the home network changes.

[7] 7. The method of claim 6, wherein the device certificate value (C_A) is generated using the following equation:

$C\_A=m^{Kpub\_u1'}$

where m is a device value, and Kpub_u1' is a user public key that is transmitted by the second user device.

[8] 8. The method of claim 7, wherein the server certificate value (C_A') is generated using the following equation:

$C\_A'=C\_A^{Kpri\_u1}$

where Kpri_u1 is the user private key of the first user.

[9] 9. The method of claim 8, wherein the determining whether or not the first user and the second user are identical comprises determining whether the server certificate value (C_A') is the same as the device value (m).

[10] 10. The method of claim 6, wherein the device certificate value (C_A) is generated using the following equation:

$C\_A=m*r^{Kpub\_u1'}$

where m is a device value, Kpub_u1' is the user public key transmitted by the second device, and r is an arbitrary random number.

[11] 11. The method of claim 10, wherein the server certificate value (C_A') is generated using the following equation:

$C\_A'=C\_A^{Kpri\_u1}$

where Kpri_u1 is the user public key of the first user.

[12] 12. The method of claim 11, wherein the determining whether the first user and the second user are identical comprises determining whether a value that is obtained by dividing the server certificate value (CA') by an arbitrary random

number (r) is the same as the device value (m).

[13] 13. The method of claim 6, further comprising:
determining the content from the second user device cannot be received and stopping transmission of content if the users are determined not to be identical.

[14] 14. The method of claim 6, further comprising:
determining whether a session private key of the first user device is identical to a session private key of the second user device by using an electronic signature if the users are determined to be identical.

[15] 15. The method of claim 14, wherein the determining whether the session private key of the first user device is identical to the session private key of the second user device comprises:
generating, at the first user device, a first electronic signature value by encryptin g an arbitrary first random number using the session private key of the first user device;
transmitting, from the first user device, the first electronic signature value and the first random number to the second user device; and
decoding, at the second user device, the first electronic signature value by using the session public key of the second user device, and determining whether a result value that is generated by decoding the first electronic signature value is identical to the first random number.

[16] 16. The method of claim 15, wherein the determining whether the session private key of the first user device is identical to the session private key of the second user device further comprises:
generating, at the second user device, a second electronic signature value by encrypting an arbitrary second random number using the session private key of the second user device;
transmitting, from the second user device, the second electronic signature value and the second random number to the first user device; and
decoding, at the first user device, the second electronic signature value by using the session public key of the first user device, and determining whether a result value that is generated by decoding the second electronic signature is identical to the second random number.

[17] 17. The method of claim 16, wherein the first random number and the second random number are related to each other.

[18] 18. A computer readable recording medium having embodied thereon a computer program for executing a method of transmitting content to a user device from a home server in a home network, the method comprising:
transmitting the content, which is encrypted by using a predetermined content

key, and transmitting the predetermined content key, which is encrypted by using a pair of a predetermined session public key and a session private key, to the user device, wherein the content that is transmitted, is bound to a user by using a user public key and a user private key of the user to whom the home server belongs.

[19] 19. A computer readable medium having embodied thereon a computer program for executing a method of transmitting content from a second user device to a first user device in a home network, the method comprising:

determining whether a user of the first user device is identical to a user of the second device based on pairs of user public keys and user private keys of the first user device and the second user device, and transmitting the content from the second user device to the first user device only if the users of the first device and the second device are determined to be identical, wherein the content is bound to a user by a user public key and a user private key of the user to whom each of the user devices belongs,

wherein the determining comprises:

receiving, from the second user device, a user public key of a second user to whom the second user device belongs;

generating a device certificate value by using a predetermined device value and the public key of the second user, and transmitting the device certificate value that is generated to the home server of the first user device;

determining whether the first user and the second user are identical based on the server certificate value that is generated by the home server by using the device certificate value and the user private key of the first user to whom the first user device belongs and the predetermined device value; and

receiving the content that is encrypted by using a predetermined content key, and a content key that is encrypted by using a predetermined session public key, wherein the content and the content key are transmitted by the second user device if the first user and the second user are determined to be identical,

wherein the session private key that corresponds to the session public key is transmitted to the user device by using a pair of the public key and private key of the user device if registration of the user device with the home network changes.

WO 2006/054843 PCT/KR2005/003762

FIG. 1

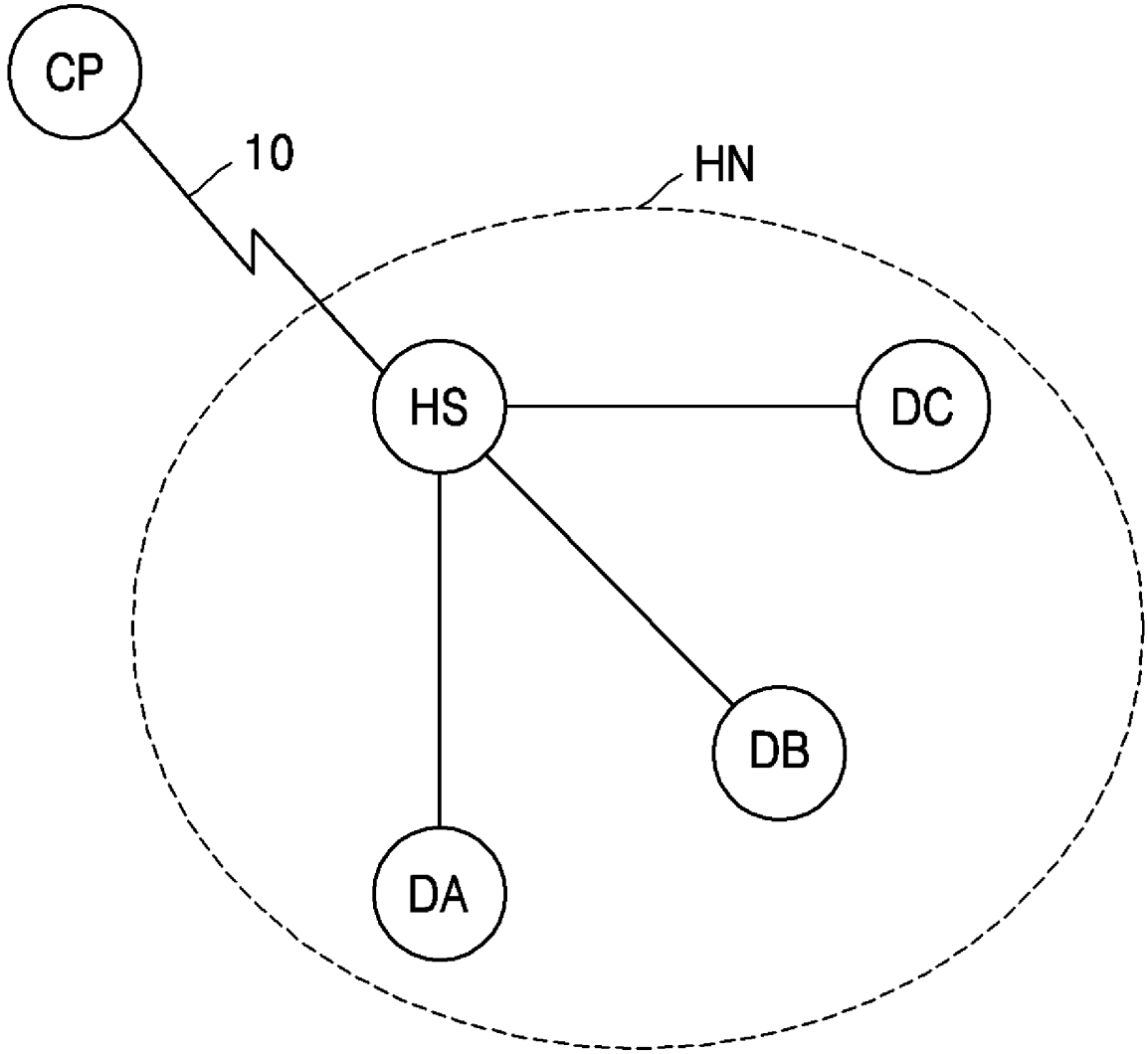


FIG. 2

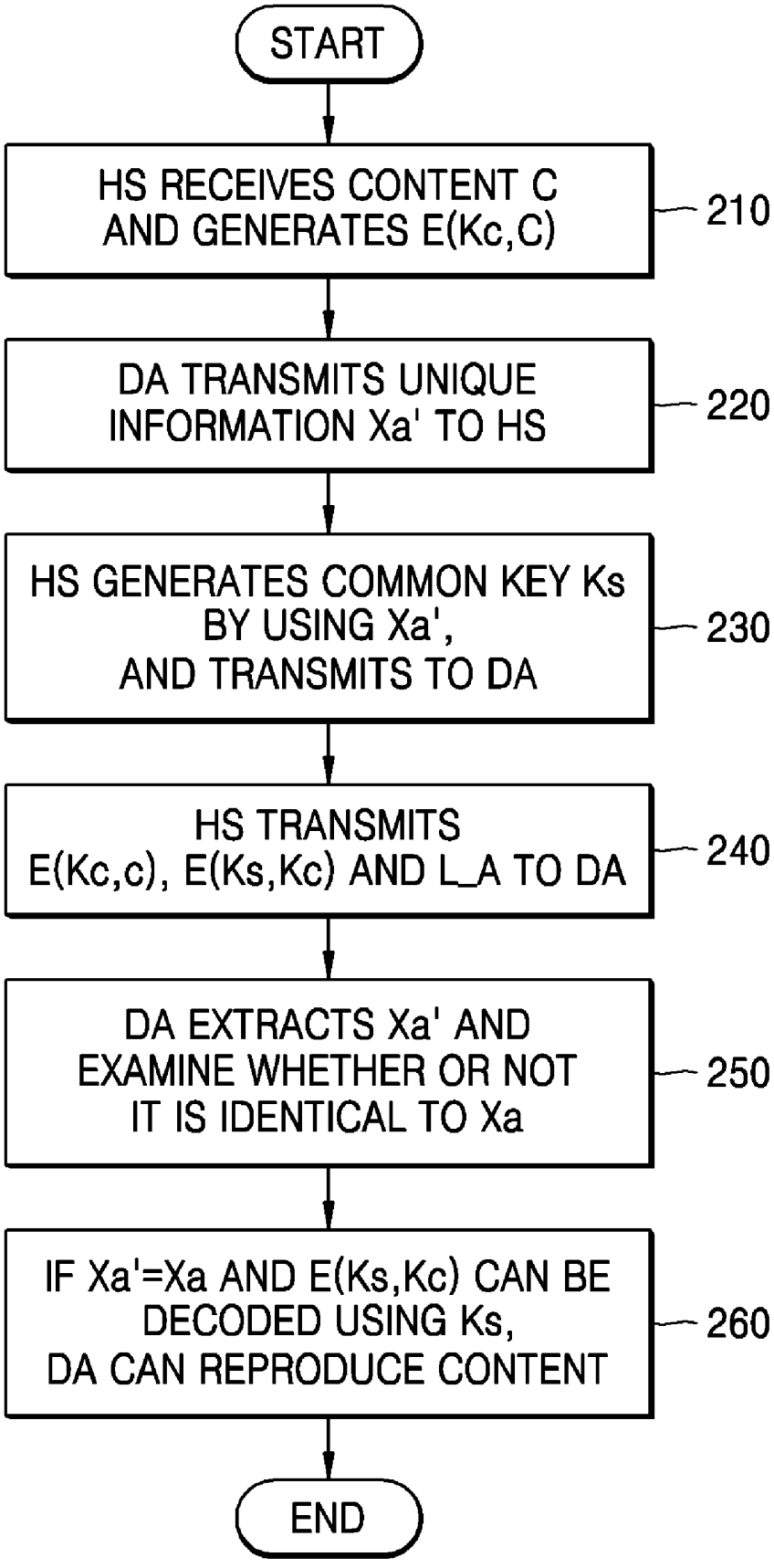

START
HS RECEIVES CONTENT C AND GENERATES E(Kc,C)
210
DA TRANSMITS UNIQUE INFORMATION Xa' TO HS
220
HS GENERATES COMMON KEY Ks BY USING Xa', AND TRANSMITS TO DA
230
HS TRANSMITS E(Kc,c), E(Ks,Kc) AND L_A TO DA
240
DA EXTRACTS Xa' AND EXAMINE WHETHER OR NOT IT IS IDENTICAL TO Xa
250
IF Xa'=Xa AND E(Ks,Kc) CAN BE DECODED USING Ks, DA CAN REPRODUCE CONTENT
260
END

FIG. 3

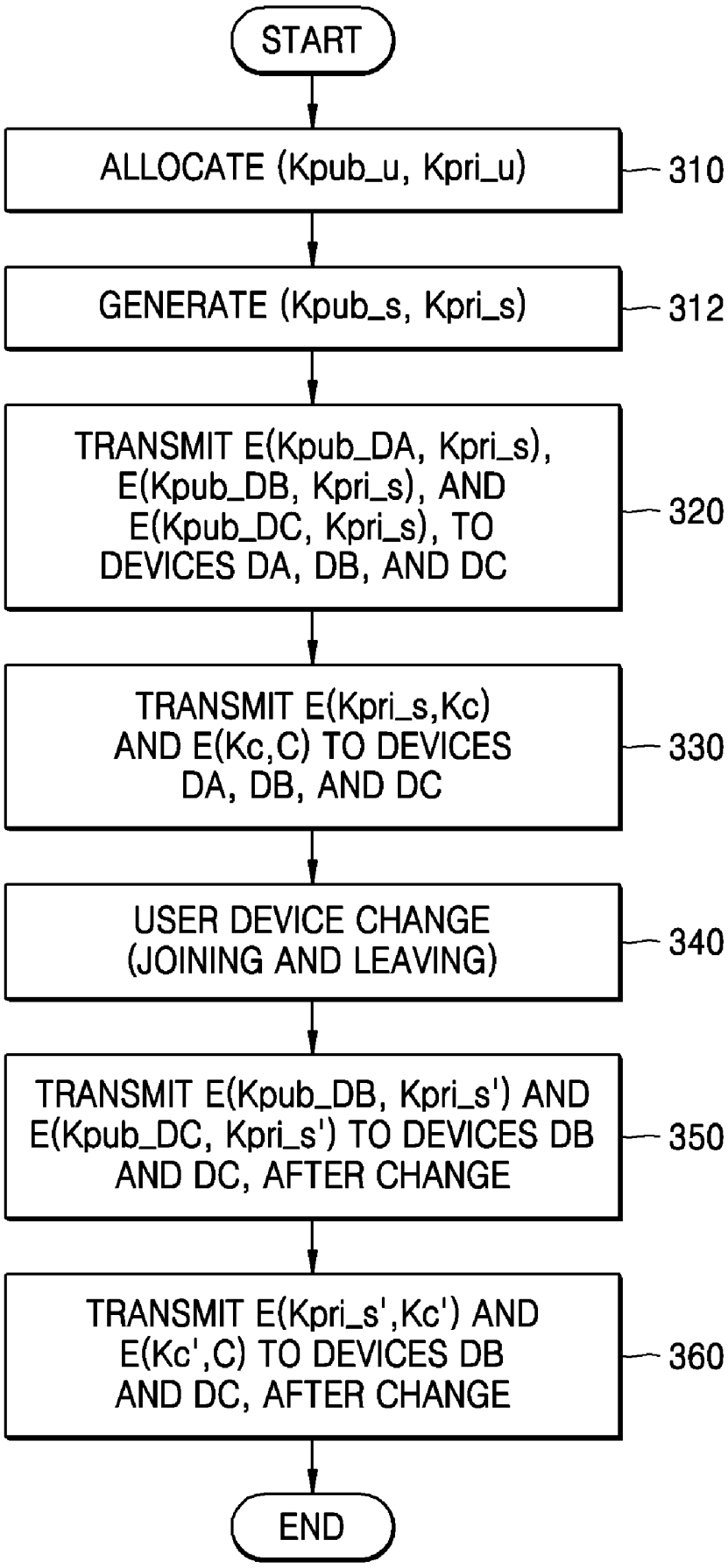

START
ALLOCATE (Kpub_u, Kpri_u)
310
GENERATE (Kpub_s, Kpri_s)
312
TRANSMIT E(Kpub_DA, Kpri_s), E(Kpub_DB, Kpri_s), AND E(Kpub_DC, Kpri_s), TO DEVICES DA, DB, AND DC
320
TRANSMIT E(Kpri_s,Kc) AND E(Kc,C) TO DEVICES DA, DB, AND DC
330
USER DEVICE CHANGE (JOINING AND LEAVING)
340
TRANSMIT E(Kpub_DB, Kpri_s') AND E(Kpub_DC, Kpri_s') TO DEVICES DB AND DC, AFTER CHANGE
350
TRANSMIT E(Kpri_s',Kc') AND E(Kc',C) TO DEVICES DB AND DC, AFTER CHANGE
360
END

FIG. 4

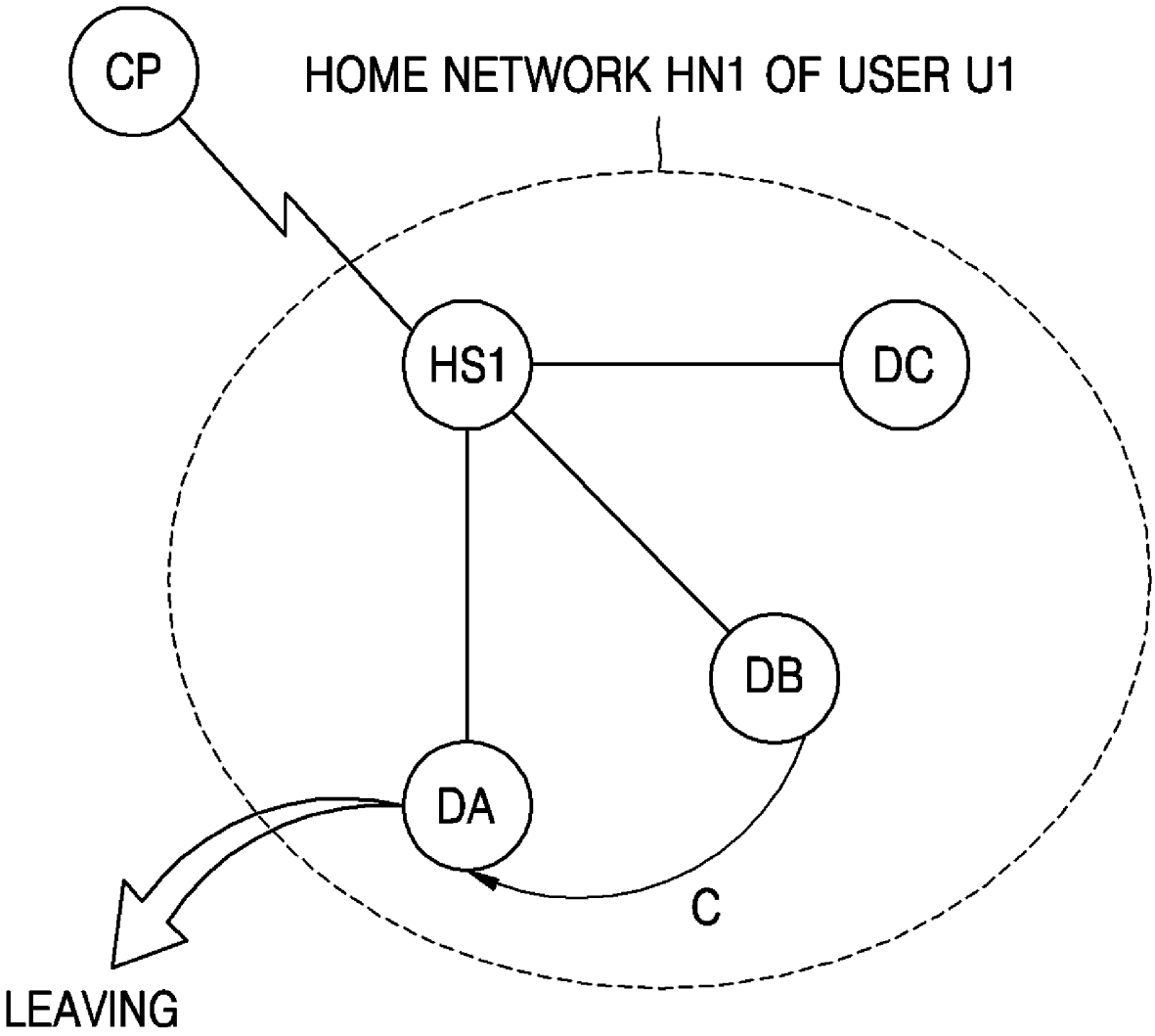


FIG. 5

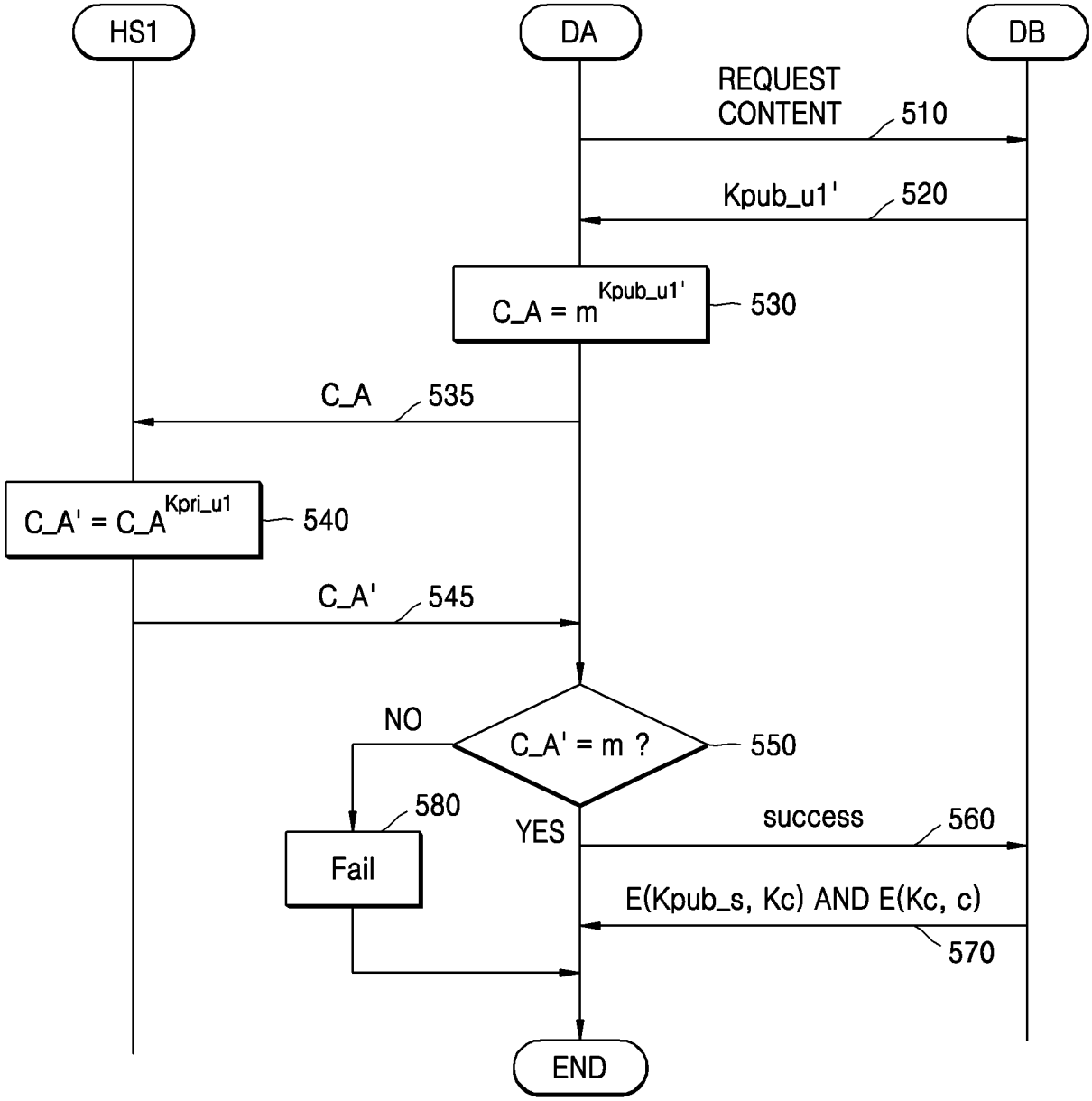

HS1
DA
DB
REQUEST CONTENT
510
Kpub_u1'
520
C_A = m^Kpub_u1'
530
C_A
535
C_A' = C_A^Kpri_u1
540
C_A'
545
NO
C_A' = m ?
550
580
Fail
YES
success
560
E(Kpub_s, Kc) AND E(Kc, c)
570
END

FIG. 6

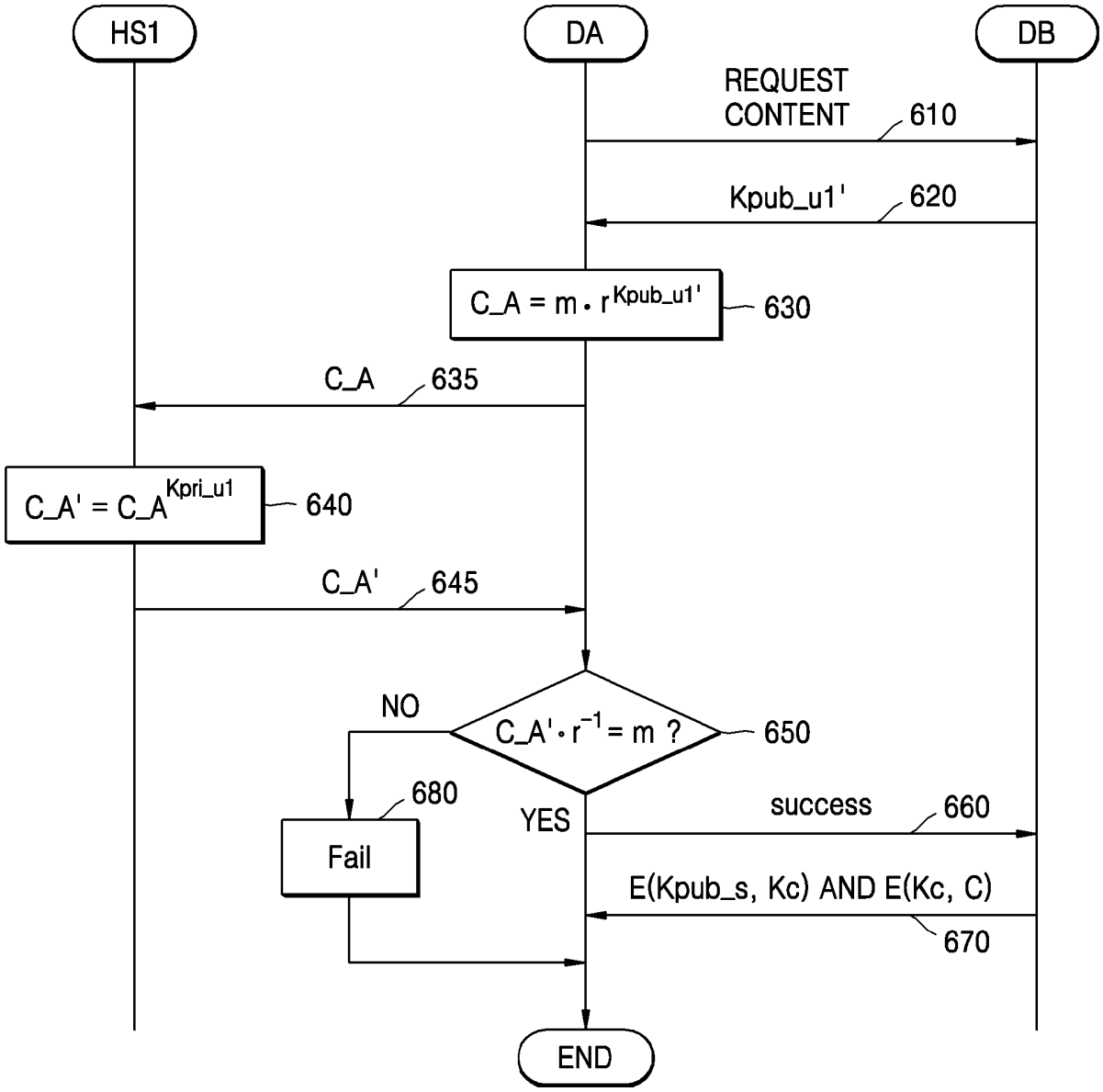
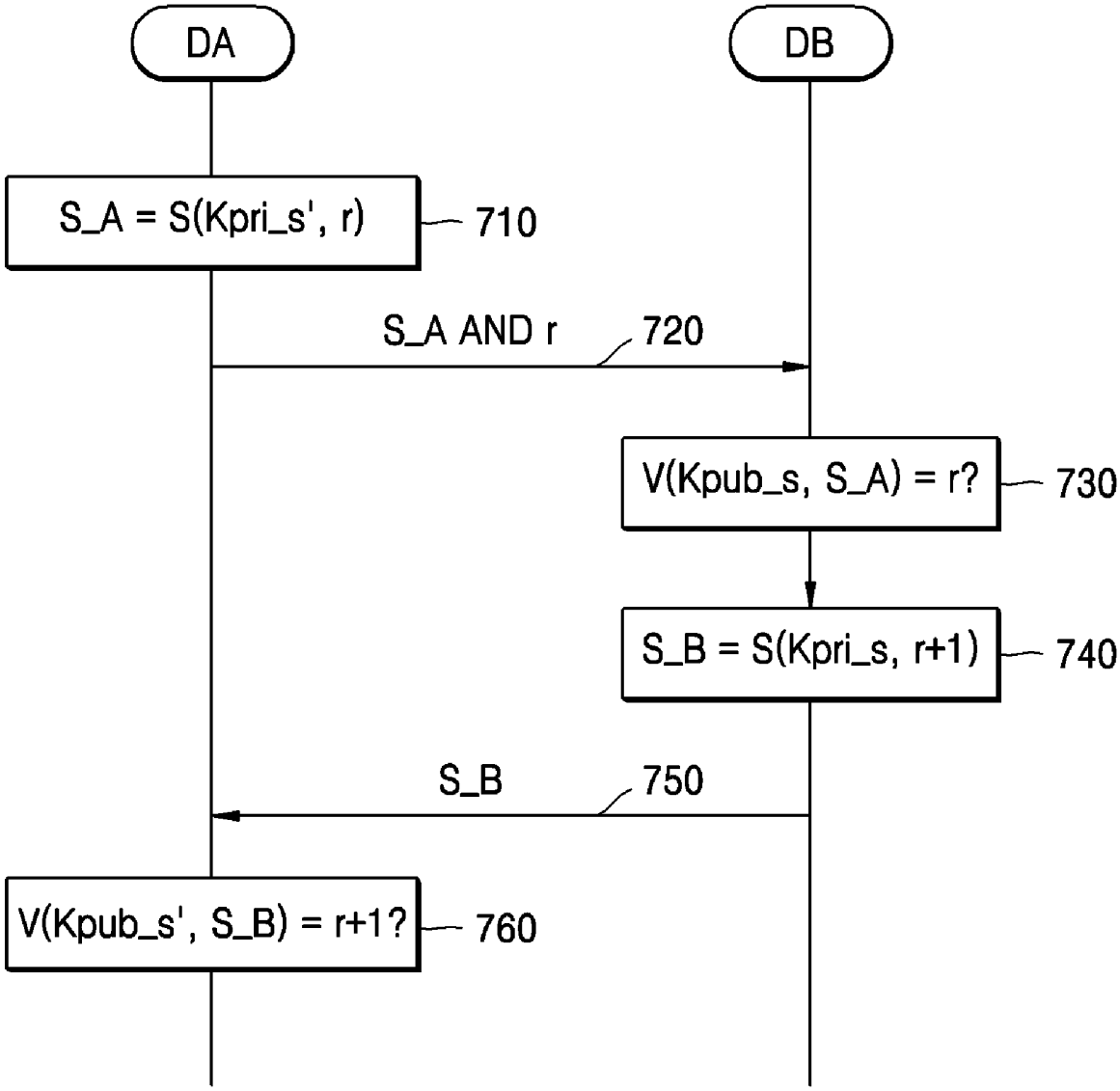

HS1
DA
DB
REQUEST CONTENT
610
Kpub_u1'
620
C_A = m • r^Kpub_u1'
630
C_A
635
C_A' = C_A^Kpri_u1
640
C_A'
645
NO
C_A' • r^-1 = m ?
650
680
Fail
YES
success
660
E(Kpub_s, Kc) AND E(Kc, C)
670
END

FIG. 7


DA
DB
S_A = S(Kpri_s', r)
710
S_A AND r
720
V(Kpub_s, S_A) = r?
730
S_B = S(Kpri_s, r+1)
740
S_B
750
V(Kpub_s', S_B) = r+1?
760

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/003762

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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)

IPC8 : H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Patents and applications for inventions since 1975
Korean Utility models and applictions for Utility models since 1975
Japanese Utility models and application for Utility models since 1975

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/0059939 A1 (Sun Microsystems, Inc.) 25 March 2004 (see abstract, figure 35, claim 1)	1 ~ 19
A	US 2004/0133908 A1 (BroadQ, LLC.) 8 July 2004 (see abstract, figure 1, claim 1)	1 ~ 19
A	US 6636968 B1 (Koninklijke Philips Electronics) 21 October 2003 (see abstract, figure 2, claim 1)	1 ~ 19

☐ 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
03 MARCH 2006 (03.03.2006)	**03 MARCH 2006 (03.03.2006)**

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
LEE, Dong Hwan
Telephone No. 82-42-481-5755

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2005/003762

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US20040059939A1	25.03.2004	US2004059939A1	25.03.2004
		US2004059939AA	25.03.2004
US20040133908A1	08.07.2004	US2004133908A1	08.07.2004
		US2004133908AA	08.07.2004
US6636968B1	21.10.2003	CN1157021C	07.07.2004
		CN1304604	18.07.2001
		CN1304604A	18.07.2001
		CN1304604T	. .T
		EP01080558A1	07.03.2001
		EP1080558A1	07.03.2001
		JP14540721	26.11.2002
		JP2002540721T2	26.11.2002
		KR1020010043748	25.05.2001
		TW543312B	21.07.2003
		US6636968BA	21.10.2003
		WO00059154A1	05.10.2000
		WO0200059154A1	05.10.2000