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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2019 (24.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/018431 A1

(51) International Patent Classification:
G06F 21/10 (2013.01) *G06F 21/74* (2013.01)

(21) International Application Number:
PCT/US2018/042542

(22) International Filing Date:
17 July 2018 (17.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/652,082 17 July 2017 (17.07.2017) US

(71) Applicant: **INSIDE SECURE** [FR/FR]; Arteparc Bachasson Batiment A, Rue de la Carriere de Batiment, CS 70025, 13590 Meyreuil (FR).

(72) Inventors: **COCCHI, Ronald P.**; 3861 Daisy Circle, Seal Beach, California 90740 (US). **GAGNON, Gregory J.**; 311 Via Mesa Grande, Redondo Beach, California 90277 (US). **FLAHARTY, Dennis R.**; 4785 Bullard Drive, Shingle Springs, California 95682 (US). **GORMAN, Michael A.**; 6154 Lawrence Street, Cypress, California 90630 (US). **CARSON, Jacob T.**; 3312 Terrace Ridge Lane, Long Beach, California 90804 (US). **SKUBISZEWSKI, Matthew A.**; 1920 Vanderbilt Ln., #1, Redondo Beach, California 90278 (US).

(74) Agent: **COOPER, Victor G.**; Gates & Cooper LLP, 6060 Center Drive, Suite 830, Los Angeles, CA 90045 (US).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

(54) Title: METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM

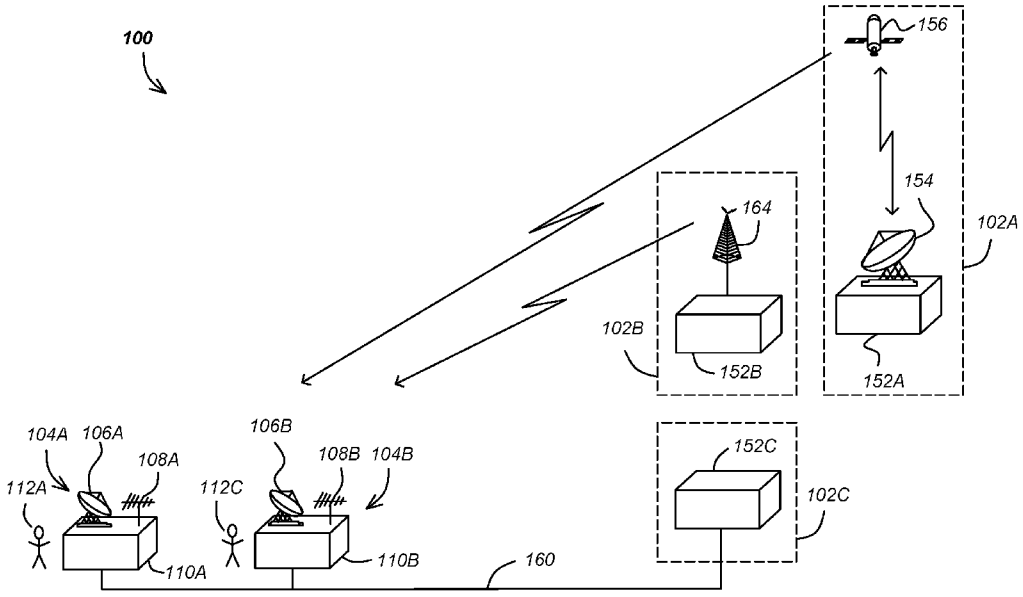


FIG. 1

(57) Abstract: A method and apparatus for brokering the enablement of the communication of encrypted media programs from a plurality of independent broadcasters to a plurality of receivers is disclosed. The system makes use of a pairing key for each provided service, which is differently encrypted by a pairing server and by the broadcaster providing the service. The encrypted versions of the pairing key are decrypted in a first receiver module using information known to the pairing service but not the broadcaster and in a second receiver module using information known to the broadcaster. The pairing key is used to cryptographically bind the first and second receiver modules.

WO 2019/018431 A1

[Continued on next page]

OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *with information concerning one or more priority claims considered void (Rule 26bis.2(d))*

METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is an international (PCT) Application of U.S. Patent Application No. 15/652,082, entitled "METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM," by Ronald P. Cocchi, Gregory J. Gagnon, Dennis R. Flaharty, Michael A. Gorman, Jacob T. Carson and Matthew A. Skubiszewski, filed July 17, 2017, which application:

claims benefit of U.S. Provisional Patent Application, No. 62/446,196, entitled "SIGNALING METHOD FOR CAS SWITCHING AND KEY DERIVATION," by Ronald P. Cocchi et al., filed January 13, 2017, which is also incorporated by reference herein; and

is a continuation-in-part of U.S. Patent Application No. 14/692,500, entitled "METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM," by Ronald P. Cocchi, Gregory J. Gagnon, and Dennis R. Flaharty, filed April 21, 2015, now issued as U.S. Patent No. 9,014,375, which application is a continuation of U.S. Patent Application No. 13/541,492, entitled "METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING

A SINGLE CONDITIONAL ACCESS SYSTEM," by Ronald P. Cocchi, Gregory J. Gagnon, and Dennis R. Flaharty, filed July 3, 2012, now issued as U.S. Patent No. 9,014,375, which application is a continuation of U.S. Patent Application No. 11/795,272, entitled "METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM," by Ronald P. Cocchi, Gregory J. Gagnon, and Dennis R. Flaharty, filed July 13, 2007, now issued as U.S. Patent No. 8,243,925, which is a national phase application of International Patent Application No.: PCT/US2005/037197, entitled "METHOD AND APPARATUS FOR SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM," by Ronald P. Cocchi, Gregory J. Gagnon, and Dennis R. Flaharty, filed October 18, 2005, which claims benefit of U.S. Provisional Patent Application No. 60/619,663, entitled "METHOD OF SUPPORTING MULTIPLE BROADCASTERS INDEPENDENTLY USING A SINGLE CONDITIONAL ACCESS SYSTEM," by Ronald P. Cocchi, Gregory J. Gagnon, and Dennis R. Flaharty, filed October 18, 2004, all of which applications are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and methods for providing conditional access to media programs, and in particular to a system and method for providing for such conditional access between multiple independent broadcasters and a plurality of customers using a single conditional access system.

2. Description of the Related Art

For many years, media programs such as television and radio programs have been broadcast to viewers/listeners free of charge. More recently, this free-of-charge dissemination model has been augmented with a fee-for-service and/or fee-for-view model in which paying subscribers are provided access to a greater variety and number of media programs, including video programs, audio programs and the like, by cable, satellite and terrestrial broadcasts.

However, while subscriber-based services are readily available in some areas, they are not available on a world-wide basis. Further, in current media program subscription business models, subscribers are typically offered services from a small number of providers (e.g. DIRECTV or ECHOSTAR, or the approved local cable provider) each of which typically provide a large number of media channels from a variety of sources (e.g. ESPN, HBO, COURT TV, HISTORY CHANNEL). To assure that only subscribers receive the media programs, each service provider typically encrypts the program material and provides equipment necessary for the customer to decrypt them so that they can be viewed.

Since they provide a large number of programs and typically at a relatively high cost, the vast majority of customers subscribe to only one of the foregoing services (e.g. DIRECTV, ECHOSTAR, *or* the local cable provider), but not multiple providers. It is expected that future business models will evolve to the point where customers will subscribe to more than one media provider, each of which provides a smaller number of media channels. The foregoing is especially true in areas where subscriber-based services are in their infancy, including for example, large parts of Asia, Africa, and South America.

One of the roadblocks to the evolution of such services is the means by which the service provider assures that only paying customers receive their media programs. Existing conditional access systems are not compatible with each

other, and it is thought to be prohibitively expensive for each provider of a limited number of media programs to produce and provide its own conditional access system to potential subscribers. Another problem is that customers would typically prefer to receive all media programs through a single device (and hence, a single conditional access system), rather than multiple such systems. Accordingly, there is a need in the art for a method and apparatus that allows multiple program providers (e.g. broadcasters) to transmit media programs to paying subscribers via a single conditional access system. The present invention satisfies that need.

SUMMARY OF THE INVENTION

To address the requirements described above, the present invention discloses a method, apparatus, article of manufacture for brokering the enabling of communication of encrypted media programs from a plurality of independent broadcasters to a plurality of receivers, each encrypted media program decryptable by a first receiver module securely communicating with a second receiver module according to a pairing key associated with one of the plurality of receivers. In one disclosed embodiment, the method comprises the steps of transmitting a service enabling request from one of the plurality of broadcasters to a broker independent from the one of the plurality of broadcasters, the request comprising an identification of the one of the plurality of receivers; receiving a first encrypted version of the pairing key $E_{S_1}[K_p]$ from the broker, the first encrypted version of the pairing key $E_{S_1}[K_p]$ decryptable by first information S_1 securely stored in the first receiver module of the one of the plurality of receivers; generating a second encrypted version of the pairing key K_p, the second encrypted version of the pairing key $E_{S_2}[K_p]$ decryptable by second information S_2 securely stored in the second receiver module; and transmitting the first encrypted version of the pairing key $E_{S_1}[K_p]$ and the second encrypted version of the pairing key $E_{S_2}[K_p]$ to the one of the plurality of receivers. In another disclosed embodiment, the apparatus is described by system for brokering the enabling of communication of encrypted media programs from a plurality of independent broadcasters to a plurality of receivers, each encrypted media program decryptable by a first receiver module securely communicating with a second receiver module according to a pairing key K_p associated with one of the plurality of receivers. The system comprises a broker, for providing a first encrypted version of the pairing key $E_{S_1}[K_p]$ in response to a service enabling

request from one of the plurality of broadcasters, the service request having an identification of one of the plurality of receivers, wherein the first encrypted version of the pairing key $E_{S_1}[K_p]$ is decryptable by first information S_1 stored in the first receiver module. In each of these embodiments, at least one of the first information S_1 and the second information S_2 may be derived from a hardware root of trust stored in at least one of the first receiver module and the second receiver module

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram illustrating a media program distribution system;

FIG. 2 is a diagram of a typical subscriber station;

FIG. 3 is a diagram illustrating a multiple broadcaster media program distribution system;

FIGs. 4A-4D are diagrams illustrating one embodiment of how the pairing system cooperatively operates with multiple service providers and equipment at the subscriber stations to implement a conditional access system;

FIG. 5A is a diagram illustrating one embodiment of the service provider;

FIG. 5B is a diagram illustrating an embodiment of a table stored in the pairing system;

FIG. 5C is a diagram illustrating an embodiment of a table stored by the service provider;

FIG. 6 is a diagram illustrating one embodiment of the STB;

FIG. 7 is a diagram illustrating an exemplary embodiment of the transport module and the CAM; and

FIG. 8 is a diagram of a computer that can be used to implement selected modules.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

FIG. 1 is a diagram illustrating a media program distribution system 100. The system 100 includes a plurality of service providers (hereinafter alternatively referred to as broadcasters) 102, including a first service provider 102A that broadcasts media programs from a satellite broadcast facility 152A via one or more uplink antennas and one or more satellites 156, a second service provider 102B, that broadcasts media programs from terrestrial broadcast facility 152B and one or more terrestrial antennas 164, and a third service provider 102C that broadcasts media programs via a cable link 160.

The system 100 also comprises a plurality of subscriber stations 104A, 104B (alternatively referred to hereinafter as subscriber station 104), each providing service to one or more subscribers 112A, 112B (alternatively referred to hereinafter as subscribers 112). Each subscriber station 104A, 104B may include a satellite reception antenna 106A, 106B (alternatively referred to hereinafter as satellite reception antenna 104) and/or a terrestrial broadcast antenna 108A, 108B (alternatively referred to hereinafter as terrestrial broadcast antenna 108) communicatively coupled to a receiver 110A, 110B (alternatively referred to hereinafter as receiver 110), which is also known as a set top box (STB) or an integrated receiver/decoder (IRD).

As described above, in prior art systems, each receiver 110A, 110B (or at least, each conditional access system used with each receiver) is capable of receiving subscriber-based media programs from only one of the media program providers

102. Hence, if a subscriber 112 wanted to receive media programs from more than one media program provider 102 on a subscription basis, the subscriber may need not only to have a multiple receivers 110 at the subscriber station 104A, but also, will require multiple conditional access systems.

FIG. 2 is a diagram of a typical subscriber station 104. Each station 104 includes at least one receiver or STB 110, which itself includes a transport module 202 that communicates with a conditional access module (CAM) 206. In one embodiment, the CAM 206 is a smart card that is removably communicatively coupleable to the transport module 202 and hence, the STB 110. In another embodiment, the CAM 206 is a device such as a chip or a collection of devices that are physically integrated with the STB 110 and irremovable. To assure that only those who subscribe to the service are provided with media programs, the service providers typically encrypt the media program M with a control word CW, thus producing and encrypted program $E_{CW}[M]$, and transmit the encrypted media program $E_{CW}[M]$ and an encrypted version of the control word $E[CW]$ to the receiver 110. The receiver 110 receives both the encrypted program $E_{CW}[M]$ and the encrypted control word $E[CW]$. The transport module 202 analyzes the incoming data stream and passes the encrypted control $E[CW]$ to the CAM 206, which decrypts the control word CW and returns the decrypted control word CW to a security module 204 or similar device in the transport module 202. The security module 204 then uses the control word CW to decrypt the encrypted media program $E_{CW}[M]$ to produce the media program M for presentation to the subscriber. This system assures that only those who are in possession of a valid CAM 206 can receive and decode media programs. However, it does not prevent the use of the CAM 206 in any other STB 110. Hence, if the CAM 206 is compromised or duplicated, unauthorized access to media programs is possible.

FIG. 3 is a diagram illustrating a multiple broadcaster Conditional Access Subscriber Administration System (CASAS) 200. The MB system 200 is similar to that which is disclosed in FIG. 1, but includes a pairing broker 304, which can communicate with the broadcast facilities 152 via a communications medium 302 such as the Internet.

FIGs. 4A-4D are diagrams illustrating one embodiment of how the pairing broker 304 cooperatively operates with multiple service providers 102 and equipment at the subscriber stations 104 to implement a conditional access system. FIGs. 4A-4D will be described in connection with and with reference to FIGs. 5 and 6, which illustrate one embodiment of the service provider 102 elements and STB 110 elements, respectively.

FIG. 4A begins with a potential customer 112 who has decided to subscribe a media program service offered by a service provider 102. To do so, the subscriber contacts the service provider 102 and transmits information sufficient to identify the STB and the CAM to the service provider 102, as shown in block 402.. In one embodiment, this information includes an STB 110 unique identifier (ID) (such as a serial number or other designation) and a CAM 206 unique identifier (CAM ID). In a preferred embodiment, this is accomplished by transmitting the information via the Internet 302 or similar network.

This can be accomplished by use of a web browser implemented in a computer 512 disposed at the subscriber station 104 and a web transaction module 502 implemented at the service provider 102. If desired, the subscriber's web browser can include the appropriate references to the URL where the request and STB ID and CAM ID should be transmitted. In one embodiment, in addition to the STB ID, the potential subscriber also transmits his/her credit card information (e.g. the account number) as well. This allows for services to be automatically billed for monthly subscription fees without further interaction. Credit card payment administration can be performed by the service provider 102

or by a third party such as PAYPAL. These functions can be performed by the subscriber administration module (SAM) 504. The SAM 504 can also comprise or be integrated with a customer relationship management (CRM) system or systems. If access is approved (e.g. if the supplied credit card information has been verified), the subscriber administration module 504 directs the web transaction module 502 to request a pairing key K_p from the pairing broker 304.

This implementation reduces the support requirements for the service provider 102. In other embodiments, the potential customer 112 can contact the service provider 102 via telephone or other means and provide the service request, STB ID, and CAM ID. Further, if desired, the pairing broker 304 can receive the service request (preferably via an appropriate Internet interface) and forward the request for service and the appropriate identifying information to the service provider 102.

The service provider 102 receives the service request the identifying information, as shown in block 404. The service provider 102 then transmits an enabling service request and the STB ID to the pairing broker 304, as shown in block 408. In block 410, the pairing broker 304 receives the service enabling request and the STB ID. A first encrypted version of a pairing key K_p is then provided. The pairing key K_p was generated either in block by the service provider 102, as shown in block 406 or, preferably by the pairing broker 304, as shown in block 406'. The first encrypted version of the pairing key K_p is provided so as to be decryptable using first information S_1 securely stored in a first receiver module such as the transport module 202 shown in FIG. 6 (the first encrypted version of the pairing key K_p therefore described as $E_{S_1}[K_p]$). In one embodiment, this is accomplished by use of a secret that is known to the pairing broker 304, but unknown to the service provider 102. The STB IDs and related first information S_1 can be stored in a table or a database 514 in the

pairing broker 304. If desired, the related first encrypted versions of the pairing key $E_{S_1}[K_p]$ can be stored as well.

In block 414, the first encrypted version of the pairing key $E_{S_1}[K_p]$ is transmitted to the service provider 102. If the pairing key K_p was generated by the pairing broker 304, the pairing key K_p is also transmitted to the service provider 102. One of both of the first encrypted version of the pairing key $E_{S_1}[K_p]$ and the pairing key K_p can be securely transmitted to the service provider 102 via a shared secret, a private key, or a public/private key security paradigm, if desired.

The foregoing process can be used to request all services from a service provider with a single pairing key K_p or repeated to request other services from the service provider 102, with each service enabled and controlled via a different pairing key K_p. For example, the service provider 102 may provide both general services (e.g. access to a number of channels as a part of a baseline fee service) and pay-per-view services (e.g. access to a particular program or set of programs on a pay-per-view basis). Therefore, if the foregoing process was undertaken to subscribe to the general services and the potential subscriber 112 desires order ahead pay per view (OPPV) services or impulse pay per view (IPPV) services as well, the foregoing process can be repeated for those services, resulting in the provision of a first encrypted version of a different pairing key for each service. The system 200 has the ability to store credit information in the security module 204, CAM 206, or elsewhere, and can therefore limit the amount of IPPV events the subscriber can purchase prior to requesting additional credits. Finally, the potential subscriber 112 can repeat this process for each service provider 102 from which they wish to receive service.

Although the pairing broker 304 need not generate or store the pairing keys K_p, it may be desirable to do so. FIG. 5B is a diagram showing a table that might be used to store and relate the STB ID to first information S_1, a service provider 102 identifier (BDCST ID), and pairing keys for general services, IPPV, and multiple OPPV services.

In block 420, the service provider 102 receives the first encrypted version of the pairing key K_p, and generates a second encrypted version of the pairing key K_p such that it is decryptable by second information S_2 securely stored in a second receiver module such as the conditional access module 206 (the second encrypted version of the pairing key K_p therefore described as $E_{S_2}[K_p]$).

The service provider 102 can store a table or database relating STB IDs and the pairing keys K_p for each of the provided services. FIG. 5C is an example of how such information may be stored. Note that the BRDCST ID column is not necessary in this case, because the identity of the service provider 102 is inherently known.

In block 422, the service provider 102 transmits an entitlement control message (ECM) or an entitlement management message (EMM) to the subscriber station. The ECM is transmitted to the STB 110 in response to a subscriber request for access to general media programs from the service provider 102, while the EMM is transmitted in response to a subscriber request for a specific program (e.g. an impulse or order ahead pay-per-view). The ECM/EMM includes the first encrypted version of the applicable pairing key $E_{S_1}[K_p]$, the second encrypted version of the pairing key $E_{S_2}[K_p]$, and the ID of the service provider 102 (BRDCST ID) which is providing the services related to the pairing key K_p. This transmission can be accomplished via the same system used to transmit the media program *M* itself, or a different communication system such

as the Internet or a public switched telephone network (PSTN) or cellphone network. In block 424, the transport module 304 receives the first encrypted version of the pairing key $E_{S_1}[K_p]$ and the second encrypted version of the pairing key $E_{S_2}[K_p]$, and the service provider ID. The second encrypted version of the pairing key $E_{S_2}[K_p]$ is provided to the conditional access module 310, where it is received, decrypted (using the second information S_2) to obtain the pairing key K_p which is stored (along with a reference to the service provider ID (BRDCST ID) from which the pairing key K_p was received), as shown in blocks 428 and 430. Similarly, the first encrypted version of the pairing key $E_{S_1}[K_p]$ is decrypted and stored in the transport module 304 (also along with a reference to the service provider ID from which the pairing key K_p was received), as shown in block 432. FIG. 6 shows an exemplary embodiment of how the data relating services, broadcasters, and pairing keys K_p might be stored in the transport module and the conditional access module.

Thereafter, the pairing key K_p is used to encrypt communications between the conditional access module 206 and the transport module 202. Henceforward, the conditional access module 206 cannot be used a different STB 110, although if desired, more than one STB 110 can be provided to a customer, each having the same first information the conditional access module to be used with different STBs 110 in the same household.

To begin service, the broadcast module 506 and/or the broadcast headend 516 encrypts media programs *M* 510 according to a control word (*CW*), encrypts the control word (*CW*) itself, and broadcasts a program stream comprising the encrypted program material $E_{CW}[M]$ and the encrypted control word $E[CW]$ to the STBs 100, as shown in blocks 450, 452 and 454. The

program stream may also comprise program guide information from the program guide module 508.

The transport module 202 in the STB 110 receives the program stream, separates out the packets of information by channel (typically according to a packet ID), and provides the encrypted control word $E[CW]$ to the conditional access module 206. The conditional access module 206 receives the encrypted control word $E[CW]$ decrypts it to recover the control word (*CW*), encrypts the control word (*CW*) with the pairing key K_p, and provides the encrypted pairing key $E_{K_p}[CW]$ to the transport module 202, as shown in blocks 460-466. Using an STB application 602 and media kernel 604, the transport module 202 decrypts the encrypted control word $E_{K_p}[CW]$ using the pairing key K_p thus recovering the control word (*CW*), as shown in block 472, and uses the decrypted control word (*CW*) to decrypt the encrypted media program $E_{CW}[M]$ to produce the media program *M*, as shown in block 474.

The foregoing system can be used to modify or change the provision of services from the service provider 102 as well. This can be accomplished by the service provider 102 deleting, adding, or modifying the pairing keys K_p in cooperation with the pairing broker 304 in essentially the same way as described above. Such modification can occur at the subscriber's behest (e.g. the subscriber desires either more, less, or different services than previously), or that of the service provider 102 (e.g. if the offered services change or the subscriber's credit card is no longer valid).

The modules described above can be implemented as one or more software modules comprising instructions being performed by one or more special or general purpose processors, or may be implemented with hardware modules having dedicated circuitry, or with both hardware and software modules. In one embodiment, for example, the pairing broker 304 is implemented by a

pairing server, and the program guide module 508, broadcast module 506, subscriber administration module 504 and web transaction module 502 are all implemented as servers, the transport module 202 and security module 204 are implemented in a secure, tamperproof electronic circuit, and the conditional access module is implemented on a smart card.

Derived Key Mechanism in SoCs:

The system and method described above uses unique secrets S_1 and S_2 into the transport module 202 and CAM 206. In the embodiments described below, either or both of the unique secrets S_1 and S_2 can be derived from a hardware root of trust that is programmed into the device itself. For example, the transport module 202 or CAM may be at least partially implemented using System-on-Chip (SoC) architectures that permit hardware root of trust values to be programmed into the SoC at the SoC manufacturing site using black-box techniques. Since the values of S_1 and S_2 are computed from the hardware root of trust using software and key values that may be provided by the security provider, this permits later allocation of these SoCs to any one of a number of potential CE device manufacturers and many independent CAS/DRM security providers (security provider in this context broadly refers to any entity that would use the derived key database for a population of fielded CE devices to protect content for purchase by another entity who had a particular CE device in the deployed location (e.g. home). SoC programming can also occur at the packaging or product manufacturing facility by execution of an in-field programming sequence on the SoC.

In traditional broadcast and cable system, content is offered to subscribers within the content distribution ecosystem directly from the service provider, i.e. satellite or cable provider. In some embodiments of such systems, security based on a hardware root of trust is used for high value content. In both

CAS and DRM content distribution paradigms, a security provider independent architecture can support multiple concurrent or serial CAS and DRM implementations using a single black box programming security platform with limited One Time Programming (OTP) resources to store secrets representing the hardware root of trust that are used to derive the S_1 and S_2 values. This "derived key" security architecture implementation can provide a means for instantaneous switching between security profiles offered by different and independent CAS and DRM security providers.

Hence, security providers may use black box OTP resources as the basis to derive security keys to enable different security schemes by altering the key generation inputs based on CAS and DRM vendor software and possibly vendor unique OTP inputs. The key generation inputs can be provided in the CAS and DRM application that could be loaded at CE device manufacturing or downloaded over the air for a fielded CE device.

Key derivation can be accomplished in a number of ways, for example, by taking the black box programmed secret OTP keys, CAS/DRM vendor (security provider) software input and possible CAS/DRM vendor unique OTP values and combining in a series of crypto graphic calculations using AES, DES or Triple DES. Where the black box programmed secret OTP keys are used as the key and the software input and CAS/DRM vendor unique OTP values are the data in the crypto graphic operation. .

By changing the key generation inputs used to compute S_1 and S_2 values, the SoC can derive unique key outputs for each CAS and DRM security provider used for a given content provider or broadcaster. CAS unique inputs such as their assigned conditional access identifier (CA ID) maybe used to differentiate derived keys for different conditional access systems CAS1 versus CAS2.

These security provider unique key generation outputs enable support for multiple security providers for fielded CE devices typically found in STBs 110,

televisions (TVs), Smart TVs and mobile devices such as smartphones. The black box security provider provides compatible headend applications to each content provider, so that the media programs are encrypted or otherwise protected using the CAS and DRM implementation used.

Another advantage of using a derived key database is that the black box programmed OTP key secrets programmed into the SoC OTP do not have to be divulged to the multiple CAS and DRM security providers, since these security providers would use the derived key databases for their content protection systems, not the OTP value. This means that if a derived key database were compromised, it only affects the specific CAS/DRM security provider that was using that specific derived key database, i.e. such compromise would not affect the fielded CE devices or derived key databases of any other such CAS/DRM security provider.

The keys and programming infrastructure provided by an independent black box security provider enables fielded CE devices to add additional revenue baring applications to the CE device manufacturer or content provider giving these entities more flexibility in managing their business and offering new services. Besides switching out a CAS/DRM vendor for any number of reasons, enabling the ability to add applications supporting new CAS/DRM vendors in fielded CE devices can result in generating significantly higher content sale revenues without requiring consumers to upgrade their CE devices. Consumer savings are realized by extending the field life of the CE device by allowing the consumer to download new software images to enable the purchase of new content services without having to replace their fielded CE devices.

Extending Fixed Secrets with Key Derivation

Key derivation techniques can be used to extend the fixed secret, S_1, shown in FIGs. 5A and 5B to decrypt either of the encrypted paring keys

$E_{S_1}[K_P]$, $E_{S_2}[K_P]$ to with secrets S_1 and S_2, respectively produce the pairing key K_p that is used to decrypt the ECW shown in FIG. 4C. The extension provides the ability to: (1) Use derived root keys to produce S_1 and alternately or in addition, using such root keys to produce S_2 and (2) Use this derivation process as a means of renewing key material for a fielded system.

For example, in a System-on-Chip architecture such as the architecture described in the above-referenced patent application U.S. Patent Application Serial No. 15/207,332, now published as U.S. Patent Publication No. 2017/0012952, hardware root of trust values can provide the basis for security providers such as the pairing broker 304 and/or one or more of the broadcasters 102 to derive a plurality of different security keys. Such keys can be used to add new security procedures or modify procedures already implemented. This can be accomplished, for example, by altering the key generation inputs based on security provider software (CAS or DRM) and possibly inputs vendor-unique hardware root of trust values. The key generation inputs can be provided in the CAS and DRM application software that could be loaded at into consumer electronics (CE) devices such as the transport module 2002 or CAM 206 when the devices are manufacture, or remotely downloaded over the air for a fielded CE device. This permits cryptographic separation of the CE devices at both S_1 and S_2.

Such hardware root of trust values can include one-time-programmable (OTP) values programmed into the transport module 202 and or CAM 206 using, for example, black box techniques also described in U.S. Patent Publication No. 2017/0012952. Such OTP values may be held secret from other entities as necessary. For example, the pairing broker 304 or third party security provider may provide a black box to the broadcaster 102 or manufacturer of the STB, permitting the storage of an OTP value without disclosing that value to the security provider or broadcaster.

Another advantage of using a derived key database is that the black box programmed OTP key secrets programmed into the SoC OTP may be held secret from (do not have to be released to) the CAS or DRM security provider, since these security providers would use the OTP key secrets to derive the keys required for their content protection system. This permits supporting multiple security provider vendors. Further, if a database of derived keys database were compromised, this compromise only affects the specific CAS / DRM security provider that was using that specific derived key database, and would not affect the fielded CE devices or derived key databases of any other such CAS/DRM security provider. This allows S_1 (and/or S_2) to be updated in the event of an attack that compromises the database of keys.

FIG. 7 is a diagram illustrating an exemplary embodiment of the transport module 202 and the CAM 206, wherein the transport module 202 includes a hardware root of trust value OTP1 702A and/or the CAM 206 has another hardware root of trust value OTP2 702B, thus permitting at least one of the first information S_1 and second information S_2 to be derived from a hardware root of trust secret stored in at least one of the transport module 202 and the CAM 206.

In the illustrated embodiment, the transport module 202 has a SoC with a processor that can perform processor instructions 704A. The processor has access to OTP 1 702 and can use deriving information such as the processor instructions 704A to derive or generate the first value S_1 via one or more operations 708A. Similarly, the CAM 206 comprises a SoC with a processor that can perform processor instructions 704B. The processor has access to OTP 1 702 and can use the processor instructions 704A to generate the first value S_1 via one or more operations 708B.

The transport module 202 may also store one or more further hardware root of trust values OTP1 706A1 and OTP2 706A2 that can also be used as

deriving information to generate the first value S_1. In one embodiment, OTP1 706A1 and OTP2 706A2 are security provider -unique, with each allocated to different security providers, allowing the transport module 202 to support CAS/DRM procedures of multiple security providers, allowing each such security provider to use their own OTP value 706A to generate first information S_1. However, security providers may be provided multiple OTP values as well.

Likewise, the CAM 206 may also store one or more further hardware root of trust values OTP1 706B1 and OTP2 706B2 that can also be used to generate the second value S_2. OTP1 706B1 and OTP2 706B2 may be allocated to the same security provider, or different security providers, allowing the CAM 206 to support CAS/DRM procedures of multiple security providers.

Hardware Environment

FIG. 8 illustrates an exemplary computer system 800 that could be used to implement the servers or the subscriber computer 512 of the present invention. The computer 802 comprises a processor 804 and a memory, such as random access memory (RAM) 806. The computer 802 is operatively coupled to a display 822, which presents images such as windows to the user on a graphical user interface 818B. The computer system 802 may be coupled to other devices, such as a keyboard 814, a mouse device 816, a printer, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the computer 802.

Generally, the computer 802 operates under control of an operating system 808 stored in the memory 806, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 818A. Although the GUI module 818A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 808, the computer program 810, or

implemented with special purpose memory and processors. The computer 802 also implements a compiler 812 which allows an application program 810 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 804 readable code. After completion, the application 810 accesses and manipulates data stored in the memory 806 of the computer 802 using the relationships and logic that was generated using the compiler 812. The computer 802 also optionally comprises an external communication device such as a modem, satellite link, Ethernet card, or other device for communicating with other computers.

In one embodiment, instructions implementing the operating system 108, the computer program 810, and the compiler 812 are tangibly embodied in a computer-readable medium, e.g., data storage device 820, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 824, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 808 and the computer program 810 are comprised of instructions which, when read and executed by the computer 802, causes the computer 802 to perform the steps necessary to implement and/or use the present invention. Computer program 810 and/or operating instructions may also be tangibly embodied in memory 806 and/or data communications devices 830, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture," "program storage device" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

Those skilled in the art will recognize many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the

above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

Conclusion

This concludes the description of the preferred embodiments of the present invention. The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

CLAIMS

What is Claimed is:

1. A method of brokering an enabling of communication of encrypted media programs from a plurality of broadcasters to a plurality of receivers, each encrypted media program decryptable by a first receiver module securely communicating with a second receiver module according to a pairing key associated with one of the plurality of receivers, comprising the steps of:

transmitting a first service enabling request from one of the plurality of broadcasters to a broker independent from the one of the plurality of broadcasters, the request comprising an identification of the one of the plurality of receivers;

receiving a first encrypted version of the pairing key $E_{S_1}[K_p]$ from the broker, the first encrypted version of the pairing key $E_{S_1}[K_p]$ decryptable by first information S_1 securely stored in the first receiver module of the one of the plurality of receivers;

encrypting the pairing key with second information S2 to generate a second encrypted version of the pairing key K_p, the second encrypted version of the pairing key $E_{S_2}[K_p]$ decryptable by the second information S_2 securely stored in the second receiver module; and

transmitting the first encrypted version of the pairing key $E_{S_1}[K_p]$ and the second encrypted version of the pairing key $E_{S_2}[K_p]$ to the one of the plurality of receivers;

wherein at least one of the first information S_1 and the second information S_2 is derived from a hardware root of trust stored in at least one of the first receiver module and the second receiver module.

2. The method of claim 1, wherein the hardware root of trust is a secret one-time programmably stored in at least one of the first receiver module and the second receiver module.

3. The method of claim 1, wherein:

the first information S_1 is derived from a first secret one time programmably stored in the first receiver module and first deriving information.

4. The method of claim 3, wherein:

the first deriving information comprises a plurality of instructions stored in the first receiver module.

5. The method of claim 4, wherein:

the first deriving information further comprises a key.

6. The method of claim 5, wherein:

the key is a security provider-unique one time programmable value known only to the security provider.

7. The method of claim 3, wherein the first deriving information is remotely downloaded to the first receiver module.

8. The method of claim 1, wherein at least one of the encrypted media programs is encrypted according to an encrypted control word $E[CW]$, and the method further comprising the steps of:

decrypting the first encrypted version of the pairing key $E_{S_1}[K_p]$ in the first receiver module;

decrypting the second encrypted version of the pairing key $E_{S_2}[K_p]$ in the second receiver module;

decrypting the encrypted control word $E[CW]$ in the second receiver module;

re-encrypting the decrypted control word CW according to the decrypted second encrypted version of the pairing key;

providing the re-encrypted control word $E_{K_p}[CW]$ from the second receiver module to the first receiver module; and

decrypting the re-encrypted control word $E_{K_p}[CW]$ using the decrypted first encrypted version of the pairing key K_p.

9. The method of claim 1, wherein the first service enabling request is for one service from the one of the plurality of broadcasters.

10. The method of claim 1, wherein the first service enabling request is for a plurality of services from the one of the plurality of broadcasters.

11. A system for brokering an enabling of communication of encrypted media programs from a plurality of independent broadcasters to a plurality of receivers, each encrypted media program decryptable by a first receiver module securely communicating with a second receiver module according to a pairing key K_p associated with one of the plurality of receivers, the system comprising:

a broker, for providing a first encrypted version of the pairing key $E_{S_1}[K_p]$ in response to a service enabling request from one of the plurality of broadcasters, the service enabling request having an identification of one of the plurality of receivers; and

wherein:

the first encrypted version of the pairing key $E_{S_1}[K_p]$ is decryptable by first information S_1 stored in the first receiver module; and

the first information S_1 is derived from a hardware root of trust stored in at least one of the first receiver module and the second receiver module.

12. The system of claim 11, wherein the hardware root of trust is a secret one-time programmably stored in at least one of the first receiver module and the second receiver module.

13. The system of claim 11, wherein:

the first information S_1 is derived from a first secret one time programmably stored in the first receiver module and first deriving information.

14. The system of claim 13, wherein:

the first deriving information comprises a plurality of instructions stored in the first receiver module.

15. The system of claim 14, wherein:

the first deriving information further comprises a key.

16. The system of claim 15, wherein:

the key is a security provider-unique one time programmable value known only to the security provider.

17. The system of claim 13, wherein the first deriving information is remotely downloaded to the first receiver module.

18. The system of claim 11, wherein the broker provides a first encrypted version of a different pairing key for each service requested from the one of the plurality of broadcasters to the one of the plurality of receivers.

19. The system of claim 11, wherein the broker provides a first encrypted version of a the same pairing key for every service requested from the one of the plurality of broadcasters to the one of the plurality of receivers.

20. The system of claim 11, wherein:

the first receiver module receives the first encrypted version $E_{S_1}[K_p]$ of the pairing key K_p and a second encrypted version of the pairing key $E_{S_2}[K_p]$ from the one of the plurality of broadcasters, the second encrypted version of the pairing key $E_{S_2}[K_p]$ being generated by the one of the plurality of broadcasters and decryptable by second information S_2 stored in the second receiver module.

21. An apparatus for brokering an enabling of communication of encrypted media programs from a plurality of independent broadcasters to a plurality of receivers, each encrypted media program decryptable by a first receiver module securely communicating with a second receiver module according to a pairing key associated with one of the plurality of receivers, the apparatus comprising:

means for transmitting a service enabling request from one of the plurality of broadcasters to a broker independent from the one of the plurality of broadcasters, the request comprising an identification of the one of the plurality of receivers;

means for receiving a first encrypted version of the pairing key $E_{S_1}[K_p]$ from the broker, the first encrypted version of the pairing key $E_{S_1}[K_p]$ decryptable by first information S_1 securely stored in the first receiver module of the one of the plurality of receivers;

means for encrypting the pairing key with second information S_2 to generate a second encrypted version of the pairing key K_p, the second encrypted version of the pairing key $E_{S_2}[K_p]$ decryptable by the second information S_2 securely stored in the second receiver module; and

means for transmitting the first encrypted version of the pairing key $E_{S_1}[K_p]$ and the second encrypted version of the pairing key $E_{S_2}[K_p]$ to the one of the plurality of receivers;

wherein at least one of the first information S_1 and the second information S_2 is derived from a hardware root of trust stored in at least one of the first receiver module and the second receiver module.

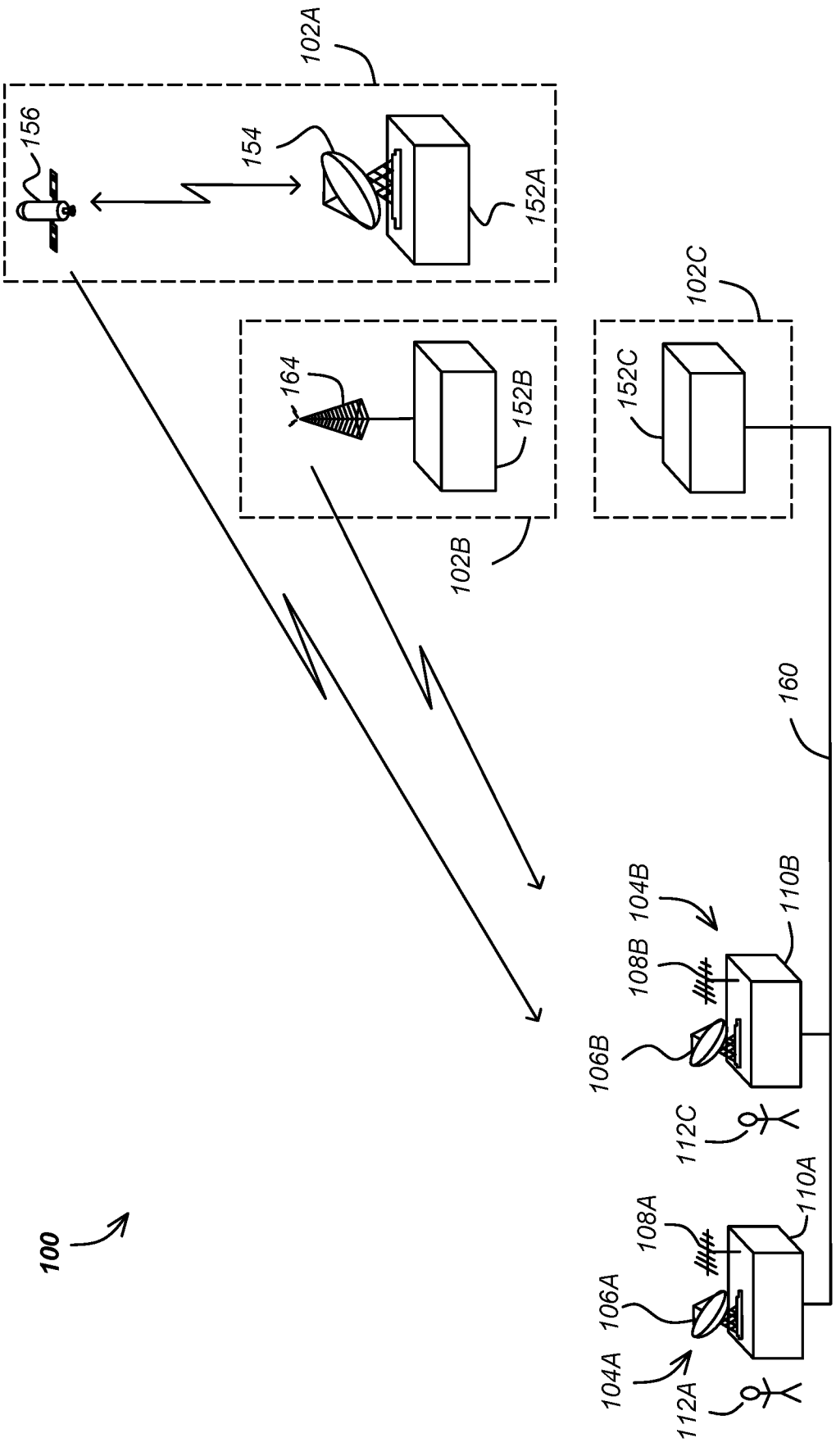
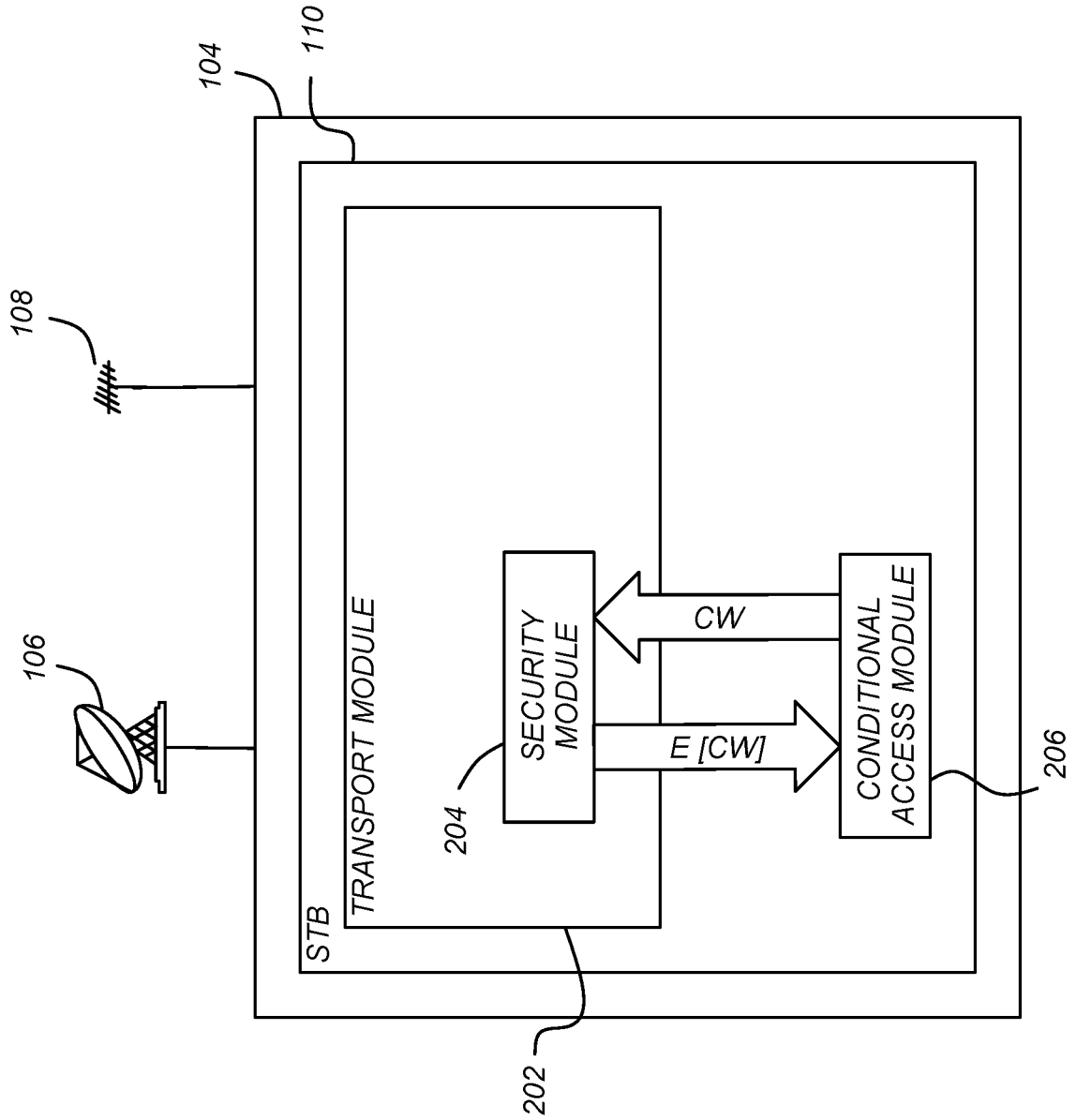

100
102A
156
154
152A
102B
164
152B
102C
152C
160
104B
108B
110B
106B
112C
110A
108A
106A
104A
112A

FIG. 1

FIG. 2


104
110
108
106
STB
TRANSPORT MODULE
SECURITY MODULE
204
CW
E [CW]
CONDITIONAL ACCESS MODULE
206
202

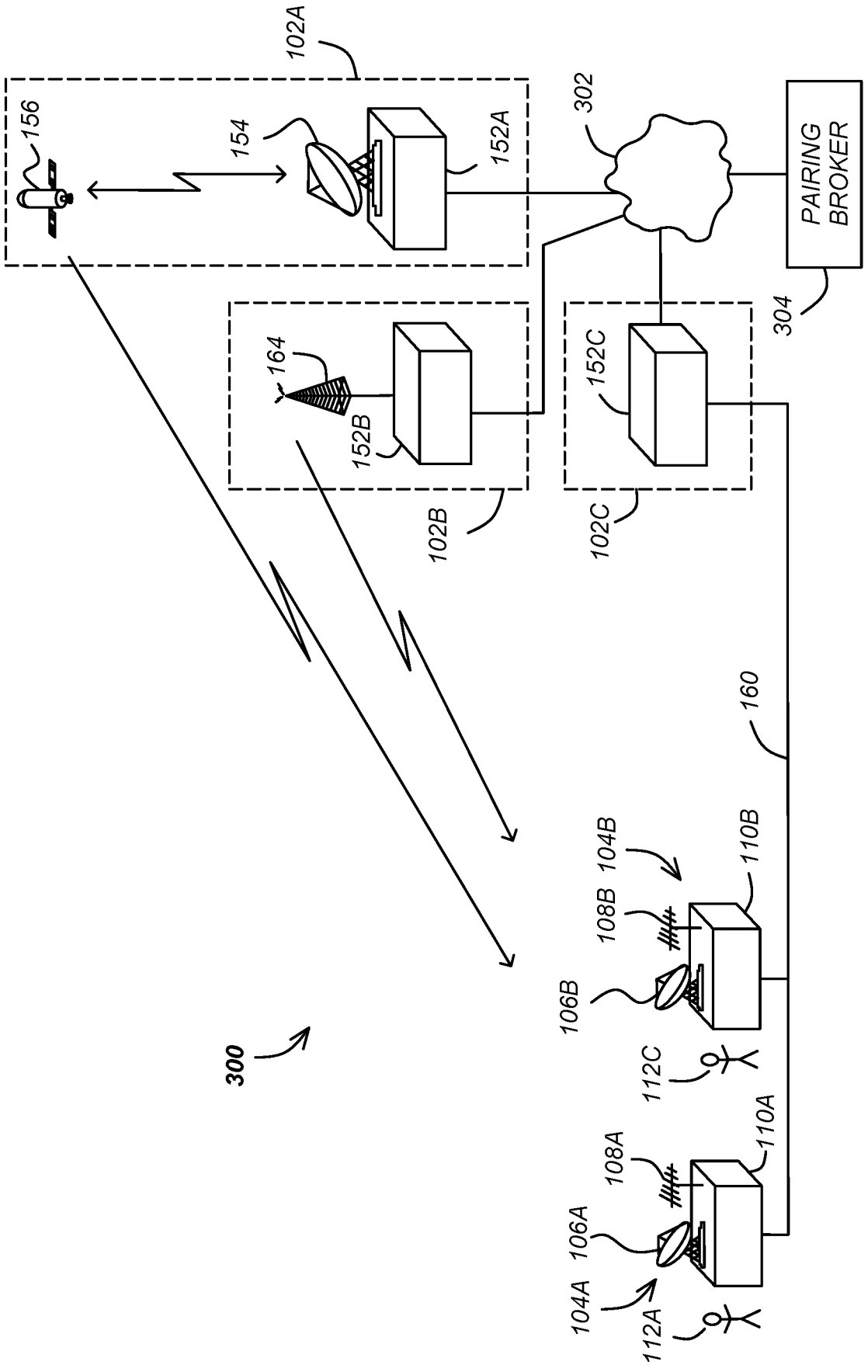

102A
156
154
152A
302
PAIRING BROKER
304
164
152B
152C
102B
102C
160
300
104B
110B
108B
106B
112C
110A
108A
106A
104A
112A

FIG. 3

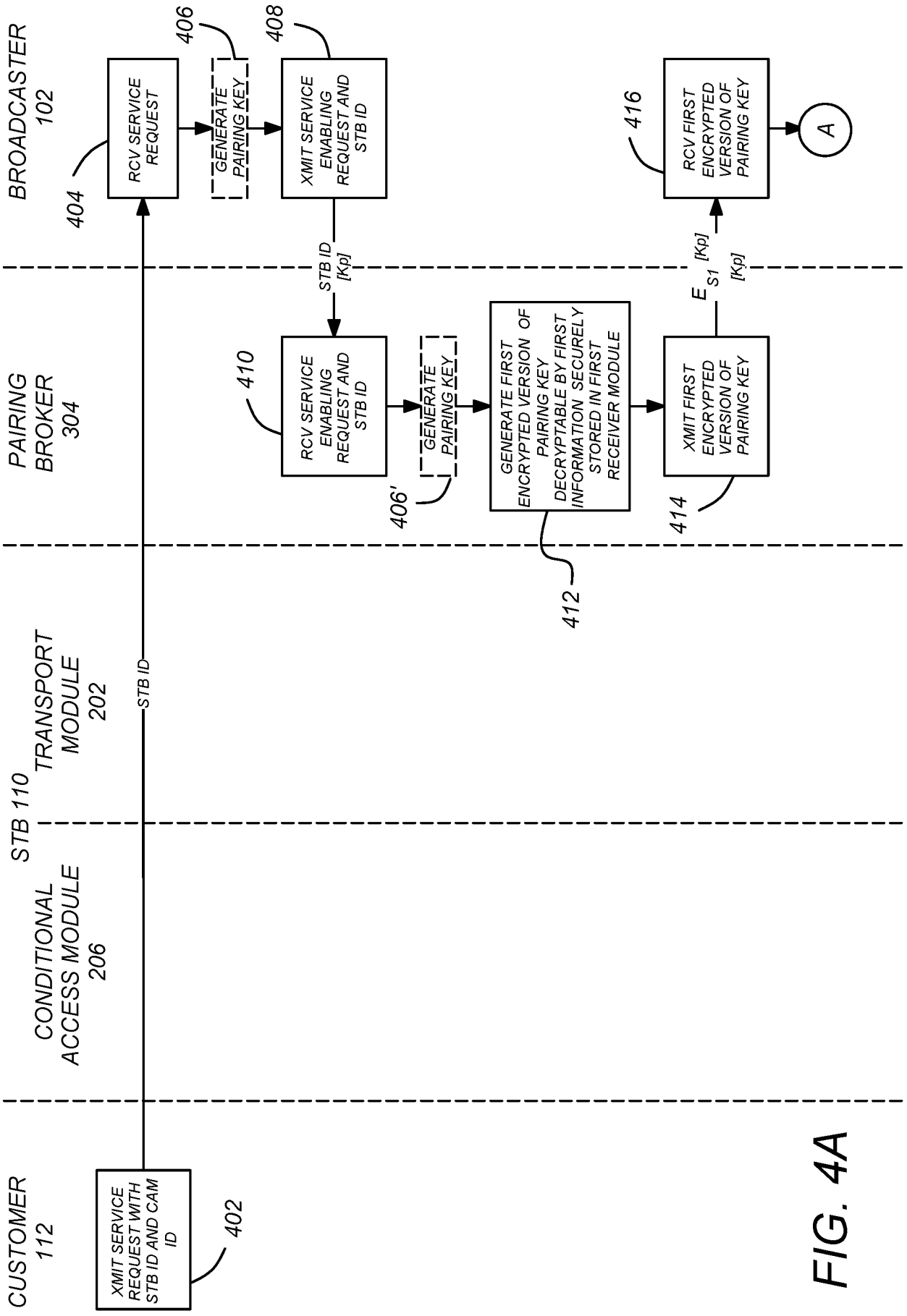

CUSTOMER 112
XMIT SERVICE REQUEST WITH STB ID AND CAM ID
402
STB 110
CONDITIONAL ACCESS MODULE 206
TRANSPORT MODULE 202
STB ID
PAIRING BROKER 304
BROADCASTER 102
404
RCV SERVICE REQUEST
406
GENERATE PAIRING KEY
408
XMIT SERVICE ENABLING REQUEST AND STB ID
STB ID [Kp]
410
RCV SERVICE ENABLING REQUEST AND STB ID
406'
GENERATE PAIRING KEY
412
GENERATE FIRST ENCRYPTED VERSION OF PAIRING KEY DECRYPTABLE BY FIRST INFORMATION SECURELY STORED IN FIRST RECEIVER MODULE
414
XMIT FIRST ENCRYPTED VERSION OF PAIRING KEY
E S1 [Kp]
[Kp]
416
RCV FIRST ENCRYPTED VERSION OF PAIRING KEY
A

FIG. 4A

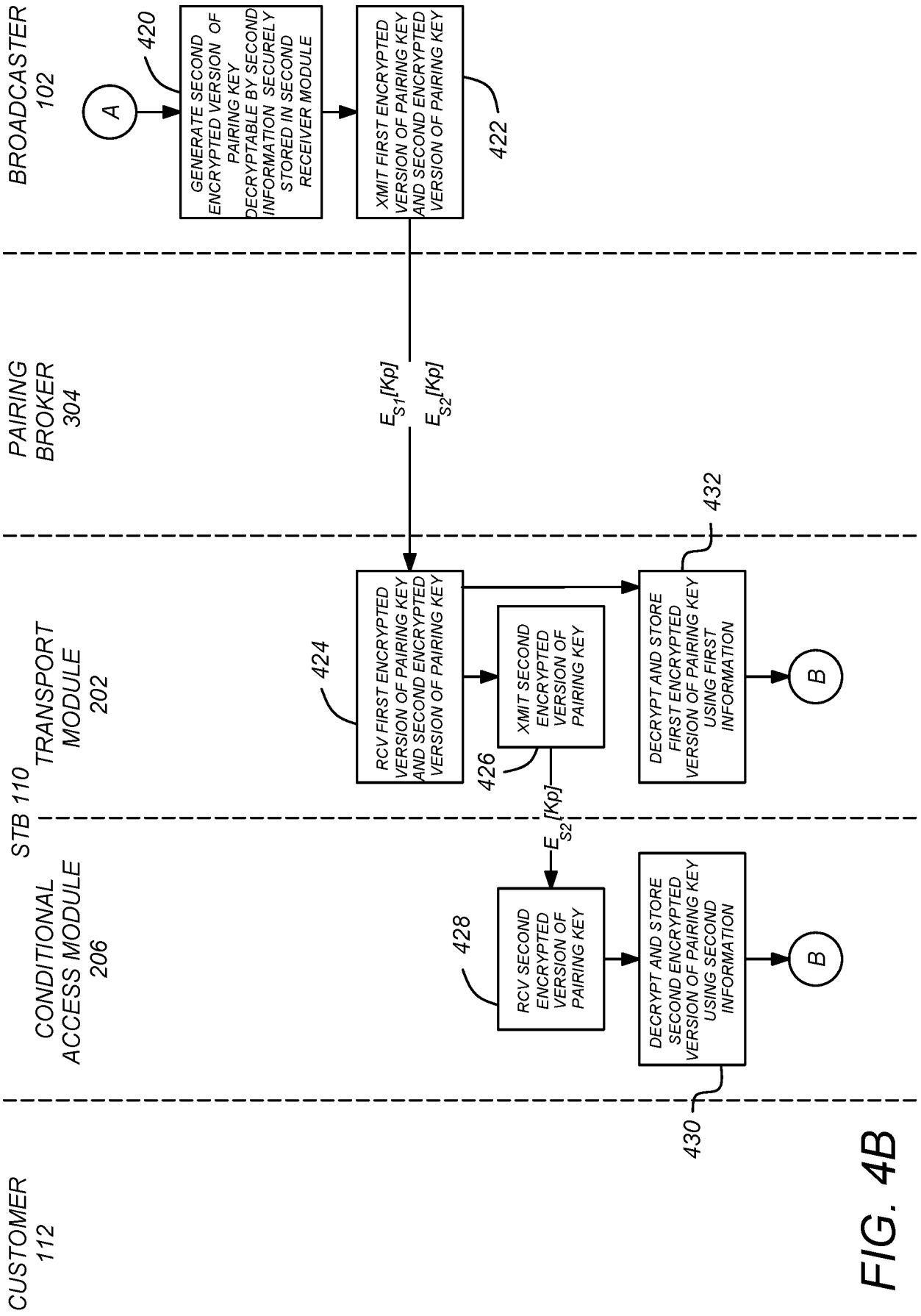

BROADCASTER 102
PAIRING BROKER 304
STB 110
TRANSPORT MODULE 202
CONDITIONAL ACCESS MODULE 206
CUSTOMER 112
A
420
GENERATE SECOND ENCRYPTED VERSION OF PAIRING KEY DECRYPTABLE BY SECOND INFORMATION SECURELY STORED IN SECOND RECEIVER MODULE
XMIT FIRST ENCRYPTED VERSION OF PAIRING KEY AND SECOND ENCRYPTED VERSION OF PAIRING KEY
422
$E_{S1}[Kp]$
$E_{S2}[Kp]$
424
RCV FIRST ENCRYPTED VERSION OF PAIRING KEY AND SECOND ENCRYPTED VERSION OF PAIRING KEY
XMIT SECOND ENCRYPTED VERSION OF PAIRING KEY
426
DECRYPT AND STORE FIRST ENCRYPTED VERSION OF PAIRING KEY USING FIRST INFORMATION
432
B
$E_{S2}[Kp]$
428
RCV SECOND ENCRYPTED VERSION OF PAIRING KEY
DECRYPT AND STORE SECOND ENCRYPTED VERSION OF PAIRING KEY USING SECOND INFORMATION
B
430

FIG. 4B

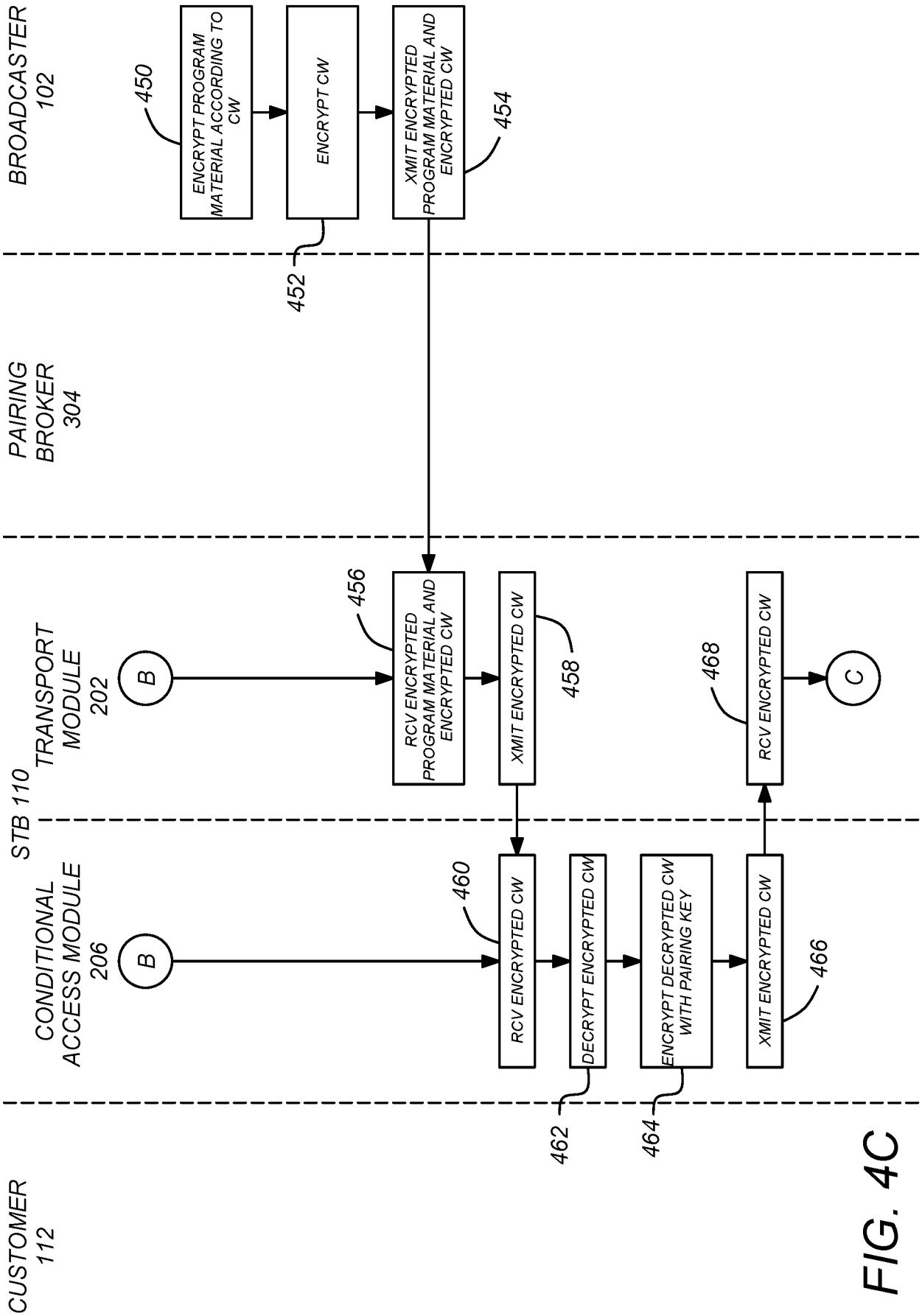

BROADCASTER 102
ENCRYPT PROGRAM MATERIAL ACCORDING TO CW
450
ENCRYPT CW
452
XMIT ENCRYPTED PROGRAM MATERIAL AND ENCRYPTED CW
454
PAIRING BROKER 304
STB 110
TRANSPORT MODULE 202
B
RCV ENCRYPTED PROGRAM MATERIAL AND ENCRYPTED CW
456
XMIT ENCRYPTED CW
458
RCV ENCRYPTED CW
468
C
CONDITIONAL ACCESS MODULE 206
B
RCV ENCRYPTED CW
460
DECRYPT ENCRYPTED CW
462
ENCRYPT DECRYPTED CW WITH PAIRING KEY
464
XMIT ENCRYPTED CW
466
CUSTOMER 112

FIG. 4C

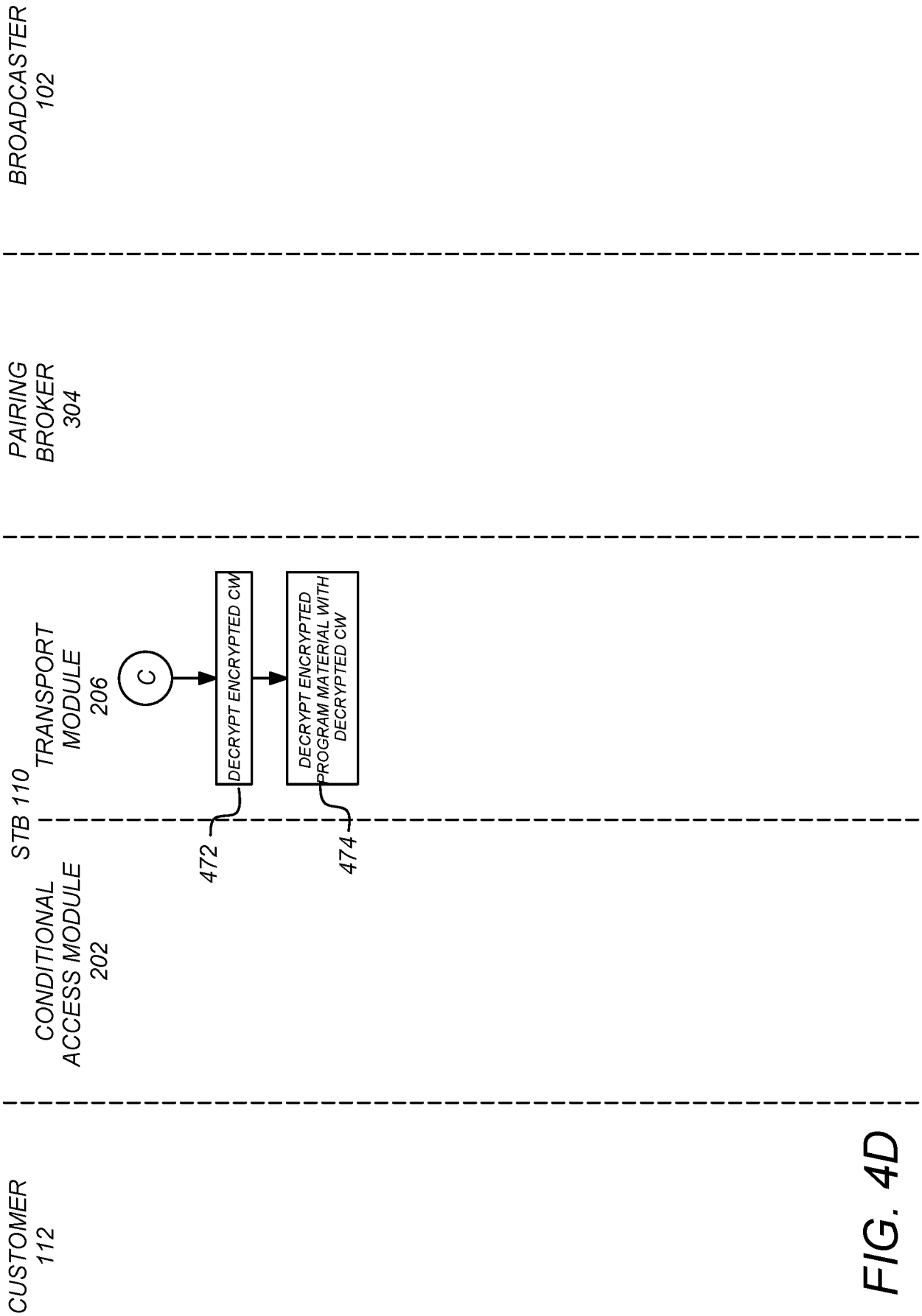

BROADCASTER
102
PAIRING
BROKER
304
STB 110
TRANSPORT
MODULE
206
C
DECRYPT ENCRYPTED CW
DECRYPT ENCRYPTED
PROGRAM MATERIAL WITH
DECRYPTED CW
CONDITIONAL
ACCESS MODULE
202
472
474
CUSTOMER
112

FIG. 4D

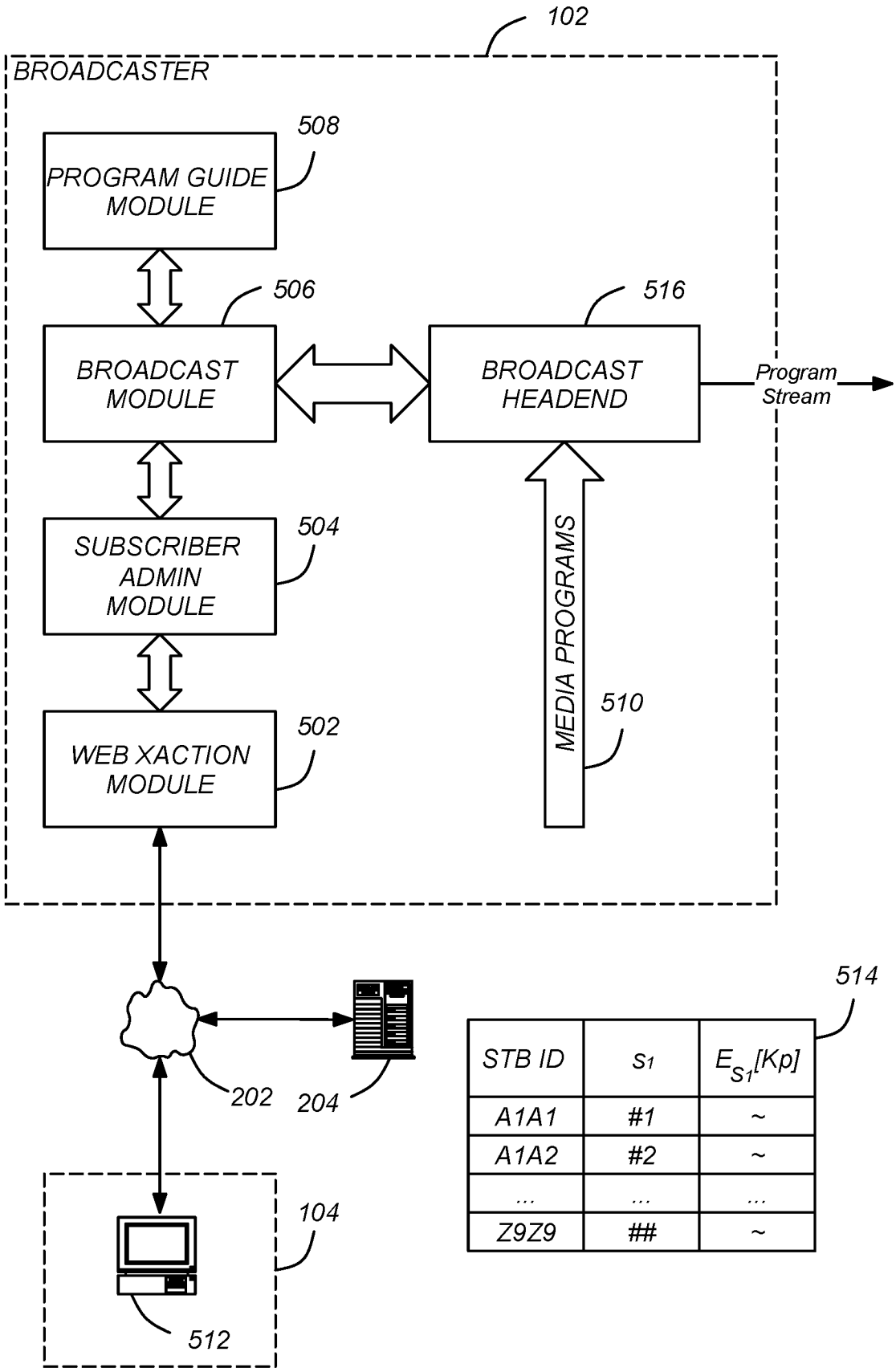

102
BROADCASTER
508
PROGRAM GUIDE MODULE
506
BROADCAST MODULE
516
BROADCAST HEADEND
Program Stream
504
SUBSCRIBER ADMIN MODULE
MEDIA PROGRAMS
510
502
WEB XACTION MODULE
202
204
104
512
514
STB ID
S1
$E_{S1}[Kp]$
A1A1
#1
~
A1A2
#2
~
...
...
...
Z9Z9
##
~

FIG. 5A

STB ID	S_1	BDCST ID	GEN SRVC	IPPV	OPPV A	OPPV B
A1A1	#1	A	Kp_{0001}	Kp_{0002}	Kp_{0003}	Kp_{0004}
A1A1	#1	B	Kp_{0201}	Kp_{0202}	Kp_{0203}	Kp_{0204}
A1A2	#2	A	Kp_{0301}	Kp_{0302}	Kp_{0303}	Kp_{0404}
A1A3	#3	B	Kp_{0401}	Kp_{0402}	Kp_{0403}	Kp_{0404}
A1A4	#4	A	Kp_{0501}	Kp_{0502}	Kp_{0503}	Kp_{0504}
...	...	...	...	...	...	...
Z9Z9	##	A	Kp	Kp	Kp	Kp

FIG. 5B

STB ID	BDCST ID = A	GEN SRVC	IPPV	OPPV A	OPPV B
A1A1	A	Kp_{0001}	Kp_{0002}	Kp_{0003}	Kp_{0004}
A1A2	A	Kp_{0301}	Kp_{0302}	Kp_{0303}	Kp_{0304}
Z1A1	A	Kp_{1301}	Kp_{1302}	Kp_{1303}	Kp_{1404}
A112	A	Kp_{1401}	Kp_{1402}	Kp_{1403}	Kp_{1404}
A1A5	A	Kp_{1501}	Kp_{1502}	Kp_{1503}	Kp_{1504}
...	...	...	...	...	...
Z9Z9	A	Kp	Kp	Kp	Kp

FIG. 5C

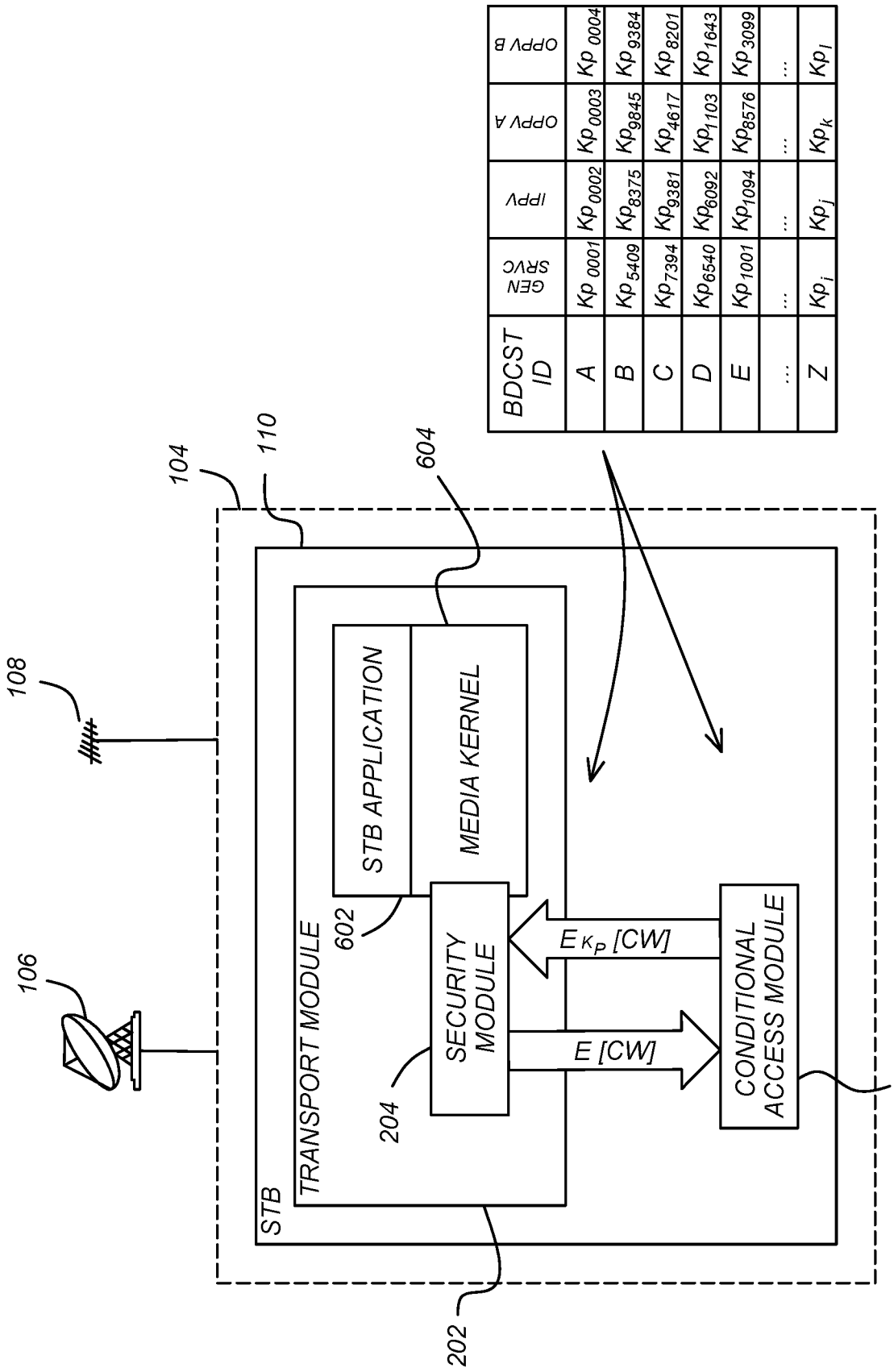

BDCST ID
GEN SRVC
IPPV
OPPV A
OPPV B
A
B
C
D
E
...
Z
Kp_{0001}
Kp_{5409}
Kp_{7394}
Kp_{6540}
Kp_{1001}
...
Kp_i
Kp_{0002}
Kp_{8375}
Kp_{9381}
Kp_{6092}
Kp_{1094}
...
Kp_j
Kp_{0003}
Kp_{9845}
Kp_{4617}
Kp_{1103}
Kp_{8576}
...
Kp_k
Kp_{0004}
Kp_{9384}
Kp_{8201}
Kp_{1643}
Kp_{3099}
...
Kp_l
104
110
604
108
106
STB APPLICATION
MEDIA KERNEL
602
TRANSPORT MODULE
SECURITY MODULE
204
E_{KP} [CW]
E [CW]
CONDITIONAL ACCESS MODULE
206
STB
202

FIG. 6

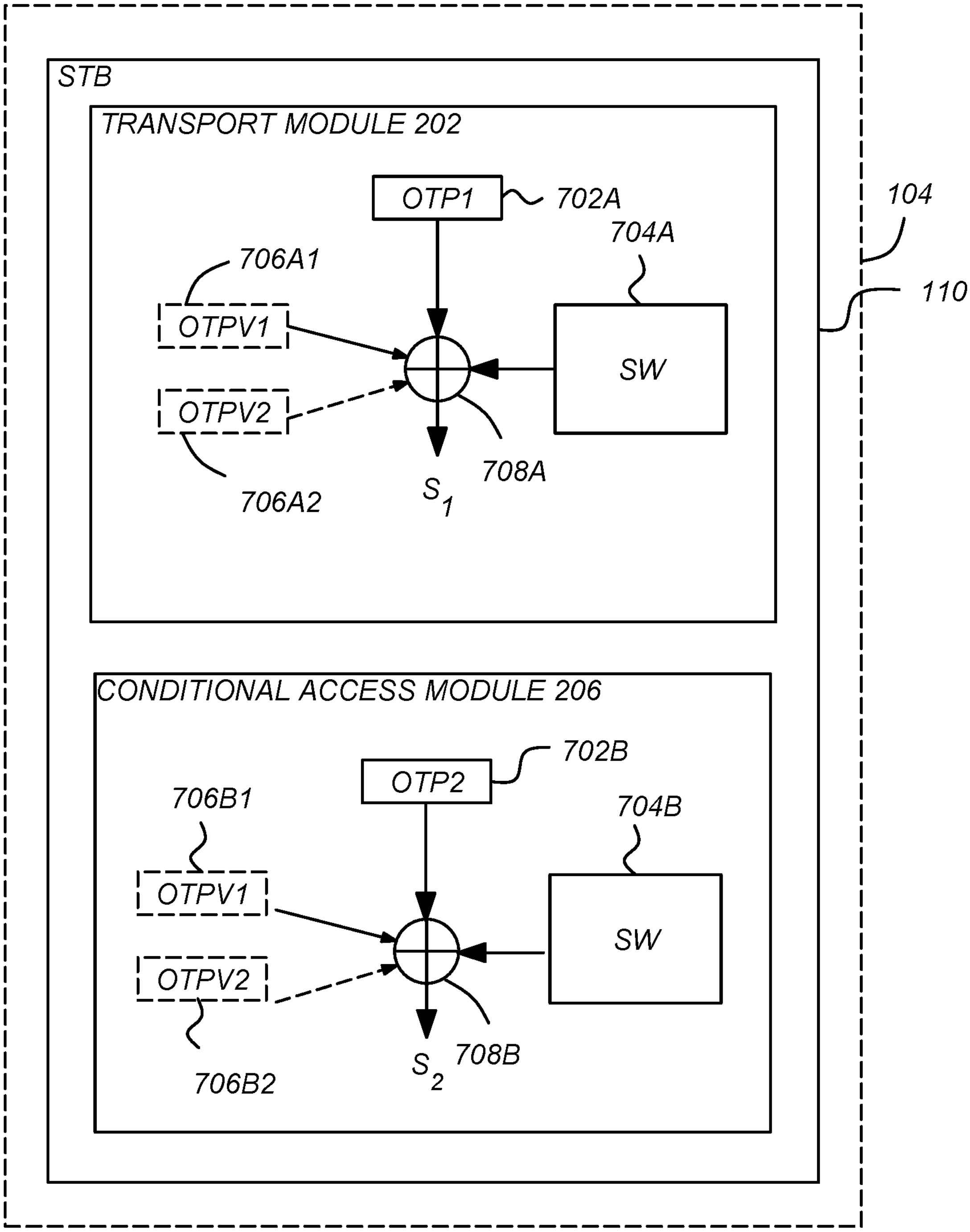

STB
TRANSPORT MODULE 202
OTP1
702A
104
704A
706A1
110
OTPV1
SW
OTPV2
708A
706A2
S1
CONDITIONAL ACCESS MODULE 206
702B
OTP2
706B1
704B
OTPV1
SW
OTPV2
S2
708B
706B2

FIG. 7

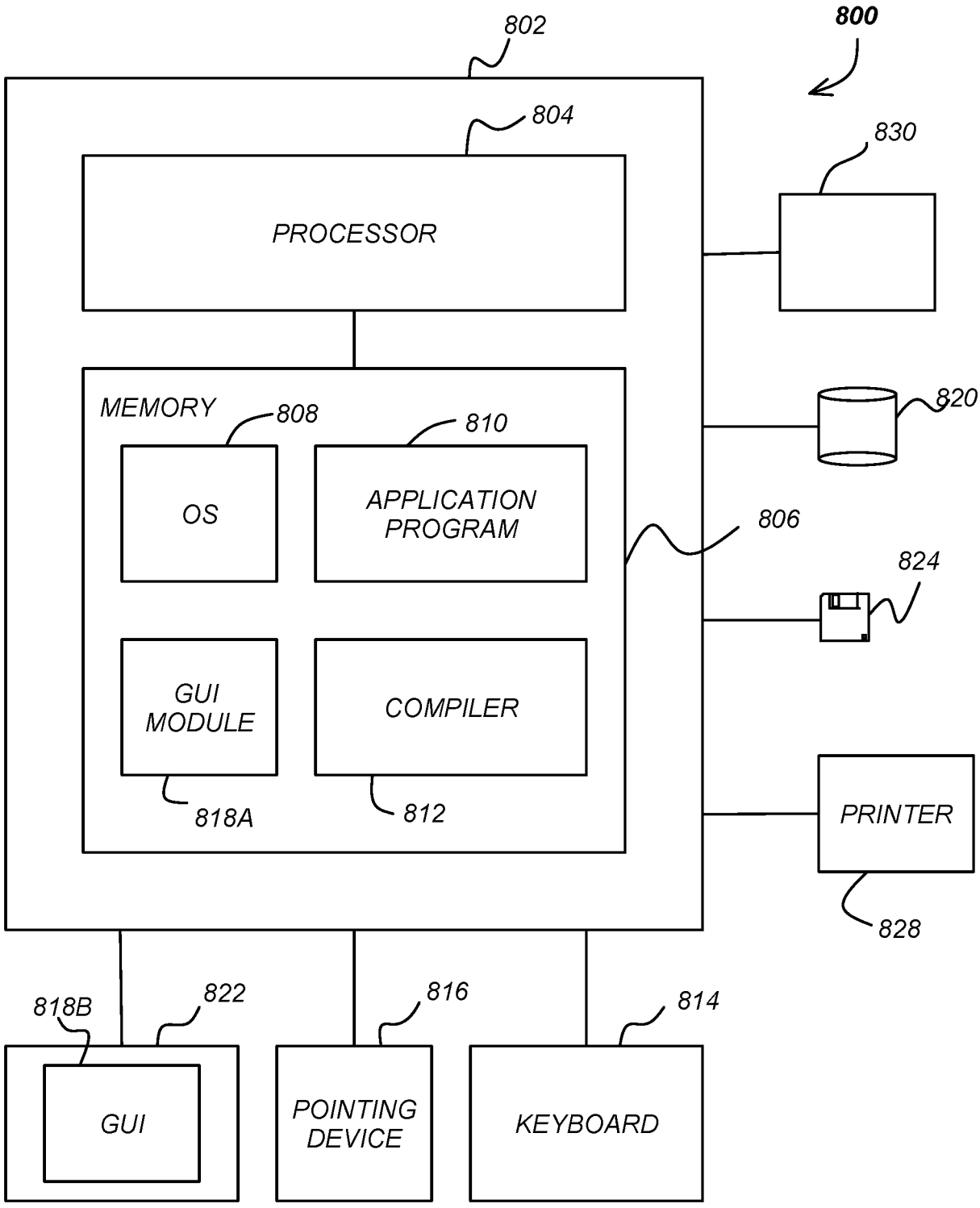

802
800
804
830
PROCESSOR
MEMORY
808
810
820
OS
APPLICATION PROGRAM
806
824
GUI MODULE
COMPILER
818A
812
PRINTER
828
818B
822
816
814
GUI
POINTING DEVICE
KEYBOARD

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/042542

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/10 G06F21/74
ADD.

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)
G06F

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/061477 A1 (KAHN RAYNOLD M [US] ET AL) 27 March 2003 (2003-03-27) abstract; figures 1,4-6 paragraph [0009] paragraph [0067] paragraph [0082] -----	1-21
A	US 2015/113278 A1 (COCCHI RONALD P [US] ET AL) 23 April 2015 (2015-04-23) abstract; figures 1A, 6 paragraph [0011] paragraph [0032] paragraph [0067] paragraph [0116] - paragraph [0142] ----- -/--	1-21

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
19 September 2018	26/09/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Harms, Christoph

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/042542

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017/012952 A1 (COCCHI RONALD P [US] ET AL) 12 January 2017 (2017-01-12) abstract; figures 1-10 paragraph [0012] - paragraph [0014] -----	1-21
A	US 5 940 504 A (GRISWOLD GARY N [US]) 17 August 1999 (1999-08-17) abstract; figures 1-8 column 3, line 30 - column 4, line 45 -----	1-21

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/042542

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003061477 A1	27-03-2003	EP 1444830 A2	11-08-2004
		JP 4267451 B2	27-05-2009
		JP 4740198 B2	03-08-2011
		JP 4861258 B2	25-01-2012
		JP 2005505989 A	24-02-2005
		JP 2007318776 A	06-12-2007
		JP 2007329939 A	20-12-2007
		US 2003061477 A1	27-03-2003
		US 2008279386 A1	13-11-2008
		WO 03032553 A2	17-04-2003
US 2015113278 A1	23-04-2015	EP 2820546 A1	07-01-2015
		US 2015113278 A1	23-04-2015
		WO 2013131065 A1	06-09-2013
US 2017012952 A1	12-01-2017	NONE	
US 5940504 A	17-08-1999	AU 2305292 A	11-02-1993
		US 5940504 A	17-08-1999
		WO 9301550 A1	21-01-1993