



(22) Date de dépôt/Filing Date: 2002/10/01

(41) Mise à la disp. pub./Open to Public Insp.: 2003/04/26

(30) Priorités/Priorities: 2001/10/26 (60/343,710) US;
2002/01/02 (10/038,217) US

(51) Cl.Int.⁷/Int.Cl.⁷ H04N 7/16, H04N 7/20

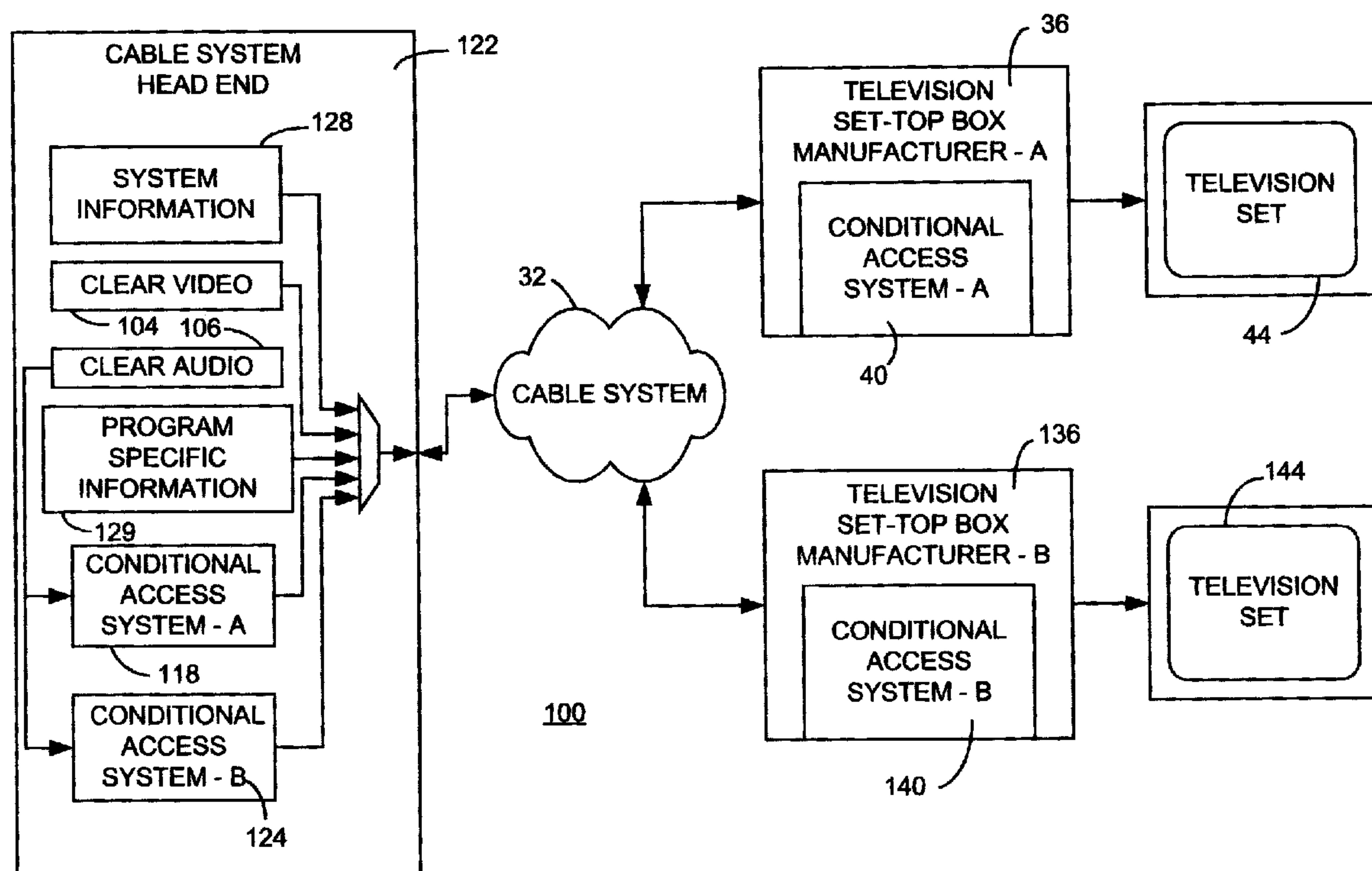
(71) Demandeur/Applicant:
SONY ELECTRONICS INC., US

(72) Inventeurs/Inventors:
CANDELORE, BRANT L., US;
UNGER, ROBERT ALLAN, US

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : SYSTEME DE CHIFFREMENT PARTIEL VISANT LES PAQUETS CRITIQUES

(54) Title: CRITICAL PACKET PARTIAL ENCRYPTION



(57) Abrégé/Abstract:

An encryption arrangement for multiple encryption of television programs. A system according to embodiments of the present invention multiple encrypts only a portion of the data required for full presentation of a television program to permit coexistence of multiple conditional access encryption systems associated with multiple manufacturer's set-top boxes within a single system. In one embodiment, only critical packets such as those carrying a payload incorporating packetized elementary stream header information is encrypted. By only encrypting a portion of the program, dramatically less bandwidth is consumed than the alternative of multiple encryption of all program data, thus permitting a larger number of programs to be carried over the same bandwidth while permitting coexistence of multiple conditional access systems in a single cable television system.

ABSTRACT OF THE DISCLOSURE

An encryption arrangement for multiple encryption of television programs. A system according to embodiments of the present invention multiple encrypts only a portion of the data required for full presentation of a television program to permit coexistence of multiple conditional access encryption systems associated with multiple manufacturer's set-top boxes within a single system. In one embodiment, only critical packets such as those carrying a payload incorporating packetized elementary stream header information is encrypted. By only encrypting a portion of the program, dramatically less bandwidth is consumed than the alternative of multiple encryption of all program data, thus permitting a larger number of programs to be carried over the same bandwidth while permitting coexistence of multiple conditional access systems in a single cable television system.

CRITICAL PACKET PARTIAL ENCRYPTION

CROSS REFERENCE TO RELATED DOCUMENTS

This application is related to U.S. provisional patent application serial number 60/296,673 filed June 6, 2001 to Candelore, et al. entitled "Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Sending Video in the Clear for Some Content, and Dual Carriage of Audio and Dual Carriage of Video and Audio for Other Content", and provisional patent application serial number 60/304,241 filed July 10, 2001 to Unger et al., entitled "Independent Selective Encryptions of Program Content for Dual Carriage", and provisional patent application serial number 60/304,131 filed July 10, 2001 to Candelore et al., entitled "Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Partial Scrambling Content on a Time Slice Basis" and to U.S. provisional patent application serial no. 60/_____, filed on October 26, 2001 to Candelore et al., entitled "Television Encryption Systems", docket number SNY-R4646P, which are hereby incorporated herein by reference.

This application is being filed simultaneously with patent applications docket number SNY-R4646.02 entitled "Time Division Partial Encryption" to Candelore et al., serial number _____; docket number SNY-R4646.03 entitled "Elementary Stream Partial Encryption" to Candelore, serial number _____; docket number SNY-R4646.04 entitled "Partial Encryption and PID Mapping" to Unger et al., serial number _____; and docket number SNY-R4646.05 entitled "Decoding and Decrypting of Partially Encrypted

1 Information" to Unger et al., serial number _____. These simultaneously
2 filed patent applications are hereby incorporated by reference herein.

4 **COPYRIGHT NOTICE**

5 A portion of the disclosure of this patent document contains material which
6 is subject to copyright protection. The copyright owner has no objection to the
7 facsimile reproduction of the patent document or the patent disclosure, as it
8 appears in the Patent and Trademark Office patent file or records, but otherwise
9 reserves all copyright rights whatsoever.

11 **FIELD OF THE INVENTION**

12 This invention relates generally to the field of encryption systems. More
13 particularly, this invention relates to systems, methods and apparatus for providing
14 partial encryption and decryption of digital of television signals.

16 **BACKGROUND OF THE INVENTION**

17 Television is used to deliver entertainment and education to viewers. The
18 source material (audio, video, etc.) is multiplexed into a combined signal which is
19 then used to modulate a carrier. This carrier is commonly known as a channel. (A
20 typical channel can carry one analog program, one or two high definition (HD)
21 digital program(s), or several (e.g. nine) standard definition digital programs.) In a
22 terrestrial system, these channels correspond to government assigned frequencies
23 and are distributed over the air. The program is delivered to a receiver that has a
24 tuner that pulls the signal from the air and delivers it to a demodulator, which in turn
25 provides video to a display and audio to speakers. In a cable system the
26 modulated channels are carried over a cable. There may also be an in-band or out-
27 of-band feed of a program guide indicating what programs are available and the
28 associated tuning information. The number of cable channels is finite and limited

1 by equipment/cable bandwidth. Cable distribution systems require a significant
2 capital investment and are expensive to upgrade.

3 Much of television content is valuable to its producers, therefore copyright
4 holders want to control access and restrict copies. Examples of typically protected
5 material include feature films, sporting events, and adult programming. Conditional
6 access (CA) systems are used to control availability of programming in content
7 delivery systems such as cable systems. CA systems come as matched sets –
8 one part is integrated into the cable system headend and encrypts premium
9 content, the other part provides decryption and is built into the set-top boxes (STB)
10 installed in user's homes. Several CA systems are used in the cable industry
11 including those provided by NDS (Newport Beach, CA), Motorola (Schaumburg, IL)
12 and Scientific Atlanta (Atlanta, GA). This matched set aspect of CA systems has
13 the effect that the "legacy" vendor is locked in as the supplier of additional STBs.
14 Since the various technologies for conditional access are not mutually compatible
15 (and are often proprietary), any new potential supplier is forced to license the
16 legacy CA. Thus, the cable operator finds itself unable to acquire newer technology
17 or competing technology from other set-top box manufacturers since the technology
18 owners are often unwilling to cooperate, or charge reasonable license fees. This
19 inflexibility can be especially troublesome when cable companies with disparate
20 CA systems are merged. Service providers would like more than one source for
21 STBs for any number of reasons.

22 Once a cable operator picks an encryption scheme, it is difficult to change
23 or upgrade the content encryption scheme without introducing a backward
24 compatible decoding device (e.g. set-top box). Providing multiple mode capability
25 in new set-top boxes to handle multiple encryption systems can add substantial
26 cost to any new set-top box, providing that the technology can be made available
27 to the STB vendor to provide the multiple decryption capability.

28 The only known current option to avoiding domination by the legacy vendor
29 (short of wholesale replacement) is using "full dual carriage". Full dual carriage
30 means that transmission is duplicated for each encrypted program – once for each

1 type of CA encryption to be used. To provide full dual carriage, the headend is
2 enhanced to provide each form of CA simultaneously. Legacy STBs should not be
3 impacted and should continue to perform their function despite any change.
4 However, full dual carriage often comes at an unpalatable price because of the
5 bandwidth impact, thus reducing the number of unique programs available.
6 Generally, the number of premium channels suffers so that the number of options
7 available to the viewer are limited and the value that can be provided by the cable
8 operator is restricted.

9 A conventional cable system arrangement is depicted in **FIGURE 1**. In such
10 a system, the cable operator processes audio/video (A/V) content 14 with CA
11 technology from manufacturer A (system A) using CA encryption equipment 18
12 compliant with system A at the cable system -headend 22. The encrypted A/V
13 content along with system information (SI) 26 and program specific information
14 (PSI) 27 is multiplexed together and transmitted over the cable system 32 to a
15 user's STB 36. STB 36 incorporates decrypting CA equipment from system A
16 (manufacturer A) 40 that decrypts the A/V content. The decrypted A/V content can
17 then be supplied to a television set 44 for viewing by the user.

18 In a cable system such as that of **FIGURE 1**, digital program streams are
19 broken into packets for transmission. Packets for each component of a program
20 (video, audio, auxiliary data, etc.) are tagged with a packet identifier or PID. These
21 packet streams for each component of all programs carried within a channel are
22 aggregated into one composite stream. Additional packets are also included to
23 provide decryption keys and other overhead information. Otherwise unused
24 bandwidth is filled with null packets. Bandwidth budgets are usually adjusted to
25 utilize about 95% of the available channel bandwidth.

26 Overhead information usually includes guide data describing what programs
27 are available and how to locate the associated channels and components. This
28 guide data is also known as system information or SI. SI may be delivered to the
29 STB in-band (part of the data encoded within a channel) or out-of-band (using a

1 special channel dedicated to the purpose). Electronically delivered SI may be
2 partially duplicated in more traditional forms - grids published in newspapers and
3 magazines.

4 In order for a viewer to have a satisfying television experience, it is generally
5 desirable that the viewer have clear access to both audio and video content. Some
6 analog cable systems have used various filtering techniques to obscure the video
7 to prevent an unauthorized viewer from receiving programming that has not been
8 paid for. In such a system, the analog audio is sometimes sent in the clear. In the
9 Motorola VideoCipher 2 Plus system used in C-band satellite transmissions, strong
10 digital audio encryption is used in conjunction with a relatively weak protection of
11 the analog video (using sync inversion). In airline in-flight movie systems, the
12 availability of audio only through rental of headphones has been used to provide the
13 full audio and video only to paying customers.

14 15 **BRIEF DESCRIPTION OF THE DRAWINGS**

16 The features of the invention believed to be novel are set forth with
17 particularity in the appended claims. The invention itself however, both as to
18 organization and method of operation, together with objects and advantages
19 thereof, may be best understood by reference to the following detailed description
20 of the invention, which describes certain exemplary embodiments of the invention,
21 taken in conjunction with the accompanying drawings in which:

22 **FIGURE 1** is a block diagram of a conventional conditional access cable
23 system.

24 **FIGURE 2** is a block diagram of a system consistent with one embodiment
25 of the present invention in which dual encrypted audio is transmitted along with
26 clear video.

27 **FIGURE 3** is a block diagram of a system consistent with an embodiment
28 of the present invention in which portions of programming are dual encrypted
29 according to a time slice mechanism.

1 **FIGURE 4** is a flow chart of a dual encryption process consistent with certain
2 embodiments of the present invention.

3 **FIGURE 5** is a flow chart of a decryption process consistent with certain
4 embodiments of the present invention.

5 **FIGURE 6** is a block diagram of a system consistent with an embodiment
6 of the present invention in which portions of programming are dual encrypted on a
7 packet basis.

8 **FIGURE 7** is a flow chart of a dual encryption process consistent with certain
9 embodiments of the present invention.

10 **FIGURE 8** is a flow chart of a decryption process consistent with certain
11 embodiments of the present invention.

12 **FIGURE 9** is a block diagram of a system consistent with an embodiment
13 of the present invention in which system information is encrypted and programming
14 is sent in the clear.

15 **FIGURE 10** is a block diagram of a generic system consistent with various
16 embodiments of the present invention.

17 **FIGURE 11** is a block diagram of a first embodiment of implementation of
18 an encryption system consistent with embodiments of the present invention in a
19 cable system headend.

20 **FIGURE 12** is a block diagram of a second embodiment of implementation
21 of an encryption system consistent with embodiments of the present invention in
22 a cable system headend.

23 **FIGURE 13** is a flow chart of an overall encryption process used to
24 implement certain embodiments of the present invention in a cable system
25 headend.

26 **FIGURE 14** is a block diagram of a first embodiment of a set-top box
27 implementation of a decoding system consistent with embodiments of the
28 present invention.

29 **FIGURE 15** is a block diagram of a second embodiment of

1 implementation of a decoding system consistent with embodiments of the
2 present invention in a cable system STB.

3 **FIGURE 16** is a block diagram of a third embodiment of implementation
4 of a decoding system consistent with embodiments of the present invention in a
5 cable system STB.

6 **FIGURE 17** illustrates the PID remapping process carried out in one
7 embodiment of a set-top box PID re-mapper.

8 **FIGURE 18** is a block diagram of an exemplary decoder chip that can be
9 utilized in a television set-top box consistent with the present invention.

11 **DETAILED DESCRIPTION OF THE INVENTION**

12 While this invention is susceptible of embodiment in many different forms,
13 there is shown in the drawings and will herein be described in detail specific
14 embodiments, with the understanding that the present disclosure is to be
15 considered as an example of the principles of the invention and not intended to limit
16 the invention to the specific embodiments shown and described. In the description
17 below, like reference numerals are used to describe the same, similar or
18 corresponding parts in the several views of the drawings. The terms "scramble"
19 and "encrypt" and variations thereof are used synonymously herein. Also, the term
20 "television program" and similar terms can be interpreted in the normal
21 conversational sense, as well as a meaning wherein the term means any segment
22 of AV content that can be displayed on a television set or similar monitor device.

24 **OVERVIEW**

25 Modern digital cable networks generally use CA systems that fully encrypt
26 digital audio and video to make programming inaccessible except to those who
27 have properly subscribed. Such encryption is designed to thwart hackers and non-
28 subscribers from receiving programming that has not been paid for. However, as
29 cable operators wish to provide their subscribers with set-top boxes from any of

1 several manufacturers, they are frustrated by the need to transmit multiple copies
2 of a single program encrypted with multiple encryption technologies compliant with
3 the CA systems of each STB manufacturer.

4 This need to carry multiple copies of the programming (called "full dual
5 carriage") uses up valuable bandwidth that could be used to provide the viewer with
6 additional programming content. Certain embodiments of the present invention
7 address this problem in which the bandwidth requirements to provide an equivalent
8 to multiple carriage are minimized. The result could be described as "Virtual Dual
9 Carriage" since the benefits of full dual carriage are provided without the full
10 bandwidth cost. Several embodiments of the present invention are presented
11 herein to accomplish effective partial scrambling. These embodiments vary by the
12 criteria used to select the portion to encrypt. The portion selected in turn affects the
13 additional bandwidth requirements and the effectiveness of the encryption. It may
14 be desirable to use one encryption process or several processes in combination in
15 a manner consistent with embodiments of the present invention.

16 Certain of the implementations of partial dual encryption described herein
17 utilize an additional (secondary) PID for each duplicated component. These
18 secondary PIDs are used to tag packets that carry duplicated content with an
19 additional encryption method. The PSI is enhanced to convey information about
20 the existence these new PIDs in such a way that inserted PIDs are ignored by
21 legacy STBs but can be easily extracted by new STBs.

22 Some implementations of partial dual encryption involve duplicating only
23 certain packets tagged with a given PID. Methods for selecting which packets to
24 encrypt are detailed hereinafter. The original (i.e. legacy) PID continues to tag the
25 packets encrypted with legacy encryption as well as other packets sent in the clear.
26 The new PID is used to tag packets encrypted by the second encryption method.
27 Packets with the secondary PID shadow the encrypted packets tagged with the
28 primary PID. The packets making up the encrypted pairs can occur in either order
29 but, in the preferred implementation, maintain sequence with the clear portion of
30 the PID stream. By use of the primary and secondary PIDs, the decoder located

1 in the set-top box can readily determine which packets are to be decrypted using
2 the decryption method associated with that set-top box, as will be clear upon
3 consideration of the following description. The processes used to manipulate PIDs
4 will be described later in greater detail.

5 The encryption techniques described herein can be broadly categorized
6 (according to one categorization) into three basic variations - encrypting just a
7 major portion (i.e. audio), encrypting just the SI, and encrypting just selected
8 packets. In general, each of the encryption techniques used in the embodiments
9 disclosed herein seek to encrypt portions of the an A/V signal or associated
10 information while leaving other portions of the A/V signal in the clear to conserve
11 bandwidth. Bandwidth can be conserved because the same clear portion can be
12 sent to all varieties of set-top boxes. Various methods are used to select the
13 portions of information to be encrypted. By so doing, the various embodiments of
14 this invention eliminate the traditional "brute-force" technique of encrypting the
15 entire content in one specific scrambling scheme, which predicates the redundant
16 use of bandwidth if alternate scrambling schemes are desired. In addition, each
17 of the partial dual encryption schemes described herein can be used as a single
18 partial encryption scheme without departing from embodiments of the present
19 invention.

20 The various embodiments of the invention use several processes, alone or
21 in combination, to send substantial portions of content in the clear while encrypting
22 only a small amount of information required to correctly reproduce the content.
23 Therefore the amount of information transmitted that is uniquely encrypted in a
24 particular scrambling scheme is a small percentage of the content, as opposed to
25 the entire replication of each desired program stream. For purposes of the
26 exemplary systems in this document, encryption system A will be considered the
27 legacy system throughout. Each of the several encryption techniques described
28 above will now be described in detail.

29 The various embodiments of the invention allow each participating CA
30 system to be operated independently. Each is orthogonal to the other. Key sharing

1 in the headend is not required since each system encrypts its own patents.
2 Different key epochs may be used by each CA system. For example, packets
3 encrypted with Motorola's proprietary encryption can use fast changing encryption
4 keys using the embedded security ASIC, while packets encrypted with NDS' smart
5 card based system use slightly slower changing keys. This embodiment works
6 equally well for Scientific Atlanta and Motorola legacy encryption.

7 8 ENCRYPTED ELEMENTARY STREAM

9 Turning now to **FIGURE 2**, one embodiment of a system that reduces the
10 need for additional bandwidth to provide multiple carriage is illustrated as system
11 100. In this embodiment, the system takes advantage of the fact that viewing
12 television programming without audio is usually undesirable. While there are
13 exceptions (e.g., adult programming, some sporting events, etc.), the typical viewer
14 is unlikely to accept routine viewing of television programming without being able
15 to hear the audio. Thus, at headend 122, the video signal 104 is provided in the
16 clear (unencrypted) while the clear audio 106 is provided to multiple CA systems
17 for broadcast over the cable network. In the exemplary system 100, clear audio
18 106 is provided to an encryption system 118 that encrypts audio data using
19 encryption system A (encryption system A will be considered the legacy system
20 throughout this document). Simultaneously, clear audio 106 is provided to
21 encryption system 124 that encrypts the audio data using encryption system B.
22 Clear video is then multiplexed along with encrypted audio from 118 (Audio A) and
23 encrypted audio from 124 (Audio B), system information 128 and program specific
24 information 129.

25 After distribution through the cable system 32, the video, system information,
26 program specific information, Audio A and Audio B are all delivered to set-top
27 boxes 36 and 136. At legacy STB 36, the video is displayed and the encrypted
28 audio is decrypted at CA system A 40 for play on television set 44. Similarly, at
29 new STB 136, the video is displayed and the encrypted audio is decrypted at CA
30 system B 140 for play on television set 144.

1 Audio has a relatively low bandwidth requirement compared with a complete
2 A/V program (or even just the video portion). The current maximum bit rate for
3 stereophonic audio at 384 Kb/second is approximately 10% of a 3.8Mb/second
4 television program. Thus, for dual carriage of only encrypted audio (with video
5 transmitted in the clear) in a system with ten channels carried with 256 QAM
6 (quadrature amplitude modulation), a loss of only about one channel worth of
7 bandwidth would occur. Therefore, approximately nine channels could be carried.
8 This is a dramatic improvement over the need to dual encrypt all channels, which
9 would result in a decrease in available channels from ten to five. Where deemed
10 necessary, e.g., sporting events, pay per view, adult programming, etc., dual
11 encryption of both audio and video can still be carried out, if desired.

12 Both legacy and new set-top boxes can function in a normal manner
13 receiving video in the clear and decrypting the audio in the same manner used for
14 fully decrypting encrypted A/V content. If the user has not subscribed to the
15 programming encrypted according to the above scheme, at best the user can only
16 view the video without an ability to hear the audio. For enhanced security over the
17 video, it possible to employ other embodiments of the invention (as will be
18 described later) here as well. (For example, the SI may be scrambled to make it
19 more difficult for a non-authorized set-top box to tune to the video portion of the
20 program.) Unauthorized set-top boxes that have not been modified by a hacker, will
21 blank the video as a result of receipt of the encrypted audio.

22 Authorized set-top boxes receive Entitlement Control Messages (ECM) that
23 are used to get access criteria and descrambling keys. The set-top box attempts
24 to apply the keys to video as well as the audio. Since the video is not scrambled,
25 it simply passes through the set-top boxes' descrambler unaffected. The set-top
26 boxes do not care that the video is in-the-clear. The un-modified and un-subscribed
27 set-top boxes behave as being un-authorized for the scrambled audio as well as the
28 clear video. The video, as well as the audio which was actually scrambled, will be
29 blanked. An on-screen display may appear on the TV stating that the viewer needs
30 to subscribe to programming. This desirably totally inhibits the casual viewer from

1 both hearing and viewing the content.

2 In one embodiment of the present invention, the encrypted audio is
3 transmitted as digitized packets over the A/V channel. Two (or more) audio
4 streams are transmitted encrypted according to the two (or more) encryption
5 systems in use by the system's set-top boxes. In order for the two (or more) STBs
6 to properly decrypt and decode their respective audio streams, SI (system
7 information) data are transmitted from the cable system's headend 122 that
8 identifies the particular channel where the audio can be found using a transmitted
9 Service Identifier to locate the audio. This is accomplished by assigning the audio
10 for system A is a first packet identifier (PID) and assigning the audio for system B
11 a second packet identifier (PID). By way of example, and not limitation, the
12 following program specific information (PSI) can be sent to identify the location of
13 the audio for two systems, one using NDS conditional access and one using
14 Motorola conditional access. Those skilled in the art will understand how to adapt
15 this information to the other embodiments of partial encryption described later
16 herein.

17 The SI can be separately delivered to both legacy and non-legacy set-top
18 boxes. It is possible to send SI information so that the legacy and non-legacy set-
19 top boxes operate essentially without interference. In the SI delivered to legacy set-
20 top boxes, the VCT (virtual channel table) would state that the desired program, e.g.
21 HBO referenced as program number 1, is on Service ID "1" and that the VCT
22 access control bit is set. The network information table (NIT) delivered to that first
23 STB would indicate that Service ID "1" is at frequency = 1234. In the SI delivered
24 to non-legacy set-top boxes, the VCT would state that the desired program, e.g.
25 HBO referenced as program number 1001, is on Service ID "1001" and that the
26 VCT access control bit is set. The network information table delivered to the non-
27 legacy STB would indicate that the Service ID "1001" is at frequency 1234. The
28 following exemplary program association Table PSI data are sent to both legacy
29 and non-legacy set-top boxes (in MPEG data structure format):
30

PAT sent on PID=0x0000

PAT 0x0000

- Transport Stream ID
- PAT version
- Program Number 1
 - PMT 0x0010
- Program Number 2
 - PMT 0x0020
- Program Number 3
 - PMT 0x0030
- Program Number 4
 - PMT 0x0040
- Program Number 5
 - PMT 0x0050
- Program Number 6
 - PMT 0x0060
- Program Number 7
 - PMT 0x0070
- Program Number 8
 - PMT 0x0080
- Program Number 9
 - PMT 0x0090
- Program Number 1001
 - PMT 0x1010
- Program Number 1002
 - PMT 0x1020
- Program Number 1003
 - PMT 0x1030
- Program Number 1004
 - PMT 0x1040
- Program Number 1005
 - PMT 0x1050
- Program Number 1006
 - PMT 0x1060
- Program Number 1007
 - PMT 0x1070
- Program Number 1008
 - PMT 0x1080
- Program Number 1009
 - PMT 0x1090

The following exemplary program map table PSI data are selectively received by legacy and non-legacy set-top boxes (in MPEG data structure format):

PMT sent on PID=0x0010

PMT 0x0010

- PMT Program number 1
- PMT Section Version 10
- PCR PID 0x0011
- Elementary Stream
 - Stream Type (Video 0x02 or 0x80)
 - Elementary PID (0x0011)
 - Descriptor
 - CA Descriptor (ECM) for CA provider #1
- Elementary Stream
 - Stream Type (Audio 0x81)
 - Elementary PID (0x0012)
 - Descriptor
 - CA Descriptor (ECM) for CA provider #1

PMT sent on PID=0x1010

PMT 0x1010

- PMT Program number 1010
- PMT Section Version 10
- PCR PID 0x0011
- Elementary Stream
 - Stream Type (Video 0x02 or 0x80)
 - Elementary PID (0x0011)
 - Descriptor
 - CA Descriptor (ECM) for CA provider #2
- Elementary Stream
 - Stream Type (Audio 0x81)
 - Elementary PID (0x0013)
 - Descriptor
 - CA Descriptor (ECM) for CA provider #2

Considering an example wherein it is desired to deliver programming in a system using either Motorola or Scientific Atlanta as well as NDS CA, the above communications are consistent with the PSI delivered by both Motorola and Scientific Atlanta in their CA systems, with only minor changes. The program association table (PAT) is changed to reference an additional program map table (PMT) for each program. Each program in this embodiment has two program numbers in the PAT. In the table above, program number 1 and program number 1001 are the same program except that they will reference different audio PIDs and

1 CA descriptors. Changes in the system to create multiple PMTs and to multiplex
2 new PAT and PMT information with the data stream can be made to appropriately
3 modify the cable system headend equipment. Again, those skilled in the art will
4 understand how to adapt these messages to other partial encryption schemes
5 described herein. An advantage of this approach is that no special hardware or
6 software is required for headend or for legacy and non-legacy set-top boxes to
7 deliver audio that is both legacy and non-legacy encrypted using this scheme.

8 This technique deters the user from use of premium programming which has
9 not been paid for by rendering it inaudible, but a hacker may attempt to tune the
10 video. To combat this, the mechanisms employed in other encryption techniques
11 consistent with the present invention (as will be described later) can be employed
12 simultaneously, if desired. Since closed captioning is generally transmitted as a
13 part of the video data, the user can still obtain readable audio information in
14 conjunction with clear video. Thus, although adequate for some applications, the
15 present technique alone may not provide adequate protection in all scenarios. In
16 another embodiment, video packets containing closed captioning information as
17 a part of the payload can additionally be scrambled.

18 In an alternative embodiment, only the video may be dual encrypted with
19 separate PIDs assigned to each set of encrypted video. While this may provide a
20 more secure encryption for general programming (since video may be more
21 important than audio), the amount of bandwidth savings compared with full dual
22 carriage is only approximately ten percent, since only the audio is shared amongst
23 all the set-top boxes. However, this approach might be used for certain content,
24 e.g. adult and sports, and help reduce the bandwidth overhead for that content
25 while the audio encryption approach may be used for other content types. In the
26 Digital Satellite Service (DSS) transport standard used for the DirecTV™ service,
27 the audio packets can be identified for encryption by use of the service channel
28 identifier (SCID) which is considered equivalent.

TIME SLICING

Another embodiment consistent with the present invention is referred to herein as time slicing and is illustrated in **FIGURE 3** as system 200. In this embodiment, a portion of each program is encrypted on a time dependent basis in a manner that disrupts viewing of the program unless the user has paid for the programming. This embodiment of the invention can be implemented as partially encrypted video and clear audio, clear video and partially encrypted audio or partially encrypted video and audio. The duration of the time slice that is encrypted, taken as a percentage of the total time, can be selected to meet any suitable desired balance of bandwidth usage, security against hackers. In general, under any of the embodiments described herein, less than 100 percent of the content is encrypted to produce a desired partial encryption. . The following example details partially encrypted video and audio.

By way of example, and not limitation, consider a system which has nine programs that are to be dual partially encrypted according to the present exemplary embodiment. These nine channels are fed to the cable headend as a multiplexed stream of packets and are digitally encoded using packet identifiers (PID) to identify packets associated with a particular one of the nine programs. In this example, assume that those nine programs have video PIDs numbered 101-109 and audio PIDs numbered 201-209. The partial encryption, according to this embodiment is time multiplexed among the programs so that only packets from a single program are encrypted at any given time. The method does not need to be content aware.

With reference to **TABLE 1** below, an exemplary embodiment of a time slice dual encryption scheme consistent with an embodiment of the invention is illustrated. For program 1 having primary video PID 101 and primary audio PID 201, during the first time period, packets having PID 101 and PID201 are encrypted using encryption system A, while the others representing the other programs are sent in the clear. In this embodiment, secondary PIDs are also assigned to both the video and the audio. The secondary PIDs are PID 111 for video and PID 211 for

1 audio respectively for program 1. The packets with the secondary PIDs are
2 encrypted using encryption system B during the first time period. The next eight
3 time periods are sent in the clear. Then for time period 10, packets having any of
4 the above four PIDs are again encrypted followed by the next eight time periods
5 being sent in the clear. In a similar manner, during the second period of program
6 2 having primary video PID 102 and primary audio PID 201 are encrypted using
7 encryption system A and packets with their associated secondary PIDs are
8 encrypted using encryption system B, and during the next eight time periods are
9 sent in the clear, and so on. This pattern can be seen clearly in **TABLE 1** by
10 examination of the first nine rows. Both audio and video packets, or audio
11 alone or video alone can be encrypted according to this technique, without
12 departing from the invention. Also, the audio and video can have their own
13 individual encryption sequence. In **TABLE 1**, P1 indicates time period number 1,
14 P2 indicated time period number 2 and so on. EA indicates that the information is
15 encrypted using CA system A and EB indicates that the information is encrypted
16 using CA encryption system B.
17

PROG.	VIDEO PID	AUDIO PID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	...
1	PID 101	PID 201	EA	clear	clear	clear	clear	clear	clear	clear	clear	EA	clear	clear	...
2	PID 102	PID 202	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	EA	clear	...
3	PID 103	PID 203	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	EA	...
4	PID 104	PID 204	clear	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	...
5	PID 105	PID 205	clear	clear	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	...
6	PID 106	PID 206	clear	clear	clear	clear	clear	EA	clear	clear	clear	clear	clear	clear	...
7	PID 107	PID 207	clear	clear	clear	clear	clear	clear	EA	clear	clear	clear	clear	clear	...
8	PID 108	PID 208	clear	clear	clear	clear	clear	clear	clear	EA	clear	clear	clear	clear	...
9	PID 109	PID 209	clear	clear	clear	clear	clear	clear	clear	clear	EA	clear	clear	clear	...
1	PID 111	PID 211	EB									EB			...
2	PID 112	PID 212		EB									EB		...
3	PID 113	PID 213			EB									EB	...
4	PID 114	PID 214				EB									...
5	PID 115	PID 215					EB								...
6	PID 116	PID 216						EB							...
7	PID 117	PID 217							EB						...
8	PID 118	PID 218								EB					...
9	PID 119	PID 219									EB				...

TABLE 1

In order to retain compatibility with an established legacy encryption system (encryption system A), the encrypted periods for each of programs one through nine are encrypted using encryption system A. Legacy STB equipment will accept such partially encrypted A/V data streams passing unencrypted packets and decrypting encrypted packets transparently. However, it is desired to obtain dual encryption using both encryption system A and encryption system B. In order to achieve this, a specified program is assigned both primary PIDs (e.g., for program 1, video PID 101 and audio PID 201) and a secondary PID (e.g., for program 1, video PID 111 and audio PID 211) to carry the elementary data streams for a given premium channel.

With reference to **FIGURE 3**, system 200 generally depicts the functionality of the cable system headend 222 wherein N channels of clear video 204 at the headend 222 are provided to an intelligent switch 216 (operating under control of a programmed processor) which routes packets that are to be transmitted in the clear to be assigned a primary PID at 220. Packets that are to be encrypted are

1 routed to both conditional access system A encrypter 218 and to conditional
2 access system B encrypter 224. Once encrypted, these encrypted packets from
3 218 and 224 are assigned primary or secondary PIDs respectively at 220. System
4 information from 228 is multiplexed or combined with the clear packets, the system
5 A encrypted packets and the system B encrypted packets and broadcast over the
6 cable system 32.

7 For discussion purposes, if the period of the time slice is 100 milli-seconds,
8 then as shown in **TABLE 1**, there are on average one and a fraction encrypted
9 periods totaling 111 milli-seconds each second for all nine-programs. If the period
10 is 50 milli-seconds, then there are on average two and a fraction encrypted periods
11 totaling 111 milli-seconds. A non-subscribing box attempting to tune video would
12 obtain a very poor image if it could maintain any sort of image lock and the audio
13 would be garbled.

14 The PSI for a partially scrambled stream is handled slightly differently from
15 the dual audio encryption example above. Essentially, the same SI and PAT PSI
16 information can be sent to both legacy and non-legacy set-top boxes. The
17 difference lies with the PMT PSI information. The legacy set-top box parses the
18 PMT PSI and obtains the primary video and audio PIDs as before. The non-legacy
19 set-top box obtains the primary PIDs like the legacy set-top box but must look at the
20 CA descriptors in the PMT PSI to see if the stream is partially scrambled. The
21 secondary PID is scrambled specifically for a particular CA provider, consequently
22 it makes sense to use the CA descriptor specific to a particular CA provider to
23 signal that PID. The invention can allow more than two CA providers to co-exist by
24 allowing more than one secondary PID. The secondary PID shall be unique to a
25 particular CA provider. The set-top box know the CA ID for the CA it has, and can
26 check all CA descriptors for the relevant one for it.

27 While it is possible to send the secondary PID data as private data in the
28 same CA descriptor used for the ECM, the preferred embodiment uses separate
29 CA descriptors. The secondary PID is placed in the CA PID field. This allows
30 headend processing equipment to "see" the PID without having to parse the private

data field of the CA descriptor. To tell the difference between the ECM and secondary PID CA descriptor, a dummy private data value can be sent.

PMT sent on PID=0x0010

PMT 0x0010

- PMT Program number 1
- PMT Section Version 10
- PCR PID 0x0011
- Elementary Stream
 - Stream Type (Video 0x02 or 0x80)
 - Elementary PID (0x0011)
 - Descriptor
 - CA Descriptor (ECM) for CA provider #1
 - CA Descriptor (ECM) for CA provider #2
 - CA Descriptor (Secondary PID) for CA provider #2
- Elementary Stream
 - Stream Type (Audio 0x81)
 - Elementary PID (0x0012)
 - Descriptor
 - CA Descriptor (ECM) for CA provider #1
 - CA Descriptor (ECM) for CA provider #2
 - CA Descriptor (Secondary PID) for CA provider #2

CA Descriptor for CA Provider #2 (ECM)

Descriptor

- Tag: Conditional Access (0x09)
- Length: 4 Bytes
- Data
 - CA System ID: 0x0942 (2nd CA provider)
 - CA PID (0x0015)

CA Descriptor for CA Provider #2 (Secondary PID)

Descriptor

- Tag: Conditional Access (0x09)
- Length: 5 Bytes
- Data
 - CA System ID: 0x1234 (2nd CA provider)
 - CA PID (0x0016)
 - Private Data

1
2 Legacy STB 36 operating under CA system A receives the data, ignores
3 the secondary PIDs, decrypts the packets encrypted under CA system A and
4 presents the program to the television set 44. New or non-legacy STB 236
5 receives the SI 228. It receives PSI 229 and uses the PMT to identify the
6 primary and secondary PID, called out in the second CA descriptor, associated
7 with the program being viewed. The packets encrypted under CA system A are
8 discarded and the packets encrypted under CA system B with the secondary
9 PID are decrypted by CA system B 240 and inserted into the clear data stream
10 for decoding and display on television set 244.

11 **FIGURE 4** illustrates one process for encoding at the cable system headend
12 that can be used to implement an embodiment of the present invention wherein CA
13 system A is the legacy system and CA system B is the new system to be
14 introduced. As a clear packet is received, at 250 for a given program, if the packet
15 (or frame) is not to be encrypted (i.e., it is not the current time slice for encryption
16 for this program), the clear packet (C) is passed on to be inserted into the output
17 stream at 254. If the current packet is to be encrypted by virtue of the current
18 packet being a part of the encryption time slice, the packet is passed for encryption
19 to both packet encryption process A 258 and packet encryption process B 262.
20 The encrypted packets from encryption process A at 258 (EA) are passed on to 254
21 for insertion into the output stream. The encrypted packets from encryption
22 process B at 262 (EB) are assigned a secondary PID at 264 for insertion into the
23 output stream at 254. This is repeated for all packets in the program.

24 **FIGURE 5** illustrates a process used in the STB 236 having the newly
25 introduced CA system B for decrypting and decoding the received data stream
26 containing C, EA and EB packets having primary and secondary PIDs as
27 described. When a packet is received at 272, it is inspected to see if it has a the
28 primary PID of interest. If not, the packet is examined to see if it has the secondary
29 PID of interest at 274. If the packet has neither the primary or secondary PID, it is

1 ignored or dropped at 278. Any intervening packets between the EA and EB
2 packets that are not the primary or secondary PID are discarded. It is an
3 implementation and mainly a buffering issue whether a decoder can receive
4 multiple EA or EB in a row before receiving the replacement matched EA or EB
5 packet. Also, just as easy to detect for secondary packets that come before and
6 not after the primary packet. It is also possible to design a circuit where either
7 case can happen – the secondary packet can be before or after the primary packet.
8 If the packet has the primary PID of interest, the packet is examined at 284 to
9 determine if it is encrypted. If not, the packet (C) is passed directly to the decoder
10 at 288 for decoding. If the packet is encrypted at 284, it is deemed to be an EA
11 packet and is dropped or ignored at 278. In some implementations, the primary
12 packet's encryption does not get checked at 284. Rather, its simple position
13 relative to the secondary packet can be checked at 284 to identify it for
14 replacement.

15 If the packet has the secondary PID at 274, the PID is remapped to the
16 primary PID at 292 (or equivalently, the primary PID is remapped to the secondary
17 PID value). The packet is then decrypted at 296 and sent to the packet decoder at
18 288 for decoding. Of course, those skilled in the art will recognize that many
19 variations are possible without departing from the invention, for example, the order
20 of 292 and 296 or the order of 272 and 274 can be reversed. As mentioned earlier,
21 284 can be replaced with a check of primary packet position with respect to the
22 secondary packet. Other variations will occur to those skilled in the art.

23 Legacy STB 36 operating under the encryption system A totally ignores the
24 secondary PID packets. Packets with the primary PID are decrypted, if necessary,
25 and passed to the decoder without decryption if they are clear packets. Thus, a so
26 called "legacy" STB operating under encryption system A will properly decrypt and
27 decode the partially encrypted data stream associated with the primary PID and
28 ignore the secondary PID without modification. STBs operating under the
29 encryption system B are programmed to ignore all encrypted packets associated

1 with the primary PID and to use the encrypted packets transmitted with the
2 secondary PID associated with a particular channel.

3 Thus, each dual partially encrypted program has two sets of PIDs associated
4 therewith. If, as described, the encryption is carried out on a period-by-period
5 basis, for the system shown with an appropriate time slice interval, the picture will
6 be essentially unviewable on a STB with neither decryption.

7 In order to implement this system in the headend 322 of **FIGURE 6**, the SI
8 and PSI can be modified for inclusion of a second set of CA descriptor information.
9 Legacy set-top boxes may not be able to tolerate unknown CA descriptors.
10 Consequently, alternatively, in the set-top box, it may be possible to "hard code"
11 offsets from the legacy CA PIDs for both the content PIDs and/or the SI/PSI and
12 ECM PIDs. Alternatively, parallel PSI may be sent. For example, an auxiliary PAT
13 can be delivered on PID 1000 instead of PID 0 for the non-legacy set-top boxes. It
14 can reference auxiliary PMTs not found in the legacy PAT. The auxiliary PMTs can
15 contain the non-legacy CA descriptors. Since auxiliary PMTs would not be known
16 to the legacy set-top boxes, there would not be any interoperation issue.

17 In systems where system A corresponds to legacy set-top boxes
18 manufactured by Motorola or Scientific Atlanta, no modifications to the STBs are
19 required. For the system B compliant STBs, for dual carriage of partially encrypted
20 programs as described herein, the video and audio decoder are adapted to listen
21 to two PIDs each (a primary and a secondary PID) instead of just one. There may
22 be one or more secondary shadow PIDs, depending on the number of non-legacy
23 CA systems in use, however a specific set-top box only listens to one of the
24 secondary PIDs as appropriate for the CA method being used by that specific STB.
25 In addition, ideally the encrypted packets from the PID carrying the mostly clear
26 video or audio are ignored. Since ignoring "bad packets" (those that cannot be
27 readily decoded as is) may already be a function that many decoders perform, thus
28 requiring no modification. For systems with decoders that do not ignore bad
29 packets, a filtering function can be used. It should be understood that the time
30 slice encryption technique could be applied to just the video or the audio. Also, the

1 video may be time slice encrypted while the audio is dual encrypted as in the
2 earlier embodiment. The time slice technique may be applied to multiple programs
3 concurrently. The number of programs that encrypted during a period of time is
4 mainly an issue of bandwidth allocation, and although the example discusses
5 scrambling a single program at a time, the invention is not limited by that. Other
6 combinations of encryption techniques described in this document will also occur
7 to those skilled in the art.

8 9 10 MTH AND N PACKET ENCRYPTION

11 Another embodiment consistent with the present invention is referred to
12 herein as Mth & N packet encryption. This is a variation of the embodiment
13 illustrated in **FIGURE 3** as system 200. In this embodiment, packets of each PID
14 representing a program are encrypted in a manner that disrupts viewing of the
15 program unless the user has paid for the programming. In this embodiment, M
16 represents the number of packets between the start of an encryption event. N
17 represents the number of packets that are encrypted in a row, once encryption
18 takes place. N is less than M. If M=9 and N=1, then every nine packets there is an
19 encryption event lasting 1 packet. If M=16 and N=2, then every sixteen packets
20 there is an encryption event lasting two packets. Each packet to be dual partially
21 encrypted is duplicated and processed using CA system A 218 and CA system B
22 224 as in the previous embodiment. The difference in operation between this
23 embodiment and the time slicing technique previously is in the operation of switch
24 216 to effect the selection of packets to encrypt under control of a programmed
25 processor.

26 By way of example, and not limitation, consider a system which has nine
27 channels of programming that are to be dual encrypted according to the present
28 exemplary embodiment. These nine channels are digitally encoded using packet
29 identifiers (PID) to identify packets associated with a particular one of nine
30 programs. In this example, assume that those nine programs have video PIDs

numbered 101-109 and audio PIDs numbered 201-209. The encryption, according to this embodiment is random program-to-program so that packets from other programs may be encrypted at the same time. This is illustrated in **TABLE 2** below in which $M=6$ and $N=2$ and in which only video is encrypted, but this should not be considered limiting. The method does not need to be content aware. In **TABLE 2**, PK1 indicated packet number 1, PK2 indicates packet number 2, and so on.

PROG.	VIDEO	PK1	PK2	PK3	PK4	PK5	PK6	PK7	PK8	PK9	PK10	PK11	PK12	...
1	PID 101	EA	EA	clear	clear	clear	clear	EA	EA	clear	clear	clear	clear	...
2	PID 102	clear	clear	clear	EA	EA	clear	clear	clear	clear	EA	EA	clear	...
3	PID 103	clear	clear	EA	EA	clear	clear	clear	clear	EA	EA	clear	clear	...
4	PID 104	clear	clear	clear	EA	EA	clear	clear	clear	clear	EA	EA	clear	...
5	PID 105	clear	clear	EA	EA	clear	clear	clear	clear	EA	EA	clear	clear	...
6	PID 106	EA	clear	clear	clear	clear	EA	EA	clear	clear	clear	clear	EA	...
7	PID 107	EA	EA	clear	clear	clear	clear	EA	EA	clear	clear	clear	clear	...
8	PID 108	clear	EA	EA	clear	clear	clear	clear	EA	EA	clear	clear	clear	...
9	PID 109	EA	clear	clear	clear	clear	EA	EA	clear	clear	clear	clear	EA	...
1	PID 111	EB	EB					EB	EB					...
2	PID 112				EB	EB					EB	EB		...
3	PID 113			EB	EB					EB	EB			...
4	PID 114				EB	EB					EB	EB		...
5	PID 115			EB	EB					EB	EB			...
6	PID 116	EB					EB	EB					EB	...
7	PID 117	EB	EB					EB	EB					...
8	PID 118		EB	EB					EB	EB				...
9	PID 19	EB					EB	EB					EB	...

TABLE 2

In the example of **TABLE 2**, each program is encrypted fully independently of the others using the $M=6$ and $N=2$ encryption scheme. Again, the illustrated example encrypts only the video, but audio could also be encrypted according to

1 this or another arrangement. If applied to just the video, audio may be dual
2 scrambled or time slice encrypted as in earlier embodiments. Alternatively, if
3 applied to just the audio, the video may be time sliced as in the earlier
4 embodiment.

5 Those skilled in the art will recognize that many variations of the technique
6 can be devised consistent with the partial scrambling concepts disclosed herein.
7 For example, a pattern of five clear followed by two encrypted followed by two clear
8 followed by one encrypted (CCCCCEECCCECCCCCEECE...) is consistent with
9 variations of the present partial encryption concept, as are random, pseudo-random
10 and semi-random values for M and N may be used for selection of packets to
11 encrypt. Random, pseudo-random or semi-random (herein collectively referred to
12 as "random" herein) selection of packets can make it difficult for a hacker to
13 algorithmically reconstruct packets in a post processing attempt to recover
14 recorded scrambled content. Those skilled in the art will understand how to adapt
15 this information to the other embodiments of partial encryption described later
16 herein. Some of the embodiments can be used in combination to more effectively
17 secure the content.

18 19 DATA STRUCTURE ENCRYPTION

20 Another partial encryption method consistent with embodiments of the
21 present invention uses a data structure as a basis for encryption. By way of
22 example and not limitation, one convenient data structure to use for encryption is
23 an MPEG video frame. This is illustrated (again with video only) in **TABLE 3** below
24 in which every tenth video frame is encrypted. In this embodiment, each program's
25 ten frame encryption cycle is distinct from each other channel, but this should not
26 be considered limiting. This concept can be viewed as a variation of the time slice
27 or Mth and N partial encryption arrangement (or other pattern) based upon video or
28 audio frames (or some other data structure) with the exemplary embodiment having
29 M=10 and N=1. Of course, other values of M and N can be used in a similar

embodiment. In **TABLE 3**, F1 represents frame number 1, F2 represents frame number 2 and so on.

PROG.	VIDEO	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	...
1	PID 101	EA	clear	clear	clear	clear	clear	clear	clear	clear	clear	EA	clear	...
2	PID 102	clear	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	...
3	PID 103	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	clear	...
4	PID 104	clear	clear	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	...
5	PID 105	clear	clear	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	...
6	PID 106	EA	clear	clear	clear	clear	clear	clear	clear	clear	clear	EA	clear	...
7	PID 107	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	clear	EA	...
8	PID 108	clear	EA	clear	clear	clear	clear	clear	clear	clear	clear	clear	EA	...
9	PID 109	EA	clear	clear	clear	clear	clear	clear	clear	clear	clear	EA	clear	...
1	PID 111	EB										EB		...
2	PID 112				EB									...
3	PID 113			EB										...
4	PID 114					EB								...
5	PID 115				EB									...
6	PID 116	EB										EB		...
7	PID 117		EB										EB	...
8	PID 118		EB										EB	...
9	PID 119	EB										EB		...

TABLE 3

Thus, again each encrypted program has two sets of PIDs associated therewith. If, as described, the encryption is carried out on a period-by-period basis, for the system shown, the picture will be essentially unviewable. For a nine program system at 30 frames per second as depicted, approximately three frames per second will be encrypted. For viewers who are not entitled to view the program, their STB will be unable to capture much more than an occasional frozen frame as the STB constantly attempts to synchronize and recover. Viewers who have

1 subscribed to the programming will be able to readily view the programming. The
2 bandwidth cost for such an encryption arrangement depends upon the frequency
3 with which the encryption is applied. In the above example, an extra factor of 1/9
4 of data are transmitted for each program. In this example, approximately one
5 program's worth of bandwidth is used. With a greater number of programs, fewer
6 packets per program are encrypted and the security of the encryption system may
7 degrade somewhat. As in the randomized M and N method, random frames may
8 be selected. Choosing random frames, in the video case, would help guarantee
9 that all frame types would be affected – intra-coded frames (I frames), predictive-
10 coded (P frames), Bi-directional-coded (B frames) and DC frames.

11 In a variation of the invention, it may be possible to encrypt fewer packets to
12 achieve an acceptable level of security. That is, perhaps in a system of nine
13 programs, only one frame per second may need to be encrypted to achieve
14 acceptable levels of security. In such a system, the overhead becomes one
15 encrypted period per second per program or approximately 1/30 of data transmitted
16 in overhead. This level of overhead is a dramatic improvement over the 50% loss
17 of bandwidth associated with full dual carriage of encryption under two encryption
18 systems. In another variation of the invention, it may be possible to encrypt only
19 certain video frames to achieve an acceptable level of security. For example, for
20 MPEG content, only intra-coded frames (I frames) may be scrambled to further
21 reduce the bandwidth overhead and still maintain an acceptable level of security.
22 These offer significant improvement over the bandwidth required for full dual
23 carriage.

24 25 26 CRITICAL PACKET ENCRYPTION

27 Substantial efficiency in bandwidth utilization can be achieved by use of a
28 selective packet-by-packet dual encryption technique. In this technique, packets
29 are selected for encryption based upon their importance to the proper decoding of
30 the audio and/or video of the program content.

1 This embodiment can reduce the bandwidth requirement compared with full
2 dual carriage of encrypted content by only scrambling a small fraction of the
3 packets. Clear packets are shared between the two (or more) dual carriage PIDs.
4 In one preferred embodiment, as will be disclosed, less than about one percent of
5 the total content bandwidth is used. In a system with a legacy encryption scheme,
6 clear program content packets can be received by both legacy and new set-top
7 boxes. As mentioned before, encrypted packets are dual carried and processed
8 by the respective set-top boxes with the appropriate CA. Each CA system is
9 orthogonal. Key sharing is not required and different key epochs may be used by
10 each CA system. For example, a system with Motorola's proprietary encryption can
11 generate fast changing encryption keys using the embedded security ASIC, while
12 an NDS smart card based system can generate slightly slower changing keys.
13 This embodiment works equally well for Scientific Atlanta and Motorola legacy
14 encryption.

15 Referring now to **FIGURE 6**, a block diagram of a system consistent with an
16 embodiment of the present invention in which portions of programming are dual
17 encrypted on a packet-by-packet basis is illustrated as system 300. In this system,
18 packets of each program are dual encrypted using, for example, legacy CA system
19 A and CA system B. The packets that are encrypted are selected based upon their
20 importance to the proper decoding of the video and/or audio stream.

21 In the system illustrated in **FIGURE 6**, the cable system headend 322
22 selects AV content 304 packets at a packet selector 316 for encryption. Packets
23 selected for encryption are chosen so that their non-receipt (by a non-paying
24 decoder) would severely affect the real-time decoding of a program, and any
25 possible post processing of recorded content. That is, only critical packets are
26 encrypted. For the video and audio, this can be accomplished by encrypting "start
27 of frame" transport stream packets containing PES (packetized elementary stream)
28 headers and other headers as part of the payload, since without this information,
29 the STB decoder cannot decompress the MPEG compressed data. MPEG2

streams identify "start of frame" packets with the "Packet Unit Start Indicator" in the transport header. Generally, packets carrying a payload that contains a group of pictures header or a video sequence header can be used to effect the present scrambling technique.

MPEG (Moving Pictures Expert Group) compliant compressed video repackages the elementary data stream into the transport stream in somewhat arbitrary payloads of 188 bytes of data. As such, the transport stream packets containing a PES header can be selected for encryption at selector 316 and dual encrypted by both the CA system A encrypter 318 and the CA system B encrypter 324. Packets to be dual partially encrypted are duplicated and the PIDs of duplicate packets encrypted by encrypter 324 are remapped at 330 to a secondary PID as in the previous embodiment. The remaining packets are passed in the clear. The clear packets, system A encrypted packets, system B encrypted packets and system information 328 are multiplexed together for broadcast over the cable system 32.

As with the previous system, the legacy STB 36 receives clear data and data encrypted under CA encryption system A and transparently passes unencrypted data combined with data decrypted by CA decryption A 40 to its decoder. In the new STB 336, the program is assigned to both a primary and a secondary PID. The clear packets with the primary PID are received and passed to the decoder. The encrypted packets with the primary PID are discarded. Encrypted packets with the secondary PID are decrypted and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding.

Using video is used as an example, each sample is known as a frame and the sample rate is typically 30 frames per second. If the samples are encoded to fit into 3.8 Mbps, each frame would occupy 127K bits of bandwidth. This data is sliced for MPEG transport into packets of 188 bytes with the first packet(s) of each frame containing the header used for instructions to process the body of the frame data. Dual encrypting just the first header packet (1504 additional bits) requires

1 only 1.2% (1504/127K) of additional bandwidth. For high definition (19 Mbps)
2 streams the percentage is even less.

3 As previously stated, transport stream packets containing a PES header are
4 the preferred target for encryption according to the present embodiment. These
5 packets contain sequence headers, sequence extension headers, picture headers,
6 quantization and other decode tables that also fall within the same packet. If these
7 packets cannot be decoded (i.e., by a hacker attempting to view unauthorized
8 programming without paying the subscription charges), not even small portions of
9 the program can be viewed. In general, any attempt to tune to the program will
10 likely be met with a blank screen and no audio whatsoever since known decoder
11 integrated circuits use the PES header to sync up to an elementary stream such
12 as video and audio in real-time. By encrypting the PES header, the decoding
13 engine in an un-authorized set-top box cannot even get started. Post processing
14 attacks, e.g. on stored content, are thwarted by critical dynamically changing
15 information in the packet containing the PES header. Those skilled in the art will
16 appreciate that for implementation of this embodiment of the invention, other critical
17 or important packets or content elements may also be identified for encryption that
18 could severely inhibit unauthorized viewing without departing from the present
19 invention. For example, MPEG intra-coded or I frame picture packets could be
20 encrypted to inhibit viewing of the video portion of the program. Embodiments the
21 present invention may be used in any combination with other embodiments, e.g.
22 scrambling the packet containing the PES header as well as random, Mth and N,
23 or data structure encryption of the other packets. Critical packet encryption may
24 be applied to video encryption, while a different method may be applied to audio.
25 Audio could be dual encrypted, for instance. Other variations within the scope of
26 the present invention will occur to those skilled in the art.

27 **FIGURE 7** is a flow chart depicting an exemplary encoding process such as
28 that which would be used at headend 322 of **FIGURE 6**. When a transport stream
29 packet is received at 350, the packet is examined to determine if it meets a

1 selection criteria for encryption. In the preferred embodiment, this selection criteria
2 is the presence of a PES header as a portion of the packet payload. If not, the
3 packet is passed as a clear unencrypted packet (C) for insertion into the output
4 data stream at 354. If the packet meets the criteria, it is encrypted under CA
5 encryption system A at 358 to produce an encrypted packet EA. The packet is
6 also duplicated and encrypted under CA encryption system B at 362 to produce
7 an encrypted packet. This encrypted packet is mapped to a secondary PID at 366
8 to produce an encrypted packet EB. Encrypted packets EA and EB are inserted
9 into the output data stream along with clear packets C at 354. Preferably, the EA
10 and EB packets are inserted at the location in the data stream where the single
11 original packet was obtained for encryption so that the sequencing of the data
12 remains essentially the same.

13 When the output data stream from 354 is received at an STB compliant with
14 CA encryption system B such as 336 of **FIGURE 6**, a process such as that of
15 **FIGURE 8** (which is similar to that of **FIGURE 5**) can be utilized to decrypt and
16 decode the program. When a packet is received having either the primary or the
17 secondary PID at 370, a determination is made as to whether the packet is clear
18 (C) or encrypted under system A (EA) at 370 or encrypted under system B (EB) at
19 374. If the packet is clear, it is passed directly to the decoder 378. In some
20 embodiments, the relative position of the primary packet, before or after, to the
21 secondary packet may be used to signal a primary packet for replacement in the
22 stream. A check of the scrambling state of the primary packet is not specifically
23 required. If the packet is an EA packet, it is dropped at 380. If the packet is an EB
24 packet, it is decrypted at 384. At this point, the secondary PID packets and/or the
25 primary PID packets are remapped to the same PID at 388. The decrypted and
26 clear packets are decoded at 378.

27 The dual partial encryption arrangement described above can greatly reduce
28 the bandwidth requirements over that required for full dual carriage. Encrypting the
29 PES header information can be effective in securing video and audio content, while

1 allowing two or more CA systems to independently "co-exist" on the same cable
2 system. Legacy system A set-top boxes are un-affected, and system B set-top
3 boxes require only an minor hardware, firmware, or software enhancement to listen
4 for two PIDs each for video and audio. Each type of STB, legacy and non-legacy,
5 retains its intrinsic CA methodology. Headend modification is limited to selecting
6 content for encryption, introducing the second encrypter, and providing a means to
7 mix the combination into a composite output stream.

8 In one embodiment, the headend equipment is configured to
9 opportunistically scramble as much of the content as the bandwidth will allow, and
10 not just the critical PES headers. These additional scrambled packets would be
11 either in the PES payload or other packets throughout the video/audio frame to
12 provide even further security of the content.

13 14 SI ENCRYPTION

15 Turning now to **FIGURE 9**, one embodiment of a system that minimizes
16 the need for any additional bandwidth is illustrated as system 400. In this
17 embodiment, the system takes advantage of the fact that system information (SI)
18 428 is required for a set-top box to tune programming. In a cable system, SI is sent
19 in the out-of-band, a frequency set aside from the normal viewing channels. It is
20 possible to also sent it in-band. If sent in-band, the SI 428 is replicated and sent
21 with each stream. For discussion purposes, assume that the SI delivered to
22 "legacy" set-top boxes from previous manufacturers is separate from the SI
23 delivered to set-tops from new manufacturers such as STB 436. Consequently,
24 each version of the SI can be independently scrambled as illustrated using
25 conditional access system A 418 and conditional access system B 424. The clear
26 video 404 and clear audio 406 are delivered in the clear, but in order to understand
27 how to find them, the SI information 428 is needed.

28 The SI delivers information about channel names and program guide
29 information such as program names and start times, etc. ... as well as the
30 frequency tuning information for each channel. Digital channels are multiplexed

1 together and delivered at particular frequencies. In the embodiment of the
2 invention, the SI information is encrypted, and only made available to authorized
3 set-top boxes. If the SI information is not received to allow knowledge of the
4 location of all the A/V frequencies in the plant, then tuning cannot take place.

5 To frustrate a hacker who might program a set-top box to trial or scan
6 frequencies, the frequencies for the channels can be offset from the standard
7 frequencies. Also, the frequencies can be dynamically changed on a daily, weekly
8 or other periodic or random basis. A typical cable headend may have roughly 30
9 frequencies in use. Each frequency is typically chosen to avoid interference
10 between, among other things, each other, terrestrial broadcast signals, and
11 frequencies used by clocks of the receiving equipment. Each channel has at least
12 1 independent alternate frequency that if used would not could not cause
13 interference, or cause the frequency of adjoining channels to be changed. The
14 actual possible frequency maps are therefore 2^{30} or 1.07×10^9 . However, a hacker
15 might simply quickly try both frequencies on each tune attempt for each of the 30
16 channels or so. If successful in locating a frequency with content, the hacker's set-
17 top box can then parse the PSI 429 to learn about the individual PIDs that make up
18 a program. The hacker will have difficulty learning that "program 1" is "CNN", and
19 that "program 5" is "TNN", and so on. That information is sent with the SI, which as
20 stated above is scrambled and otherwise unavailable to the un-authorized set-top
21 box. However, a persistent hacker might yet figure those out by selecting each one
22 and examining the content delivered. So in order to frustrate the identification of
23 channels, the assignment of a program within a single stream can move around,
24 e.g. program 2 and program 5 swapped in the example above so that "program 1"
25 is "TNN" and "program 5" is "CNN". Also, it is possible to move programs to
26 entirely different streams with entirely new program groupings. A typical digital
27 cable headend can deliver 250 programs of content including music. Each can be
28 uniquely tuned. The possible combinations for re-ordering are 250! (factorial).
29 Without a map of the content provided by either the delivered SI or by a hacker, the

1 user is faced with randomly selecting each program in a stream to see if it is the
2 one interest.

3 Thus, at headend 422, the video signal 404 and the audio signal 406 are
4 provided in the clear (unencrypted) while the SI 428 is provided to multiple CA
5 systems for delivery over the cable network. Thus, in the exemplary system 400,
6 clear SI 428 is provided to an encryption system 428 that encrypts SI data using
7 encryption system A. Simultaneously, clear SI 428 is provided to encryption
8 system 424 that encrypts the SI data using encryption system B. Clear video and
9 audio are then multiplexed along with encrypted SI from 418 (SI A) and encrypted
10 audio from 424 (SI B) out of band system information 428.

11 After distribution through the cable system 32, the video, the audio, system
12 information A and system information B are all delivered to set-top boxes 36 and
13 436. At STB 36, the encrypted SI is decrypted at CA system A 40 to provide tuning
14 information to the set-top box. The set-top box tunes a particular program to allow
15 it to be displayed on television set 44. Similarly, at STB 436, the encrypted SI is
16 decrypted at CA system B 440 to provide tuning information for the set-top box,
17 allow a particular program to be tuned and displayed on television set 444.

18 An advantage of this approach is that no additional A/V bandwidth is
19 required in the content delivery system, e.g. cable system. Only the SI is dual
20 carried. No special hardware is required. Any offset frequencies from the standard
21 ones can be easily accommodated by most tuners. SI decryption can be performed
22 in software or can be aided by hardware. For example, legacy Motorola set-top
23 boxes have an ability to descramble the SI delivered in the Motorola out-of-band
24 using a hardware decrypter built into the decoder IC chip.

25 A determined hacker can potentially use a spectrum analyzer on the coax
26 cable to learn where the A/V channels are located. Also, it may be possible for the
27 hacker to program a set-top box to auto-scan the frequency band to learn where the
28 A/V channels are – a relatively slow process. If the A/V channel frequencies
29 changed dynamically, then that could foil the hackers, since they would need to be
30 constantly analyzing or scanning the band. Also, the program numbers and

1 assigned PIDs can vary. However, dynamically changing frequencies, program
2 numbers, and PIDs might create operational difficulties to a service provider, e.g.
3 cable operator.

4 5 GENERALIZED REPRESENTATION

6 Each of the above techniques can be represented generically by the system
7 500 of **FIGURE 10**. This system 500 has a cable system headend 522 with clear
8 video 504, clear audio 506, SI 528, and PSI 529 any of which can be selectively
9 switched through an intelligent processor controlled switch 518, which also serves
10 to assign PIDs (in embodiments requiring PID assignment or reassignment), to
11 conditional access system A 504 or conditional access system B 524 or passed
12 in the clear to the cable system 32. As previously, the program or SI encrypted
13 according to the legacy CA system A can be properly decoded by STB 36. The CA
14 system B encrypted information is understood by STBs 536 and decrypted and
15 decoded accordingly, as described previously.

16 17 PID MAPPING CONSIDERATIONS

18 The PID mapping concepts described above can be generally applied to the
19 dual partial encryption techniques described herein, where needed. At the cable
20 headend, the general concept is that a data stream of packets is manipulated to
21 duplicate packets selected for encryption. Those packets are duplicated and
22 encrypted under two distinct encryption methods. The duplicated packets are
23 assigned separate PIDs (one of which matches the legacy CA PID used for clear
24 content) and reinserted in the location of the original selected packet in the data
25 stream for transmission over the cable system. At the output of the cable system
26 headend, a stream of packets appears with the legacy encrypted packets and clear
27 packets having the same PID. A secondary PID identifies the packets that are
28 encrypted under the new encryption system. In addition to the PID remapping that
29 takes place at the headend, MPEG packets utilize a continuity counter to maintain
30 the appropriate sequence of the packets. In order to assure proper decoding, this

continuity counter should be properly maintained during creation of the packetized data stream at the headend. This is accomplished by assuring that packets with each PID are assigned continuity counters sequentially in a normal manner. Thus, packets with the secondary PID will carry a separate continuity counter from those of the primary PID. This is illustrated below in simplified form where PID 025 is the primary PID and PID 125 is the secondary PID, E represents an encrypted packet, C represents a clear packet, and the end number represents a continuity counter.

025C04	025E05	125E11	025C06	025C07	025C08	025C09	125E12
--------	--------	--------	--------	--------	--------	--------	--------

In this exemplary segment of packets, packets with PID 025 are seen to have their own sequence of continuity counters (04, 05, 06, 07, 08, 09, ...). Similarly, the packets with secondary PID 125 also have their own sequence of continuity counters (11, 12, ...).

At the STB, the PIDs can be manipulated in any number of ways to correctly associate the encrypted packets with secondary PID with the correct program. In one implementation, the packet headers of an input stream segment illustrated below:

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10
--------	--------	--------	--------	--------	--------	--------	--------

are manipulated to create the following output stream segment:

125C04	025E11	125E05	125C06	125C07	125C08	125C09	125E10
--------	--------	--------	--------	--------	--------	--------	--------

The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). For the encrypted packets, the primary PID and secondary PID are retained, but the continuity counters are swapped. Thus, the stream of packets can now be properly decrypted and decoded without errors

1 caused by loss of continuity using the secondary PID. Other methods for
2 manipulation of the PIDs, e.g. mapping the PID (125) on the scrambled legacy
3 packet to a NOP PID (all ones) or other PID value not decoded, and the continuity
4 counters can also be used in embodiments consistent with the present invention.

5 The primary and secondary PIDs are conveyed to the STBs in the program
6 map table (PMT) transmitted as a part of the program system information (PSI)
7 data stream. The existence of a secondary PID can be established to be ignored
8 by the STB operating under CA encryption system A (the "legacy" system), but new
9 STBs operating under CA encryption system B are programmed to recognize that
10 secondary PIDs are used to convey the encrypted part of the program associated
11 with the primary PID. The set-top boxes are alerted to the fact that this encryption
12 scheme is being used by the presence of a CA descriptor in the elementary PID "for
13 loop" of the PMT. There typically would be a CA descriptor for the video
14 elementary PID "for loop", and another one in the audio elementary PID "for loop".
15 The CA descriptor uses a Private Data Byte to identify the CA_PID as either the
16 ECM PID or the secondary PID used for partial scrambling, thus setting up the STB
17 operating under system B to look for both primary and secondary PIDs associated
18 with a single program. Since the PID field in the transport header is thirteen bits
19 in length, there are 2^{13} or 8,192 PIDs available for use, any spare PIDs can be
20 utilized for the secondary PIDs as required.

21 In addition to the assignment of a PID for each program component or
22 selected portion thereof, a new PID may be assigned to tag ECM data used in the
23 second encryption technique. Each PID number assigned can be noted as a user
24 defined stream type to prevent disrupting operation of a legacy STB. MPEG
25 defines a reserved block of such numbers for user defined data stream types.

26 While conceptually the PID mapping at the cable headend is a simple
27 operation, in practice the cable headend equipment is often already established
28 and is therefore modified to accomplish this task in a manner that is minimally
29 disruptive to the established cable system while being cost effective. Thus, the
30 details of the actual implementation within the cable system headend are

1 somewhat dependent upon the actual legacy hardware present in the headend,
2 examples of which are described in greater detail below.

3 4 Headend IMPLEMENTATIONS

5 Those skilled in the art will appreciate that the above descriptions as related
6 to **FIGURES 2, 3, 6, 9 and 10** are somewhat conceptual in nature and are used to
7 explain the overall ideas and concepts associated with the various embodiments
8 of the present invention. In realizing a real world implementation of the present
9 invention, those skilled in the art will recognize that a significant real world issue
10 to contend with is providing a cost effective implementation of the various partial
11 encryption methods within existing legacy headend equipment at established cable
12 providers. Taking two of the primary legacy cable systems as examples, the
13 following describes how the above techniques can be implemented at a cable
14 headend.

15 First, consider a cable system headend using a Motorola brand conditional
16 access system. In such a system the modifications shown in **FIGURE 11** can be
17 done to provide a cost effective mechanism for partial dual encryption
18 implementation. In a typical Motorola system, a HITS (Headend In The Sky) or
19 similar data feed is provided from a satellite. This feed provides aggregated
20 digitized content that is supplied to cable providers and is received by a receiver /
21 descrambler / scrambler system 604 such as the Motorola Integrated Receiver
22 Transcoder (IRT) models IRT 1000 and IRT 2000, and Motorola Modular Processing
23 System (MPS). A clear stream of digitized television data can be obtained from the
24 satellite descrambler functional block 606 of the receiver / descrambler / scrambler
25 604. This clear stream can be manipulated by a new functional block shown as
26 packet selector / duplicator 610. This new block 610 may be implemented as a
27 programmed processor or may be otherwise implemented in hardware, software
28 or a combination thereof.

1 Packet selector / duplicator 610 selects packets that are to be dual
2 encrypted under any of the above partial dual encryption methods. Those packets
3 are then duplicated with new PIDs so that they can be later identified for encryption.
4 For example, if packets at the input of 610 associated with a particular program
5 have PID A, then packet selector / duplicator 610 identifies packets to be encrypted
6 and duplicates those packets and remaps them to PIDs B and C respectively, so
7 that they can be identified later for encryption under two different systems.
8 Preferably, the duplicate packets are inserted into the data stream adjacent one
9 another in the location of the originally duplicated packet now with PID C so that
10 they remain in the same order originally presented (except that there are two
11 packets where one previously resided in the data stream). Assume, for the
12 moment, that the new CA system to be added is NDS encryption. In this case, PID
13 A will represent clear packets, PID B will represent NDS encrypted packets and
14 PID C will represent Motorola encrypted packets. The packets having PID B may
15 be encrypted under the NDS encryption at this point in 610 or may be encrypted
16 later.

17 The packets with PIDs B and C are then returned to the system 604 where
18 packets with PID C are encrypted under Motorola encryption at cable scrambler
19 612 as instructed by the control system 614 associated with the Motorola
20 equipment. The output stream from cable scrambler 612 then proceeds to another
21 new device - PID remapper and scrambler 620, which receives the output stream
22 from 612 and now remaps the remaining packets with PID A to PID C and encrypts
23 the PID B packets under the NDS encryption algorithm under control of control
24 system 624. The output stream at 626 has clear unencrypted packets with PID C
25 and selected packets which have been duplicated and encrypted under the
26 Motorola encryption system with PID C along with encrypted packets under the
27 NDS encryption system with PID B. This stream is then modulated (e.g.,
28 Quadrature Amplitude Modulated and RF modulated) for distribution over the cable
29 system. The preferred embodiment maps the unencrypted packets on PID A to
30 match the scrambled packets on PID C because the audio and video PIDs called

1 out in legacy program specific information (PSI) is correct that way. The control
2 computer, the scrambler, and legacy set-top boxes only know about PID C.
3 Alternatively, the scrambled packets on PID C could be mapped back to PID A, but
4 this would likely mean editing the PSI, that was automatically generated, to map
5 the PID numbers from PID C back to PID A in the PID remapper and scrambler
6 620.

7 In the above example, the PID remapper and scrambler 620 may also be
8 used to demultiplex PSI information, modify it to reflect the addition of the NDS
9 encryption (through the use of CA descriptors in the PMT) and multiplex the
10 modified PSI information back into the data stream. The ECMs to support NDS
11 encryption may also be inserted into the data stream at PID remapper and
12 scrambler 620 (or could be inserted by packet selector / duplicator 610).

13 Thus, in order to add NDS encryption (or another encryption system) to a
14 cable system headend using Motorola equipment, packets are duplicated and PIDs
15 are remapped in the data stream from the satellite descrambler. The remapped
16 PIDs are then used to identify packets that are to be scrambled under each CA
17 system. Once the legacy system encryption has taken place, the clear PID is then
18 remapped so that both clear and encrypted packets in the legacy system share the
19 same PID (or PIDs). PID remapping as in 620 and packet selection and duplication
20 as in 610 can be implemented using a programmed processor or using custom or
21 semi-custom integrated circuitry such as an application specific integrated circuit
22 or a programmable logic device or field programmable gate array. Other
23 implementations are also possible without departing from the present invention.

24 **FIGURE 12** depicts a similar equipment configuration such as that used in
25 implementing the partial dual encryption of the present invention in a Scientific
26 Atlanta based cable headend. In this embodiment, the HITS feed or similar is
27 received at IRD 704 which incorporates a satellite descrambler 706. This may be
28 a Motorola IRT or MPS with only the satellite descrambler function enabled. The
29 output of the satellite descrambler 706 again provides a clear data stream that can
30 be manipulated by a new packet selector / duplicator 710 which selects packets

1 to be encrypted, duplicates them and maps the PIDs of the duplicate packets to
2 new PIDs. Again, for example, packets to remain in the clear are assigned PID A,
3 packets to be encrypted under the new system (e.g., NDS) are assigned PID B and
4 packets to be encrypted under the Scientific Atlanta encryption system are
5 assigned PID C. The packets with PID B may be encrypted at this point under the
6 NDS encryption system.

7 The stream of packets is then sent to a multiplexer 712 (e.g., a Scientific
8 Atlanta multiplexer) where the packets having PID C are encrypted under the
9 Scientific Atlanta encryption system at 714 under control of control system 718
10 associated with multiplexer 712. The stream of data is then supplied internal to
11 multiplexer 712 to a QAM modulator 720. In order to properly remap the packets,
12 the QAM modulated signal at the output of multiplexer 712 is provided to a new
13 processor system 724 where the QAM modulated signal is demodulated at a QAM
14 demodulator 730 and the clear PID A packets are remapped to PID C at PID
15 remapper 734 under control of a control system 738. Encryption under the NDS
16 encryption algorithm can also be carried out here rather than in 710. The data
17 stream with remapped PIDs and dual partial encryption is then QAM and RF
18 modulated at 742 for distribution over the cable system.

19 In the above example, the PID remapper and scrambler 734 may also be
20 used to demultiplex PSI information, modify it to reflect the addition of the NDS
21 encryption (adding the CA descriptors to the PMT) and multiplex the modified PSI
22 information back into the data stream. The ECMs to support NDS encryption may
23 also be inserted into the data stream at PID remapper and scrambler 734 (or could
24 be inserted by packet selector / duplicator 710). PID remapping and or scrambling
25 as in 734 along with QAM demodulation and QAM modulation as in 730 and 742
26 respectively, and packet selection and duplication as in 710 can be implemented
27 using a programmed processor or using custom or semi-custom integrated circuitry
28 such as an application specific integrated circuit or a programmable logic device
29 or field programmable gate array. Other implementations are also possible without
30 departing from the present invention.

1 The above embodiments of the present invention allow legacy scrambling
2 equipment to scramble only the packets desired in an elementary stream instead
3 of the entire elementary stream. The scrambling of certain packets of an
4 elementary stream is accomplished by using a PID number for packets that are not
5 going to be scrambled, e.g., PID A. Packets that will be scrambled will be placed
6 on PID C. The scrambling equipment will scramble the packets on PID C (the ones
7 that have been selected for scrambling). After the scrambling has taken place, the
8 unscrambled packets have the PID number mapped to the same as the scrambled
9 packet – PID A becomes PID C. The legacy set-top boxes will receive an
10 elementary stream with both scrambled and un-scrambled packets.

11 The packets in these embodiments are handled as a stream. The entire
12 stream is sent to the legacy scrambling equipment for scrambling. This keeps all
13 of the packets in exact time synchronous order. If packets were extracted from a
14 stream and sent to the legacy scrambling equipment, time jitter might be
15 introduced. The present embodiment avoids that problem by keeping all the
16 packets in a stream. The embodiment does not require cooperation from the
17 legacy scrambling equipment provider because that equipment is not involved in
18 the remapping of packets- from PID A to PID C. This remapping is preferable
19 because the PID called out by the PSI generated by the legacy scrambling system
20 does not need to change. The legacy system knows about PID C, but not PID A.
21 The entire elementary stream to be scrambled by the legacy scrambling equipment
22 is found on a single PID that the scrambling system has been instructed to
23 scramble.

24 In the above examples, the use of NDS as the second encryption system
25 should not be considered limiting. Moreover, although two widely used systems -
26 Motorola and Scientific Atlanta have been depicted by way of example, similar
27 modifications to legacy systems to permit PID remapping and dual partial
28 encryption can be used. In general, the technique described above involves the
29 process generally described as 800 in **FIGURE 13**. A feed is received at 806 which
30 is descrambled as it is received at 810 to produce a clear data stream of packets.

1 At 814, packets are selected according to the desired partial dual encryption
2 technique (e.g., audio only, packets containing PES header, etc.). At 818, the
3 selected packets are duplicated and the duplicate pairs are remapped to two new
4 PIDs (e.g., PID B and PID C). The duplicated packets are then encrypted based
5 upon PID (that is, PID C is encrypted according to legacy encryption and PID B is
6 encrypted according to the new encryption system) at 822. The clear packets (e.g.,
7 PID A) are then remapped to the same PID as the legacy encrypted PID (PID C) at
8 826.

9 The order in which some of the elements of the process of **FIGURE 13** are
10 carried out can vary according to the particular legacy system being modified to
11 accommodate the particular dual encryption arrangement being used. For
12 example, encryption under a new encryption system can be carried out either at the
13 time of duplication or later at the time of remapping the legacy packets, as
14 illustrated in **FIGURE 11** and **12**. Additionally, various demodulation and re-
15 modulation operations can be carried out as needed to accommodate the particular
16 legacy system at hand (not shown in **FIGURE 13**).

17 SET-TOP BOX IMPLEMENTATIONS

18 Several set-top box implementations are possible within the scope of the
19 present invention. The method used at the headend to select packets for
20 encryption is irrelevant to the STB.

21 One such implementation is illustrated in **FIGURE 14**. In this embodiment,
22 packets from a tuner and demodulator 904 are provided to a decoder circuit 908's
23 demultiplexer 910. The packets are buffered into a memory 912 (e.g., using a
24 unified memory architecture) and processed by the STB's main CPU 916 using
25 software stored in ROM memory 920.

26 Selected PIDs can be stripped from the incoming transport via the STB's PID
27 filter, decrypted and buffered in SDRAM, similar to the initial processing required
28 in preparation for transfer to an HDD in a PVR application. The host CPU 916 can
29

1 then "manually" filter the buffered data in SDRAM for elimination of the packets
2 containing unneeded PIDs. There are some obvious side effects to this process.

3 The host overhead is estimated to be about 1% of the bandwidth of the CPU.
4 In the worst case, this is equivalent to 40K bytes/Second for a 15 Mbit/S video
5 stream. This reduction is possible since at most only 4 bytes of each packet is
6 evaluated and the location is on 188 byte intervals so the intervening data does not
7 have to be considered. Each packet header in SDRAM can therefore be directly
8 accessed through simple memory pointer manipulation. Additionally, Packets are
9 cached in blocks and evaluated en masse to reduce task switching of the host.
10 This would eliminate an interrupt to other tasks upon the reception of each new
11 packet. This may produce a increased latency for starting decode of a stream upon
12 channel change to allow time for cache fill. This may be negligible depending upon
13 the allocated SDRAM cache buffer size.

14 The host filtered packets in the SDRAM buffer are then transferred to the AV
15 Queue through existing hardware DMA processes and mimics a PVR
16 implementation. The filtered packets are then provided to the decoder 922 for
17 decoding.

18 A second technique for implementation in a set-top box is illustrated in
19 **FIGURE 15**. Since RISC processor AV decoder module in 930 processes the
20 partial transport PIDs and strips/concatenates for decode, the firmware within
21 decoder IC 930 can be altered to exclude individual packets in a partial transport
22 stream based upon criteria in each packet header. Alternatively, the demultiplexer
23 910 can be designed to exclude the packets. Legacy scrambled packet(s) pass
24 through the CA module still encrypted. By using the decoder IC 930 to perform the
25 removal of the legacy scrambled packets and assuming that the packets encrypted
26 under the new encryption algorithm (e.g., NDS) is immediately adjacent the legacy
27 encrypted packet (or at least prior to next primary stream video packet) then the
28 pruning of the legacy packet in effect accomplishes the merging of a single, clear
29 stream into the header strip and video queue.

1 A third technique for implementation of partial decryption in a set-top box is
2 illustrated in **FIGURE 16**. In this embodiment, the PID remapping is carried out
3 either within a circuit such as an ASIC, Field Programmable Gate Array (FPGA),
4 or a programmable logic device (PLD) 938 or other custom designed circuit placed
5 between the tuner and demodulator 904 and the decoder IC 908. In a variation of
6 this embodiment, the decoder IC 908 can be modified to implement the PID
7 remapping within demultiplexer 940. In either case, the legacy encrypted packets
8 are dropped and the non-legacy packets re-mapped either in circuit 938 or
9 demultiplexer 940.

10 This third technique can be implemented in one embodiment using the PLD
11 depicted in **FIGURE 17**. This implementation assumes that there will be not be
12 more than one encrypted packet of a particular PID appearing in a row, thus, the
13 implementation could be modified to accommodate bursts of encrypted packets
14 such as with the M and Nth encryption arrangement described above (as will be
15 explained later). The input stream passes through a PID identifier 950 which
16 serves to demultiplex the input stream based upon PID. Primary PID packets are
17 checked for continuity at 958. If a continuity error is detected, the error is noted and
18 the counter is reset at 960.

19 The original input packet stream contains packets tagged with many PIDs.
20 The PID identifier 950 separates packets with the two PIDs of interest (primary and
21 secondary PIDs) from all other packets. This capability can be scaled to process
22 multiple PID pairs. These other packets are bypassed directly to the revised output
23 stream. This processing results in a three or four byte clocking delay.

24 Packets with the secondary PID are routed by the PID identifier 950 to a
25 continuity count checker 954 which verifies sequence integrity for this PID. Any
26 errors are noted at 956, but specific handling of errors is not relevant to
27 understanding the present invention. The packet's continuity value is preserved for
28 use in checking the sequence of packets to follow. A corresponding continuity

1 check 958 is done for packets with the primary PID using the independent primary
2 counter, and again any errors are noted at 960.

3 The secondary packet is checked for a secondary flag at 962. This Boolean
4 indicator is used to remember if a secondary packet has been processed since the
5 last clear packet. More than one secondary packet between clear packets is an
6 error in this embodiment and is noted at 964. Presence of a secondary packet is
7 remembered by setting the secondary flag at 966.

8 The continuity counter of the secondary packet is changed at 968 to fit into
9 the sequence of the clear packets. Data for this substitution comes from the value
10 used to verify continuity of the primary stream at 958. The revised packet is sent
11 out from 968 and merged into the revised stream forming the output stream.

12 After packets with primary PIDs have had their continuity checked at 958,
13 they are differentiated at 970 by the scrambling flags in the header. If the packet
14 is scrambled, the primary flag is queried at 974. This primary flag Boolean
15 indicator is used to remember if a primary encrypted packet has been processed
16 since the last clear packet. More than one encrypted primary packet between clear
17 packets is an error in this embodiment and is noted at 976 before the packet is
18 discarded at 978. Presence of a encrypted primary packet is remembered by
19 setting the primary flag at 980. If there is no downstream consumer for the primary
20 encrypted packet, it can be discarded at 978. In some cases it may be necessary
21 for the packet to continue on (in which case its continuity counter can use the
22 discarded secondary continuity value).

23 If the primary PID scramble test at 970 detects a clear packet, the state of
24 the secondary and primary flags is tested at 984. Valid conditions are neither set
25 and both set, since encrypted packets should come in matched pairs. A sequence
26 of one without the other should be noted as an error at 988. However, the order of
27 appearance is inconsequential in this embodiment. It should be noted that there
28 may be other ways to flag a primary packet for deletion other than the scrambling
29 bits in the transport header, e.g. the transport_priority bit. Also, it is possible not

1 to use any bits what-so-ever, e.g. using the primary packet's simple positional
2 information, before or after the secondary packet, as an indicator for replacement.

3 Clear packets with the primary PID then have their PID value changed at 992
4 to the secondary PID before being output in the revised output stream.
5 Alternatively, the secondary PID packets can be remapped to the primary PID
6 value. The content can be decoded when the decoder is provided with the correct
7 PID for decoding the content (whether the primary or secondary PID). Presence of
8 a clear packet also clears the primary and secondary Boolean flags.

9 In all the embodiments proposed, the secondary packet can be inserted
10 adjoining the primary packet to be replaced even when a series of primary packets
11 are tagged for replacement. However, in some instances, it may facilitate headend
12 partial scrambling if multiple encrypted packets can be inserted into the stream
13 without the intervening secondary packets. In order to accommodate multiple
14 consecutive encrypted packets (such as with the Mth and N partial encryption
15 method), the use of primary and secondary flags can be replaced with a counter
16 matching test function. Thus, in place of elements 962, 964 and 966, a secondary
17 encrypted packet counter can be incremented. In place of elements 970, 974, 976
18 and 980, a primary encrypted packet counter can be incremented. Element 984
19 can be replaced with a comparison of the primary and secondary encrypted packet
20 counters to assure that the same number of encrypted packets are received in both
21 the primary and secondary paths. Instead of clearing flags at 992, the counters are
22 cleared. Using this variation, multiple encrypted packets may be consecutively
23 received and the number received are compared to monitor the integrity of the data
24 stream. Other variations will occur to those skilled in the art.

25 The function described above in connection with **FIGURE 17** can be
26 integrated into an A/V decoder chip that functions similar to that of the
27 commercially available Broadcom series 70xx or 71xx decoder used in commercial
28 set-top boxes. **FIGURE 18** illustrates a block diagram for such a decoder chip
29 where the functions already provided in the commercial chip are essentially

1 unchanged. Normally, commercial decoder chips expect there to be a one-to-one
2 correspondence between the PIDs and program components (e.g., audio or video).

3 The decoder illustrated in **FIGURE 18** permits multiple PIDs to be
4 programmed into the decoder via a connection to the STB central processor so that
5 both primary and secondary PIDs can be handled for main audio, main video and
6 a secondary video used for picture-in-picture (PiP) functions. In this embodiment,
7 the raw data stream is received by a Packet sorter 1002 that provides a function
8 similar to that described in connection with **FIGURE 17** above to demultiplex the
9 stream of packets based upon PID. Preferably, the decoder of **FIGURE 18** carries
10 out the PID sorting function of 1002 using hard wired logic circuitry rather than
11 programmed software. Program guide and stream navigation information is output
12 for use by an STB's main processor, for example. The packets associated with the
13 main audio program are buffered in a FIFO 1006, decrypted in a decrypter 1010
14 and then buffered at 1014 for retrieval by an MPEG audio decoder 1018 as needed.
15 Decoded MPEG audio is then provided as an output from the decoder.

16 In a similar manner, packets associated with the main video program are
17 buffered in a FIFO 1024, decrypted in a decrypter 1028 and then buffered at 1032
18 for retrieval by an MPEG video decoder 1036 as needed. Decoded MPEG video
19 for the main channel is then provided to a compositor 1040 and then provided as
20 an output from the decoder. Similarly, packets associated with picture-in-picture
21 video are buffered in a FIFO 1044, decrypted in a decrypter 1048 and then buffered
22 at 1052 for retrieval by an MPEG video decoder 1056 as needed. Decoded MPEG
23 video for the picture-in-picture channel is then provided to the compositor 1040
24 where it is combined with the main channel video and then provided as a decoded
25 video output from the decoder. Other packets not associated with the main or
26 picture-in-picture channel are discarded. Of course, other functions may be
27 incorporated in the decoder chip or deleted without departing from embodiments
28 of the present invention.
29

1 CONCLUSION

2 As previously mentioned, in order to thwart a persistent threat by hackers,
3 several of the above partial encryption arrangements can be combined to further
4 enhance security. For example, the critical packet encryption can be used in any
5 combination with SI encryption, Mth an N, random encryption, time slice and other
6 techniques to further enhance security. In one embodiment, as many packets
7 would be encrypted as bandwidth is available. The amount of encryption might
8 depend on whether the content was a regular program or premium (such as a pay-
9 per-view or VOD), whether it was an adult program or a regular movie, and the
10 security level that the various cable operators feel comfortable operating. Those
11 skilled in the art will appreciate that many other combinations are possible to
12 further enhance the security of the encryption without departing from the present
13 invention.

14 The present invention, as described above in its various embodiments, has
15 been described in terms of a digital A/V system using MPEG 2 coding. Thus, the
16 various packet names and protocol specifically discussed is related the MPEG 2
17 coding and decoding. However, those skilled in the art will appreciate that the
18 concepts disclosed and claimed herein are not to be construed in such a limited
19 scope. The same or analogous techniques can be used in any digital cable system
20 without limitation to MPEG 2 protocols. Moreover, the present techniques can be
21 used in any other suitable content delivery scenario including, but not limited to,
22 terrestrial broadcast based content delivery systems, Internet based content
23 delivery, satellite based content delivery systems such as, for example, the Digital
24 Satellite Service (DSS) such as that used in the DirecTVTM system, as well as
25 package media (e.g. CDs and DVDs). These various alternatives are considered
26 equivalent for purposes of this document, and the exemplary MPEG 2 cable
27 embodiment should be considered to be an exemplary embodiment presented for
28 illustrative purposes.

29 In addition, the present invention has been described in terms of decoding
30 partially encrypted television programs using a television set-top box. However, the

1 present decoding mechanism can equally be implemented within a television
2 receiver without need for an STB, or music player such as an MP3 player. Such
3 embodiments are considered equivalent.

4 Also, while the present invention has been described in terms of the use of
5 the encryption techniques described to provide a mechanism for dual partial
6 encryption of a television program, these partial encryption techniques could be
7 used as a single encryption technique or for multiple encryption under more than
8 two encryption systems without limitation. More than two encryption systems
9 would be accommodated with additional duplicated packets that are encrypted.
10 Alternatively, the encryption key for one of the duplicated packets may be shared
11 amongst the multiple encryption systems. Additionally, although specifically
12 disclosed for the purpose of encryption of television programming, the present
13 inventions can be utilized for single or dual encryption of other content including,
14 but not limited to content for download over the Internet or other network, music
15 content, packaged media content as well as other types of information content.
16 Such content may be played on any number of playback devices including but not
17 limited to personal digital assistants (PDAs), personal computers, personal music
18 players, audio systems, audio / video systems, etc. without departing from the
19 present invention.

20 Those skilled in the art will recognize that the present invention has been
21 described in terms of exemplary embodiments that can be realized by use of a
22 programmed processor. However, the invention should not be so limited, since the
23 present invention could be implemented using hardware component equivalents
24 such as special purpose hardware and/or dedicated processors which are
25 equivalents to the invention as described and claimed. Similarly, general purpose
26 computers, microprocessor based computers, micro-controllers, optical computers,
27 analog computers, dedicated processors and/or dedicated hard wired logic may be
28 used to construct alternative equivalent embodiments of the present invention.

29 Those skilled in the art will appreciate that the program steps and associated
30 data used to implement the embodiments described above can be implemented

1 using disc storage as well as other forms of storage such as for example Read
2 Only Memory (ROM) devices, Random Access Memory (RAM) devices; optical
3 storage elements, magnetic storage elements, magneto-optical storage elements,
4 flash memory, core memory and/or other equivalent storage technologies without
5 departing from the present invention. Such alternative storage devices should be
6 considered equivalents.

7 The present invention, as described in embodiments herein, can be
8 implemented using a programmed processor executing programming instructions
9 that are broadly described above in flow chart form that can be stored on any
10 suitable electronic storage medium or transmitted over any suitable electronic
11 communication medium. However, those skilled in the art will appreciate that the
12 processes described above can be implemented in any number of variations and
13 in many suitable programming languages without departing from the present
14 invention. For example, the order of certain operations carried out can often be
15 varied, additional operations can be added or operations can be deleted without
16 departing from the invention. Error trapping can be added and/or enhanced and
17 variations can be made in user interface and information presentation without
18 departing from the present invention. Such variations are contemplated and
19 considered equivalent.

20 While the invention has been described in conjunction with specific
21 embodiments, it is evident that many alternatives, modifications, permutations and
22 variations will become apparent to those skilled in the art in light of the foregoing
23 description. Accordingly, it is intended that the present invention embrace all such
24 alternatives, modifications and variations as fall within the scope of the appended
25 claims.
26

What is claimed:

1. A method of encrypting a digital television signal, comprising:
examining unencrypted packets of data in the digital television signal to identify a predetermined packet type;
encrypting packets identified as being of the predetermined packet type; and
replacing the unencrypted packets of the predetermined packet type with the encrypted packets in the digital television signal to produce a partially encrypted digital television signal.
2. The method according to claim 1, further comprising distributing the partially encrypted digital television signal.
3. The method according to claim 1, wherein the predetermined packet type comprises a packet carrying information that is needed to decode the digital television signal.
4. The method according to claim 1, wherein the digital television signal complies with an MPEG standard, and wherein the predetermined packet type comprises packets carrying a payload that comprises a packetized elementary stream (PES) header.
5. The method according to claim 1, wherein the digital television signal complies with the digital satellite service transport standard, and wherein the predetermined packet type comprises packets carrying a payload of a packetized elementary stream header.
6. The method according to claim 1, wherein the predetermined packet type comprises video packets carrying a payload of a video sequence header.
7. The method according to claim 1, wherein the predetermined packet type comprises video packets carrying a payload of a group of pictures header.

1 8. The method according to claim 1, wherein the predetermined packet type
2 comprises video packets carrying a payload of closed captioning information.
3

4 9. The method according to claim 1, further comprising assigning a packet
5 identifier to the unencrypted packets.
6

7 10. The method according to claim 9, further comprising assigning the packet
8 identifier to the encrypted packets.
9

10 11. The method according to claim 9, wherein the packet identifier comprises
11 a primary packet identifier; and further comprising assigning a secondary packet
12 identifier to the encrypted packets.
13

14 12. An electronic storage medium storing instructions which, when executed on
15 a programmed processor, carry out the method of encrypting a television signal
16 according to claim 1.
17

18 13. An electronic transmission medium carrying an encrypted television signal
19 encrypted by the method according to claim 1.
20

21 14. The method according to claim 1, wherein the television signal is
22 compressed, and wherein the predetermined packet type comprises a packet
23 carrying information that is needed to decompress the television signal.
24

25 15. The method according to claim 3, further comprising selecting packets
26 according to a second selection criteria and encrypting the selected packets.

1 16. A method of encrypting a digital television signal, comprising:
2 examining unencrypted packets of data in the digital television signal to
3 identify a predetermined packet type;
4 encrypting packets identified as being of the predetermined packet type
5 using a first encryption method to produce first encrypted packets;
6 encrypting the packets identified as being of the predetermined packet type
7 using a second encryption method to produce second encrypted packets; and
8 replacing the unencrypted packets of the predetermined packet type with the
9 first encrypted packets and the second encrypted packets in the digital television
10 signal to produce a partially dual encrypted television signal.
11

12 17. The method according to claim 16, further comprising distributing the
13 partially dual encrypted digital television signal.
14

15 18. The method according to claim 16, wherein the predetermined packet type
16 comprises a packet carrying information that is needed to decode the digital
17 television signal.
18

19 19. The method according to claim 17, wherein the television signal is
20 compressed, and wherein the predetermined packet type comprises a packet
21 carrying information that is needed to decompress the digital television signal.
22

23 20. The method according to claim 17, wherein the predetermined packet type
24 comprises packets carrying information needed to access the digital television
25 signal.
26

27 21. The method according to claim 17, wherein the digital television signal
28 complies with an MPEG standard, and wherein the predetermined packet type
29 comprises transport stream packets carrying a payload that comprises a
30 packetized elementary stream (PES) header.

1 22. The method according to claim 17, wherein the digital television signal
2 complies with the digital satellite service transport standard, and wherein the
3 predetermined packet type comprises packets carrying a payload of a packetized
4 elementary stream header.

5
6 23. The method according to claim 17, wherein the predetermined packet type
7 comprises video packets carrying a payload of a video sequence header.

8
9 24. The method according to claim 17, wherein the predetermined packet type
10 comprises video packets carrying a payload of a group of pictures header.

11
12 25. The method according to claim 17, wherein the predetermined packet type
13 comprises video packets carrying a payload of closed captioning information.

14
15 26. The method according to claim 17, further comprising assigning a packet
16 identifier to the unencrypted packets.

17
18 27. The method according to claim 26, further comprising assigning the packet
19 identifier to the first encrypted packets.

20
21 28. The method according to claim 17, further comprising assigning a secondary
22 packet identifier to the second encrypted packets.

23
24 29. An electronic storage medium storing instructions which, when executed on
25 a programmed processor, carry out the method of encrypting a digital television
26 signal according to claim 17.

27
28 30. An electronic transmission medium carrying an encrypted digital television
29 signal encrypted by the method according to claim 11.

1 31. A method of encrypting a digital television signal, comprising:
2 examining packets of data in the digital television signal to identify a
3 predetermined packet type;
4 encrypting packets identified as being of a predetermined packet type; and
5 distributing the digital television signal with encrypted packets of the
6 predetermined packet type along other packets that are unencrypted.

7
8 32. The method according to claim 31, wherein the encrypting comprises
9 encrypting packets identified as a packets that are needed to decode the digital
10 television signal.

11
12 33. The method according to claim 31, wherein the digital television signal is
13 compressed, and wherein the predetermined packet type comprises a packet type
14 that is needed to decompress the digital television signal.

15
16 34. The method according to claim 33, wherein the digital television signal
17 complies with an MPEG standard, and wherein the predetermined packet type is
18 identified as transport stream packet carrying a payload that comprises a
19 packetized elementary stream (PES) header.

20
21 35. The method according to claim 31, wherein the digital television signal
22 complies with the digital satellite service transport standard, and wherein the
23 predetermined packet type comprises packets carrying a payload of a packetized
24 elementary stream header.

25
26 36. The method according to claim 31, wherein the predetermined packet type
27 comprises video packets carrying a payload of a video sequence header.

28
29 37. The method according to claim 31, wherein the predetermined packet type
30 comprises video packets carrying a payload of a group of pictures header.

1 38. The method according to claim 31, wherein the predetermined packet type
2 comprises video packets carrying a payload of closed captioning information.
3

4 39. The method according to claim 31, wherein the digital television signal
5 complies with an MPEG standard, and wherein the predetermined packet type is
6 identified as a packet containing MPEG I-picture packets.
7

8 40. An electronic storage medium storing instructions which, when executed on
9 a programmed processor, carry out the method of encrypting a digital television
10 signal according to claim 31.
11
12

1 41. An encrypted television program, comprising:
2 a plurality of unencrypted packets; and
3 a plurality of encrypted packets, wherein the encrypted packets contain
4 information required to decode the television program.
5

6 42. The encrypted television program according to claim 41, wherein the
7 unencrypted packets and encrypted packets comprise transport stream packets.
8

9 43. The encrypted television program according to claim 41, wherein the
10 encrypted transport stream packets comprise packets containing MPEG packetized
11 elementary stream (PES) headers.
12

13 44. The encrypted television program according to claim 41, wherein the digital
14 television program complies with the digital satellite service transport standard, and
15 wherein the encrypted packets comprise packets carrying a payload of a
16 packetized elementary stream header.
17

18 45. The encrypted television program according to claim 41, wherein the
19 encrypted packets comprise video packets carrying a payload of a video sequence
20 header.
21

22 46. The encrypted television program according to claim 41, wherein the
23 encrypted packets comprise video packets carrying a payload of a group of pictures
24 header.
25

26 47. The encrypted television program according to claim 41, wherein the
27 encrypted packets comprise video packets carrying a payload of closed captioning
28 information.
29

1 48. The encrypted television program according to claim 41, wherein the digital
2 television program is encoded according to an MPEG standard, and wherein the
3 encrypted and unencrypted packets are identified by a packet identifier.
4

5 49. The encrypted television program according to claim 41, wherein the digital
6 television program is encoded according to an MPEG standard, and wherein the
7 unencrypted packets are identified by a primary packet identifier, and wherein the
8 encrypted packets are identified by a secondary packet identifier.
9

10 50. The method according to claim 41, wherein the television program is
11 compressed, and wherein the predetermined packet type comprises a packet type
12 that is required to decompressing the television program.
13
14

1 51. A television set-top box, comprising:
2 a receiver receiving a digital television signal comprising:
3 a plurality of unencrypted packets; and
4 a plurality of encrypted packets, wherein the encrypted packets
5 contain information required to decode the digital television signal;
6 a decrypter that decrypts the encrypted packets; and
7 a decoder that decodes the unencrypted packets and the decrypted packets
8 to produce a signal suitable for play on a television set.

9
10 52. The apparatus according to claim 51, wherein the unencrypted packets and
11 encrypted packets comprise transport stream packets.

12
13 53. The apparatus according to claim 51, wherein the encrypted transport
14 stream packets comprise packets containing MPEG packetized elementary stream
15 (PES) headers.

16
17 54. The apparatus according to claim 51, wherein the digital television signal
18 complies with an MPEG standard, and wherein the encrypted and unencrypted
19 packets are identified by a packet identifier.

20
21 55. The apparatus according to claim 51, wherein the digital television signal
22 complies with an MPEG standard, and wherein the unencrypted packets are
23 identified by a primary packet identifier, and wherein the encrypted packets are
24 identified by a secondary packet identifier.

25
26 56. The apparatus according to claim 51, wherein the digital television signal is
27 compressed, and wherein the encrypted packets comprises a packet type that is
28 needed to decompress the digital television signal.

29

1 57. The apparatus according to claim 56, further comprising decompressing
2 means for decompressing the compressed digital television signal.
3

4 58. The apparatus according to claim 51, wherein the digital television signal
5 complies with the digital satellite service transport standard, and wherein the
6 encrypted packets comprise packets carrying a payload of a packetized elementary
7 stream header.
8

9 59. The apparatus according to claim 51, wherein the encrypted packets
10 comprise video packets carrying a payload of a video sequence header.
11

12 60. The apparatus according to claim 51, wherein the encrypted packets
13 comprise video packets carrying a payload of a group of pictures header.
14

15 61. The apparatus according to claim 51, wherein the encrypted packets
16 comprise video packets carrying a payload of closed captioning information.
17

1 62. A method of decoding a partially encrypted television program, comprising:
2 receiving a digital television program comprising a plurality of packets,
3 wherein certain packets of the plurality of packets are encrypted and a remainder
4 of the packets are unencrypted, wherein the encrypted packets contain information
5 that is required for correct decoding of the television program;
6 decrypting the encrypted packets to produce decrypted packets; and
7 decoding the decrypted packets and the unencrypted packets to produce a
8 decoded television signal.

9
10 63. The method according to claim 62, wherein the partially encrypted television
11 program is a digital television program, and wherein the certain encrypted packets
12 comprise packets that are needed to decode the television program.

13
14 64. The method according to claim 62, wherein the partially encrypted television
15 program is compressed, and wherein the certain packets comprises packets
16 carrying information that is needed to decompress the television program.

17
18 65. The method according to claim 64, wherein the partially encrypted television
19 program complies with an MPEG standard, and wherein the certain packets
20 comprise transport stream packets carrying a payload that comprises a packetized
21 elementary stream (PES) header.

22
23 66. An electronic storage medium storing instructions which, when executed on
24 a programmed processor, carry out the method of decrypting a television program
25 according to claim 64.

26
27 67. The method according to claim 64, wherein the receiving, decrypting and
28 decoding are carried out in a television device.
29

1 68. The method according to claim 67, wherein the television device comprises
2 a television set-top box.

3
4 69. The method according to claim 64, wherein the partially encrypted television
5 program complies with the digital satellite service transport standard, and wherein
6 the encrypted packets carry a payload of a packetized elementary stream header.

7
8 70. The method according to claim 64, wherein the encrypted packets comprise
9 video packets carrying a payload of a video sequence header.

10
11 71. The method according to claim 64, wherein the encrypted packets comprise
12 video packets carrying a payload of a group of pictures header.

13
14 72. The method according to claim 64, wherein the encrypted packets comprise
15 video packets carrying a payload of closed captioning information.
16

1 73. A method of decoding partially encrypted content, comprising:
2 receiving partially encrypted content comprising unencrypted content,
3 content encrypted under both a first encryption system and a second encryption
4 system, the encrypted content comprising information needed for correct decoding
5 of the partially encrypted content; and
6 decrypting the encrypted content under the first encryption system to
7 produce decrypted content.

8
9 74. The method according to claim 73, further comprising decoding the
10 unencrypted content and the decrypted content to decode the partially encrypted
11 content.

12
13 75. The method according to claim 73, wherein the partially encrypted content
14 comprises a digital television program, and wherein the encrypted content
15 comprises packets that are needed for correct decoding the television program.

16
17 76. The method according to claim 73, wherein the partially encrypted content
18 comprises a digital television program, and wherein the digital television program
19 is compressed, and wherein the encrypted content comprises packets carrying
20 information that is needed to decompress the television program.

21
22 77. The method according to claim 77, wherein the digital television program
23 complies with an MPEG standard, and wherein the encrypted content comprises
24 transport stream packets carrying a payload that comprises a packetized
25 elementary stream (PES) header.

26
27 78. The method according to claim 76, wherein the digital television signal
28 complies with the digital satellite service transport standard, and wherein the
29 encrypted packets carry a payload of a packetized elementary stream header.
30

1 79. The method according to claim 73, wherein the encrypted content comprises
2 video packets carrying a payload of a video sequence header.

3
4 80. The method according to claim 73, wherein the encrypted content comprises
5 video packets carrying a payload of a group of pictures header.

6
7 81. The method according to claim 73, wherein the encrypted content comprises
8 video packets carrying a payload of closed captioning information.

9
10 82. An electronic storage medium storing instructions which, when executed on
11 a programmed processor, carry out the method of decoding according to claim 73.

12
13 83. The method according to claim 73, wherein the receiving, decrypting and
14 decoding are carried out in a television device.

15
16 84. The method according to claim 73, wherein the television device comprises
17 a television set-top box.

18
19 85. The method according to claim 73, wherein the receiving, decrypting and
20 decoding are carried out in an integrated circuit.

21
22 86. The method according to claim 85, wherein the integrated circuit comprises
23 one of an application specific integrated circuit and a field programmable gate
24 array.

25
26 87. The method according to claim 73, wherein the receiving, decrypting and
27 decoding are carried out in a plurality of integrated circuits.

1 88. The method according to claim 87, wherein the plurality of integrated circuit
2 comprises at least one of an application specific integrated circuit and a field
3 programmable gate array.
4
5

1 89. A method of decoding a partially encrypted television program, comprising:
2 receiving the partially encrypted television program comprising a plurality of
3 clear packets, a plurality of packets encrypted under a first encryption algorithm,
4 and a plurality of packets encrypted under a second encryption algorithm;
5 wherein the packets encrypted under the first and second encryption
6 algorithms are packets that are needed for proper decoding of the television
7 program;
8 decrypting the packets encrypted under the first encryption algorithm to
9 produce decrypted packets; and
10 decoding the decrypted packets and the clear packets.

11
12 90. The method according to claim 89, wherein the television program
13 comprises a digital television program.

14
15 91. The method according to claim 89, wherein the partially encrypted television
16 program is compressed, and wherein the encrypted packets comprises packets
17 carrying information that is needed to decompress the television program.

18
19 92. The method according to claim 91, wherein the program is encoded
20 according to an MPEG standard, and wherein the encrypted packets comprise
21 transport stream packets carrying a payload that comprises a packetized
22 elementary stream (PES) header.

23
24 93. The method according to claim 89, wherein the partially encrypted television
25 program complies with the digital satellite service transport standard, and wherein
26 the encrypted packets carry a payload of a packetized elementary stream header.

27
28 94. The method according to claim 89, wherein the encrypted packets comprise
29 video packets carrying a payload of a video sequence header.

1 95. The method according to claim 89, wherein the encrypted packets comprise
2 video packets carrying a payload of a group of pictures header.

3
4 96. The method according to claim 89, wherein the encrypted packets comprise
5 video packets carrying a payload of closed captioning information.

6
7 97. An electronic storage medium storing instructions which, when executed on
8 a programmed processor, carry out the method of decoding a television signal
9 according to claim 89.

10
11 98. The method according to claim 89, wherein the receiving, decrypting and
12 decoding are carried out in an integrated circuit.

13
14 99. The method according to claim 98, wherein the integrated circuit comprises
15 an application specific integrated circuit.

16
17 100. The method according to claim 89, wherein the receiving, decrypting and
18 decoding are carried out in a television device.

19
20 101. The method according to claim 100, wherein the television device comprises
21 a television set-top box.

1 102. A method of decoding a partially encrypted television program, comprising:
2 receiving the partially encrypted television program comprising a plurality of
3 clear packets, a plurality of packets encrypted under a first encryption algorithm,
4 and a plurality of packets encrypted under a second encryption algorithm;
5 wherein the packets encrypted under the first and second encryption
6 algorithms are packets that are needed to properly decode the television program;
7 wherein the clear packets are identified by a first packet identifier;
8 wherein the packets encrypted under the first encryption algorithm are
9 identified by a second packet identifier (PID), and wherein the packets encrypted
10 under the second encryption algorithm are identified by a third packet identifier
11 (PID); and
12 decrypting the packets encrypted under the first encryption algorithm to
13 produce decrypted packets.
14

15 103. The method according to claim 102, further comprising decoding the
16 decrypted packets and the clear packets.
17

18 104. The method according to claim 102, wherein the partially encrypted
19 television program comprises a digital partially encrypted television program.
20

21 105. The method according to claim 102, wherein the partially encrypted
22 television program is compressed, and wherein the encrypted packets comprise
23 packets carrying information that is needed to decompress the television program.
24

25 106. The method according to claim 102, wherein the partially encrypted
26 television program complies with an MPEG standard, and wherein the encrypted
27 packets comprise transport stream packets carrying a payload that comprises a
28 packetized elementary stream (PES) header.
29

1 107. The method according to claim 102, wherein the partially encrypted
2 television program complies with the digital satellite service transport standard, and
3 wherein the encrypted packets carry a payload of a packetized elementary stream
4 header.

5
6 108. The method according to claim 102, wherein the encrypted packets
7 comprise video packets carrying a payload of a video sequence header.

8
9 109. The method according to claim 102, wherein the encrypted packets
10 comprise video packets carrying a payload of a group of pictures header.

11
12 110. The method according to claim 102, wherein the encrypted packets
13 comprise video packets carrying a payload of closed captioning information.

14
15 111. An electronic storage medium storing instructions which, when executed on
16 a programmed processor, carry out the method of decoding according to claim 102.

17
18 112. The method according to claim 102, wherein the receiving, decrypting and
19 decoding are carried out in an integrated circuit.

20
21 113. The method according to claim 112, wherein the integrated circuit comprises
22 one of an application specific integrated circuit and a field programmable gate
23 array.

24
25 114. The method according to claim 103, wherein the receiving, decrypting and
26 decoding are carried out in a television device.

27
28 115. The method according to claim 114, wherein the television device comprises
29 a television set-top box.

1 116. A method of encrypting a packetized stream of information, comprising:
2 examining packets of data in the stream of information to identify a
3 predetermined packet type, wherein the predetermined packet type is needed to
4 decode the data stream; and

5 encrypting packets identified as being of a predetermined packet type.
6

7 117. The method according to claim 116, wherein the stream of information
8 represents a television program and wherein the encrypting comprises encrypting
9 packets identified as a packets that are needed to decode the television program.
10

11 118. The method according to claim 116, wherein the television program is
12 compressed, and wherein the predetermined packet type comprises a packet type
13 that is needed to decompress the television program.
14

15 119. The method according to claim 116, wherein the television program
16 complies with an MPEG standard, and wherein the predetermined packet type is
17 identified as transport stream packet carrying a payload that comprises a
18 packetized elementary stream (PES) header.
19

20 120. The method according to claim 116, wherein the television program
21 complies with an MPEG standard, and wherein the predetermined packet type is
22 identified as a packet containing MPEG I-picture packets.
23

24 121. The method according to claim 116, wherein the television program
25 complies with the digital satellite service transport standard, and wherein the
26 predetermined packet type comprises packets carrying a payload of a packetized
27 elementary stream header.
28

29 122. The method according to claim 116, wherein the predetermined packet type
30 comprises video packets carrying a payload of a video sequence header.

1 123. The method according to claim 116, wherein the predetermined packet type
2 comprises video packets carrying a payload of a group of pictures header.

3
4 124. The method according to claim 116, wherein the predetermined packet type
5 comprises video packets carrying a payload of closed captioning information.

6
7 125. An electronic storage medium storing instructions which, when executed on
8 a programmed processor, carry out the method of encrypting a digital television
9 signal according to claim 116.
10

1 126. A method of manipulating packetized digital content, comprising:
2 examining unencrypted packets to identify a predetermined packet type;
3 duplicating the packets identified as being of the predetermined packet type
4 to produce first and second duplicate packets; and
5 inserting the first and second duplicate packets into the digital content to
6 produce partially duplicated content having first and second duplicate packets
7 instead of the identified packets.

8
9 127. The method according to claim 126, further comprising identifying the first
10 duplicate packets in the partially duplicated content and encrypting the first
11 duplicate packets to produce first encrypted duplicate packets.

12
13 128. The method according to claim 127, further comprising inserting the first
14 encrypted duplicated packets into the digital content in place of the first duplicate
15 packets to produce partially encrypted content.

16
17 129. The method according to claim 128, further comprising identifying the
18 second duplicate packets and encrypting the second duplicate packets to produce
19 second encrypted duplicate packets.

20
21 130. The method according to claim 129, further comprising inserting the second
22 encrypted duplicate packets into the digital content in place of the second duplicate
23 packets to produce partially dual encrypted content.

1 131. A method of manipulating packetized digital content, comprising:
2 examining unencrypted packets to identify a predetermined packet type;
3 duplicating the packets identified as being of the predetermined packet type
4 to produce first and second duplicate packets;
5 encrypting the first and second duplicate packets; and
6 inserting the first and second encrypted packets into the digital content to
7 produce partially encrypted content.

8
9 132. The method according to claim 131, wherein the first and second duplicate
10 packets are encrypted under first and second encryption algorithms.
11
12

1 133. A method of manipulating packetized digital content, comprising:
2 examining unencrypted packets to identify a predetermined packet type;
3 duplicating the packets identified as being of the predetermined packet type
4 to produce first and second duplicate packets;
5 encrypting the first duplicate packets; and
6 inserting the encrypted first duplicate packets into the digital content to
7 produce partially encrypted content.
8
9

1 134. A method of allowing multiple conditional access providers in a content
2 delivery system, comprising:

3 examining unencrypted packets of content to identify packets of a
4 predetermined type;

5 encrypting packets of the predetermined type using a first encryption method
6 used by a first conditional access provider to produce first encrypted packets;

7 encrypting packets of the predetermined type using a second encryption
8 method used by a second conditional access provider to produce second encrypted
9 packets;

10 replacing the packets of the predetermined type with the first and second
11 encrypted packets to produce partially dual encrypted content; and

12 distributing the partially dual encrypted content in the content delivery
13 system.

14
15 135. The method according to claim 134, further comprising combining
16 entitlement control messages for the first and second conditional access provider
17 with the partially encrypted content.
18
19
20

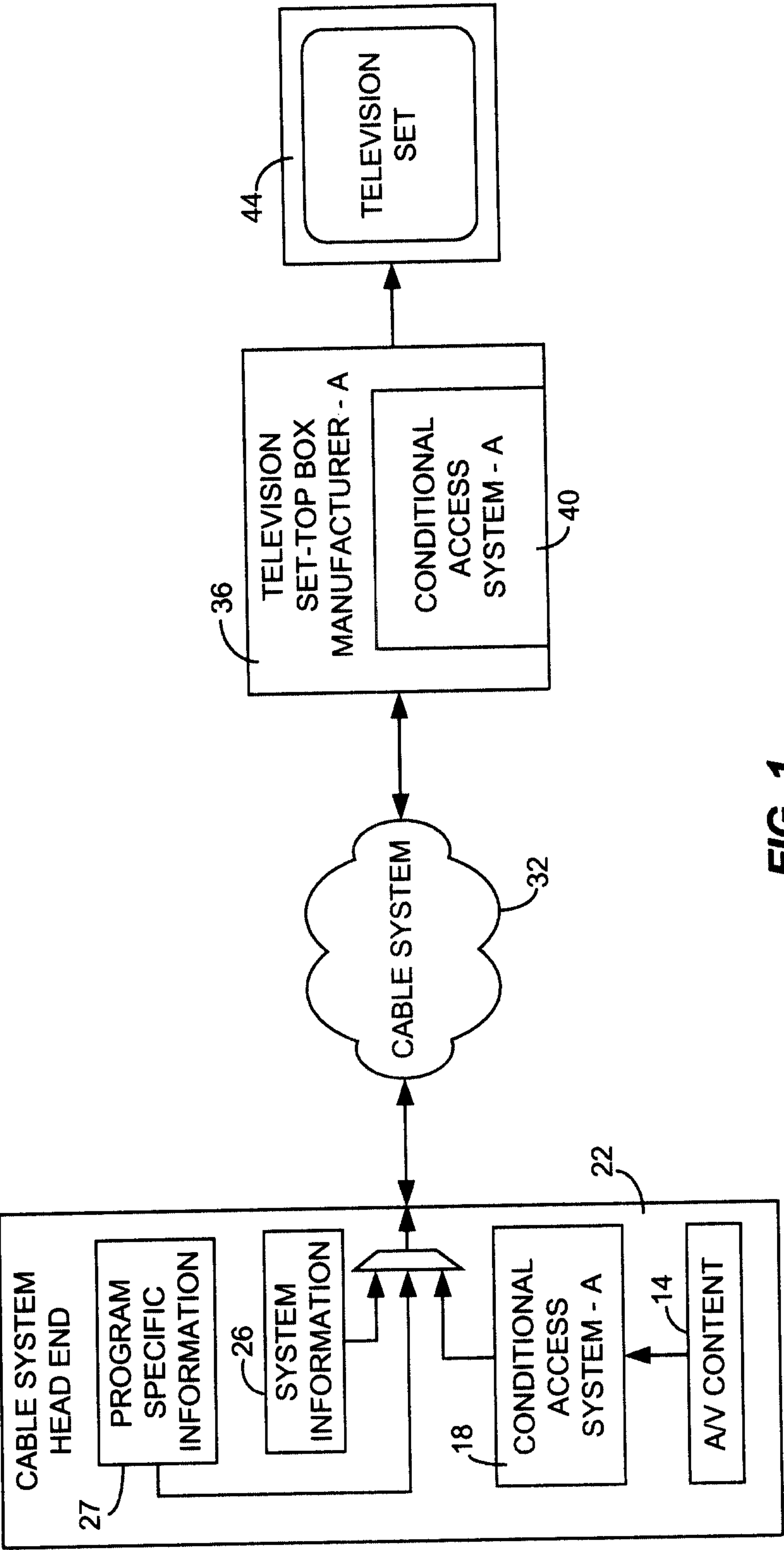


FIG. 1
(PRIOR ART)

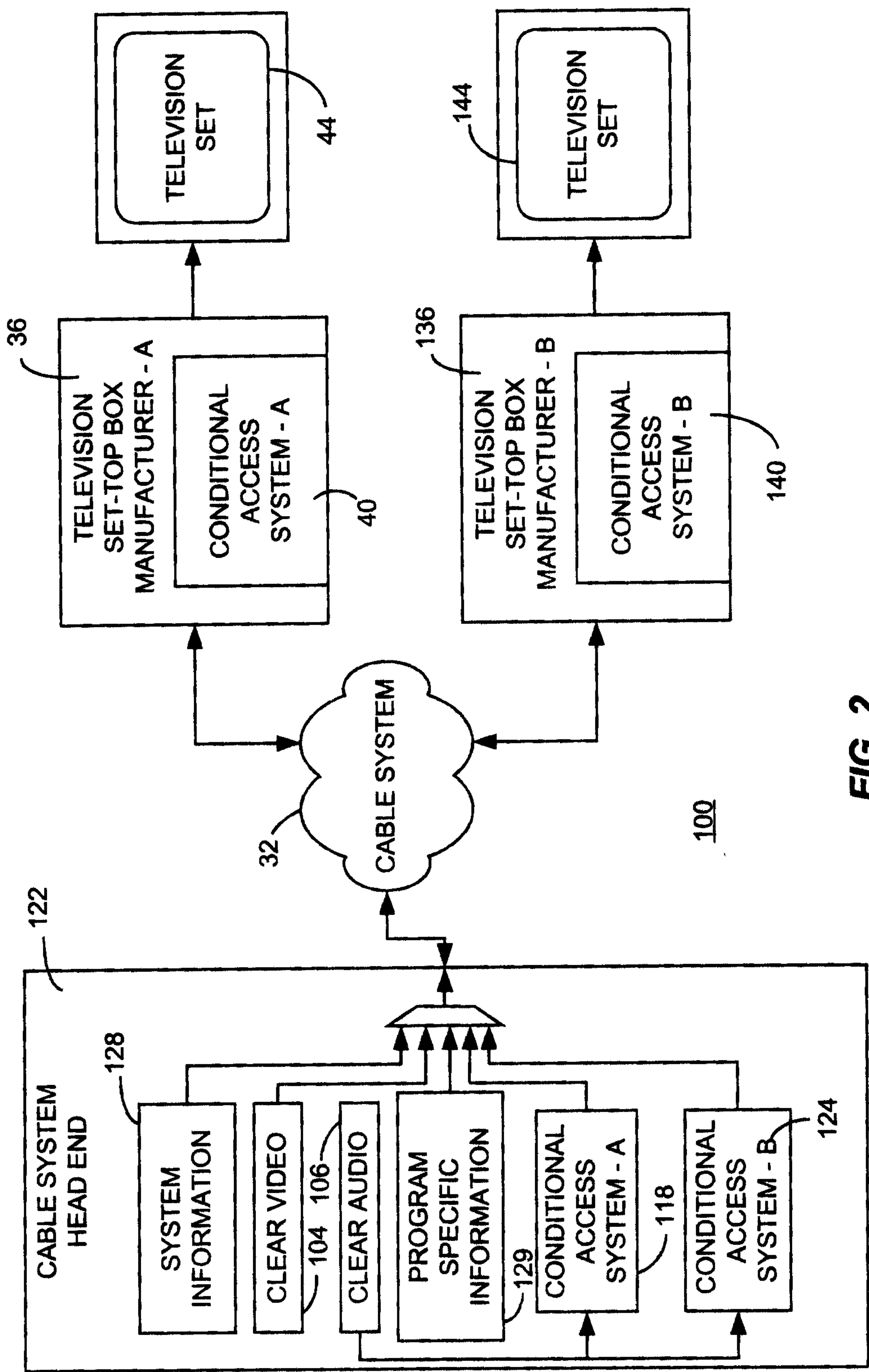


FIG. 2

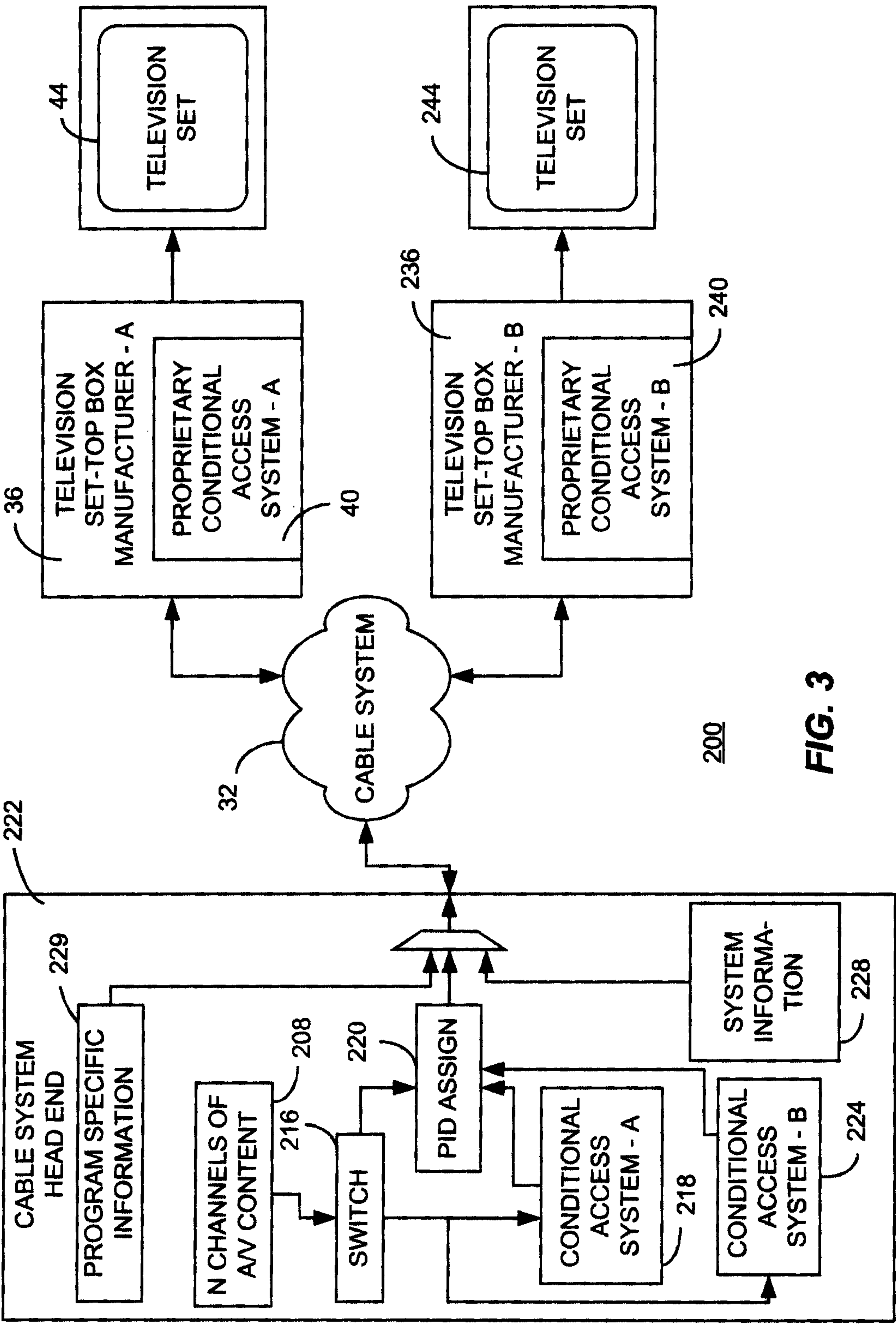
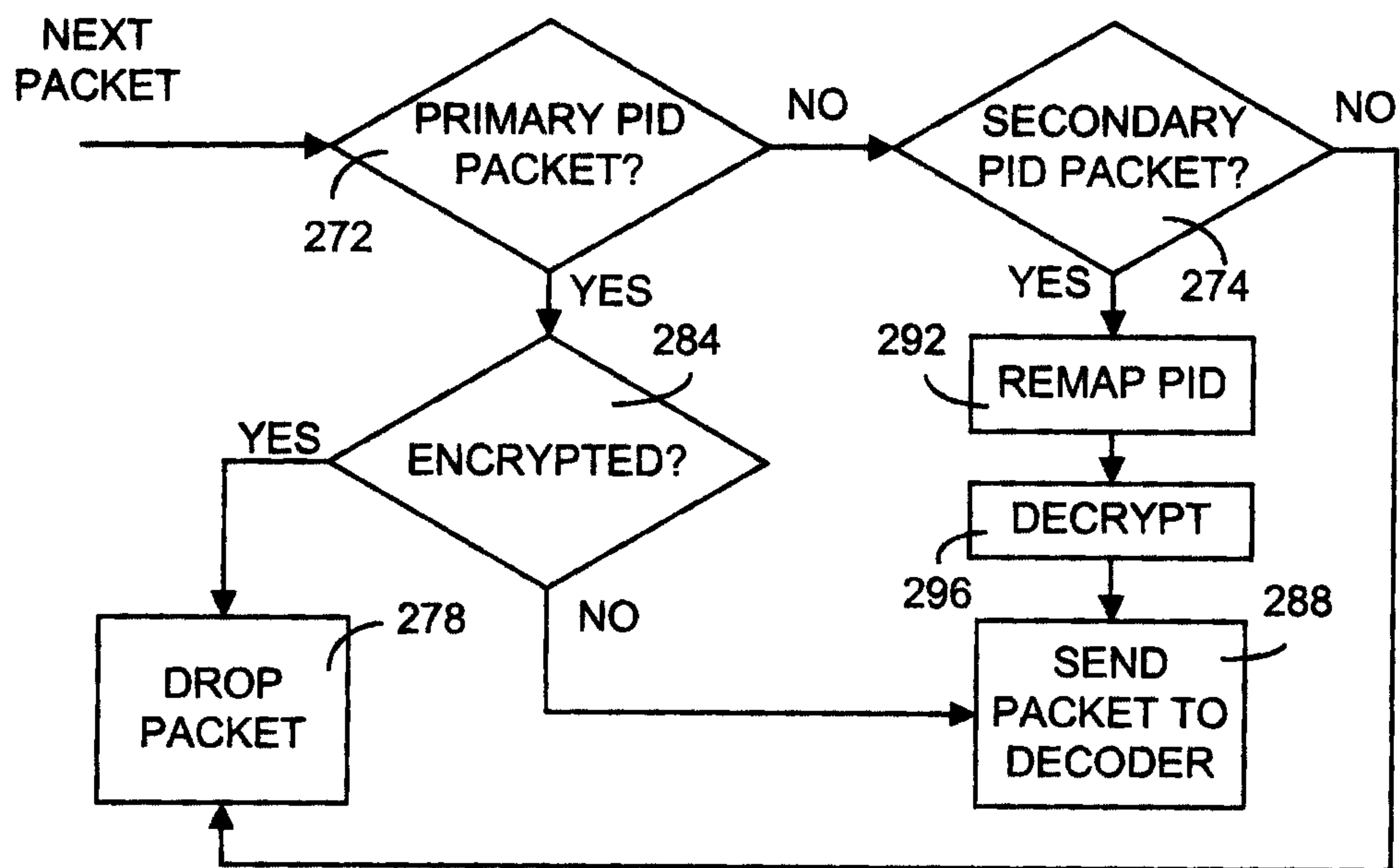
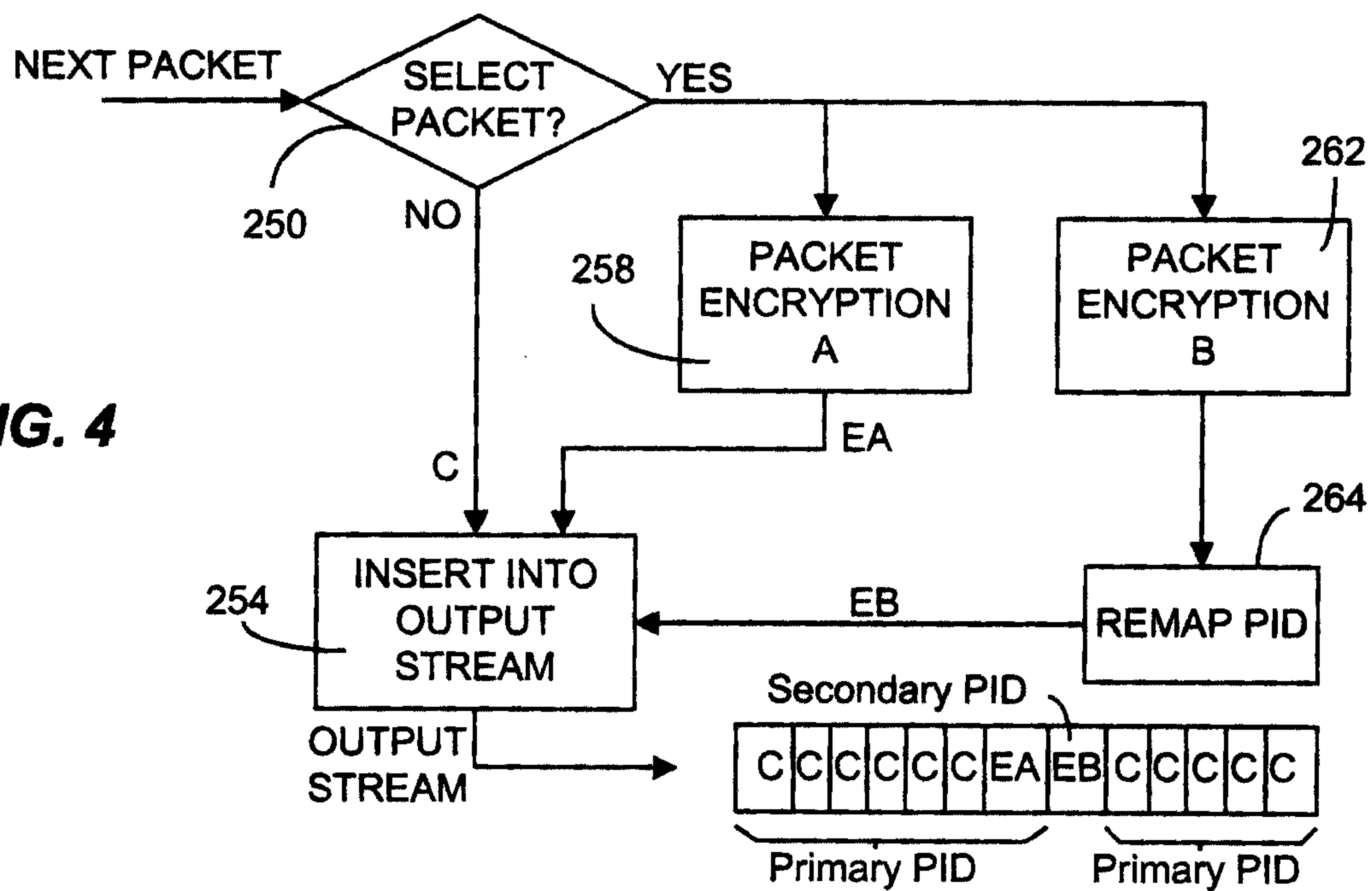


FIG. 3

FIG. 4**FIG. 5**

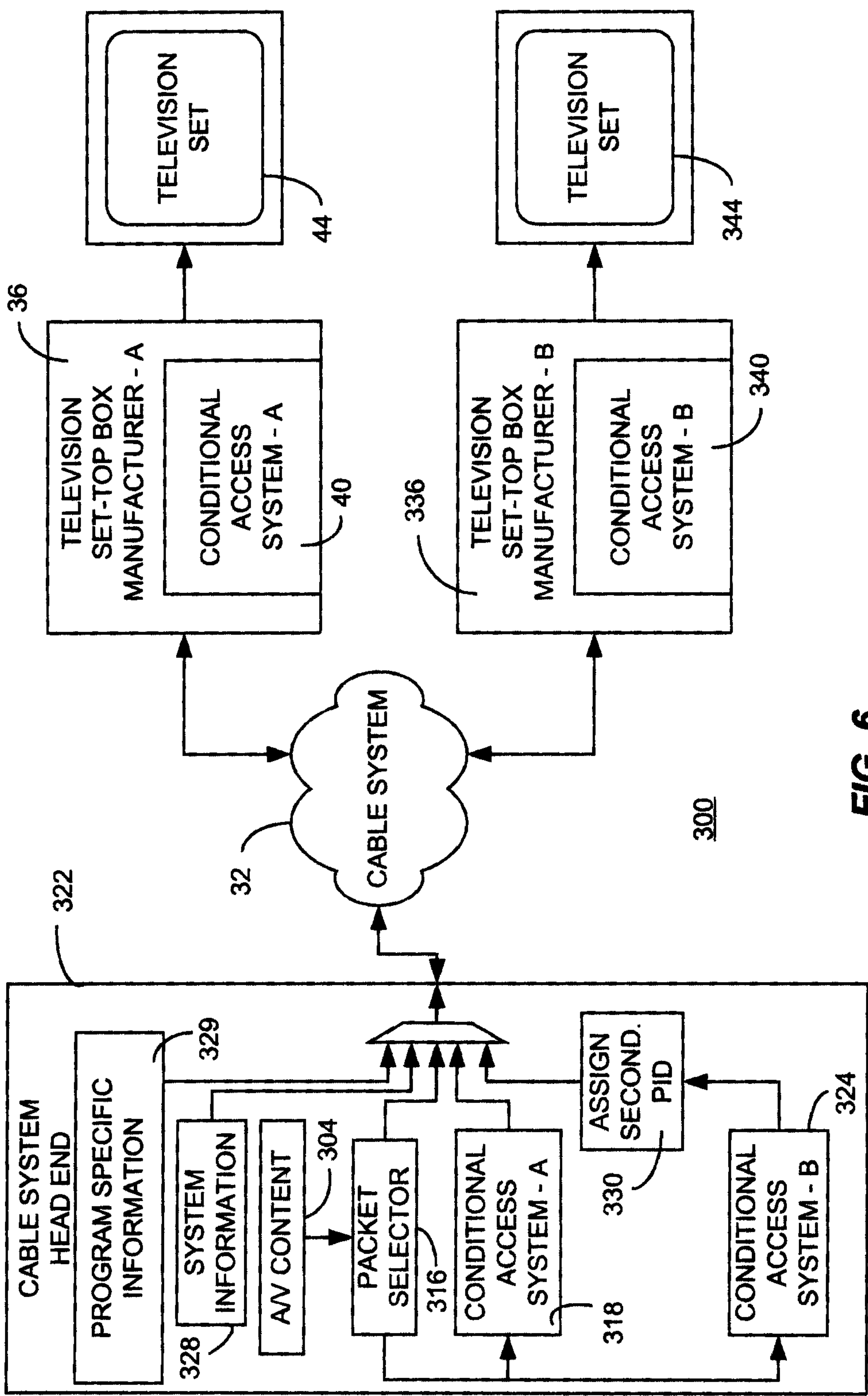
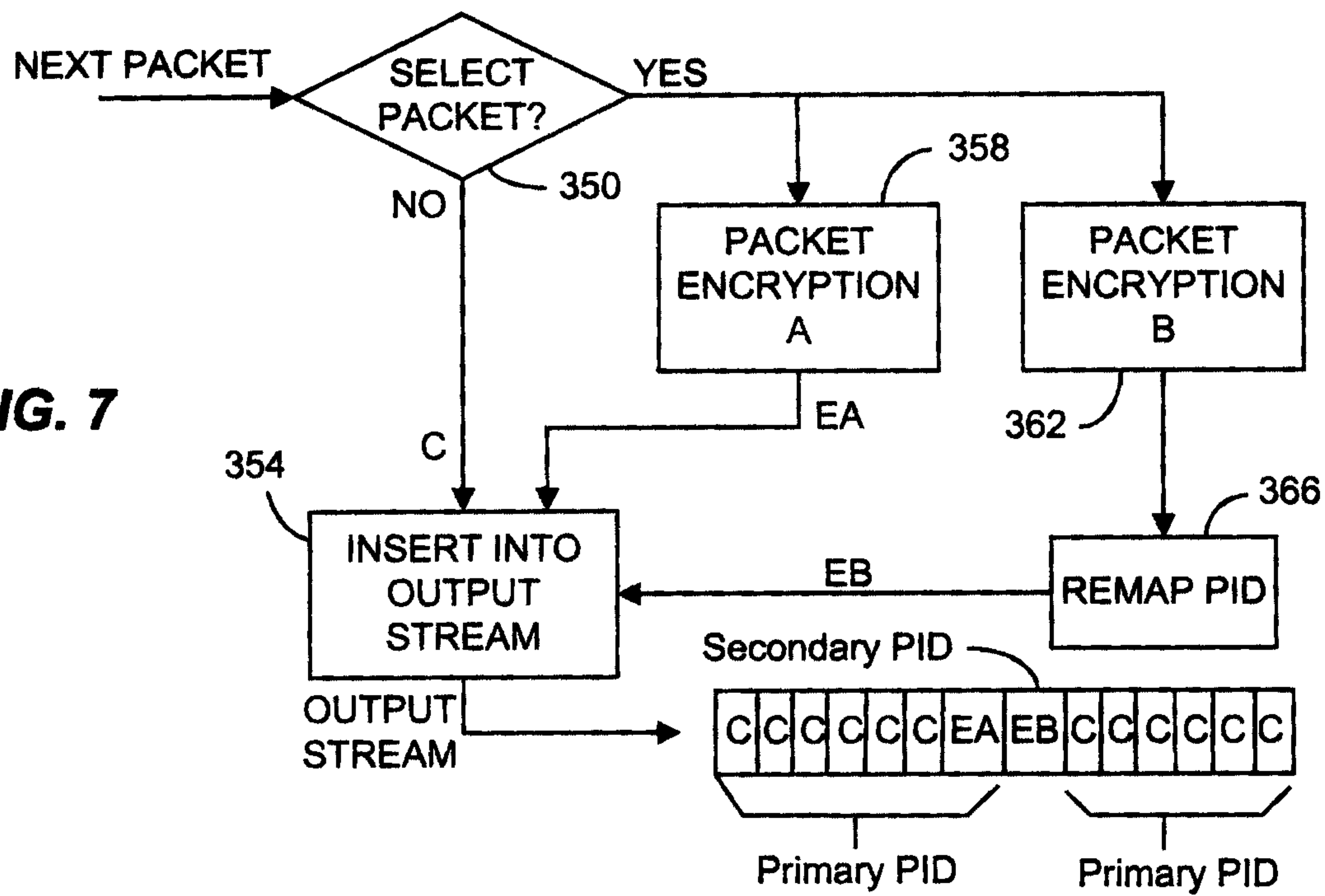
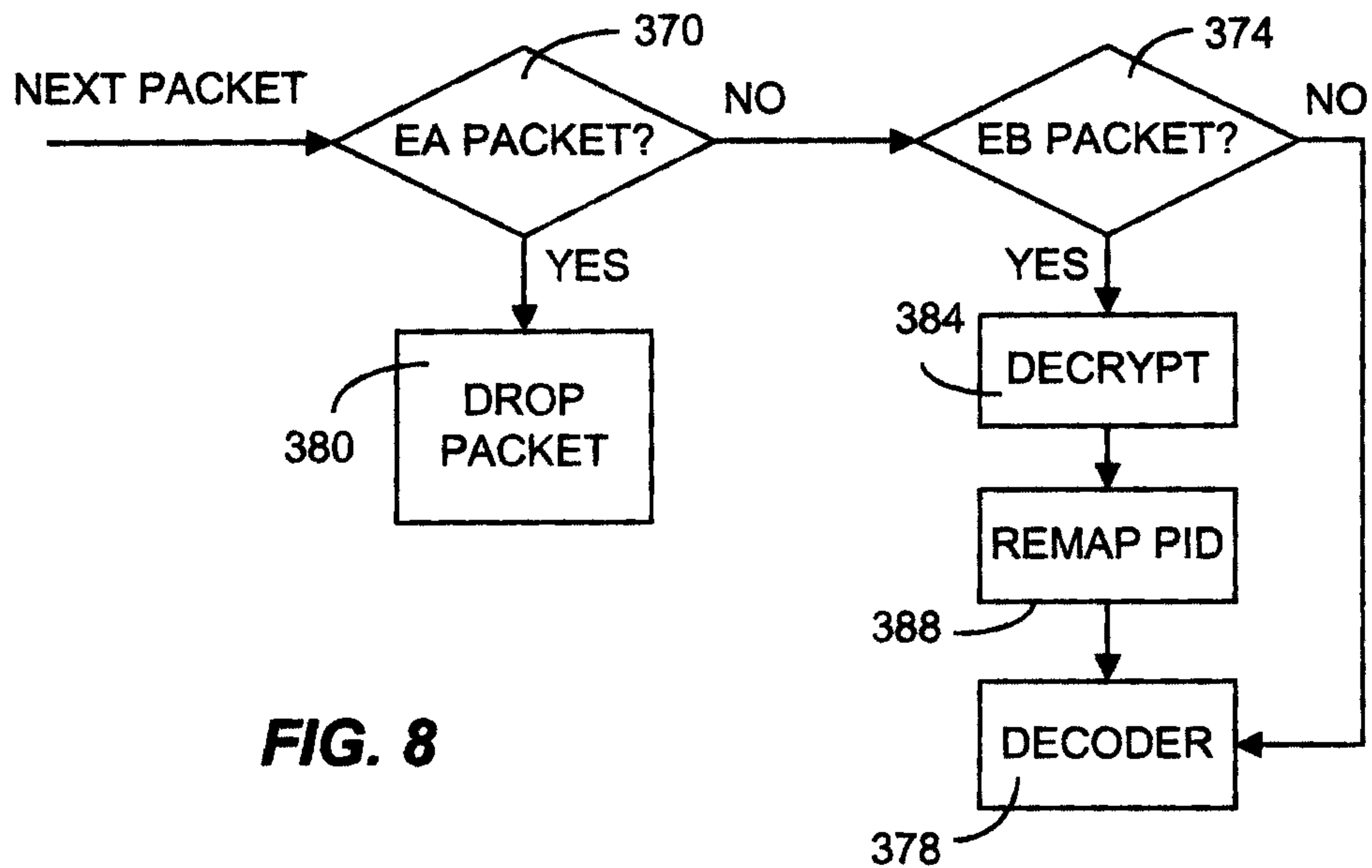


FIG. 6

FIG. 7**FIG. 8**

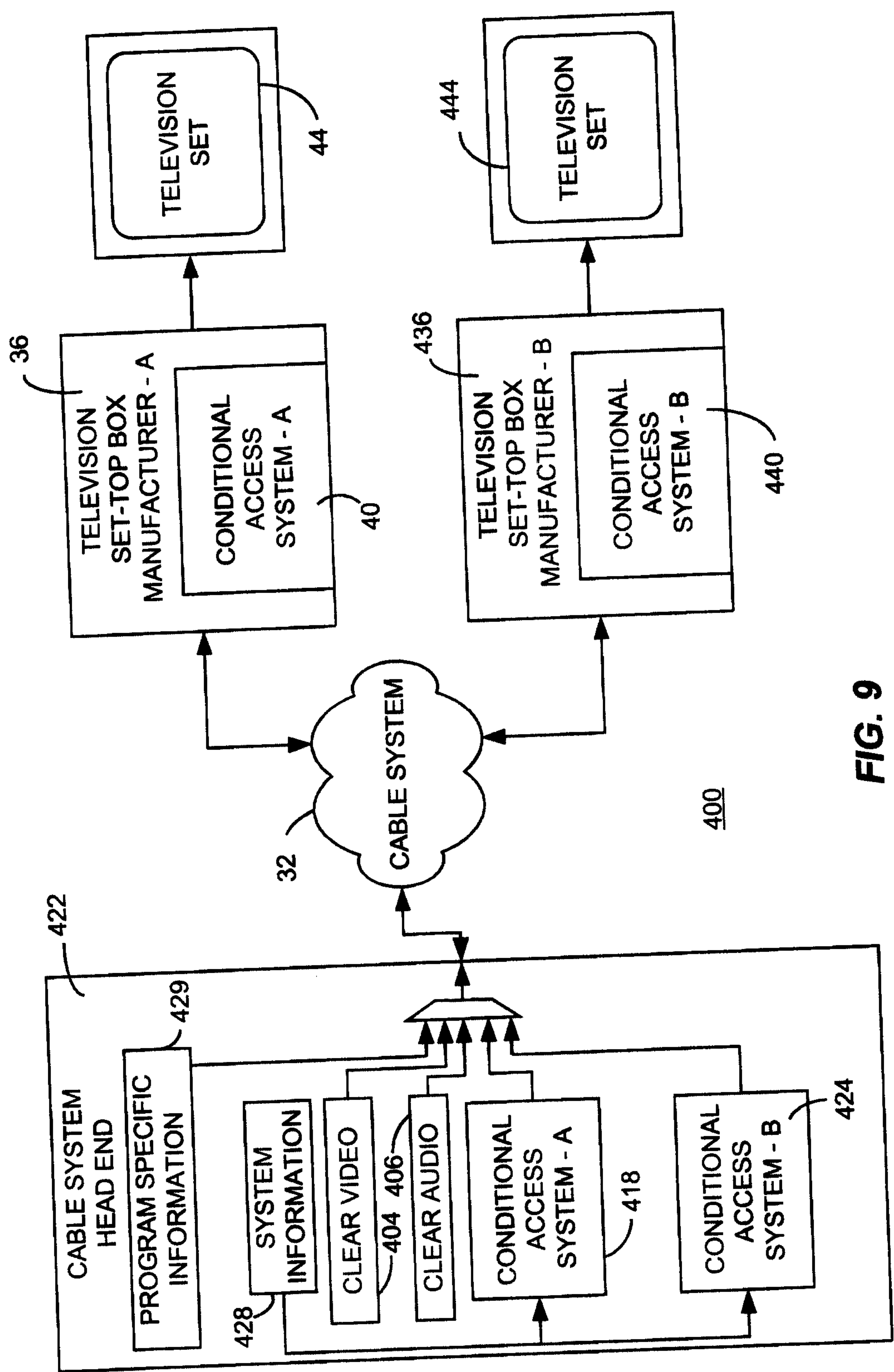


FIG. 9

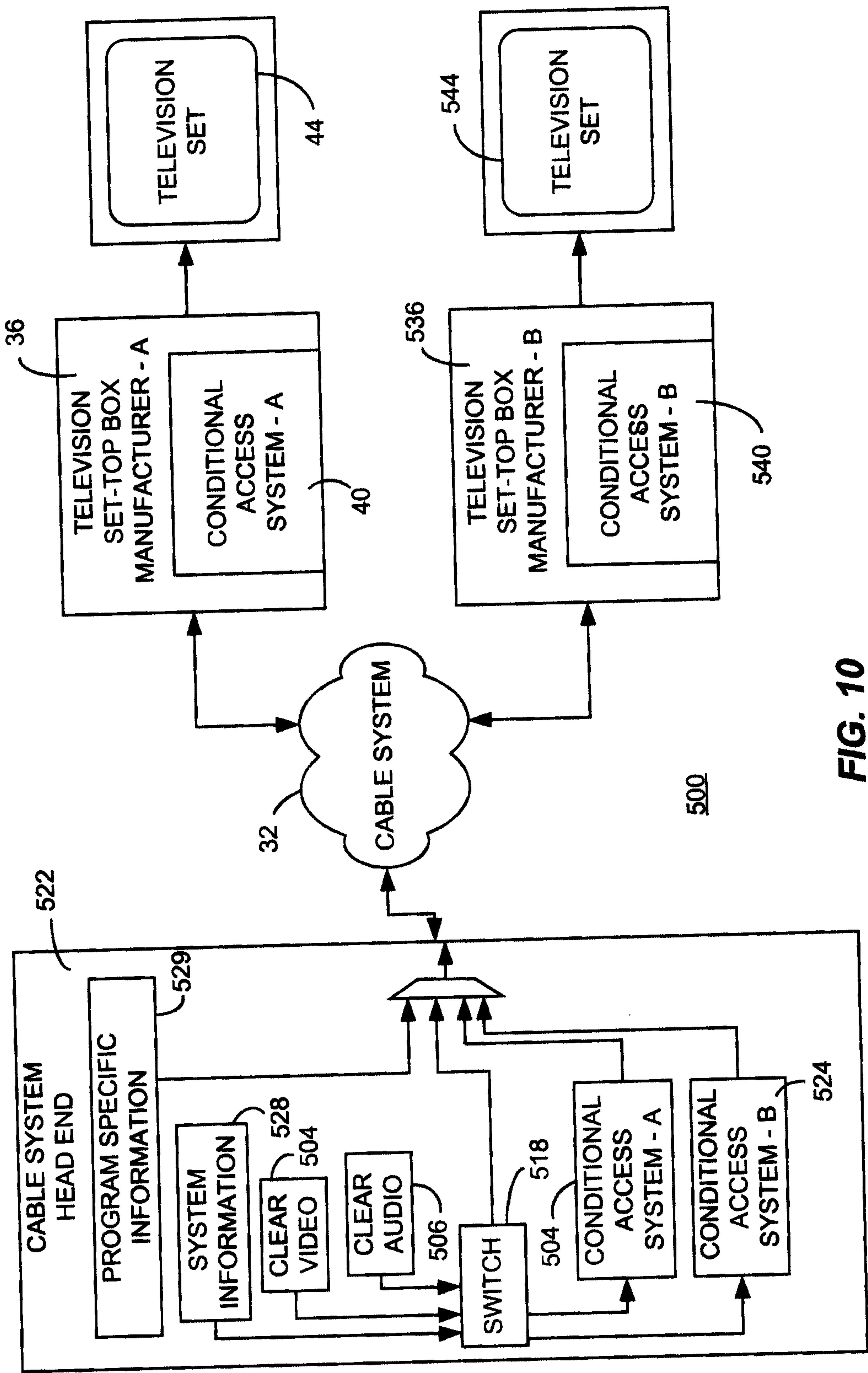


FIG. 10

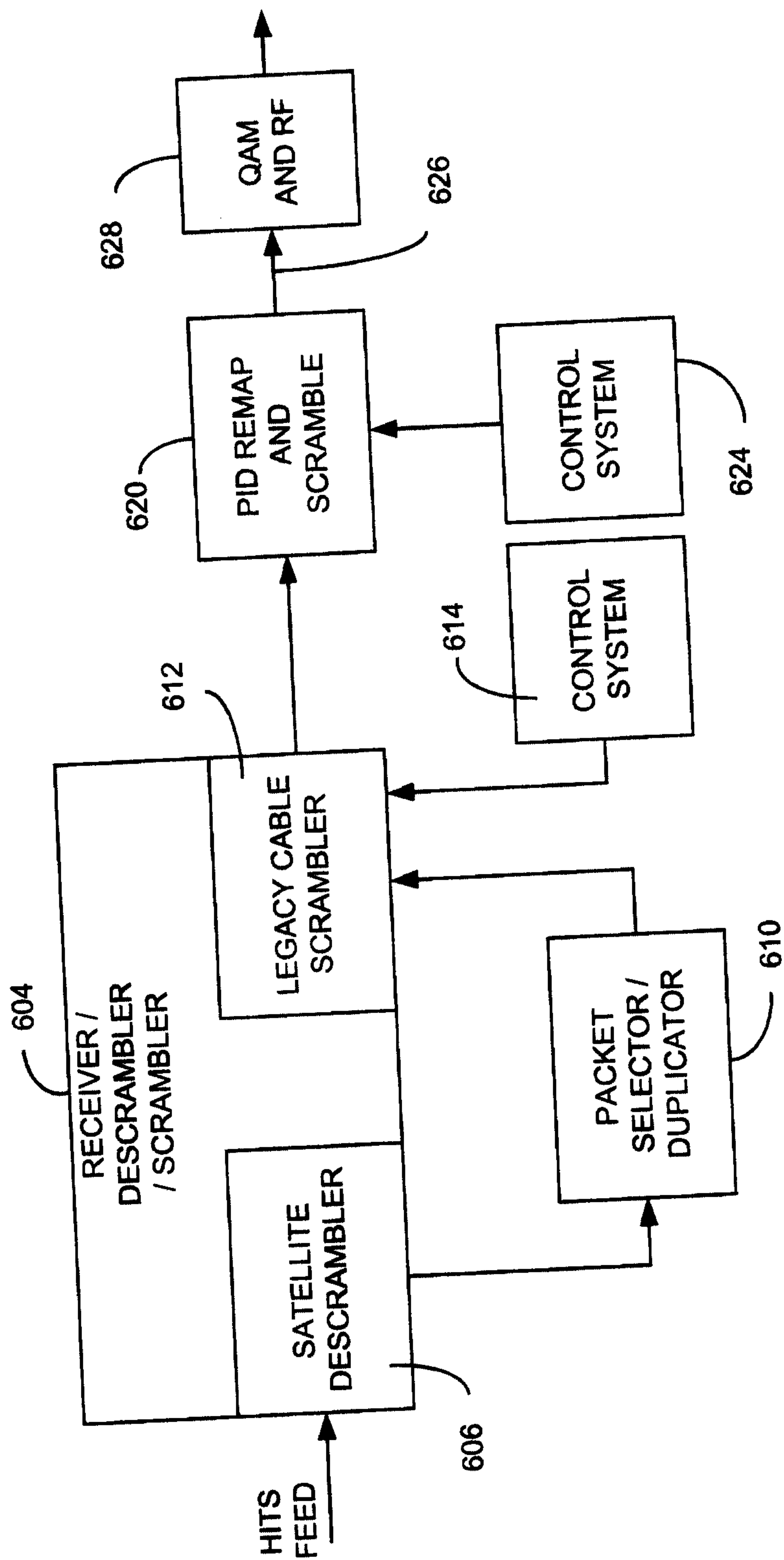


FIG. 11

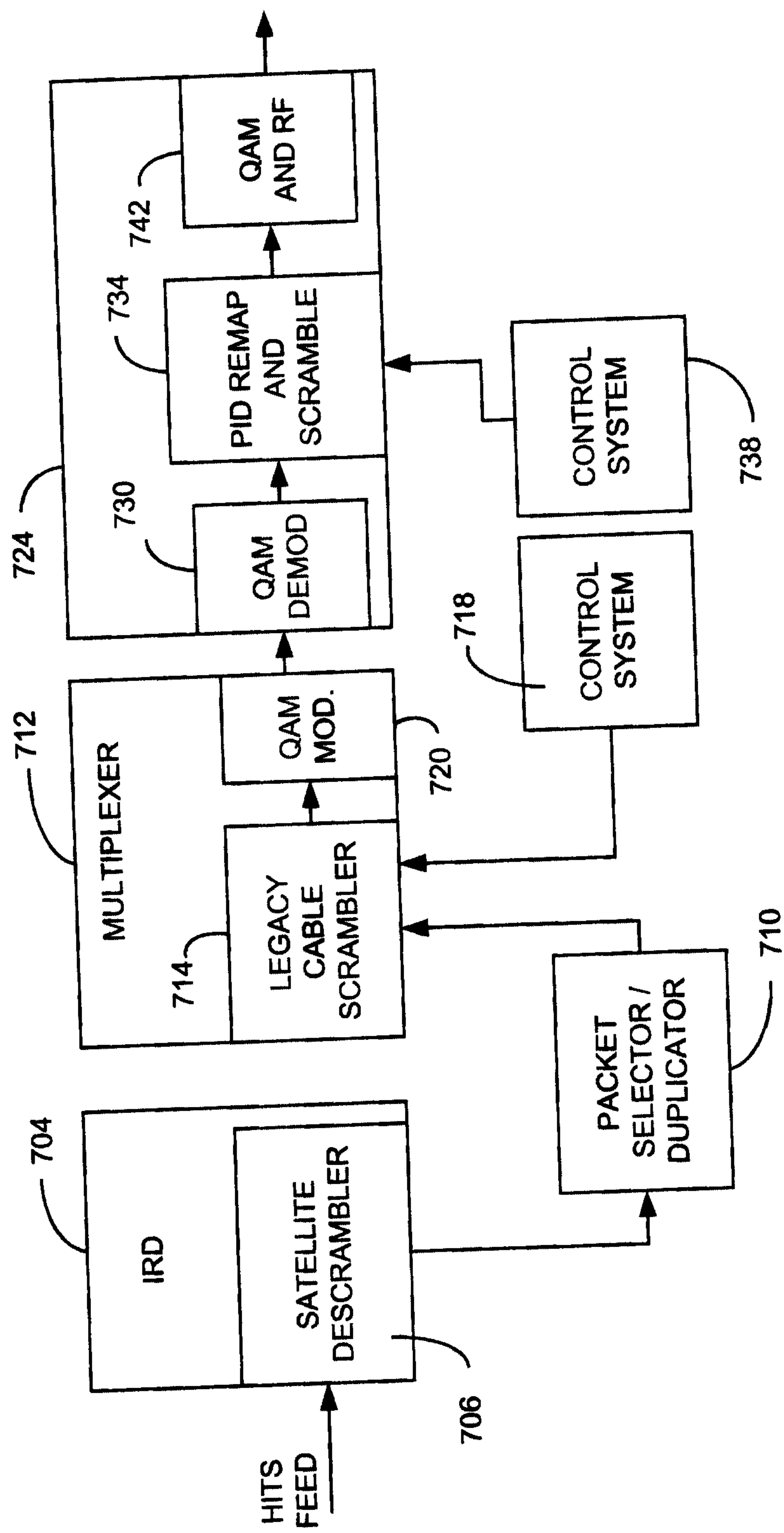
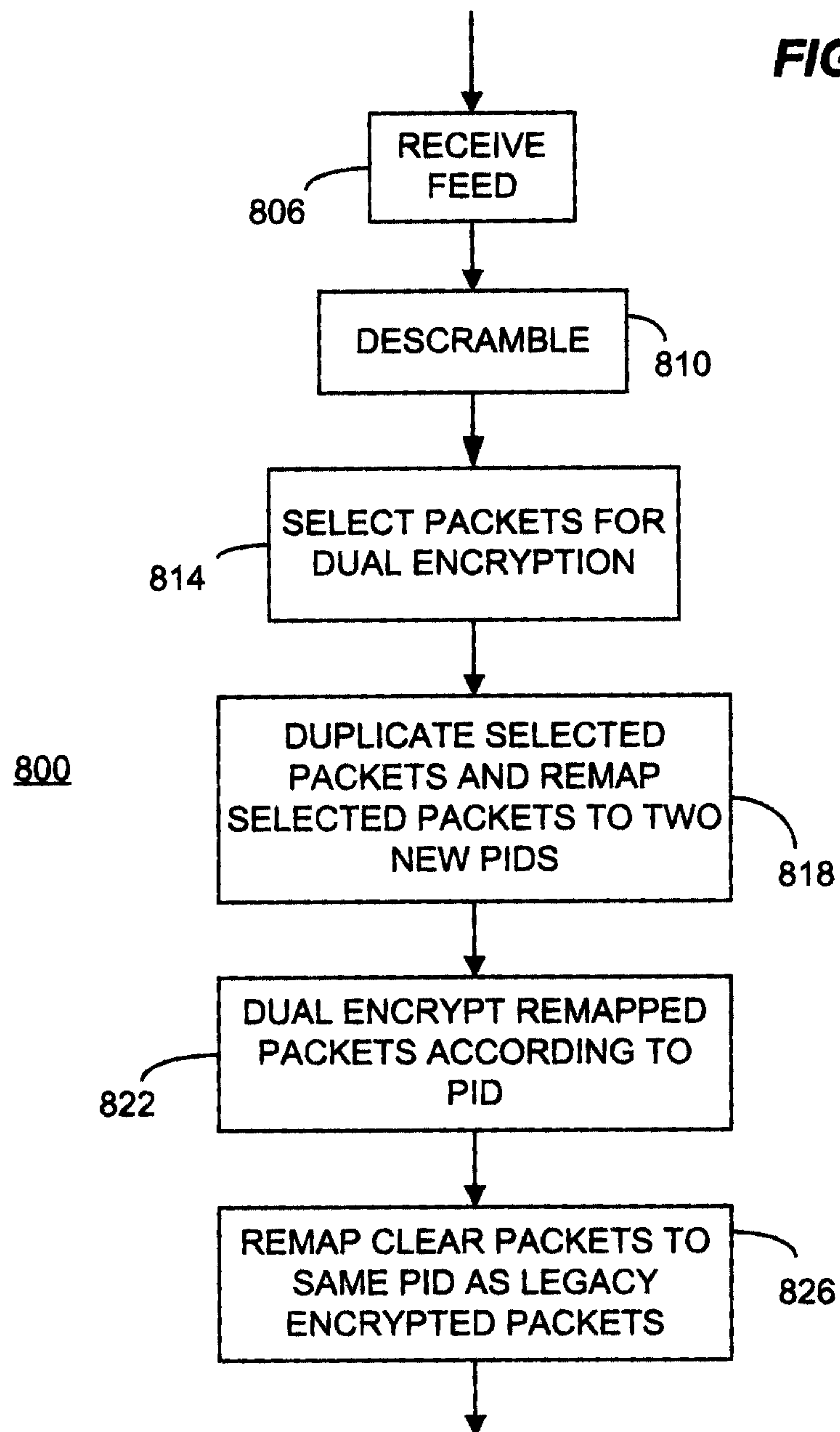


FIG. 12

FIG. 13

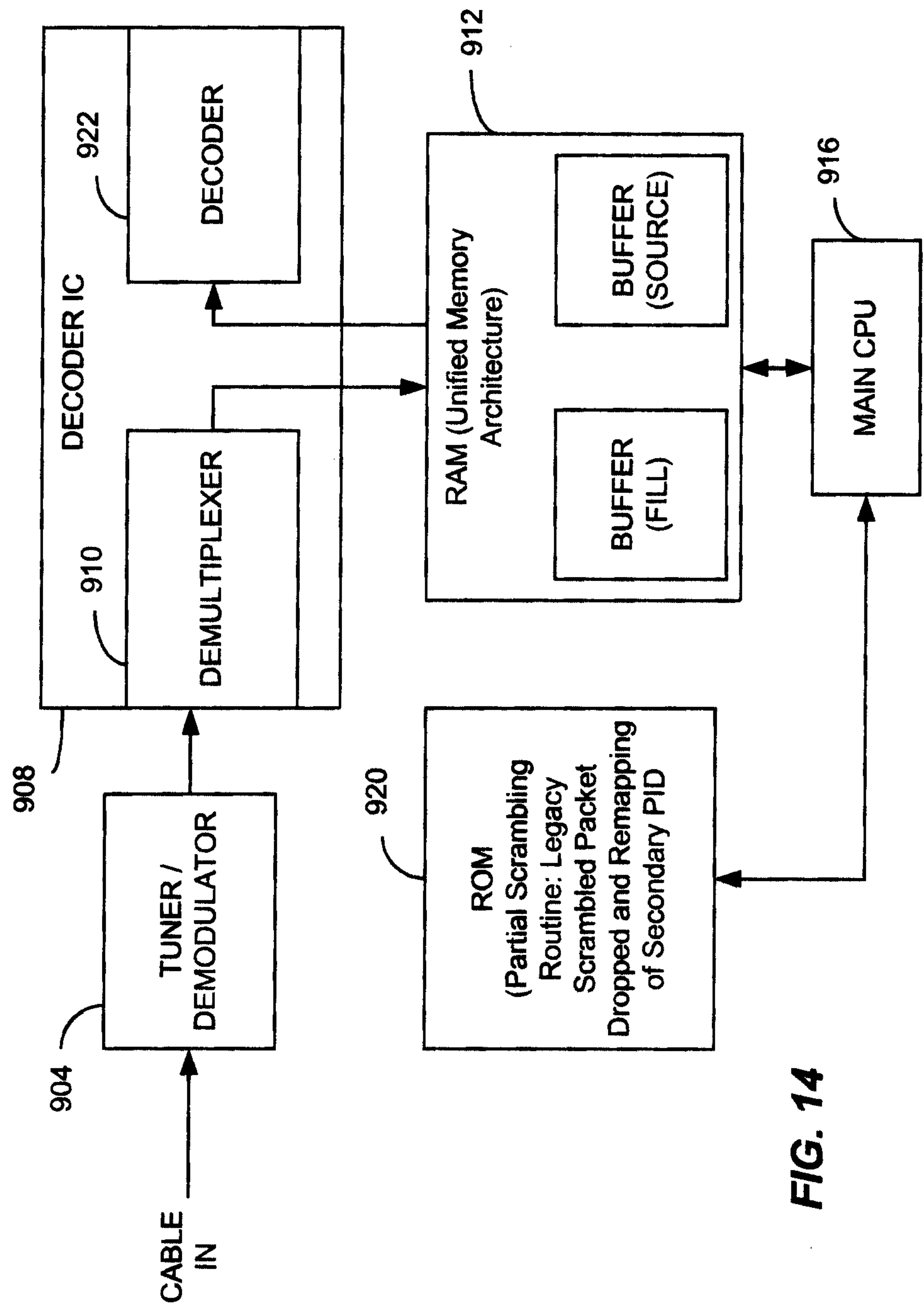


FIG. 14

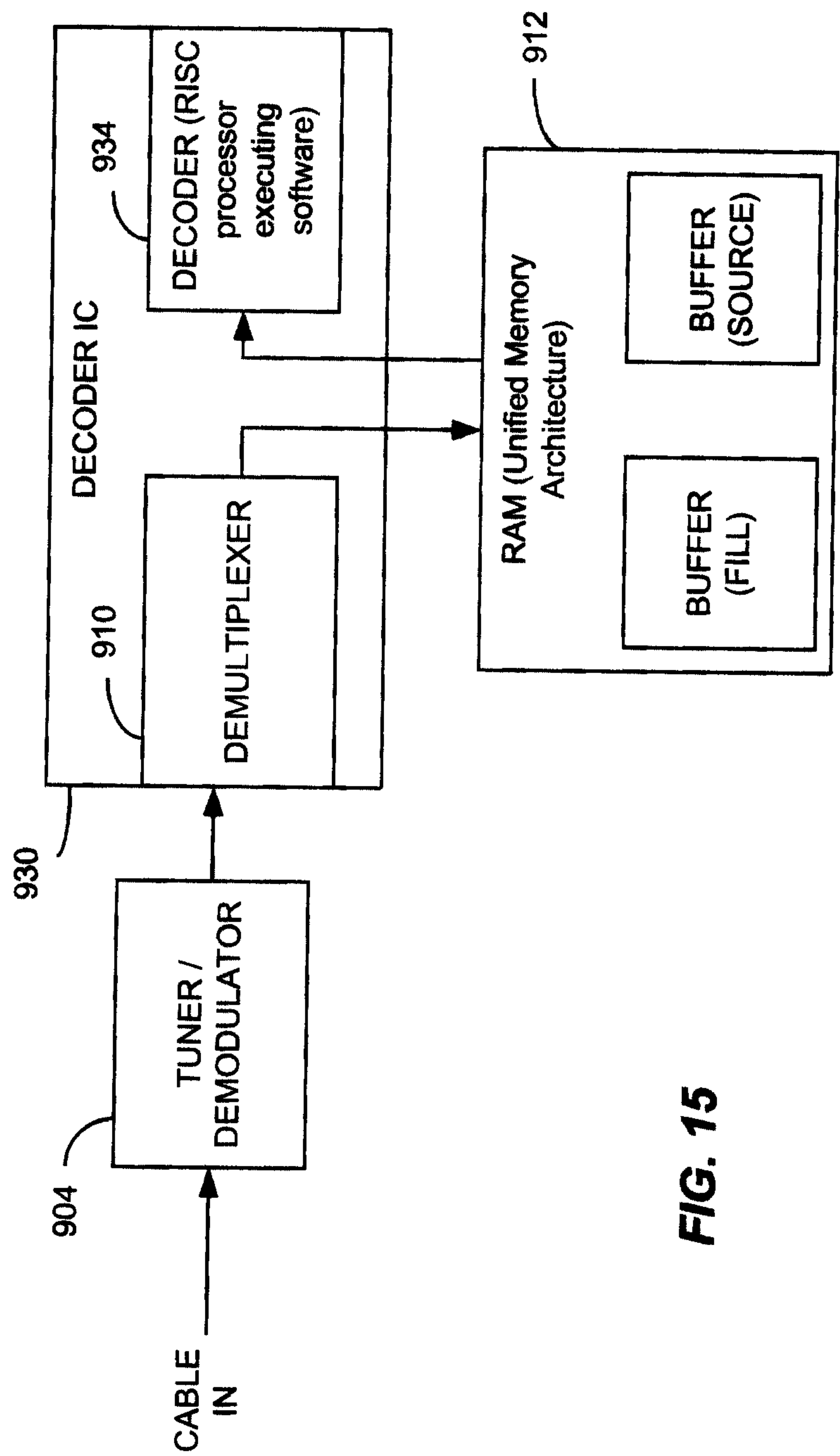


FIG. 15

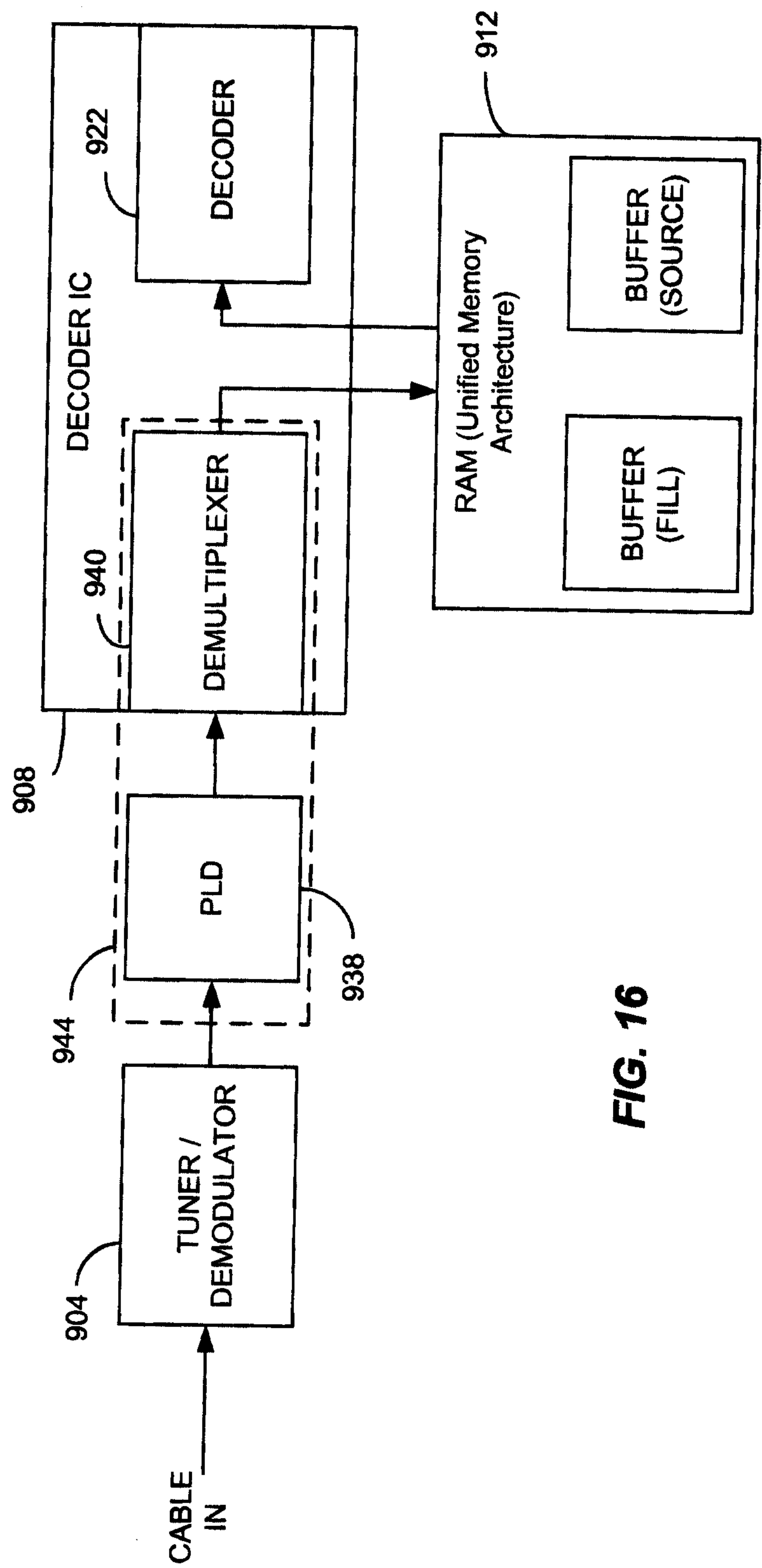
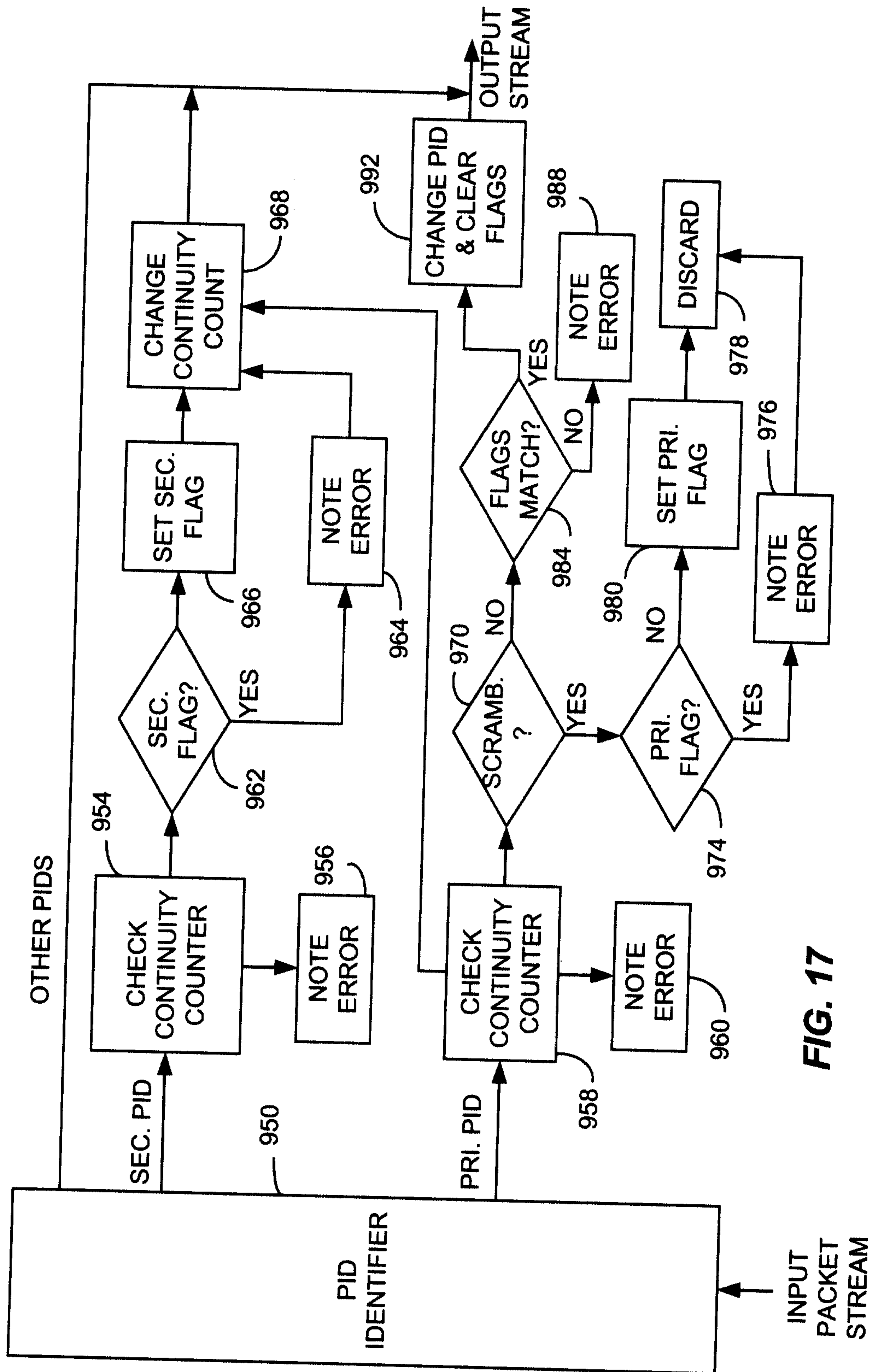


FIG. 16

**FIG. 17**

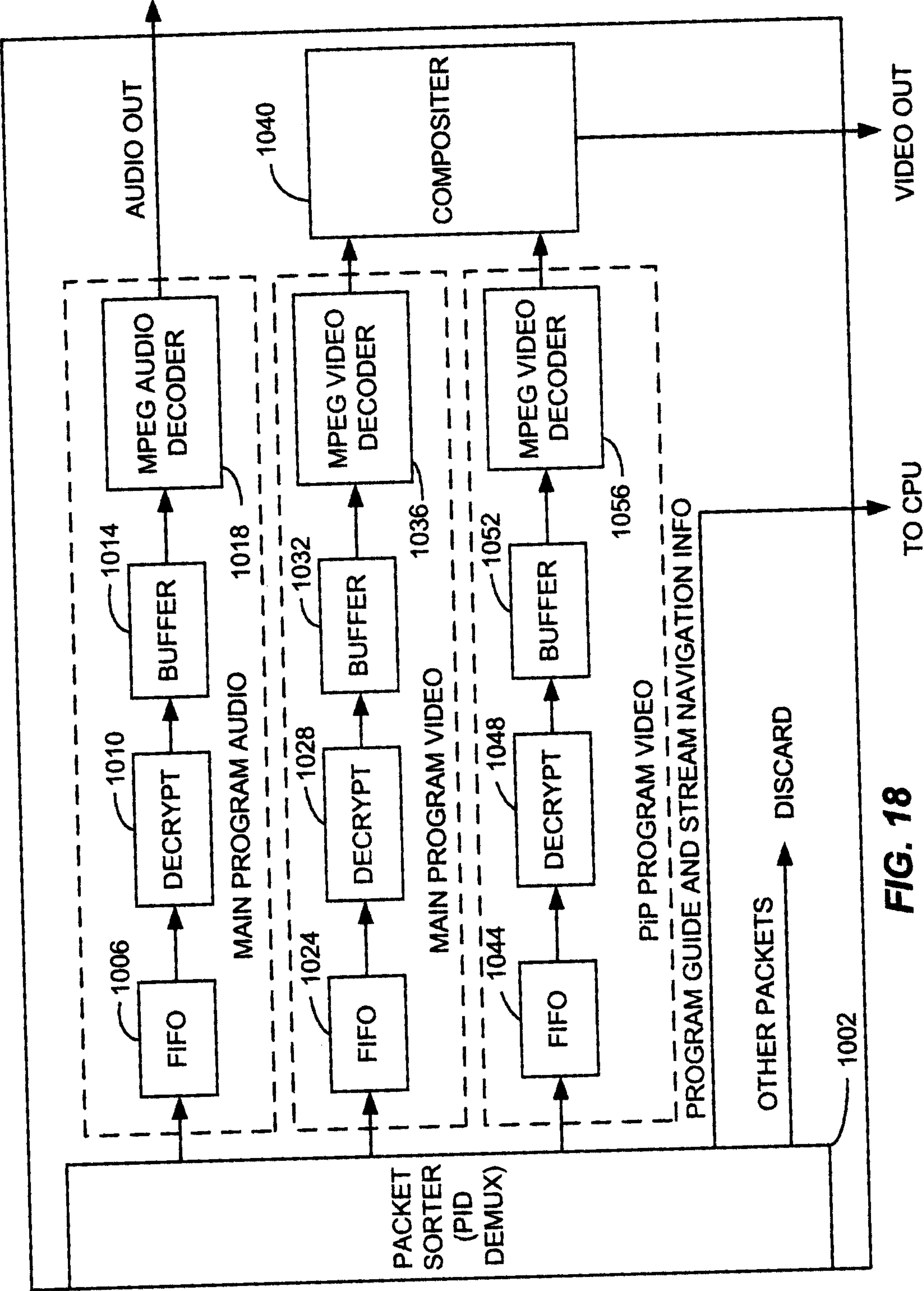


FIG. 18

