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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 July 2009 (16.07.2009)

PCT

(10) International Publication Number
WO 2009/086669 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number: PCT/CN2007/003958

(22) International Filing Date: 29 December 2007 (29.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING** [FR/FR]; 46 Quai Alphonse Le Gallo, F-92100 Boulogne Billancourt (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LIU, Yong, Liang** [CN/CN]; 8th Floor, Building A, Technology Fortune Center, No. 8, Xueqing Road, Haidian District, Beijing 100085 (CN). **ZHOU, Guanghua** [CN/CN]; 8th Floor, Building A, Technology Fortune Center, No.8 Xueqing Road, Haidian District, Beijing 100085 (CN). **ZHANG, Yi** [CN/CN]; 8th Floor, Building A, Technology Fortune Center, No. 8, Xueqing Road, Haidian District, Beijing 100085 (CN).

(74) Agent: KANGXIN PARTNERS, P. C.; Floor 16, Tower A, Indo Building, A48 Zhichun Road, Haidian District, Beijing 100098 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, 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, KR, 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: SYSTEM AND METHOD FOR DATA TRANSMISSION

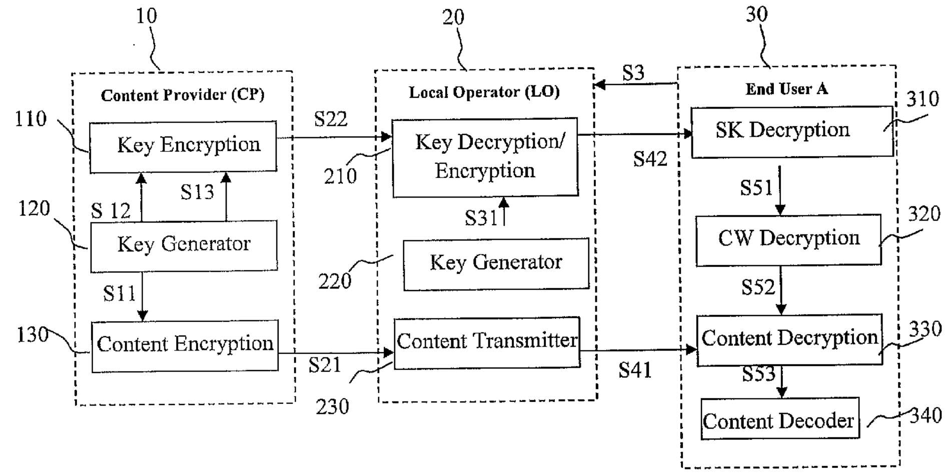


FIG.2

(57) Abstract: A method for transmission data in a system is provided. The system includes a first device, plurality of second devices, and plurality of third devices, the method includes steps of encrypting the data with a first key and encrypting the first key with a second key at the first device, sending the encrypted data from the first device to the second device, decrypting the second key and encrypting the first key with a third key by the second device, sending the encrypted data from the second device to the third device, and decrypting the third key and the first key by the third device.

SYSTEM AND METHOD FOR DATA TRANSMISSION

TECHNICAL FIELD

This invention relates data transmission system, especially to a system and method for data transmission.

BACKGROUND

Nowadays, most business entities provide their services to the end users, which lead to Business-to-Business (B2B) transactions mode. This traditional B2B business mode cannot cater diverse applications emerging. For example, a Content Provider intends to provide his video stream to a great number of end users, but there is no direct communication network between them. However, there is a Local Operator and there is a communication network between the Local Operator and the end users and a communication network between the Local Operator and the Content Provider. So the Content Provider can provide contents to the end users via the Local Operator. Thus a B2B2C (Business to Business to Customer) business mode occurs. However, in this business mode, a problem will arise, how to guarantee the control of the contents at the CP end and at the Local Operator end, because both entities want to get profits by controlling the contents distribution.

CONTENT OF THE INVENTION

To guarantee the control of contents by the CP and the LO, there is a security system is provided.

In an aspect, a method for data transmission in a system is provided. The system includes a first device, plurality of second devices, and plurality of third devices. The method includes steps of encrypting the data with a first key and encrypting the first key with a second key at the first device, sending the encrypted data from the first device to the second device, decrypting the second key and encrypting the first key with a third key by the second device, sending the encrypted data from the second device to the third device, and decrypting the third key and the first key by the third device.

Further, before encrypting the data with the first key, the data has been encrypted by control words.

In another aspect, a data transmission system is provided. The system includes a first device, plurality of second devices, and plurality of third devices. The first device includes an encryption module for encrypting the data with a first key and encrypting the first key with a second key, a first transmitter for sending the encrypted data to the second device; the second device including a decryption module for decrypting the second key, an encryption module for encrypting the first key with a third key by the second device, and a second transmitter for sending the encrypted data to the third device, and the third device includes a decryption module for decrypting the third key and the first key.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG.1 shows an exemplary data transmission system structure.

FIG.2 shows in detail the devices and processes in the data transmission system of FIG.1.

FIG.3 shows the detailed processes at the Content Provider, the Local Operator, and the End User.

FIG.4 shows a second exemplary data transmission system structure.

FIG. 5shows in detail the devices and processes in the data transmission system of FIG.4.

FIG.6 shows the detailed processes at the Content Provider, the Local Central Licensing Servers the Local Operators, and the End Users.

DETAILED IMPLEMENTATION

See Fig.1. It shows an embodiment of present B2B2C data transmimssion system. There are three entities, Content Provider part (CP) 10, Local Operator (LO) part 20, and End User part 30. There are might be several Local Operators 20 and a great number of End Users 30, with one Local Operator 20 serving multiple End

Users 30. Content Provider (CP) 10 distributes Contents to the End users 30 via LOs 20. The contents can be data, media streams, etc. There is an Elecronic Purse Module (EPM) in each End User.

See Fig. 2 which shows CP 10, LO 20, and End User 30 in detail. In Content Provider 10, there is a Key Encryption module 110, a Key Generator module 120, and a content encryption module 130. The LO 20 includes a Key Decryption/Encryption module 210, a Key Generator 220, and a Content Transmitter 230. At the End User A 30, there is a SK Decryption module 310, a CW Decryption module 320, a Content Decryption module 330, and a Content Decoder 340.

The Content Provider 10 distributes its license or generates keys to all potential End User 30 in advance. The End User 30 can get the license by buying it from CP or from a third party which is trusted or authorized by CP.

When the CP 10 distributes contents to the LO 20, the Key Gernerator 120 creates Control Words (CWs), uses these CWs to scramble the contents to get {E(Content)}, and send {E(CW)} to the content Encryption module 130 (see step S11). Then it will also create a Service Key (SK) to encrypt the CWs and get {E(CW)}(see step S12). Then the Key Encryption module 110 encrypts SK with each potential End User's key to get {$E_{(CP,EU)}$(SK)}. This process is used to protect the content and guarantee only the End Users can access the contents. Finally, {$E_{(CP,EU)}$ is encrypted with a LO's key to get{E_{LO}($E_{(CP,EU)}$(SK))}(see step S13). This process is to guarantee only the LO with LO's key that can get {$E_{(CP,EU)}$(SK)}, the encrypted contents to be provided to its End Users. Then {E(Content)} will be sent to the Content Transmitter 230 in the LO 20 via step S21{E(CW)}and {E_{LO}($E_{(CP,EU)}$(SK))} will be sent to the Key Decryption/Encryption 210 in LO 20 via step S22. Step S21 and S22 can be at the same time or in a different sequence.

The LO has a key distributed by the CP, which can decrypt the {E_{LO}($E_{(CP,EU)}$(SK))} and get the {$E_{(CP,EU)}$(SK)}. The decryption process can be carried out in Key Decryption/Encryption module 210.When an End User A wants to access the contents, it will send an authorization request to the LO 20 via step S3. The Key Generator 220 will generates a second End User A's key and sends it to the Key Decryption/Encryption module 210 via step S31. At the Key Decryption/Encryption module 210, it will encrypt {$E_{(CP,EU)}$(SK)} with the second End User A's key generated by the Key Generator 220 to get $E_{(LO, Ua)}$($E_{(CP,EUa)}$(SK)). Then {E(CW)} and $E_{(LO, Ua)}(E_{(CP,EUa)}(SK))$ will be sent to the SK Descryption Module 310 via step S42. The Content Transmitter 230 at LO will send E(Content) to the SK Decryption module via step S41.. The step S41 and S42 can be at the same time or in other sequences. The LO has a key distributed by the CP, which can decrypt the $\{E_{LO}(E_{(CP,EU)}(SK))\}$ and get the $\{E_{(CP,EU)}(SK)\}$. This process is intended to protect the $\{E_{(CP,EU)}(SK)\}$ can only be accessed by the End User A 30.

The End User A first uses the authorized key by the LO 20 and CP 10 to get SK (step S51), then uses the SK to decrypt the {E (CW)} and get the clearing contents(step S 52), and send the clearing contents to the Content Decoder 340 to decode via step S53.

There is also an EPM in each End User. The End User uses it to pay fees to get keys from the CP. In the above embodiment, the data provision from the LO to the End User is a Pull mode, and each time the End User requests contents from the LO, it needs to pay the LO for getting the End User's key from the LO. However, the data transmission can also be a push mode, which means LO will continuously provide the encrypted contents to the End User. When the End User wants to look through the content, it will pay for the End User's key from the EPM to the LO.

These processes are also aggregated in the Fig.3. In Fig.3, the processes at the CP 10 are described in S1110, the processes at the LO 20 are described in S1112, and the processes at the End User 30 are shown in S1113.

In above embodiment, the encryption/decryption method can be Advanced Encryption Standard (AES), Rivest Shamir Adlemen (RSA) encryption, and so on. Though the embodiment is elaborated by a LO and an End User A, there can be plurality of LOs and End Users. People skilled in the art can obtain the implementation after knowing above teaching.

See Fig. 4 it showsn another embodiment of the data transmission system. There is a Content Provider (CP) 40, plurality of Local Operators (LOs) 60. For each LO, there is a Local Central Licensing Servers (LCLSs) 50 communicating with it. And each LO 60 serves a great number of End User 70).

In an embodiment, there are three symmetric or three pairs of asymmetric keys shared between CP 40 and each LCLS 50, LCLS 50 and each End User 70, LO 60 and each End User 70 respectively. For example, if the key shared between CP 40 and each LCLS 50 is a symmetric key, they have the same secret key, if they share an asymmetric key, CP has the public key and each LCLS has the secret key.

CP 40 distribute the encrypt Content to the End User 70 via LCLS 50 and LO 60.

In order to get the content decrypted, the End User 70 should get the license from LO 60 which serving it. This process can be described as following steps:

(1) End User 70 requests LO 60 for license for some contents,

(2) LO 60 forwards this request to LCLS 50,

(3) LCLS 50 creates a license for that user and sends the license to LO 60, and

(4) LO 60 sends the license to the End User 70.

The following part describes the system and method illustrates above steps detailedly.

See Fig. 5 which shows CP 40, LCLS 50, LO 60, and End User 70 in detail. At the Content Provider 40, there is a Key Encryption module 410, a Key Generator module 420, and a Content Encryption module 430. The LCLS 50 includes a Key Decryption module 510, a Key Encryption module 520, a Key Generator 530, and a Content Transmitter 540. The LO 60 includes a Key Generator 610, a Key Encryption module 620, and a Content Transmitter 630. And the End User 70 includes a Key Decryption 710, a CW Decryption 720, a Content Decryption 730, and a Content Decoder 740.

The Key Generator 420 creates control words (CWs). Content Encryption module 430 encrypts VOD contents with the CWs and get E (content) (see step S11'). The Key Generator 420 further generates SK and sends the key to the Key Encryption module 410 where the Key Encryption module 410 encrypts CWs with SK to generate {E(CW)}(see step S12'). The Key Generator 420 generates a key for LCLS and sends the key to the Key Encryption module 410 to encrypt the SK, and E_{LCLS}(SK) is generated (see step S13'). LCLS's key is a key between the CP 40 and LCLS 50.

Then E(content) will be sent from the Content Encryption module 430 to the Content Transmitter 530 via step S21'. {E(CW)} and E_{LCLS}(SK) are transmitted from the Key Encryption module 410 to the Key Decryption module 510 via step S22'. The Key Decryption module 510 decrypts the E_{LCLS}(SK) with the key provided by the CP 40 to get SK and saves SK via step S51'.

When an End User 70 sends a request for contents to the LO (step S3'), LO 60 will forward the request to the LCLS 50 (step S4'). After the LCLS 50 received the request, it will encrypt SK with a first End User A's key (public key or sharing key between the LCLS 50 and the End User 70) generated by the Key Generator 530 to get $E_{(LCLS, EUa)}$(SK) by the Key Encryption module 520 via step S52'. E'(Content) is sent from the Content Transmitter 530 to the Content Transmitter 630 via step S54'. And then the Key Encryption module 520 sends {E(CW)} and $E_{(LCLS, EUa)}$(SK) to the Key Encryption 620 via step S53'.

At the LO side, Key Generator 610 generates a second End User A's key and sends it to the Key Encryption 620 where the $E_{(LCLS, EUa)}$(SK) is encrypted with the second End User A's key to generate $E_{(LO, EUa)}(E_{(LCLS, EUa)}$(SK)) and sends it to the Key Decryption module 710 at the End User 70 via step S63'. E'(Content) and {E(CW)} are sent to the Content Decryption module 730 and the CW Decryption module 720 respectively via step S61' and step S62'.

The steps S61', S62', and S63' can be in different order.

At the End User, it first uses the first End User's key and the second End User's key to decrypt SK from $E_{(LO, EUa)}(E_{(LCLS, EUa)}$(SK)) by the SK Description module 730 and send the decrypted result to the CW Decryption module 720 during step S71'. And then the CWs are decrypted by SK by the CW Decryption module 720 with corresponding keys and sends the result to the Content Decryption module 730 during step S72', at last the clearing content will be decoded by the Content Decoder Module 740.

Fig.6 illustrates the detailed processes at the CP (S2110), LCLS(S2111), LO(S2112), and End User(S2113), which will not be elaborated here.

A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made. Additionally, one of ordinary skill will understand that other structures and processes may be substituted for those disclosed and the resulting implementations will perform at least substantially the same function(s), in at least substantially the same way(s), to achieve at least substantially the same result(s) as the implementations disclosed. Accordingly, these and other implementations are contemplated by this application and are within the scope of the following claims.

CLAIMS

1. A method for data transmission in a system, the system including a first device, plurality of second devices, and plurality of third devices, the method including steps of

encrypting the data with a first key and encrypting the first key with a second key at the first device,

sending the encrypted data from the first device to the second device,

decrypting the second key and encrypting the first key with a third key by the second device,

sending the encrypted data from the second device to the third device, and

decrypting the third key and the first key by the third device.

2. The method for data transmission in a system according to claim 1, wherein before encrypting the data with the first key, the data has been encrypted by control words.

3. A data transmission system, the system including a first device, plurality of second devices, and plurality of third devices, wherein

the first device includes an encryption module for encrypting the data with a first key and encrypting the first key with a second key, a first transmitter for sending the encrypted data to the second device;

the second device including a decryption module for decrypting the second key, an encryption module for encrypting the first key with a third key by the second device, and a second transmitter for sending the encrypted data to the third device, and

the third device includes a decryption module for decrypting the third key and the first key.

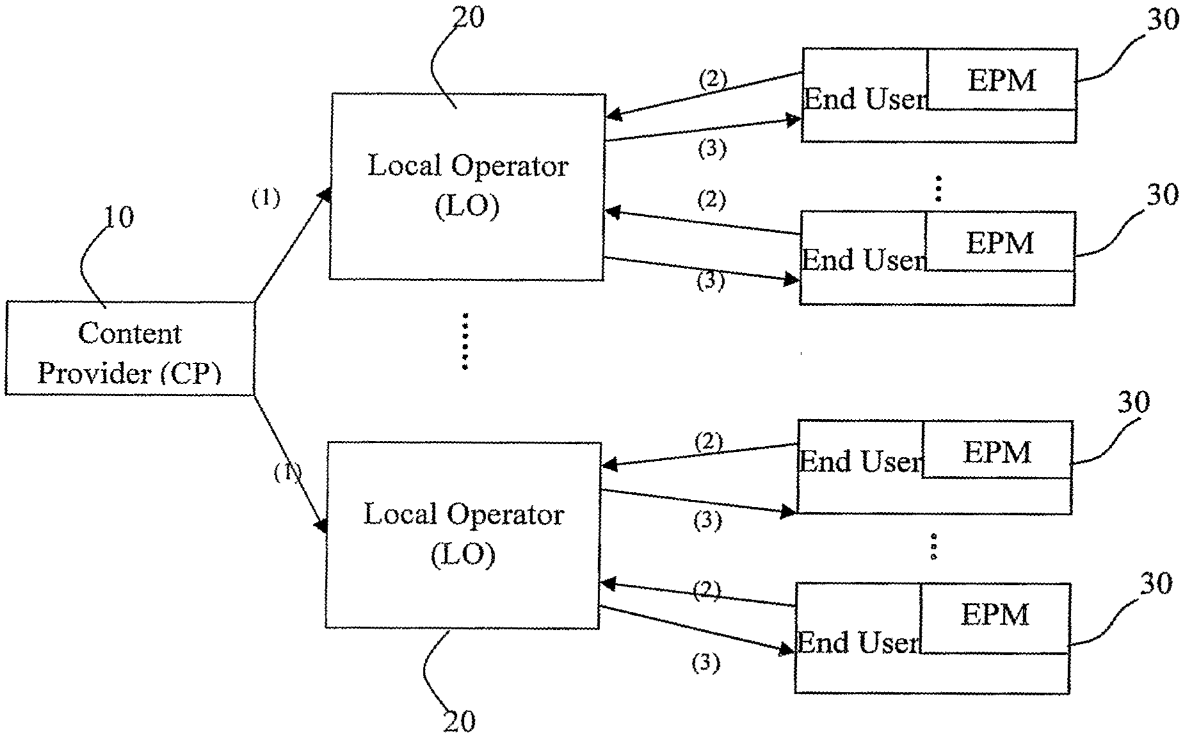

20
30
(2)
End User
EPM
(3)
Local Operator
(LO)
(1)
(2)
30
10
End User
EPM
(3)
Content
Provider (CP)
30
(2)
End User
EPM
(1)
Local Operator
(LO)
(3)
30
(2)
EPM
End User
(3)
20

FIG.1

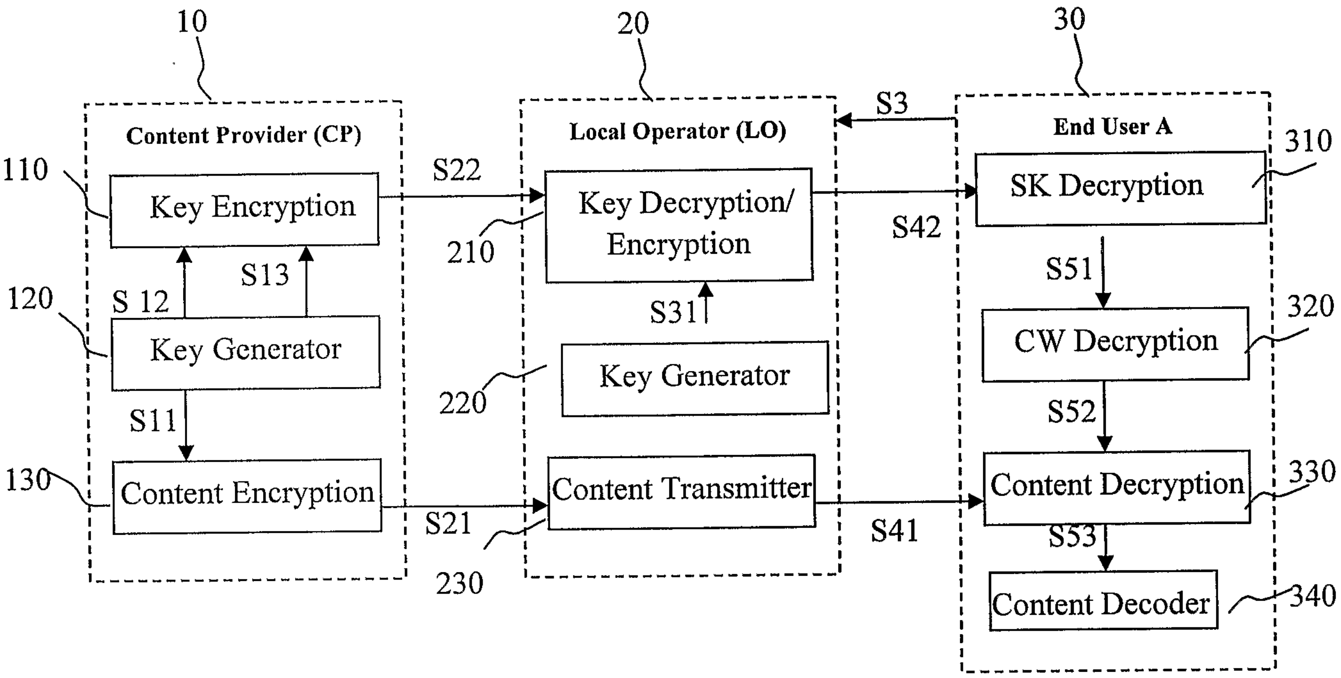

10
20
30
Content Provider (CP)
Local Operator (LO)
End User A
S3
110
Key Encryption
S22
Key Decryption/ Encryption
210
SK Decryption
310
S42
120
S 12
S13
Key Generator
S31
S51
CW Decryption
320
220
Key Generator
S11
S52
130
Content Encryption
S21
Content Transmitter
230
S41
Content Decryption
330
S53
Content Decoder
340

FIG.2

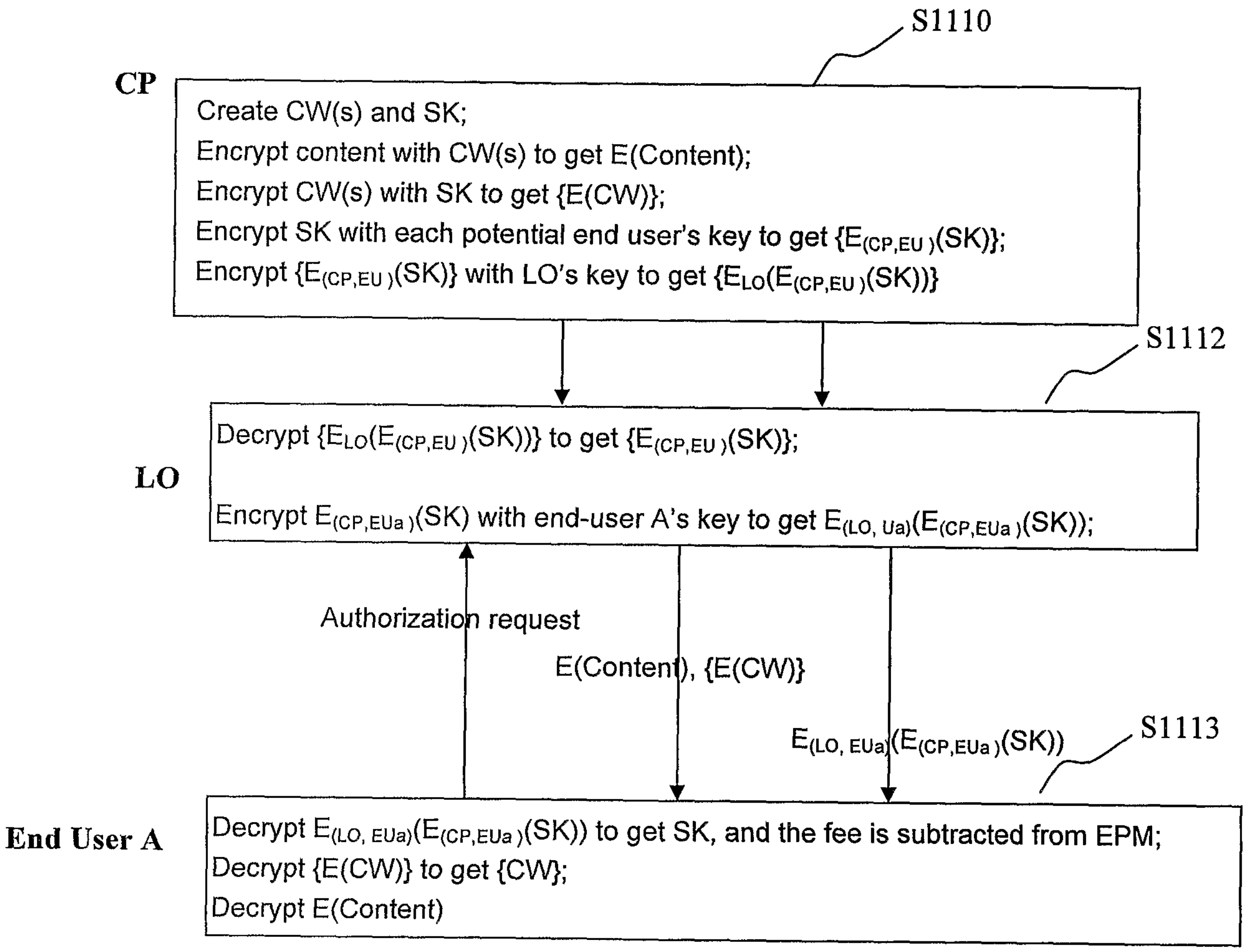

S1110
CP
Create CW(s) and SK;
Encrypt content with CW(s) to get E(Content);
Encrypt CW(s) with SK to get {E(CW)};
Encrypt SK with each potential end user's key to get {$E_{(CP,EU)}$(SK)};
Encrypt {$E_{(CP,EU)}$(SK)} with LO's key to get {E_{LO}($E_{(CP,EU)}$(SK))}
S1112
LO
Decrypt {E_{LO}($E_{(CP,EU)}$(SK))} to get {$E_{(CP,EU)}$(SK)};
Encrypt $E_{(CP,EUa)}$(SK) with end-user A's key to get $E_{(LO, Ua)}$($E_{(CP,EUa)}$(SK));
Authorization request
E(Content), {E(CW)}
$E_{(LO, EUa)}$($E_{(CP,EUa)}$(SK))
S1113
End User A
Decrypt $E_{(LO, EUa)}$($E_{(CP,EUa)}$(SK)) to get SK, and the fee is subtracted from EPM;
Decrypt {E(CW)} to get {CW};
Decrypt E(Content)

FIG.3

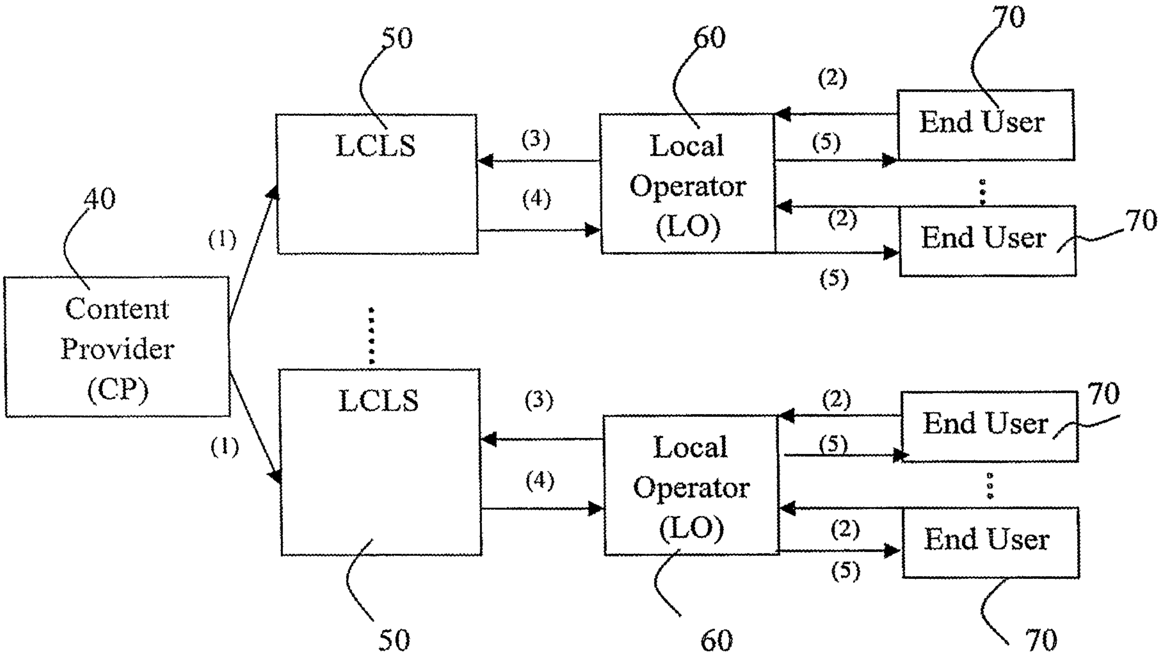

50
60
70
(2)
LCLS
(3)
Local Operator (LO)
(5)
End User
(4)
(2)
End User
70
40
(1)
(5)
Content Provider (CP)
LCLS
(3)
(2)
End User
70
(1)
Local Operator (LO)
(5)
(4)
(2)
End User
(5)
50
60
70

FIG.4

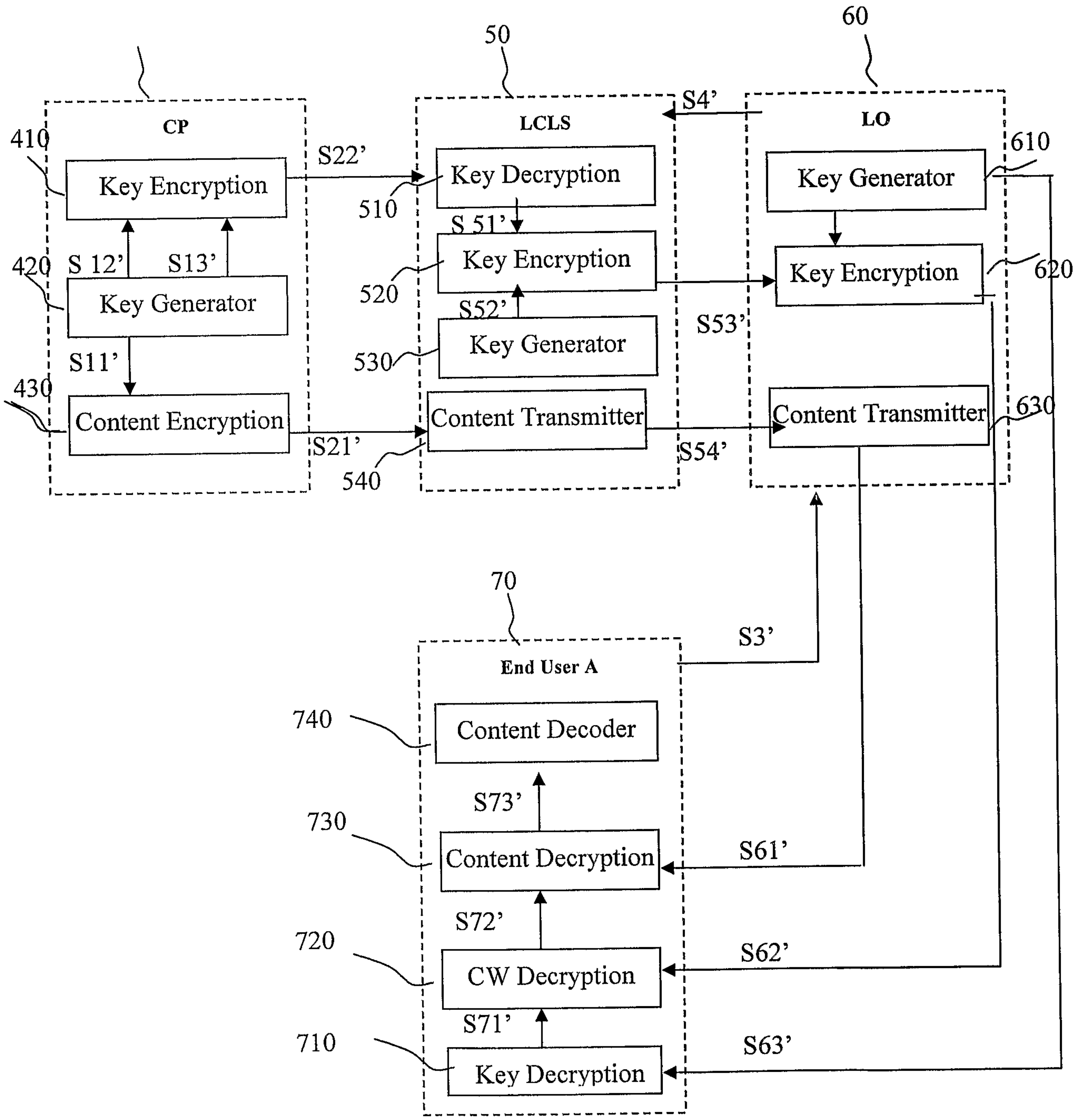
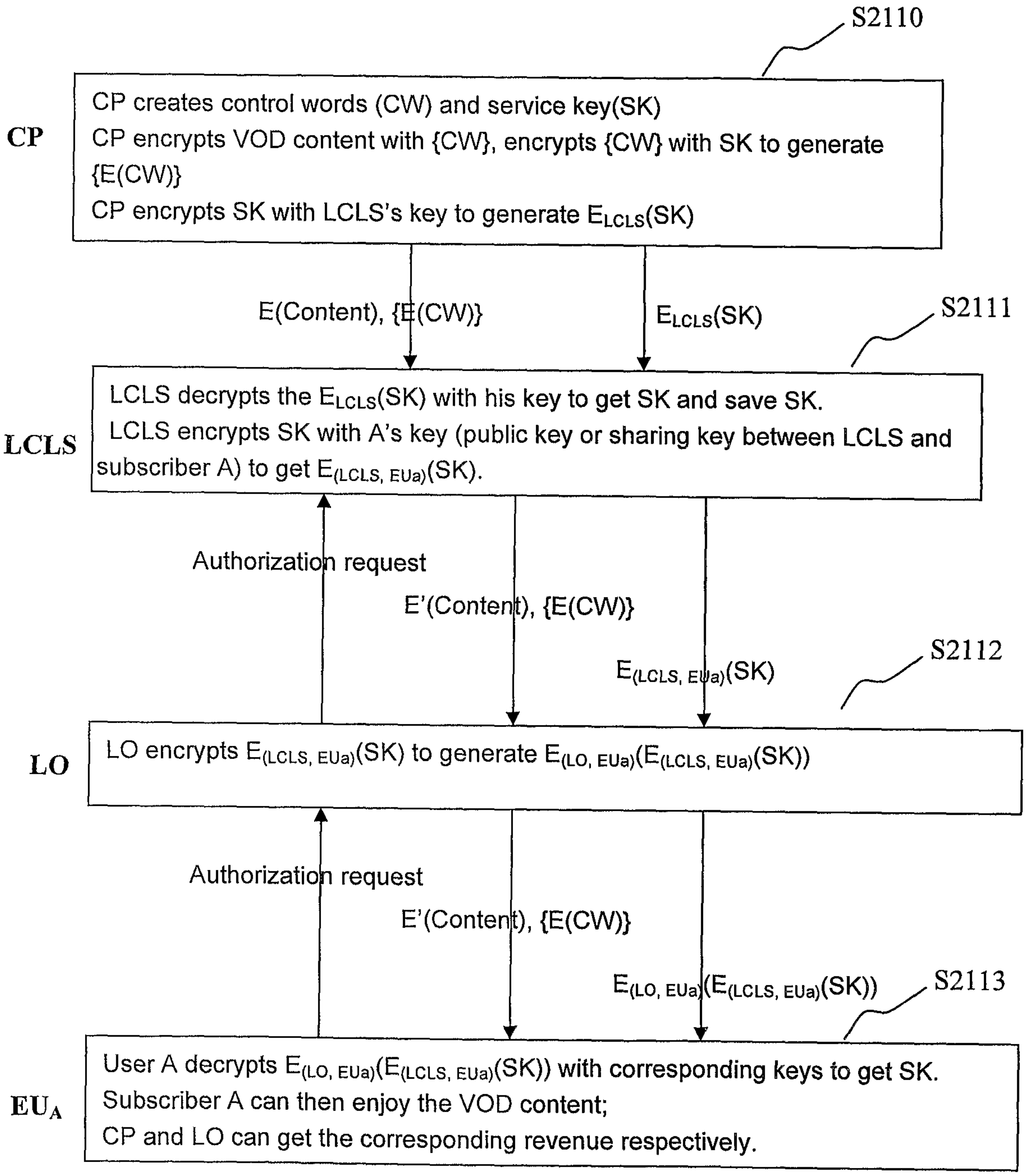

60
50
CP
LCLS
LO
S4'
410
Key Encryption
S22'
Key Decryption
510
S 51'
Key Generator
610
Key Encryption
Key Encryption
620
420
S 12'
S13'
Key Generator
520
S52'
Key Generator
530
S53'
S11'
430
Content Encryption
S21'
Content Transmitter
540
Content Transmitter
630
S54'
70
S3'
End User A
740
Content Decoder
S73'
730
Content Decryption
S61'
S72'
720
CW Decryption
S62'
S71'
710
Key Decryption
S63'

FIG.5



CP creates control words (CW) and service key(SK)
CP encrypts VOD content with {CW}, encrypts {CW} with SK to generate {E(CW)}
CP encrypts SK with LCLS's key to generate E_{LCLS}(SK)

LCLS decrypts the E_{LCLS}(SK) with his key to get SK and save SK.
LCLS encrypts SK with A's key (public key or sharing key between LCLS and subscriber A) to get $E_{(LCLS,\ EUa)}$(SK).

LO encrypts $E_{(LCLS,\ EUa)}$(SK) to generate $E_{(LO,\ EUa)}(E_{(LCLS,\ EUa)}$(SK))

User A decrypts $E_{(LO,\ EUa)}(E_{(LCLS,\ EUa)}$(SK)) with corresponding keys to get SK.
Subscriber A can then enjoy the VOD content;
CP and LO can get the corresponding revenue respectively.

Figure 6 VOD Flow chart for some instance of value-added content

FIG.6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/003958

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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：H04L9/00,9/08,9/06,9/32

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

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

CNPAT,CNKI,WPI,EPDOC,PAJ: cryptographic, encrypt+, deccrpt+, key, transmission, first, second, third, copyright, right, security, safe, copy, protect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN1306359A, (VICTOR CO OF JAPAN LTD.), 1 Aug. 2001(01.08.2001), page 6 line 15 to page 8 line 26, figure 1	1-3
Y	CN1347225A, (YANY G), 1 May 2002(01.05.2002), page 4 lines 7-25	1-3
A	US2003/0056118A1, (Troyansky et al.), 20 Mar. 2003(20.03.2003), the whole document	1-3
A	US7203311B1, (Kahn et al.), 10 Apr. 2007(10.04.2007), the whole document	1-3

□ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search 11 Sep. 2008(11.09.2008)	Date of mailing of the international search report **16 Oct. 2008 (16.10.2008)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer ZHAO Xiaochun Telephone No. (86-10)62413419

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/003958

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1306359A	01.08.2001	US2001/0009006A1	19.07.2001
		EP1119129A2	25.07.2001
		JP2001-274785A	05.10.2001
CN1347225A	01.05.2002	None	
US2003/0056118A1	20.03.2003	US7260215B1	21.08.2007
US7203311B1	10.04.2007	EP1176826A2	30.01.2002
		JP2002-111655A	12.04.2002
		US2007/0133795A1	14.06.2007

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/003958

CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i
H04L9/32 (2006.01)i