

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
23 February 2006 (23.02.2006)

PCT

(10) International Publication Number
WO 2006/020141 A2

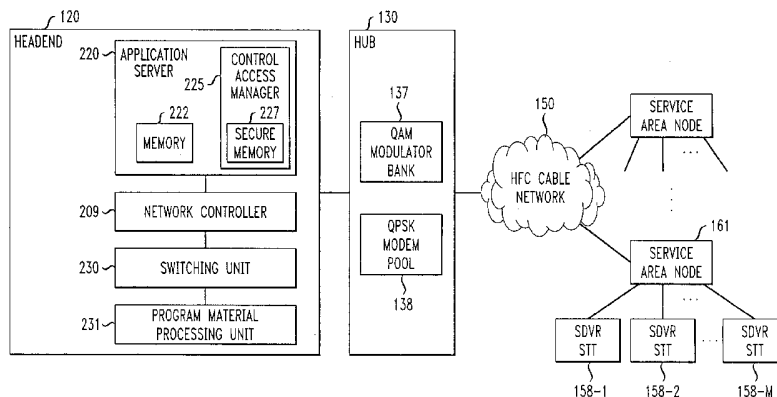
- (51) International Patent Classification:
H04L 9/00 (2006.01)
- (21) International Application Number:
PCT/US2005/025313
- (22) International Filing Date: 15 July 2005 (15.07.2005)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10/894,884 20 July 2004 (20.07.2004) US
- (71) Applicant (for all designated States except US): TIME WARNER CABLE, INC. [US/US]; 290 Harbor Drive, Stamford, CT 06902 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): HELMS, William [—/US]; 8911 Comanche Road, Longmont, CO 80503 (US). HAYASHI, Michael, T. [—/US]; 16497 East Dorado Avenue, Aurora, CO 80015 (US). LEDDY, Kevin, J. [—/US]; 25 Sturges Ridge Road, Wilton, CT 06897 (US). CHRISTMAN, David, A. [—/US]; 26 Flicker Lane, Rowayton, CT 06853 (US).

- (74) Agent: SKLAR, Brandon, N.; Kaye Scholer LLP, 425 Park Avenue, New York, NY 10022 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— without international search report and to be republished upon receipt of that 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.

(54) Title: TECHNIQUE FOR SECURELY COMMUNICATING AND STORING PROGRAMMING MATERIAL IN A TRUSTED DOMAIN



(57) Abstract: A "trusted domain" is established within which content received from a communications network, e.g., a cable TV network, is protected from unauthorized copying thereof, in accordance with the invention. In an illustrative embodiment, the trusted domain includes a device associated with a user which receives content from the cable TV network. The content may be encrypted using a content key in accordance, e.g., with a 3DES encryption algorithm before it is stored in the device. In addition, a first encrypted content key version and a second encrypted content key version are generated by respectively encrypting the content key with a public key associated with the device and another public key associated with the user, in accordance with public key cryptography. The first and second encrypted content key versions are stored in association with the encrypted content in the device storage. The encrypted content can be migrated from a first device to a second device, and can be decrypted in the second device if the second device is associated with the same user, and also provided with the second encrypted content key version.

WO 2006/020141 A2

Description

TECHNIQUE FOR SECURELY COMMUNICATING AND STORING PROGRAMMING MATERIAL IN A TRUSTED DOMAIN

Field of the Invention

The invention relates to a communications technique, and more particularly to a technique for securely communicating and storing programming material in a
5 communications system, e.g., a cable TV system.

Background of the Invention

A set-top terminal (STT) serves as a gateway between a user's television and a cable TV network delivering programming content. Such programming content may
10 be delivered as a broadcast. It may also be delivered on an on-demand basis, for which services such as video on demand (VOD), subscription VOD, movies on demand, etc., are offered. In addition, a "network personal video recorder (NPVR)" service has been developed, allowing the user to perform trick mode functions (rewind, fast-forward, pause, etc.) on a presentation of programming content through
15 use of a network. In fact, a network architecture and functionalities for implementing the NPVR service are described, e.g., in copending commonly assigned Application Serial No. 10/302,550, filed on November 22, 2002, hereby incorporated by reference. The NPVR service also allows a user to "reserve" past and future programs for his/her review, even if such reserved programs were not identified by the user before their
20 broadcast.

An STT receives, through the cable TV network, programming content which may be encrypted, e.g., in accordance with the data encryption standard (DES) technique, to secure its delivery. DES is a well known symmetrical cipher which utilizes a single key for both encryption and decryption of messages. Because the
25 DES algorithm is publicly known, learning the DES key would allow an encrypted message to be read by anyone. As such, both the message sender and receiver must keep the DES key a secret from others. A DES key typically is a sequence of eight bytes, each containing eight bits. To enhance the DES integrity, the DES algorithm

-2-

may be applied successive times. With this approach, the DES algorithm enciphers and deciphers data, e.g., three times in sequence, using different keys, resulting in a so-called triple DES (3DES) technique.

In contrast to the DES technique, a public key encryption technique, e.g., an
5 RSA technique (named for its developers, Rivest, Shamir, and Adleman), uses two different keys. A first key, referred to as a private key, is kept secret by a user. The other key, referred to as a public key, is available to anyone wishing to communicate with the user in a confidential manner. The two keys uniquely match each other, collectively referred to as a "public key-private key pair." However, the private key
10 cannot be easily derived from the public key. A party wishing to send a message to the user may utilize the public key to encrypt a message before transmitting it. The user then utilizes the private key to decrypt the message. Conversely, the private key may be used to encrypt a message, in which case the message can subsequently be decrypted with the public key. For example, the keys for the RSA algorithm are
15 mathematically generated, in part, by combining prime numbers. The security of the RSA algorithm, and the like, depends on the use of very large numbers for its keys, which typically are 512 bits long.

In prior art, programming content may be encrypted using a DES key, in accordance with a DES algorithm, to secure its delivery from a headend of a cable TV
20 system to an STT. In order for the STT to decrypt the encrypted programming content, the DES key is transmitted from the headend to the STT in an entitlement control message (ECM), which is encrypted using a 3DES key in accordance with a 3DES algorithm. The 3DES key (also known as a "multi-session key (MSK)") is sent to the STT in a separate entitlement management message (EMM), which is encrypted
25 using an STT public key in accordance with a public key algorithm, whose private key counterpart is securely maintained in the STT. Thus, after receiving the encrypted EMM and ECM, the STT decrypts the encrypted EMM using the STT private key to obtain the 3DES key therein. Using such a 3DES key, the STT decrypts the encrypted ECM to obtain the DES key therein. Using such a DES key, the STT can decrypt the
30 encrypted programming content it received.

Recently, some STTs for cable TV were improved to incorporate digital video

-3-

recorder (DVR) functions (“DVR STTs”). Like a DVR, e.g., a TiVo or ReplayTV device, a DVR STT typically includes a hard drive, e.g., a disk, for digitally recording TV programs. Also like a DVR, a DVR STT allows a cable TV subscriber to record his/her favorite TV programs for later review, and exercise a season-pass-like option
5 to record every episode of his/her favorite program for a period. It may automatically record programs for the user based on his/her viewing habit and preferences. The presentation of the recorded programming content can be manipulated by exercising rewind, pause and fast-forward functions.

However, cable operators have observed that providing to subscribers
10 unrestricted content might result in an unacceptable amount of unauthorized copying. Accordingly, there is a continuing need for a strategy that allows content to be stored by a subscriber, but at the same time prevents (or controls) copying and distributing the content to unauthorized parties. A number of techniques have been developed to address this need. One such technique involves use of an indicator, e.g., an encryption
15 mode indicator (EMI), which may be inserted into a data stream used to transmit content from a source device to a destination device. The EMI provides to the destination device information concerning the status of the content; the status may indicate that the content can be freely copied, copied once, never copied, etc. The destination device reads the EMI and determines whether or not the content may be
20 copied. If copying is permitted, the destination device may then copy the content. For details on such a content protection technique, one may refer to: “5C Digital Transmission Content Protection White Paper,” Hitachi, Ltd et al., Revision 1.0, July 14, 1998.

Another technique requires a device intending to transmit protected content to
25 determine whether or not the receiving device is authorized to receive such content. This may be achieved, e.g., by requiring the receiving device to demonstrate knowledge of a set of secret device keys. Only after the receiving device has established its legitimacy does the transmitting device deliver the content. An example of one such content protection system is described in “High-Bandwidth
30 Digital Content Protection System,” Digital Content Protection LLC, Revision 1.1, June 9, 2003.

Similarly, there is a need for a strategy that enables a subscriber to perform authorized copying of protected content, e.g., copying content from a set-top terminal to a second device in the subscriber's home, while at the same time preventing unauthorized copying. This need is of growing importance given the increasing popularity of home networking. In recent years, numerous systems for providing interconnectivity among devices in a home have been developed, allowing home networks to include not only cable set-top terminals but also personal computers, cellphones, PDA devices, etc. An example of a system for interconnecting various devices in a home is described in International Patent Application Publication No. WO 02/21841, published on March 14, 2003.

Summary of the Invention

The invention overcomes the prior art limitations by defining a "trusted domain" within which programming content is protected from unauthorized access and copying. For example, in a cable TV system, the trusted domain includes not only the system portion where programming content traditionally is secured by, and within total control of, a cable operator, including, e.g., the headend, delivery network, etc., but also user devices at subscribers' premises which are capable of receiving and securely storing programming content. Using the inventive trusted domain approach, the cable operator can guarantee certain subscriber access and usage with respect to content held within the domain. For example, a motion picture held within a cable operator's trusted domain (e.g., on a hard drive of a user device) cannot be distributed over the Internet in viewable form and cannot become a source for duplication of multiple viewable copies.

To realize a trusted domain, two cryptographic elements (e.g., encryption keys), associated with a subscriber and his/her user device(s), respectively, are utilized to control access to content stored in the user device(s) within the domain. For example, the stored content in the user device may be encrypted using a secret key in accordance with a DES technique. Thus, when the encrypted content is transported from the user device to a new device associated with the same subscriber within the domain, the new device needs a first cryptographic element (e.g., the secret key) to

-5-

decrypt the encrypted content for viewing. To that end, the new device also receives from the source device a first encrypted version of the first cryptographic element. The latter is generated by encrypting the first cryptographic element using a second cryptographic element (e.g., a public key in accordance with a public key algorithm) associated with the subscriber. The new device provides the first encrypted version of the first cryptographic element to a remote apparatus, e.g., in a headend, where the first cryptographic element is recovered based on at least the first encrypted version of the first cryptographic element and data representative of the subscriber. The new device then receives from the apparatus a second encrypted version of the first cryptographic element. The latter is generated by encrypting the recovered first cryptographic element using a third cryptographic element (e.g., a public key in accordance with a public key algorithm) associated with the new device. Based on at least the second encrypted version of the first cryptographic element, the first cryptographic element can be recovered in the new device to decrypt the encrypted content transported thereto.

Brief Description of the Drawings

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying drawing showing illustrative embodiments of the invention, in which:

FIG. 1 illustrates components of a broadband communications system, in accordance with an embodiment of the invention;

FIG. 2 illustrates a subscriber registry maintained in a headend of the system of Fig. 1;

FIG. 3 illustrates a device key table maintained in a headend of the system of Fig. 1;

FIG. 4 illustrates a subscriber key table maintained in a headend of the system of Fig. 1;

FIG. 5 illustrates components of a first secure digital video recorder (SDVR) STT, in accordance with an embodiment of the invention;

FIG. 6 illustrates storage in the first SDVR STT;

-6-

FIG. 7 is a flowchart depicting a routine for encrypting and storing a content file, in accordance with an embodiment of the invention;

FIG. 8 is a flowchart depicting a routine for generating an encrypted content key associated with a subscriber, in accordance with an embodiment of the invention;

5 FIG. 9 illustrates components of a second SDVR STT, in accordance with an embodiment of the invention; and

FIG. 10 is a flowchart depicting a routine for generating an encrypted content key associated with the second SDVR STT, in accordance with an embodiment of the invention; and

10 FIG. 11 is a flowchart depicting a routine for transferring a content file from a first device to a second device, e.g., via a home network, in accordance with an embodiment of the invention.

Detailed Description

15 The invention is directed to a technique for securing programming content within a protected area from unauthorized access and copying. Such a protected area hereinafter is referred to as a "trusted domain." In a cable TV system, the trusted domain includes not only the system portion where programming content traditionally is secured by, and within total control of, a cable operator, including, e.g., the

20 headend, delivery network, etc., but also user devices at subscribers' premises which are capable of receiving and storing programming content, e.g., a DVR STT, and which implement a conditional access mechanism in accordance with the invention. For the sake of convenience, a DVR STT which implements the inventive conditional access mechanism hereinafter is referred to as a "secure DVR STT (SDVR STT)."

25 The trusted domain may further encompass other devices at a subscriber's premises, e.g., a series of devices connected (wired or wireless) to an SDVR STT, which hold or exchange data encrypted through, and managed under, the inventive conditional access mechanism. The trusted domain is intact with respect to the stored content so long as the content remains so encrypted and continues to be managed under the

30 inventive mechanism, regardless of which device holds the content. Once the content is decrypted by the conditional access mechanism, for example, when data is sent

from the SDVR STT to a television monitor for display, the decrypted content is no longer within the trusted domain, and thus no longer may no longer be secure.

Using the inventive trusted domain approach, the cable operator can guarantee certain subscriber access and usage with respect to content held within the domain.

5 For example, a motion picture held within a cable operator's trusted domain (e.g., on a hard drive of an SDVR STT) cannot be distributed over the Internet in viewable form and cannot become a source for duplication of multiple viewable copies. On the other hand, a motion picture held outside the trusted domain (e.g., in unencrypted form on a third party's DVR hard drive) can be distributed over the Internet or copied onto
10 removable media in viewable form.

Fig. 1 illustrates components of a broadband communications system, e.g., a cable TV system, embodying the principles of the invention. Headend 120 receives programming content attributed to various program channels, and provides cable television services to STTs including, e.g., SDVR STTs 158-1 through 158-M, where
15 M represents an integer. It should be noted that the same cable television services are also provided to prior art STTs with no programming content storage capability which, however, are not of interest here. It should also be noted that the terms "transmission channel" and "program channel" should not be confused. A "transmission channel" signifies a designated frequency band through which a
20 transport stream containing programming content and/or data is transmitted. A "program channel" signifies the source of programming content or the service selected by a user to view. For example, a user may select program channel 2 to view programming content provided by CBS, program channel 14 to view programming content provided by ESPN, etc.

25 In a conventional manner, headend 120 delivers programming content downstream to SDVR STTs 158-1 through 158-M in a service area or neighborhood, where M represents an integer. As shown in Fig. 1, SDVR STTs 158 are connected to network 150 through a service area node 161. In this instance, network 150 is a multi-channel delivery network comprises a well-known hybrid fiber coaxial (HFC) cable
30 network.

Programming content is delivered downstream from headend 120 to SDVR STTs 158 through “in-band” transmission channels. In one embodiment, these transmission channels may be 6 MHz bands populating a forward passband, e.g., 350-750 MHz band, of a coaxial cable. QAM modulator bank 137 in hub 130 modulates the transport streams containing the programming content onto selected in-band channels, in accordance with a QAM scheme.

In addition, downstream data, e.g., control messages, emergency information, etc., may be communicated from headend 120 to SDVR STTs 158 via one or more forward data channels (FDCs), sometimes referred to as “out-of-band” channels. The FDCs may occupy the 70-130 MHz band of a coaxial cable. QPSK modem pool 138 in hub 130 modulates downstream data onto selected FDCs, in accordance with a QPSK scheme.

Upstream data, e.g., application data, file requests, etc., may be transmitted from SDVR STTs 158 to headend 120 via one or more reverse data channels (RDCs), which occupy a reverse passband, e.g., 5-40 MHz band, of a coaxial cable. The data traversing the RDCs is modulated in accordance with a QPSK scheme. QPSK modem pool 138 in hub 130 receives the QPSK signals containing the data from the RDCs and performs any necessary demodulation before transmitting the underlying data to headend 120. Using a contention-based access mechanism established by the Digital Audio Visual Council (DAVIC), a standard setting organization, each STT can share an RDC with other STTs in the network. This mechanism enables an STT, e.g., SDVR STT 158-1, to transmit upstream messages without a dedicated connection to a QPSK demodulator. The mechanism also provides equal access to the STTs that share the RDC, and enables detection and recovery from reverse path collisions that occur when two or more of the STTs transmit an upstream message simultaneously. As also specified by DAVIC, for communications purposes, each STT and network controller 209 are identified by the Internet protocol (IP) addresses assigned thereto. However, these IP addresses may be randomly assigned each time the broadband communication system is reconfigured. As a result, the IP address of an STT or that of network controller 209 may change after a system reconfiguration. Nevertheless,

each STT and network controller 209 are also assigned a media access control (MAC) address on a permanent basis, surviving any system reconfiguration.

Headend 120 includes, among others, program material processing unit 231, application server 220, network controller 209, and switching unit 230. In a well-known manner, program material processing unit 231 receives programming content from various sources attributed to different program channels, and generates transport streams containing the programming content, e.g., in accordance with a well known MPEG-2 scheme. Under control of network controller 209, the transport streams are switched by switching unit 230 to appropriate modulators in QAM modulator bank 137 in hub 130, where the transport streams are modulated onto the corresponding in-band transmission channels for delivery to STTs over network 150.

Application server 220 may include one or more server systems that provide software applications and services for STT users. For example, application server 220 may contain one or more software applications for providing database services, network management services, interactive program guide services, billing services, etc. Server 220 may maintain in memory 220 a subscriber registry, denoted 360 in Fig. 2. Registry 360 is illustrated in the form of a table, where column 363 includes, for each STT in the system, an identifier identifying the STT (STID). In this example, each STT is identified by its MAC address. For example, SDVR STT 158-1 may be identified by a MAC address denoted MAC-1. Column 364 includes a subscriber ID (e.g., subscriber's name, ID number, etc.) identifying a subscriber to the cable television services who is associated with each respective STT. For example, referring to row 368-1, STT 158-1 is associated with the subscriber identified by S-1. In this example, subscriber S-1 may be, for example, an individual who purchased or leased SDVR STT 158-1 and registered with the operator as the user thereof. It should be noted that a given subscriber may be associated with more than one STT. Referring to row 368-2, for example, SDVR STT 158-2 is also associated with subscriber S-1. In this example, subscriber S-1 may have purchased or leased STT 158-2 for use as a second STT in his or her home.

In this instance, application server 220 also includes access control manager 225 for realizing the aforementioned access control mechanism in accordance with the

-10-

invention. To that end, manager 225 maintains access control related data pertaining to SDVR STTs and/or subscribers. For example, manager 225 may maintain in memory 222 a library of device public keys associated with the SDVR STTs in the cable TV system. When an SDVR STT is provided to a subscriber, a “public key-private key pair” has been assigned to the SDVR STT in anticipation of data encryption in accordance with a public key algorithm. The “device private key” of the SDVR STT is stored in a secure memory therein while the “device public key” may be transmitted to manager 225 through an RDC during an initialization process of the SDVR STT. Alternatively, during registration of the SDVR STT, the subscriber may provide the cable operator with the serial number of the SDVR STT, if the cable operator has not already had it, for the cable operator to look up the public key associated with the SDVR STT. The library of device public keys is illustrated in the form of a table, denoted 273 in Fig. 3. Device key table 273 comprises column 276 which includes an STID of each SDVR STT in the system, which is its MAC address in this instance. For example, SDVR STT 158-1 is identified by address MAC-1 as mentioned before. Column 277 registers a device public key assigned to each respective STT. In this example, each device public key is 512 bits long. Referring to row 279-1, for example, STT 158-1 is assigned a public key denoted DPUBKEY-1. It should be noted that table 273 is intended for illustrative purposes only. In other embodiments, different identifiers, e.g., IP addresses, may be used in table 273 to identify various STTs in the network.

In accordance with the invention, each subscriber associated with an SDVR STT is also assigned a public key-private key pair in anticipation of another data encryption in accordance with a public key algorithm. Manager 225 may maintain a subscriber key table, denoted 283 in Fig. 4. Subscriber key table 283 includes column 286 which enumerates an identifier of each subscriber associated with an SDVR STT, e.g., S-1, S-2, S-3, etc. Columns 287 and 288 contain, respectively, a “subscriber public key” and the “subscriber private key” counterpart assigned to each subscriber. Referring to row 289-1, for example, subscriber S-1 is assigned a subscriber public key denoted SPUBKEY-1 and subscriber private key denoted SPRIKEY-1. Such a key pair may be assigned to each subscriber by the cable operator during a service

registration by the subscriber. Because the subscriber private keys need to be kept secret, table 283 may be maintained by manager 225 in secure memory 227.

Fig. 5 illustrates components of a generic SDVR STT (e.g. 158-1) in accordance with the invention, which include, among others, processor 330, interface 250, memory 210, storage 610, and encryption module 165. Processor 330
5 orchestrates the operations of SDVR STT 158-1. Interface 250 includes cable modem 258 capable of demodulating signals containing programming content and data from in-band channels and FDCs, and modulating data signals onto RDCs. Interface 250 also performs other well-known formatting and reformatting functions necessary to
10 transmit or receive programming content and data.

Memory 210 stores a variety of software applications and data including, e.g., an operating system (not shown) which provides the basic functionality for SDVR STT 158-1, and STID 214 for identifying SDVR STT 158-1, which is its MAC address MAC-1 in this instance. Memory 210 may be, e.g., a non-volatile random-
15 access memory.

The aforementioned device private key assigned to STT 158-1, namely, DPRIKEY-1, is stored in secure memory 212 in encryption module 165 in such a manner that it cannot be discovered or tampered with easily and certainly not without notice. On the other hand, the device public key assigned to SDVR STT 158-1,
20 namely, DPUBKEY-1, a copy of which is registered in table 273 in headend 120 as discussed before, is stored in memory 210.

Storage 610 is used for storing programming content, which in this instance may be a removable hard disk drive. It will be appreciated that storage 610 may comprise other forms of memory including, e.g., a digital video disk (DVD) drive,
25 memory sticks, network-based storage, etc. Processor 330 may also perform such DVR functions as recording selected programming content in one or more content files, and storing them in storage 610. As used herein, the term "content file" refers to a container that holds a distinct quantity of programming content. A content file may contain, e.g., a digitally recorded version of a movie such as "Citizen Kane."

30 Cable operators have observed that providing to subscribers an unrestricted right to save programming content often results in an unacceptable amount of

-12-

unauthorized copying. Accordingly, the aforementioned access control mechanism in accordance with the invention is implemented to prevent such unauthorized copying. In accordance with the inventive mechanism, encryption module 165 generates a content key, e.g., a 3DES key for encrypting, in accordance with a 3DES algorithm, a content file provided by processor 330 before its storage. In this illustrative embodiment, a different content key is generated for encrypting each respective content file. However, it will be appreciated that a single content key may be used to encrypt all content files in the same storage. It will also be appreciated that multiple content keys may be used to encrypt a single content file.

10 In addition, module 165 encrypts each generated content key to form “encrypted content key version 1 (V-1),” and “encrypted content key version 2 (V-2),” and stores the encrypted content key versions (denoted 603 and 604 respectively in Fig. 6) in association with the corresponding encrypted content file 602 (i.e., encrypted using the content key) in storage 610. In this illustrative embodiment, the encrypted content key V-1 is formed by encrypting the content key with the device public key (i.e., DPUBKEY-1) assigned to SDVR STT 158-1. On the other hand, the encrypted content key V-2 is formed by encrypting the content key with the subscriber public key (i.e., SPUBKEY-1) assigned to subscriber S-1 associated with SDVR STT 158-1 in this instance.

20 By way of example, subscriber S-1 may direct SDVR STT 158-1 to record specified programming content, say, the “Citizen Kane” movie as it is broadcast over cable network 150. Accordingly, processor 330 generates a content file containing the specified movie content received from interface 250. Fig. 7 is a flowchart depicting a routine for encrypting and storing a content file. Instructed by such a routine, encryption module 165 at step 308 generates the aforementioned content key associated with the specified content file. At step 310, module 165 encrypts the content file using the content key, in accordance with the aforementioned 3DES algorithm. At step 315, module 165 stores the encrypted content file 602 in storage 610. At step 318, module 165 retrieves the device public key DPUBKEY-1 from memory 210. At step 320, module 165 uses DPUBKEY-1 to encrypt the content key in accordance with a first public key algorithm, e.g., an RSA algorithm. As

-13-

mentioned above, the resulting encrypted content key is referred to as the “encrypted content key V-1.” At step 325, module 165 stores the encrypted content key V-1, denoted 603, in storage 610. In one embodiment, the encrypted content key V-1 is stored in the form of metadata associated with the encrypted content file.

5 To generate the encrypted content key V-2, denoted 604, module 165 retrieves from storage 610 the encrypted content key V-1, from secure memory 212 device private key DPRIKEY-1, and from memory 210 STID 214 which is MAC-1 in this instance. Module 165 uses DPRIKEY-1 to decrypt the encrypted content key V-1, thereby recovering the content key in the clear. Module 165 then transmits the
10 content key to headend 120 via an RDC in a secure manner. The secure transmission of a content key from STT 158-1 to headend 120 may be accomplished using a prior art encryption technique, e.g., a prior art public key encryption technique where a system private key is stored in headend 120, and the corresponding system public key is made public to, and stored in, all STTs including SDVR STT 158-1. In this
15 instance, module 165 in SDVR STT 158-1 transmits, to control access manager 225 in application server 220, a message containing STID 214 and the content key encrypted using the system public key, in accordance with the prior art public key encryption technique.

Fig. 8 is a flowchart depicting a routine for generating the encrypted content
20 key V-2, in accordance with one embodiment. At step 427, manager 225 receives the encrypted content key and STID 214 in the message from SDVR STT 158-1, and at step 430 decrypts, using the aforementioned system private key, the encrypted content key to recover the content key in the clear. At step 431, manager 225 consults subscriber registry 360 and uses STID 214, which is MAC-1 in this instance, to
25 determine the associated subscriber ID, which is S-1 in this instance. At step 432, manager 225 retrieves from subscriber key table 283 the subscriber public key, SPUBKEY-1 associated with S-1. At step 435, manager 225 uses the subscriber public key SPUBKEY-1 to encrypt the content key in accordance with a second public key algorithm, thereby generating the encrypted content key V-2. At step 440,
30 manager 225 transmits the encrypted content key V-2 to SDVR STT 158-1 via an FDC.

-14-

After receiving the encrypted content key V-2 from manager 225, module 165 stores the encrypted content key V-2, denoted 604 in storage 610. In one embodiment, the encrypted content key V-2 is stored in the form of metadata associated with the encrypted content file 602. To decrypt the encrypted content file 602 for viewing the "Citizen Kane" movie content, module 165 may decrypt the associated encrypted content key V-1 (603) using DPRIKEY-1 in memory 212, thereby recovering the content key in the clear. Module 165 then applies the recovered content key to decrypt the encrypted content file 602.

Alternatively, STT 158-1 may be provided with the subscriber public key SPUBKEY-1. In a similar process used to create encrypted content key V-1, module 165 may use SPUBKEY-1 to generate encrypted content key V-2.

To show the portability of the encrypted content file 602, supposing that subscriber S-1 has purchased SDVR STT 158-2 for use as a second STT in his or her home, he or she may wish to transfer the content file to SDVR STT 158-2 and watch the program on a television set connected to SDVR STT 158-2. Alternatively, supposing that SDVR STT 158-1 is broken or is no longer functional for any reason, subscriber S-1 may wish to use SDVR STT 158-2 to view the stored programming content. To permit subscriber S-1 to copy the programming content for limited purposes such as these, the invention relies on encrypted content key V-2 (604), which is not associated with any particular device, to "migrate" programming content stored on a first device (e.g., STT 158-1) to a second device (e.g., STT 158-2). Specifically, in order for the second device to obtain the content key to decrypt the copy of the encrypted content file in STT 158-2, the latter needs an encrypted content key V-1 associated therewith. In accordance with an aspect of the invention, the content key V-1 associated with STT 158-2 can be successfully derived from the encrypted content key V-2 (604) provided that the subscriber associated with STT 158-2 be also S-1, which is the case here and reflected by subscriber registry 360 in Fig. 2. Referring to rows 368-1 and 368-2 of registry 360, in this instance both STT 158-1 having the MAC-1 address and STT 158-2 having the MAC-2 address are associated with S-1.

Assuming that SDVR STT 158-2 in Fig. 9 has in storage 910 a copy of the

-15-

encrypted content file 602 and an encrypted content key V-2 (604) from SDVR STT 158-1 (e.g., by physically removing storage 610 from SDVR STT 158-1 to SDVR STT 158-2, i.e., storage 610 the same as storage 910), encryption module 965 of STT 158-2 retrieves the encrypted content key V-2 (604) from storage 910, and STID 914 from memory 990. Module 965 transmits a message containing the encrypted content key V-2 (604) and STID 914 to headend 120.

At headend 120, the encrypted content key V-2 (604) is utilized to generate an encrypted content key V-1 associated with the SDVR STT 158-2, which is needed for STT 158-2 to derive the content key for decrypting the encrypted content file 602.

Fig. 10 is a flowchart depicting a routine for generating an encrypted content key V-1 associated with STT 158-2, in accordance with an embodiment of the invention. At step 571, manager 225 in headend 120 receives from the new device STT 158-2 the encrypted content key V-2 (604) and STID 914. At step 572, manager 225 consults subscriber registry 360, and uses STID 914 (i.e., MAC-2) to determine the corresponding subscriber ID (i.e., S-1). At step 573, manager 225 retrieves from subscriber key table 283 the subscriber private key SPRIKEY-1 associated with subscriber S-1. At step 574, manager 225 uses the subscriber private key to decrypt the encrypted content key V-2 (604) and thereby recover the content key in the clear.

At step 576, manager 225 consults device key table 273 and retrieves the device public key DPUBKEY-2 associated with STID 914 which is MAC-2 in this instance. At step 577, manager 225 uses the device public key DPUBKEY-2 associated with STT 158-2 to encrypt the content key. The resulting encrypted version of the content key is referred to as the "new-device (ND) encrypted content key version 1 (V-1)." At step 579, manager 225 transmits the ND encrypted content key V-1 to STT 158-2 through an FDC.

Module 965 in SDVR STT 158-2 receives the ND encrypted content key V-1 from headend 120. Module 965 stores the ND content key V-1 in storage 910. At a subsequent point in time, module 965 may retrieve device private key DPRIKEY-2 from memory 912, and use it to decrypt the ND encrypted content key V-1 and recover the content key. Module 965 may then utilize the content key to decrypt the encrypted content file 602 for viewing the "Citizen Kane" movie content.

-16-

In a second embodiment, a system-wide public key-private key pair is used in place of the subscriber key pairs stored in table 283. A system public key is made public to a collection of STTs in the network. A system private key (not shown) is stored in headend 120 by manager 225, e.g., in memory 227. Thus, for example, in
5 this second embodiment after SDVR STT 158-1 uses a content key to encrypt a content file, resulting in encrypted content file 602, it uses the system public key (not shown) in memory 210 to encrypt the content key, thereby generating an encrypted content key V-2. SDVR STT 158-1 stores the encrypted content key V-2 in association with content file 602. It should be noted that the encrypted content key
10 V-1 in SDVR STT 158-1 remains the same as the previous embodiment.

To realize portability of the content file, SDVR STT 158-1 may transfer the content file and encrypted content key V-2 therein to a second device, e.g., SDVR STT 158-2, an encrypted content key V-1 associated with SDVR STT 158-2 may be generated as follows. Module 965 in SDVR STT 158-2 transmits the received
15 encrypted content key V-2 to headend 120. Manager 225 in headend 120 receives the encrypted content key V-2, retrieves the system private key from memory 227, and uses it to decrypt the encrypted content key V-2, recovering the content key in the clear. Manager 225 then consults device key table 273 and retrieves the device public key DPUBKEY-2 associated with SDVR STT 158-2. Manager 225 uses the device
20 public key DPUBKEY-2 to encrypt the content key, producing an ND encrypted content key V-1. The ND encrypted content key is transmitted to SDVR STT 158-2, where it is stored in storage 910 in association with content file 602. It should be noted that the ND encrypted content key V-2, also stored in storage 910, is the same as the received encrypted content key V-2 from SDVR STT 158-1. At a subsequent
25 point in time, module 965 may retrieve device private key DPRIKEY-2 from memory 912, and use it to decrypt the ND encrypted content key V-1 and recover the content key. Module 965 may then utilize the content key to decrypt the encrypted content file 602 for viewing the "Citizen Kane" movie content.

In a third embodiment, a subscriber may transfer content from one device to
30 another, e.g., via a home network without involving headend 120, and control access manager 220 in particular. For example, subscriber S-1 establishes a home network

-17-

within his/her home and connects both SDVR STT 158-1 and SDVR STT 158-2 to the network. The "Citizen Kane" movie is stored in the form of encrypted content file 602 in storage 610 of SDVR STT 158-1 as described before. Suppose that subscriber S-1 wishes to transfer a copy of encrypted content file 602 from SDVR STT 158-1 to SDVR STT 158-2 via the home network. Fig. 11 is a flowchart depicting a routine for transferring one such content file from a first device to a second device. SDVR STT 158-2 may act as an initiator and transmit to SDVR STT 158-1 a request for a copy of content file 602. SDVR STT 158-2 may also transmit to SDVR STT 158-1 its own device public key, which is in this instance DPUBKEY-2.

10 Module 165 receives the request and the device public key associated with SDVR STT 158-2 (step 1105), and in response, identifies the desired content file 602 in storage 610. At step 1120, module 165 retrieves encrypted content key V-1 (603) from storage 610. At step 1125, module 165 retrieves DPRIKEY-1 from memory 212 and (at step 1130) uses DPRIKEY-1 to decrypt encrypted content key V-1 (603),
15 thereby recovering the content key in the clear. At step 1150, module 165 uses the received DPUBKEY-2 to encrypt the recovered content key. The resulting encrypted version of the content key becomes the ND encrypted content key V-1. At step 1160, module 165 transmits the ND encrypted content key V-1 to SDVR STT 158-2, along with a copy of encrypted content file 602.

20 Module 965 in SDVR STT 158-2 receives the ND encrypted content key V-1 from SDVR STT 158-1. Module 965 stores the ND content key V-1 and content file 602 in storage 910. At a subsequent point in time, module 965 may retrieve device private key DPRIKEY-2 from memory 912, and use it to decrypt the ND encrypted content key V-1 and recover the content key in the clear. Module 965 may then utilize
25 the content key to decrypt the encrypted content file 602 for viewing the "Citizen Kane" movie content.

 The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous other arrangements which embody the principles of the invention and are thus within its
30 spirit and scope.

 For example, while STTs are illustratively used in the above-described

-18-

embodiments, other comparable or functionally equivalent devices (e.g., point-of-deployment (POD) or CableCARD™ devices) may be used in addition to, or in lieu of, such STTs.

In addition, in the embodiment shown in Fig. 1, the network transport is
5 illustratively realized using HFC cable network 150. However, other networks such as digital subscriber line (DSL) networks, ethernet networks and satellite networks may be used, instead.

Finally, the system components of Fig. 1 are disclosed herein in a form in which various functions are performed by discrete functional blocks. However, any
10 one or more of these functions could equally well be embodied in an arrangement in which the functions of any one or more of those blocks or indeed, all of the functions thereof, are realized, for example, by one or more appropriately programmed processors.

-19-

Claims:

1. A device for receiving encrypted content from a storage unit, the device and the storage unit both being associated with a user, the encrypted content being decrypted in the device using a first cryptographic element, the device comprising:
- 5 being decrypted in the device using a first cryptographic element, the device comprising:
- a first interface for receiving a first encrypted version of the first cryptographic element from the storage unit, the first encrypted version of the first cryptographic element being generated by encrypting the first cryptographic element using a second cryptographic element which is associated with the user, the first encrypted version of the first cryptographic element being provided to an apparatus remote from the device, the apparatus recovering the first cryptographic element based on at least the first encrypted version of the first cryptographic element and data representative of the user;
- 10 using a second cryptographic element which is associated with the user, the first encrypted version of the first cryptographic element being provided to an apparatus remote from the device, the apparatus recovering the first cryptographic element based on at least the first encrypted version of the first cryptographic element and data representative of the user;
- a second interface for receiving from the apparatus a second encrypted version of the first cryptographic element, the second encrypted version of the first cryptographic element being generated by encrypting the recovered first cryptographic element using a third cryptographic element which is associated with the device; and
- 15 a second interface for receiving from the apparatus a second encrypted version of the first cryptographic element, the second encrypted version of the first cryptographic element being generated by encrypting the recovered first cryptographic element using a third cryptographic element which is associated with the device; and
- a module for recovering the first cryptographic element to decrypt the encrypted content based on at least the second encrypted version of the first cryptographic element.
- 20 a module for recovering the first cryptographic element to decrypt the encrypted content based on at least the second encrypted version of the first cryptographic element.
2. The device of claim 1 wherein the first interface includes the second interface.
- 25 The device of claim 1 wherein the first interface includes the second interface.
3. The device of claim 1 wherein the content includes entertainment programming content.
4. The device of claim 1 wherein the first cryptographic element includes a secret key in accordance with a data encryption standard (DES) technique.
- 30 a secret key in accordance with a data encryption standard (DES) technique.

-20-

5. The device of claim 1 wherein the second cryptographic element includes an encryption key in accordance with a public key algorithm.

6. The device of claim 1 wherein the third cryptographic element includes
5 an encryption key in accordance with a public key algorithm.

7. The device of claim 1 comprising a terminal having storage.

8. The device of claim 1 comprising a terminal having digital video
10 recorder functions.

9. A system for securing, in a device, content which is encrypted using a content key, the system comprising:

a server for generating a first encrypted content key by encrypting the
15 content key using a first cryptographic element; and

an interface for providing the first encrypted content key to the device where the encrypted content is stored in association with the first encrypted content key and a second encrypted content key which is generated by encrypting the content key using a second cryptographic element, which is associated with the device.

20

10. The system of claim 9 wherein the first encrypted content key is provided to the device through a communications network.

11. The system of claim 10 wherein the communications network includes
25 a multi-channel delivery network.

12. The system of claim 10 wherein the communications network includes a hybrid fiber coaxial (HFC) cable network.

13. The system of claim 9 wherein the content includes entertainment
30 programming content.

-21-

14. The system of claim 9 wherein the content key includes a secret key in accordance with a DES technique.

5 15. The system of claim 9 wherein the content key is generated in the device.

16. The system of claim 9 wherein the first cryptographic element includes an encryption key in accordance with a public key algorithm.

10 17. The system of claim 9 wherein the second cryptographic element includes an encryption key in accordance with a public key algorithm.

18. The system of claim 9 wherein the first cryptographic element is associated with a user of the device.

15

19. The system of claim 9 wherein the first cryptographic element is associated with the system.

20 20. Apparatus for decrypting encrypted content in a device remote from the apparatus, the encrypted content in the device being decrypted using a content key, the apparatus comprising:

an interface for receiving from the device a first encrypted content key;
a database for searching for a first cryptographic element which is associated with a user of the device, the content key being recovered by decrypting the first encrypted content key using the first cryptographic element, a second encrypted content key being generated by encrypting the recovered content key using a second cryptographic element which is associated with the device; and

25

a server for providing at least the second encrypted content key to the device where the content key is recoverable based on at least the second encrypted content key.

30

-22-

21. The apparatus of claim 20 wherein the first cryptographic element is identified based on data representative of the user of the device.

5 22. The apparatus of claim 21 wherein the data includes an identity of the user.

23. The apparatus of claim 20 wherein the content key includes a secret key in accordance with a DES technique.

10 24. The apparatus of claim 20 wherein the first cryptographic element includes an encryption key in accordance with a public key algorithm.

25. The apparatus of claim 20 wherein the second cryptographic element includes an encryption key in accordance with a public key algorithm.

15

26. The apparatus of claim 20 wherein the content includes entertainment programming content.

20 27. A method for use in a first device to which encrypted content is transported from a second device, the first device and the second device both being associated with a user, the encrypted content being decrypted in the first device using a first cryptographic element, the method comprising:

25 receiving a first encrypted version of the first cryptographic element from the second device, the first encrypted version of the first cryptographic element being generated by encrypting the first cryptographic element using a second cryptographic element which is associated with the user;

30 providing the first encrypted version of the first cryptographic element to an apparatus remote from the first device, the apparatus recovering the first cryptographic element based on at least the first encrypted version of the first cryptographic element and data representative of the user;

-23-

receiving from the apparatus a second encrypted version of the first cryptographic element, the second encrypted version of the first cryptographic element being generated by encrypting the recovered first cryptographic element using a third cryptographic element which is associated with the first device; and

5 recovering the first cryptographic element to decrypt the encrypted content based on at least the second encrypted version of the first cryptographic element.

28. The method of claim 27 wherein the content includes entertainment
10 programming content.

29. The method of claim 27 wherein the first cryptographic element includes a secret key in accordance with a DES technique.

30. The method of claim 27 wherein the second cryptographic element
15 includes an encryption key in accordance with a public key algorithm.

31. The method of claim 27 wherein the third cryptographic element
20 includes an encryption key in accordance with a public key algorithm.

32. A method for use in a system for securing, in a device, content which is encrypted using a content key, the method comprising:

generating a first encrypted content key by encrypting the content key using a first cryptographic element; and

25 providing the first encrypted content key to the device where the encrypted content is stored in association with the first encrypted content key and a second encrypted content key which is generated by encrypting the content key using a second cryptographic element, which is associated with the device.

33. The method of claim 32 wherein the first encrypted content key is
30 provided to the device through a communications network.

-24-

34. The method of claim 33 wherein the communications network includes a multi-channel delivery network.

5 35. The method of claim 33 wherein the communications network includes an HFC cable network.

36. The method of claim 32 wherein the content includes entertainment programming content.

10 37. The method of claim 32 wherein the content key includes a secret key in accordance with a DES technique.

38. The method of claim 32 wherein the content key is generated in the device.

15

39. The method of claim 32 wherein the first cryptographic element includes an encryption key in accordance with a public key algorithm.

20 40. The method of claim 32 wherein the second cryptographic element includes an encryption key in accordance with a public key algorithm.

41. The method of claim 32 wherein the first cryptographic element is associated with a user of the device.

25 42. The method of claim 32 wherein the first cryptographic element is associated with the system.

30 43. A method for use in an apparatus for decrypting encrypted content in a device remote from the apparatus, the encrypted content in the device being decrypted using a content key, the method comprising:

receiving from the device a first encrypted content key;

-25-

searching a database for a first cryptographic element which is associated with a user of the device;

using the first cryptographic element to decrypt the first encrypted content key, thereby recovering the content key;

5 using a second cryptographic element which is associated with the device to encrypt the recovered content key, thereby generating a second encrypted content key; and

providing the second encrypted content key to the device where the content key is recoverable based on at least the second encrypted content key.

10

44. The method of claim 43 wherein the first cryptographic element is identified based on data representative of the user of the device.

15 45. The method of claim 44 wherein the data includes an identity of the user.

46. The method of claim 43 wherein the content key includes a secret key in accordance with a DES technique.

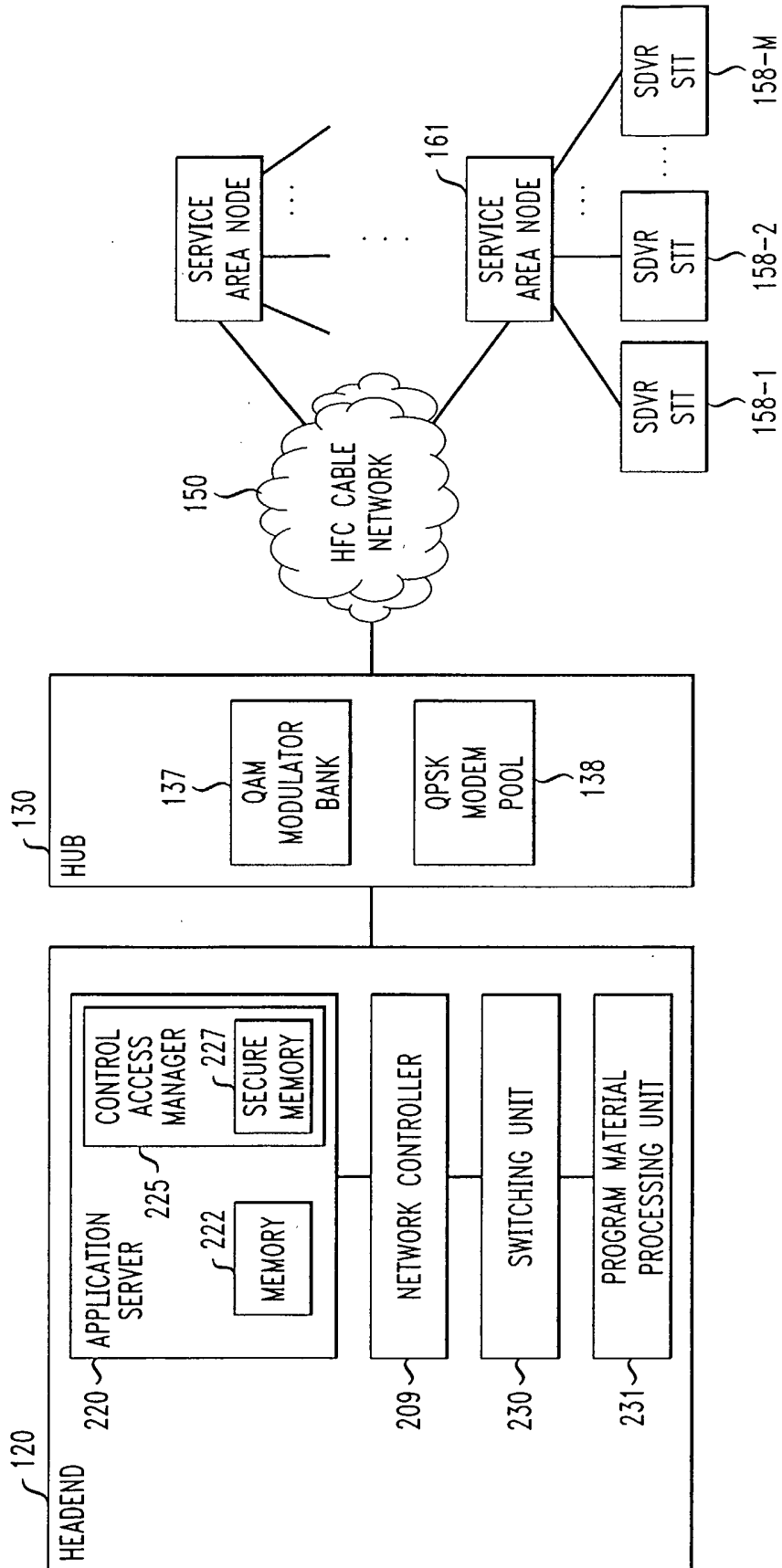
20 47. The method of claim 43 wherein the first cryptographic element includes an encryption key in accordance with a public key algorithm.

48. The method of claim 43 wherein the second cryptographic element includes an encryption key in accordance with a public key algorithm.

25

49. The method of claim 43 wherein the content includes entertainment programming content.

FIG. 1



2/6

FIG. 2

360

363		364	
STID		SUBSCRIBER ID	
368-1	MAC-1	S-1	
368-2	MAC-2	S-1	
	MAC-3	S-2	
⋮	⋮	⋮	⋮

FIG. 3

273

276		277	
STID		DEVICE PUBLIC KEY	
279-1	MAC-1	DPUBKEY-1	
	MAC-2	DPUBKEY-2	
	MAC-3	DPUBKEY-3	
⋮	⋮	⋮	⋮
	MAC-M	DPUBKEY-M	

3/6

FIG. 4

283

	286	287	288
	SUBSCRIBER ID	SUBSCRIBER PUBLIC KEY	SUBSCRIBER PRIVATE KEY
289-1 {	S-1	SPUBKEY-1	SPRIKEY-1
	S-2	SPUBKEY-2	SPRIKEY-2
	S-3	SPUBKEY-3	SPRIKEY-3
	⋮	⋮	⋮

FIG. 5

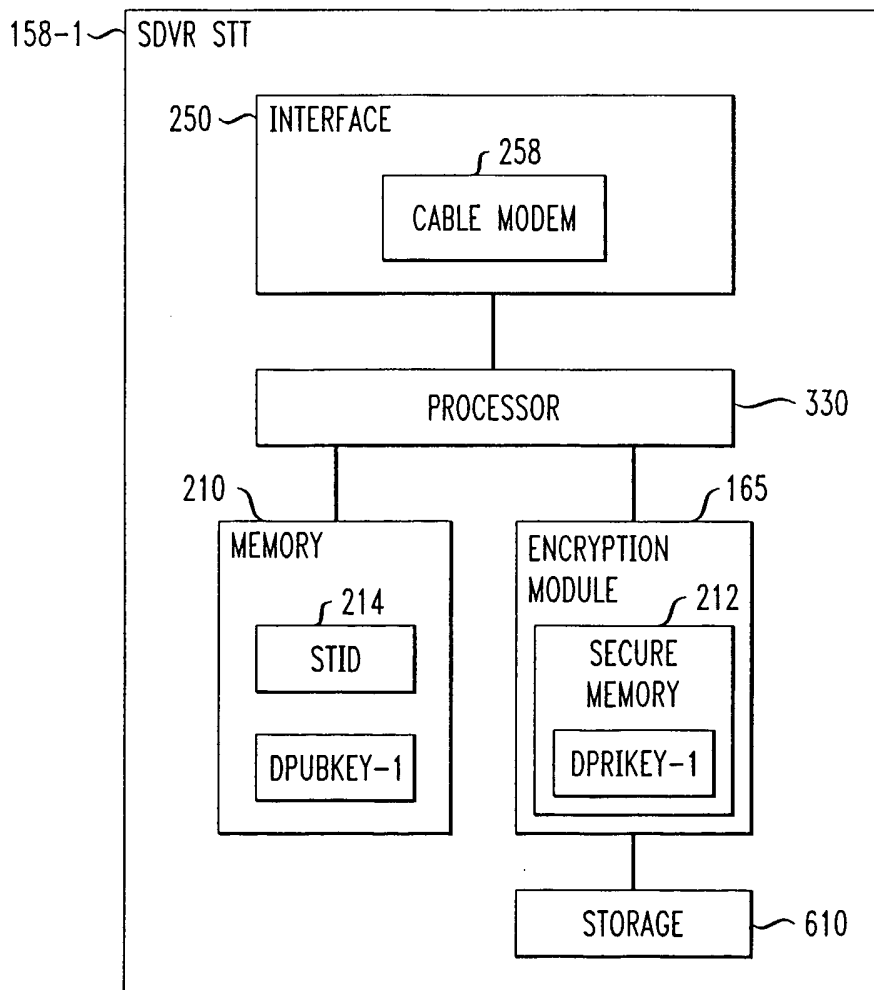


FIG. 6

610

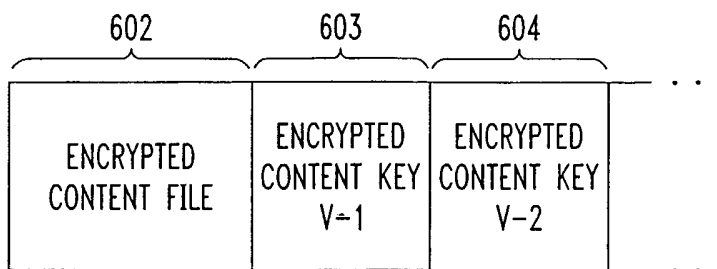


FIG. 7

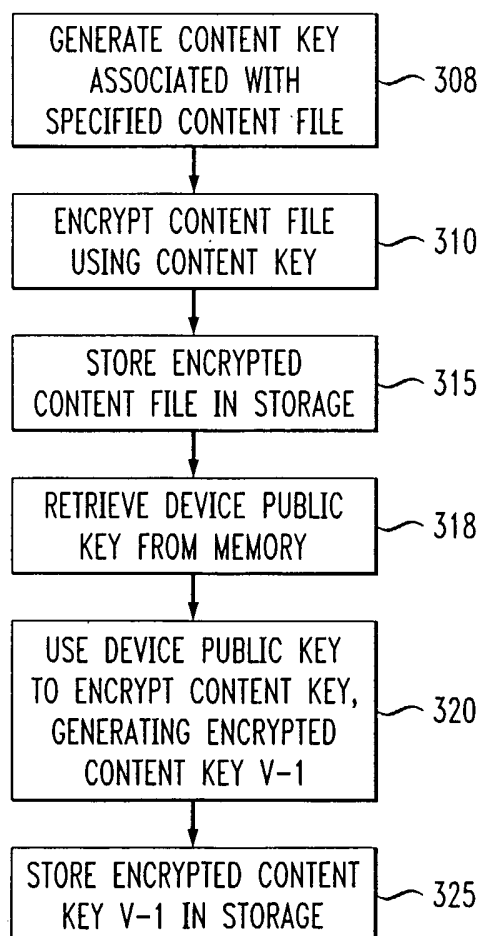


FIG. 8 5/6

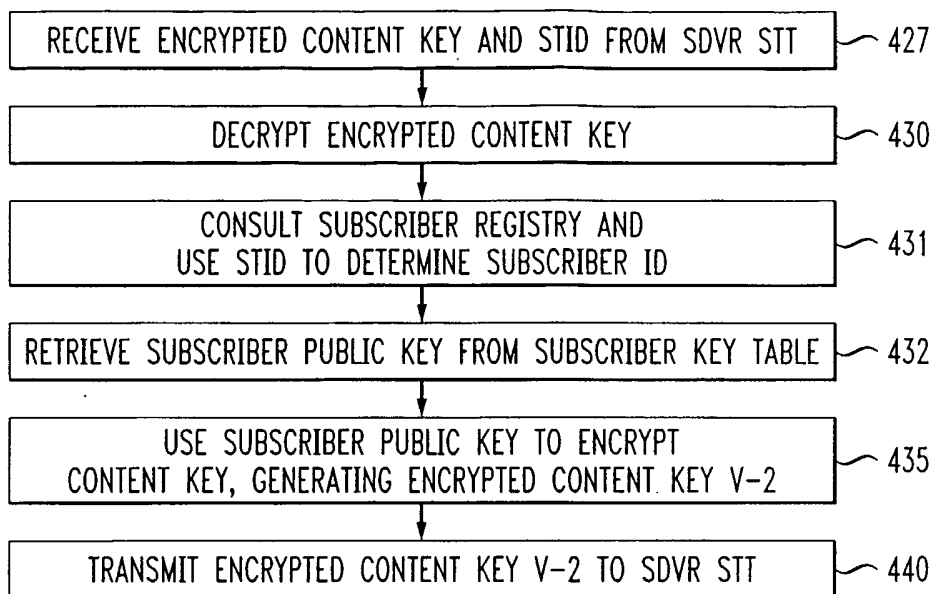


FIG. 9

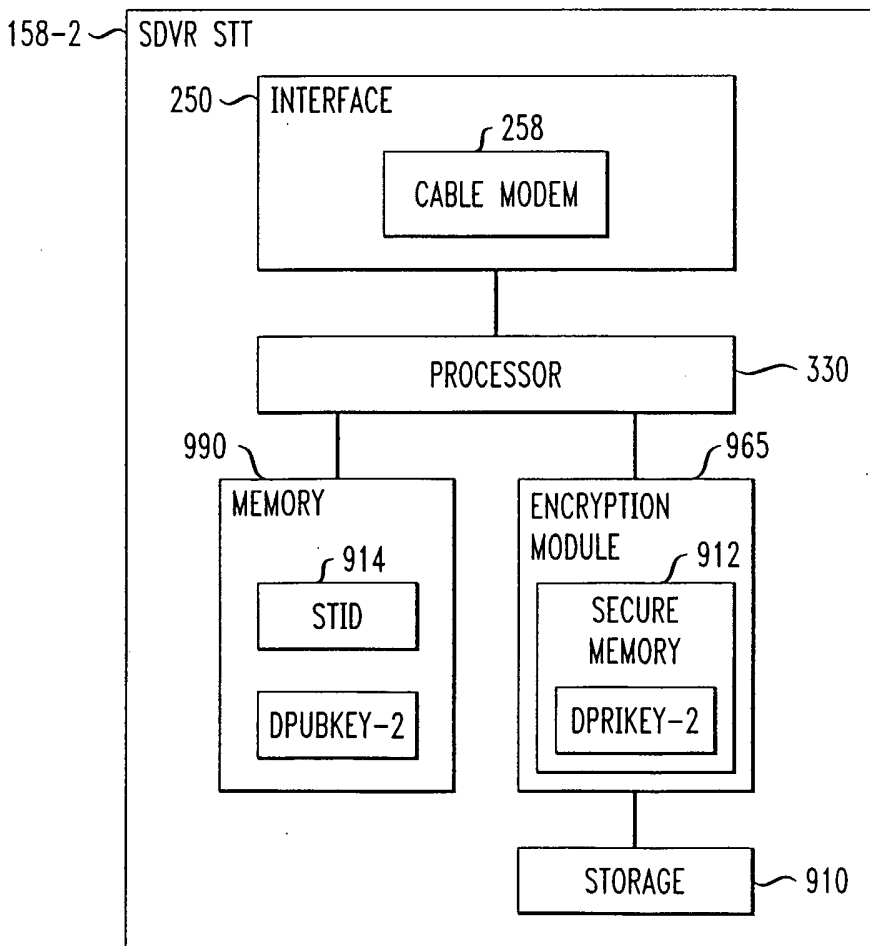


FIG. 10

6/6

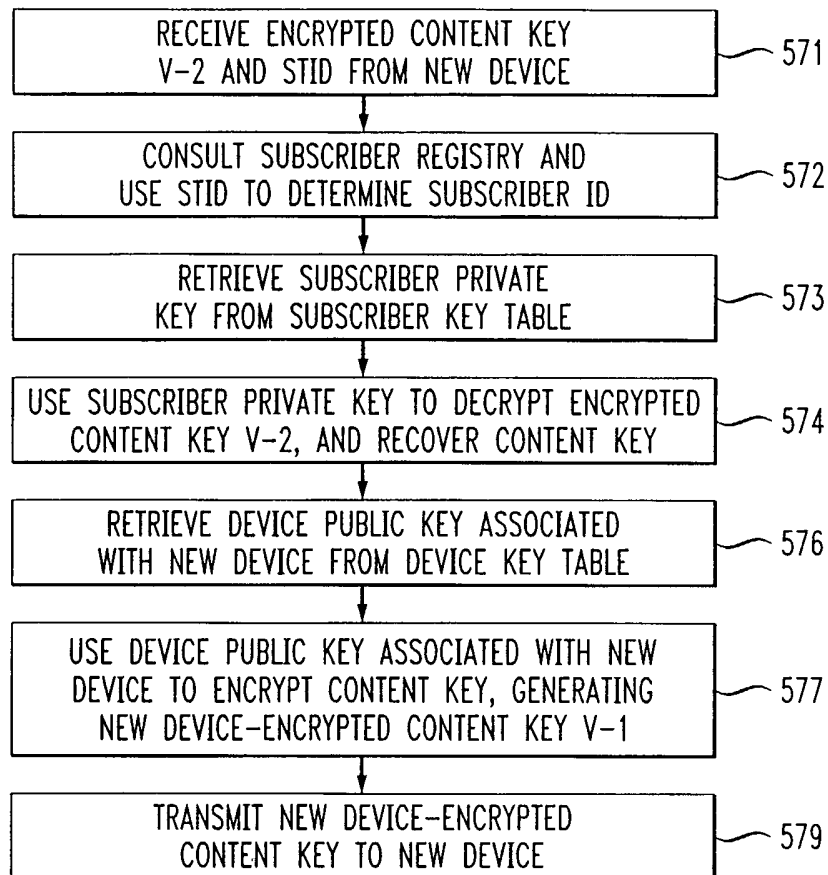


FIG. 11

