

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 03/081913 A2

(51) International Patent Classification⁷: **H04N 7/16**, 7/167

(21) International Application Number: PCT/EP03/02985

(22) International Filing Date: 21 March 2003 (21.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 12 656.9 21 March 2002 (21.03.2002) DE

(71) Applicant (*for all designated States except US*):
SCM MICROSYSTEMS GMBH [DE/DE]; Os-
kar-Messter-Strasse 13, 85737 Ismaning (DE).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **GENEVOIS, Christophe** [FR/FR]; 34, avenue Marx Dormoy, F-83740 La Cadière d'Azur (FR).

(74) Agent: **DEGWERT, Hartmut**; Prinz & Partner GbR, Manzingerweg 7, 81241 München (DE).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SELECTIVE MULTIMEDIA DATA ENCRYPTION

(57) Abstract: A conditional access system for multimedia data is disclosed that offers acceptable security at drastically reduced requirements on hardware performance. A selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream. For specific embodiments that include decryption circuitry inside a user smart card, the level of security of such system is even higher than that of conventional ones.



WO 03/081913 A2

Selective Multimedia Data Encryption

5 The present invention relates to a conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets. The invention also relates to a method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets.

10 Data security is an important aspect in multimedia commerce. Conditional access systems (CAS) mainly rely on scrambling of a transport stream containing protected multimedia contents. In Digital Video Broadcast ("DVB"), for example, only subscribers with a conditional access module ("CAM") and a valid subscriber card (Smart Card "SC") can descramble a scrambled transport stream
15 and obtain TV contents in the clear for application to a TV set. The conditional access module must have the capability to process an MPEG stream in real-time at a processing rate of at least about 1.5 MB/sec, thereby placing high demands of performance on the hardware used in the CAM.

20 The present invention provides a conditional access system for multimedia data that offers acceptable security at drastically reduced requirements on hardware performance. For specific embodiments that include decryption circuitry inside a user smart card, the level of security of such system is even higher than that of conventional ones.

25 According to the invention, a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining base transport stream at insertion positions corresponding to the original positions

of the particular data packets in the base transport stream. Since only selected data packets must be processed for encryption/decryption, the amount of processing is drastically reduced.

According to a specific embodiment of the invention, a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event's encryption key, and inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport stream.

In one aspect of the invention, the base transport stream is a clear transport stream, i.e. data are not scrambled. By selectively encrypting the transport stream, a high level of security is achieved even if the base transport stream is in the clear, because only selected data packets must be decrypted and decryption can be done with low-performance hardware such as can be embodied in a smart-card (Smart Card) - which is inherently safe.

In another aspect of the invention, the base transport stream is a scrambled transport stream, i.e. data are scrambled in accordance with a specific standard, such as the DVB standard. By selectively encrypting the scrambled transport stream, a high level of security is added to that achieved by scrambling.

The invention uses the fact that in a typical compressed multimedia data stream such as an MPEG stream, the contents of particular data packets are propagated to successive data packets, i.e. successive data packets are dependant on contents of preceding data packets, so that by encrypting only particular data packets, many successive data packets are affected, resulting in a sufficient overall scrambling of the data stream. Given the moderate hardware requirements, decryption can be performed by available Smart Cards, enabling a hardware implementation where the security entirely resides in the Smart Card.

Further, because the key can be changed frequently and a highly efficient encryption algorithm such as, for example, DES or 3DES can be used, the security in the proposed system is sufficient for the particular needs. A possibility to enhance security is to use a non public encryption algorithm.

5 For low value multimedia contents, or in a pay-per-event environment, it will generally be sufficient to send a fixed event decryption key prior to actual transmission of the selectively encrypted transport stream. For higher value multimedia contents, the event decryption key can be changed frequently. In a DVB environment, for example, the event decryption keys can be transmitted with
10 the EMMs (Entitlement Management Message) in the transport stream. A user key available in the user smart card (Subscriber Card) will be used to decrypt in the EMMs, the event decryption keys. Another possibility is to have the event decryption key available in an one-event smart card, that will be sold to users.

In the preferred embodiment of the invention, the event decryption key is
15 transmitted to an authorised receiver provided with a "light" conditional access module. As used here, "light" means that the conditional access module will not necessarily include hardware or software decryption or descrambling resources as the decryption may be performed in the user smart card. The selectively encrypted transport stream is transmitted to the receiver. The light conditional
20 access module detects encrypted data packets, removes the encrypted data packets from the received transport stream, decrypts the encrypted data packets with the event decryption key, and inserts the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the clear transport stream.
25 Preferably, the encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions.

Further advantages and features of the invention will appear from the following description of preferred embodiments with reference to the drawings. In the drawings:

Figs. 1 to 6 are block diagrams with descriptive legends for different embodiments of a head-end equipment for producing selectively encrypted data streams containing digitised multimedia data;

5 Figs. 7 to 10 are block diagrams with descriptive legends for different embodiments of a user equipment for decoding selectively encrypted data streams containing digitised multimedia data;

Fig. 11 is a diagram illustrating a first embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption;

10 Fig. 12 is a diagram illustrating a method of producing a clear transport stream from a scrambled or corrupted transport stream produced with the method of Fig. 11;

Fig. 13 is a diagram illustrating a second embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream
15 by selective encryption; and

Fig. 14 is a diagram illustrating a third embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption, wherein the scrambled or corrupted transport stream consists of selectively encrypted packets and DVB scrambled packets.

20 With reference now to Fig. 1, a first embodiment of a head-end component is shown for producing a selectively encrypted transport stream containing digital multimedia data. Specifically, the component includes a head-end PC (Personal Computer) 10 with an interface 12 for an SC (Smart Card) 14 and a serial high speed bi-directional communication interface 16 (e.g. a 1394 or a USB2
25 interface). The SC 14 has an internal processor with scrambling or encrypting capability and a safe memory for storing a plurality of private user keys. The head-end component further includes a professional (transmitter) STB (Set-Top-Box) 18 that has CI (Common Interface) and TS (Transport Stream) interface 20

and an RF port 22 for connection to a satellite link 24. The head-end component finally includes an interface module 26 to establish a high-speed serial connection between interface 20 of STB 18 and interface 16 of PC 10. Module 26 is preferably a PC card according to the PCMCIA standard and includes a
5 microprocessor and a memory in addition to a CI and TS interface and a high-speed serial interface.

With reference to Fig. 11, to generate a selectively encrypted transport stream SETS from a base transport stream BTS consisting of successive digital data packets numbered 1, 2, ... 13 ..., selected data packets are extracted from the BTS
10 and encrypted, or scrambled, with circuitry on SC 14, using an "event key". In the Fig. 1 embodiment, the BTS is a clear digital transport stream consisting of successive data packets and available within the PC 10. In Fig. 11, the encryption or scrambling step is referred to as "Packet scrambling". It should be understood that the base transport stream BTS can be a clear TS as indicated in Fig. 11, or a
15 scrambled transport stream and, in particular, a conventional DVB-scrambled transport stream.

The keys used in the selective encryption/scrambling method include a user key pair and an event key pair, as indicated in Fig. 1, and each key pair can be symmetric or asymmetric, as also indicated in Fig. 1. The user keys (user_key_2)
20 are stored in the memory of SC 14 in the case of private keys (public and private key pairs). The user keys are transmitted with the EMM in a DVB environment for decryption of the event keys used for the selective encryption/scrambling.

In the next step, referred to as "Packet buffering/insertion" in Fig. 11, the encrypted or scrambled data packets are inserted into the buffered transport
25 stream at positions in time ahead of corresponding positions in the original BTS. For example, scrambled data packet #2 is inserted between data packet # -3 and data packet # -1, and now available position between data packets #1 and #3 is filled with scrambled data packet #5. As a result, a selectively encrypted, or scrambled, transport stream SETS is provided, as shown in Fig. 11.

The SETS is communicated to the STB 18 via module 26 for broadcast transmission over satellite link 24, as seen in Fig. 1.

With reference to Fig. 7, a first embodiment of a user-end component is shown for recovering in accordance with the method illustrated in Fig. 12, from a
5 selectively encrypted transport stream, as may be produced with the component in Fig. 1 and in accordance with the Fig. 11 method, a clear transport stream.

The user component shown in Fig. 7 includes a PC card module 30 referred to as a "Selective Crypto Module", that includes a CI & TS interface 32 (Common Interface and interface for Transport Stream), an incorporated smart-card reader
10 34, a microprocessor with memory unit 36 and a packet filtering and insertion logic 38. The user component works with a smart-card 40 to be inserted in the reader 34 and referred to in Fig. 7 as a "Pay Per Event Smart Card". Of course, this is just one of many possible scenarios in a protected DVB environment.

The module 30 is inserted into a CI slot of a conventional Set-Top-Box that
15 has the capability of receiving a selectively encrypted/scrambled transport stream such as produced by the equipment in Fig. 1, having the encrypted/scrambled transport stream converted into a clear stream by means of the module 30, and forwarding a video/audio to signal an appliance such as a TV set.

With reference to Fig. 12, a selectively encrypted transport stream SETS is
20 received, and encrypted data packets are extracted for decryption or descrambling by circuitry on SC 40. The user key for such decryption is stored in a safe memory of SC 40. This step is referred to as "Packet descrambling" in Fig. 12. As a next step, the descrambled data packets are inserted in the buffered transport stream at locations corresponding in time to the original positions in the base
25 transport stream BTS. As a result, a clear transport stream CTS is obtained.

In this embodiment, the selective decryption is performed with circuitry on the SC 40. This is possible because the selective encryption proposed here can be dealt with on the user side with a moderate hardware performance requirement, as is typically embodied in a smart card. In other embodiments of the invention,

however, the selective decryption may be performed by circuitry incorporated in, or software/firmware residing in, module 30.

With reference to Figs. 2 to 6, different embodiments of the head-end component are shown but they all may have the same functionality as that in Fig. 1. Specifically, the Fig. 1 embodiment works without a PC, and the encryption of the selected data packets is performed in module 26 which is a PC card smart card reader for SC 14. Alternatively, the encryption may be performed by circuitry on SC 14, as shown in Fig. 3 where the SC 14 has a scrambler 29. The selection of the data packets to be encrypted is either performed by software executed by a microprocessor 27 within module 26 or by a hardware filter incorporated in module 26. In Fig. 4, the scrambler 29 is shown as incorporated in module 26. In Fig. 5, the functionality of module 26 is incorporated in STB 18, which is equipped with a smart card reader 13 for SC 14. The scrambler 29 is incorporated in SC 14. In Fig. 6, the only difference over Fig. 5 is that the scrambler 29 is incorporated in STB 18.

With reference to Figs. 8, details of the user smart card (SC) 40 (see Fig. 7) are shown. SC 40 has an interface 35 that corresponds to interface 34 in module 30. It also has a private packet descrambler 50 for the decryption of the selectively encrypted data packets, and a microcomputer 52 with a microprocessor and a memory for storing an event key, or a user key in case of an event key to be down-loaded with the EMMUs. In Fig. 8, it is assumed that SC 40 is a "Pay Per Event Smart Card".

With reference to Figs. 9 and 10, different embodiments of the user component are shown but they all may have the same functionality as that in Fig. 7. Specifically, in the Fig. 9 embodiment, the user component includes a user Set-Top-Box (STB) 37 with an interface 39 for module 30. Module 30 has incorporated therein a conventional DVB descrambler 41. In this embodiment, decryption of the selected data packets is performed on SC 40 while DVB descrambling is performed on module 30 which is a conditional access module (CAM) upgraded to cope with the needs of selective data packet encryption. In the

Fig. 10 embodiment, the functionality of module 30 has been incorporated in STB 37, as is known from conventional embedded conditional access systems. Accordingly, STB 37 has an interface 53 for SC 40. Decryption of the selectively encrypted data packets is still performed by circuitry on SC 40, i.e. by
5 descrambler 50.

Having disclosed basic embodiments of the invention, further improvements are apparent from Figs. 13 and 14.

In Fig. 13, the processing of a data packet for selective encryption is shown in detail. The data packets selected here for encryption are preferentially those the
10 contents of which are propagated to succeeding data packets in an MPEG transport stream so that a relatively powerful scrambling effect is achieved with a relatively reduced percentage of encrypted data packets. This is an important factor if the decryption of the selectively encrypted data packets is to be performed on a smart card with inherently moderate processing capacity, but with
15 an inherently high level of security.

In Fig. 14, the generation of a partially DVB-scrambled and selectively encrypted transport stream is illustrated. As is easily seen, all data packets other than the selectively encrypted data packets are DVB-scrambled. Specifically, a clear content is partially selectively encrypted and partially DVB scrambled, the
20 DVB keys being processed from the clear content of selectively encrypted packet.

By this way, a stream completely scrambled without using EMM to broadcast DVB keys is provided. The scrambled stream contains the CW that are processed from a selectively encrypted packet that has been decrypted. The level of security is still high as those control words could only be recovered if the "one-event card"
25 is available to decrypt the selectively encrypted packets. This solution has the advantage that the stream is completely scrambled and that the content's broadcast is independent from EMMs so independent from broadcasting companies (as TPS, Canal + ...etc).

In figure 14, the process to have the scrambling stream is illustrated:

- to-be-selectively-encrypted packets are sel 1, sel 2, sel 3
- To-be-DVB-scrambled packets are 1.1,1.2, ...,1.n,2.1,2.2,....,2.n,3.1, 3.2...
- CW(Sel i) is the control word calculated from clear Sel i content and that
5 will be used to scramble packets i.1,i.2,....,i.n
- As soon as CW (Sel i) is processed, Sel i is encrypted in the head end Smart Card (for example)
- CW(Sel i) is fed to the DVB scrambler to processed the scrambled i.1,i.2,....,i.n
- 10 - Encrypted Sel i is inserted in advance to i.1,i.2,....,i.n

When a user STB receives the scrambled stream,

- it will send encrypted packet Sel i to the smart card,
- The smart card will decrypt Sel i,
- The smart card will process CW(Sel i),
- 15 - Sel i will be sent to the DVB descrambler,
- The DVB descrambler will descramble packets i.1,i.2,....,i.n with Sel i.

Claims

1. A conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets, characterised in that a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport stream.

2. A conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets, characterised in that a selectively encrypted transport stream is formed from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining base transport stream at insertion positions corresponding to the original positions of the particular data packets in the base transport stream.

3. The system of claim 1 or claim 2, wherein an event decryption key is provided to an authorised receiver provided with the conditional access system, the selectively encrypted transport stream is transmitted to the receiver, the conditional access system detects encrypted data packets, removes the encrypted data packets from the received transport stream, decrypts the encrypted data packets with the event decryption key, and inserts the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the base transport stream.

4. The system of claim 3, wherein the event decryption key is provided on a one-event smart card.
5. The system of claim 3, wherein the event decryption key is provided on a one-limited-period smart card.
- 5 6. The system of claim 3, wherein the event decryption key in a DVB environment is transmitted in specific EMMs protected by a user encryption key, the corresponding user decryption key being provided in the CAS, on a user smart card or on a user SIM
- 10 7. The system of claims 2 and 3, wherein the conditional access system has a buffer memory to store clear data packets while an encrypted data packet is decrypted.
8. The system of claim 1 or claim 3, wherein said encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions.
- 15 9. The system of claim any of claims 3 to 8, wherein said conditional access system includes a chip card with decryption circuitry thereon.
10. The system of claim 9, wherein the chip card is a SIM card.
11. The system of any of the preceding claims, wherein the decryption key is transmitted to a receiver with the selectively encrypted data stream.
- 20 12. The system of claim 11, wherein the event decryption key is frequently changed.
13. The system of any of claims 1 to 11, wherein the event decryption key is a fixed key distributed on a pay-per-event basis.
- 25 14. The system of claim 13, wherein the event decryption key is transmitted in a GSM network prior to an event and loaded into a SIM or smart card inserted in a SIM or smart card reader of a mobile phone.

15. The system of any of the preceding claims, wherein the event decryption key is provided encrypted with a user encryption key and a corresponding user decryption key is also provided to an authorized user.

16. The system of any of the preceding claims, comprising a head-end encoder
5 for producing the selectively encrypted data stream, the head-end encoder including a Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon.

17. The system of any of claims 1 to 15, comprising a head-end encoder for producing the selectively encrypted data stream, the head-end encoder including a
10 Common Interface CI for a PC card module that has encryption circuitry thereon.

18. The system of any of claims 1 to 15, comprising a head-end encoder for producing the selectively encrypted data stream, the head-end encoder including a Personal Computer PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC.

15 19. The system of any of claims 1 to 15, comprising a head-end encoder for producing the selectively encrypted data stream, the head-end encoder including an encoder CI module with a CI&TS (Common Interface and Transport Stream) interface to a professional Set-Top-Box STB.

20 20. The system of any of claims 1 to 19 wherein the base data stream is a clear data stream.

21. The system of any of claims 1 to 19 wherein the base data stream is a DVB-scrambled data stream.

22. The system of any of claims 1 to 19 wherein all data packets other than the selectively encrypted data packets are DVB-scrambled.

25 23. The system of claim 19, wherein the encoder CI module further comprises a high speed interface to a PC, a base transport stream being sent to the PC via the

high speed interface to be selectively encrypted by the PC or by a PC peripheral, said PC peripheral being one of the following

- a smart card reader SCR for a smart card SC having encryption circuitry thereon;
- 5 - an encryption PCMCIA module having encryption circuitry and forming a SCR for a head-end smart card.

24. The system of any of the preceding claims, wherein said particular data packets are of a nature such that their contents are propagated to successive data packets.

- 10 25. The system of any of claims 1 to 24, wherein said particular data packets are data packets containing sign bits of DCT coefficients in an MPEG stream.

26. The system of any of claims 1 to 24, wherein every n^{th} data packet of the transport stream is encrypted, n being a fixed number.

- 15 27. The system of any of claims 1 to 24, wherein every n^{th} data packet of the transport stream is encrypted, n being a variable number.

28. The system of claim 27, wherein the variable number n is randomly variable.

29. The system of claim 27, wherein the variable number n is variable as a function of data packet contents.

- 20 30. The system of any of claims 3 to 29, wherein the conditional access system is embedded in a user Set-Top-Box (STB).

31. The system of any of claims 3 to 29, wherein said conditional access system includes a PC card with a Common Interface CI for connection to a user Set-Top-Box (STB).

32. The system of claim 30 or claim 31, wherein said user Set-Top-Box (STB) is capable of detecting a current encryption level of the transport stream and to direct the transport stream, in accordance with the detected encryption level, to decryption circuitry associated with that encryption level.

5 33. The system of claim 30 or claim 31, wherein the user Set-Top-Box (STB) is capable of detecting at least some of the following encryption levels of the transport stream :

- None
- DVB only
- 10 - DVB and selective encryption
- Selective encryption only;

and the Set-Top-Box (STB) is capable of directing the transport stream to at least one of the following decryption means:

- None
- 15 - An embedded conditional access system in the Set-Top-Box (STB) able to cope with DVB only,
- An embedded conditional access system in the Set-Top-Box (STB) able to cope with selective encryption only,
- An embedded conditional access system in the Set-Top-Box (STB) able to cope with DVB and with selective encryption,
- 20 - A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-Box (STB) able to cope with DVB only,
- A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-Box (STB) able to cope with selective encryption only,
- 25

- A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-Box (STB) able to cope with DVB and with selective encryption,
- 5 - A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-Box (STB) able to cope with DVB only,
- A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-Box (STB) able to cope with selective encryption only,
- 10 - A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-Box (STB) able to cope with DVB and with selective encryption,
- A Smart Card (SC) in a Smart Card Reader (SCR).

34. A method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets, characterised in that a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the clear transport stream.

35. A method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets, characterised in that a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream.

36. A method of producing a scrambled transport stream from a clear transport stream containing digitised multimedia data in successive data packets, characterised in that

- 5 - selected data packets are determined within the clear transport stream;
- the selected data packets are processed to obtain control words CW therefrom;
- data packets following each selected data packet are DVB scrambled using control words CW obtained from the preceding
10 selected data packet; and
- the selected data packets are encrypted with an event encryption key.

37. The method of claim 36, wherein the encrypted selected data packets are inserted in the scrambled transport stream at positions ahead in time with respect
15 to the original positions of the selected data packets in the clear transport stream.

Fig 1 : HeadEnd Component : Professional STB, CI to High speed bi-directional I/F module and PC with SC I/F and High Speed bi-directional I/F

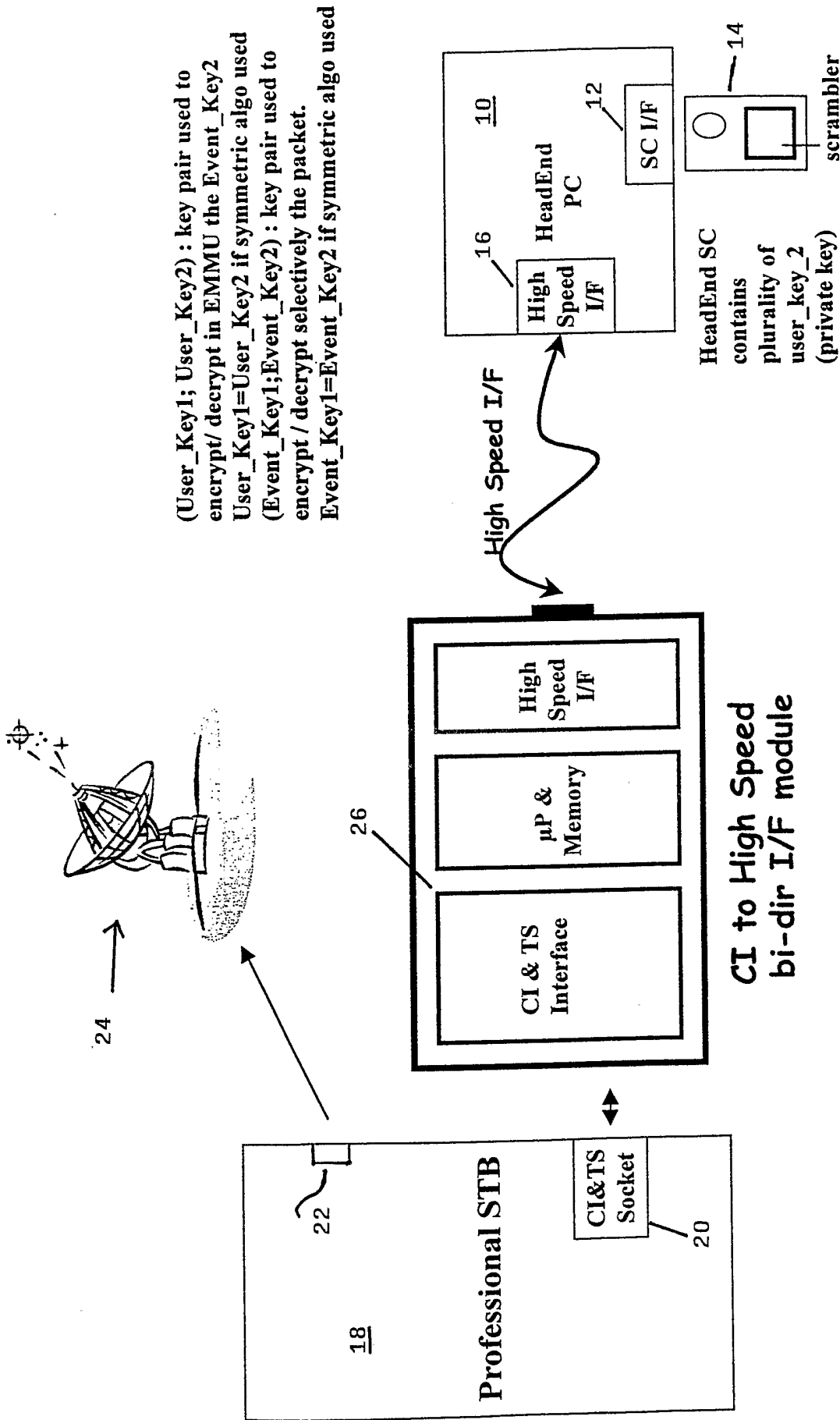


Fig 2 : HeadEnd Component : Professional STB, CI module including SCR, encryption by SC

The process is the same as the previous one except that

- encryption is performed in the module or in the headend SC
- selection of packet to be encrypted performed by the μP (software filter) or by a hardware filter.

The Head end component with the PC would be the preferential one as it offers more flexibility.

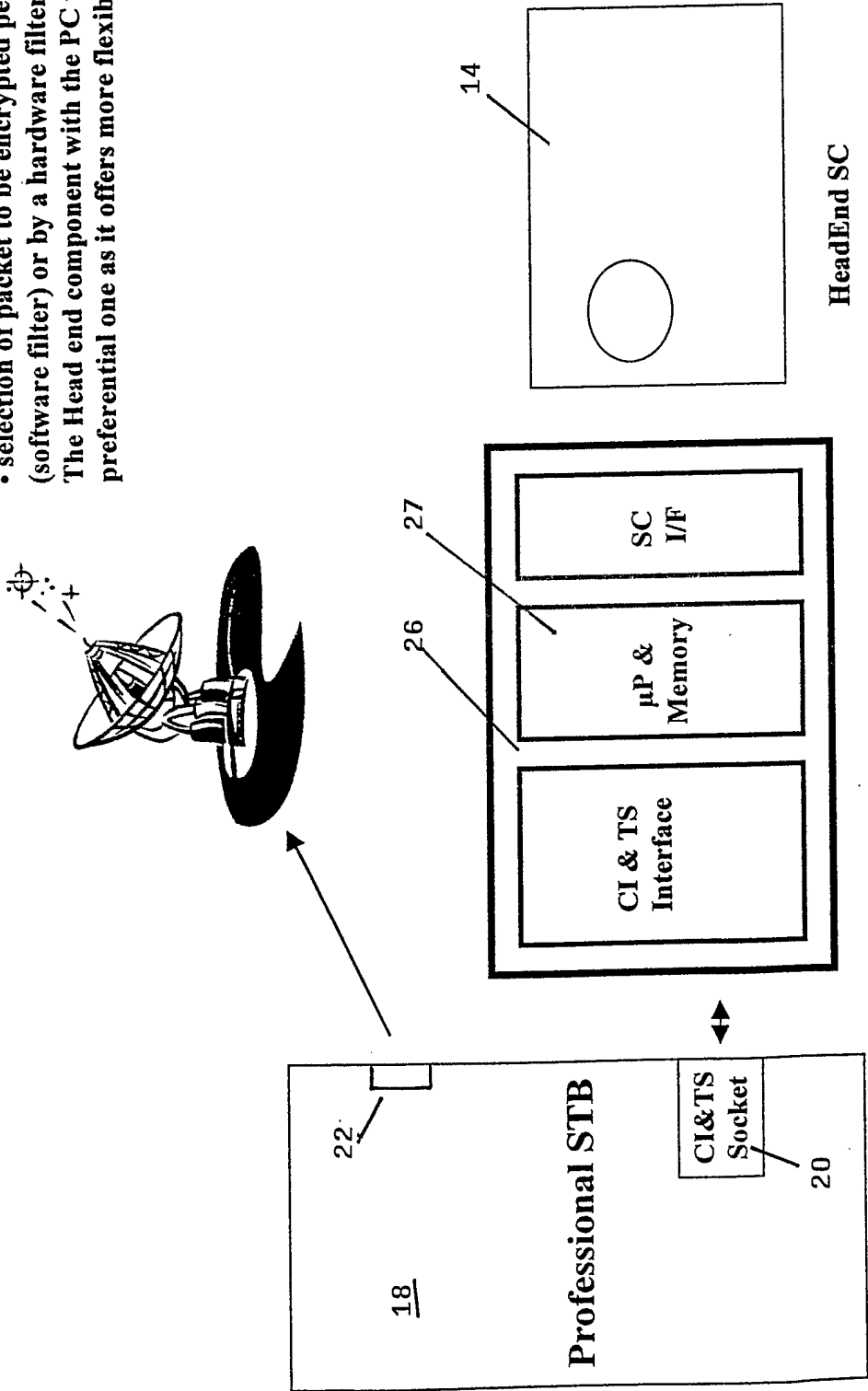


Fig 3 : HeadEnd Component : Professional STB, CI module including SCR, encryption by Haedend SC

The process is the same as the previous one except that

- encryption is performed in the headend SC
- selection of packet to be encrypted performed by the μ P (software filter) or by a hardware filter.

The Head end component with the PC would be the preferential one as it offers more flexibility.

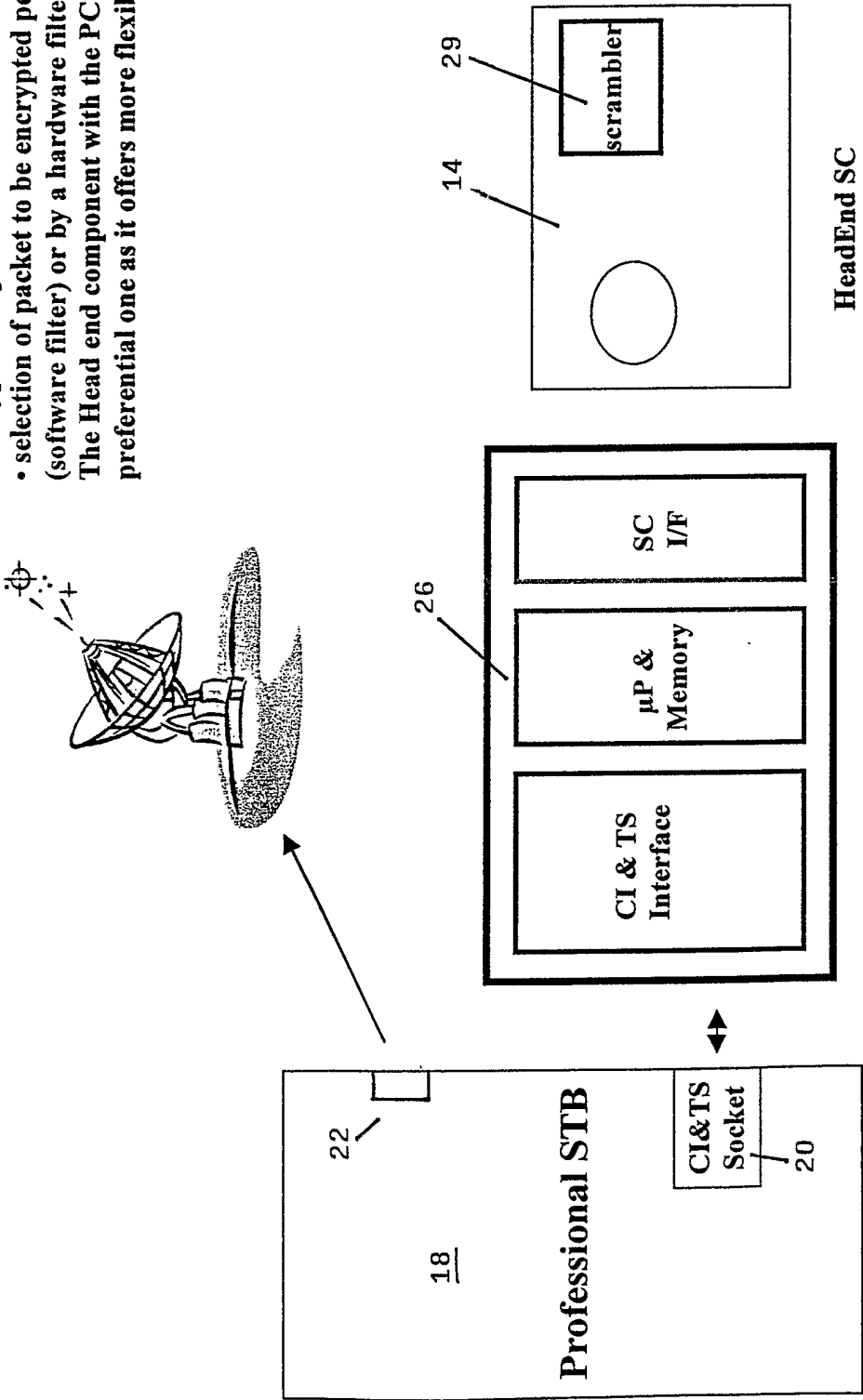


Fig 4 : HeadEnd Component : Professional STB, CI module including SCR, encryption by module

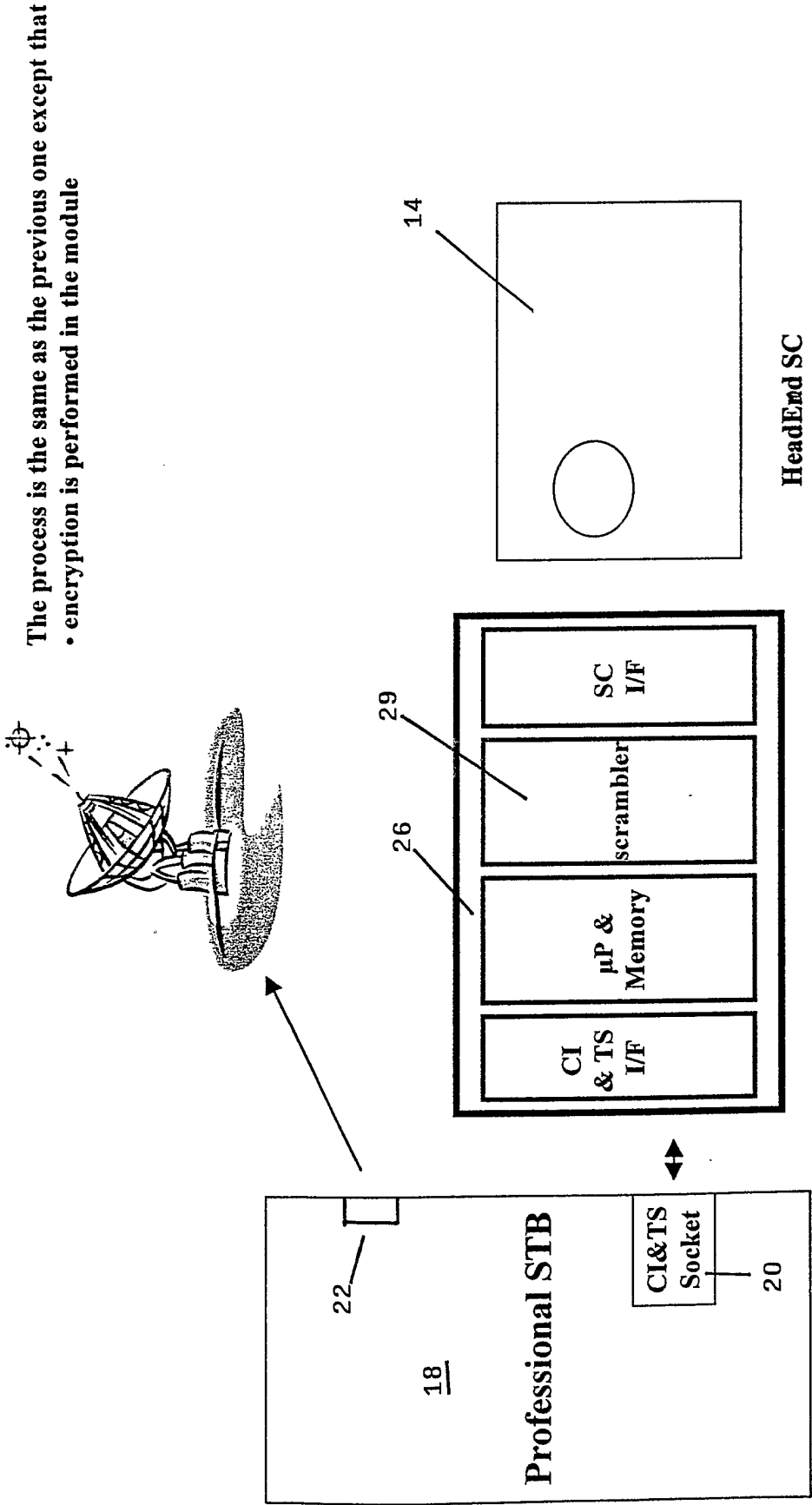


Fig 5 : HeadEnd Component : Professional STB including SCR, encryption by Headend SC

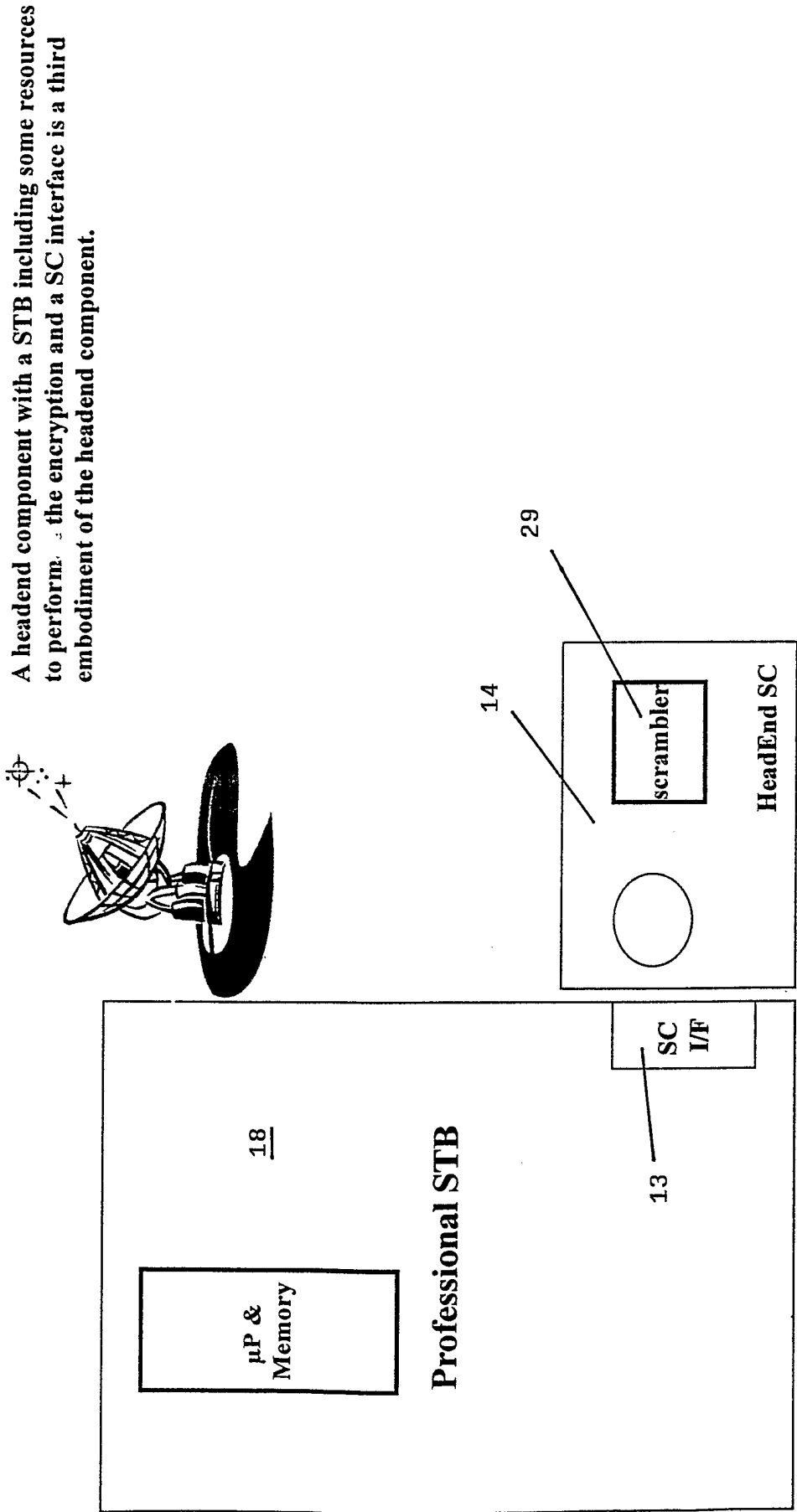


Fig 6 : HeadEnd Component : Professional STB including SCR, encryption by STB

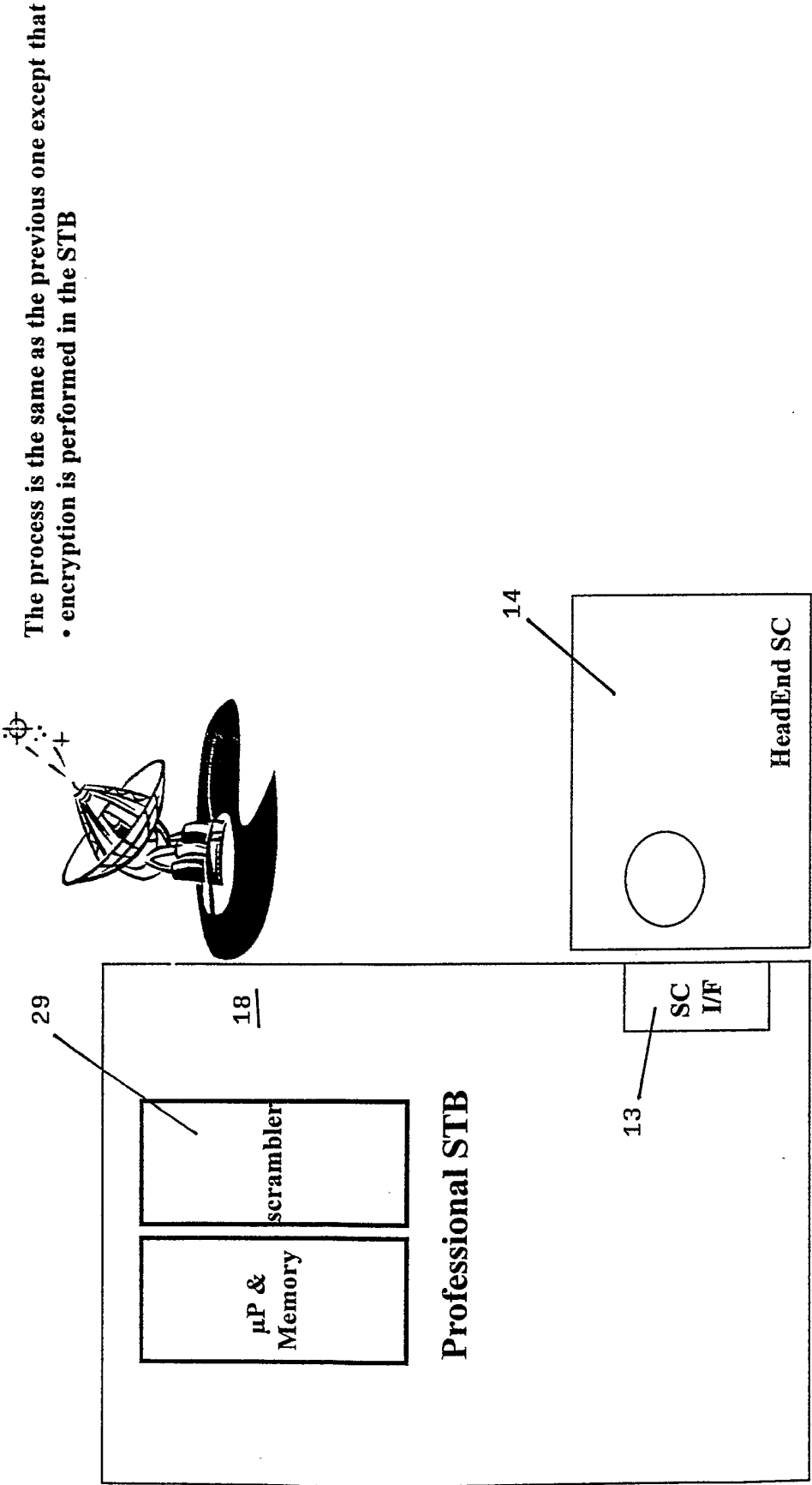


Fig 7 : User decoder : STB + Selective Crypto Module + User SC

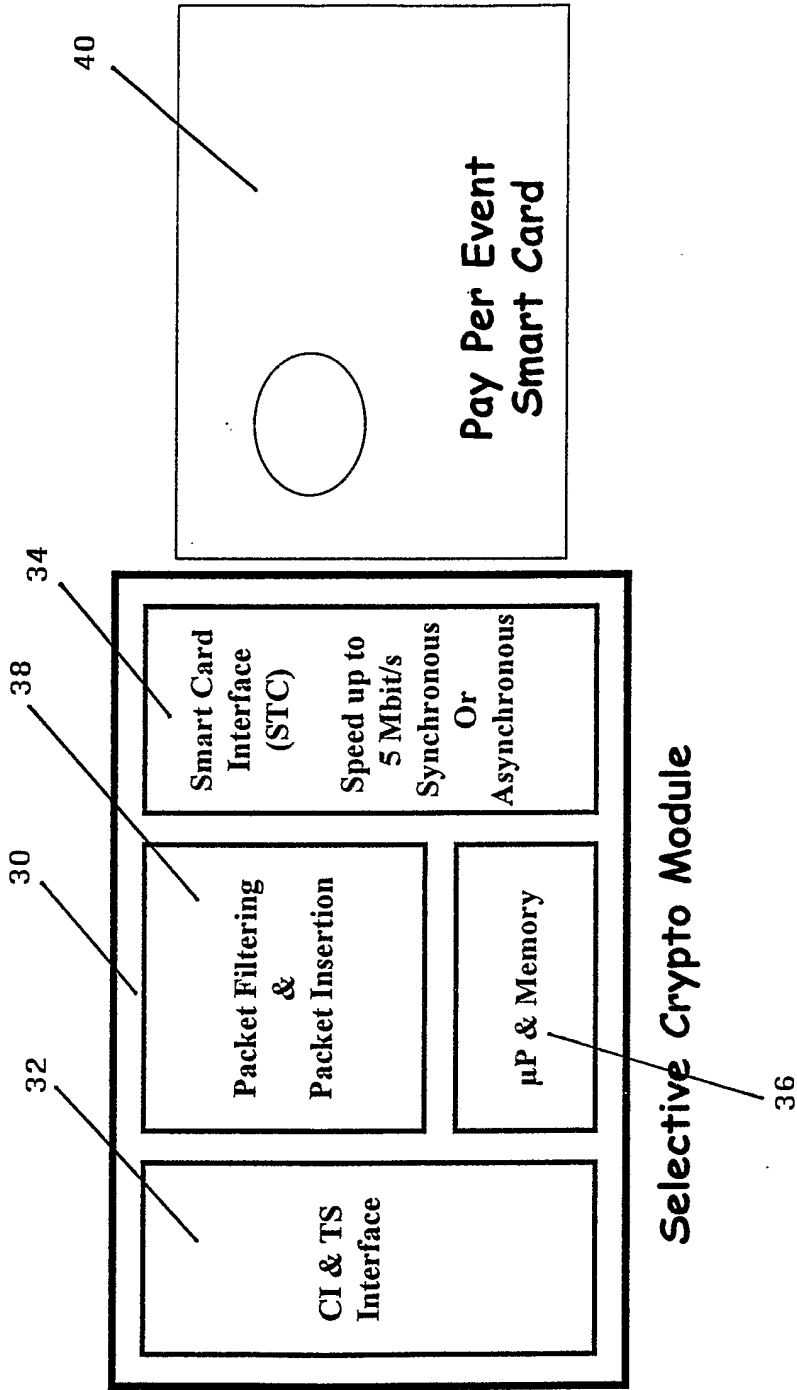


Fig 8 : User SC

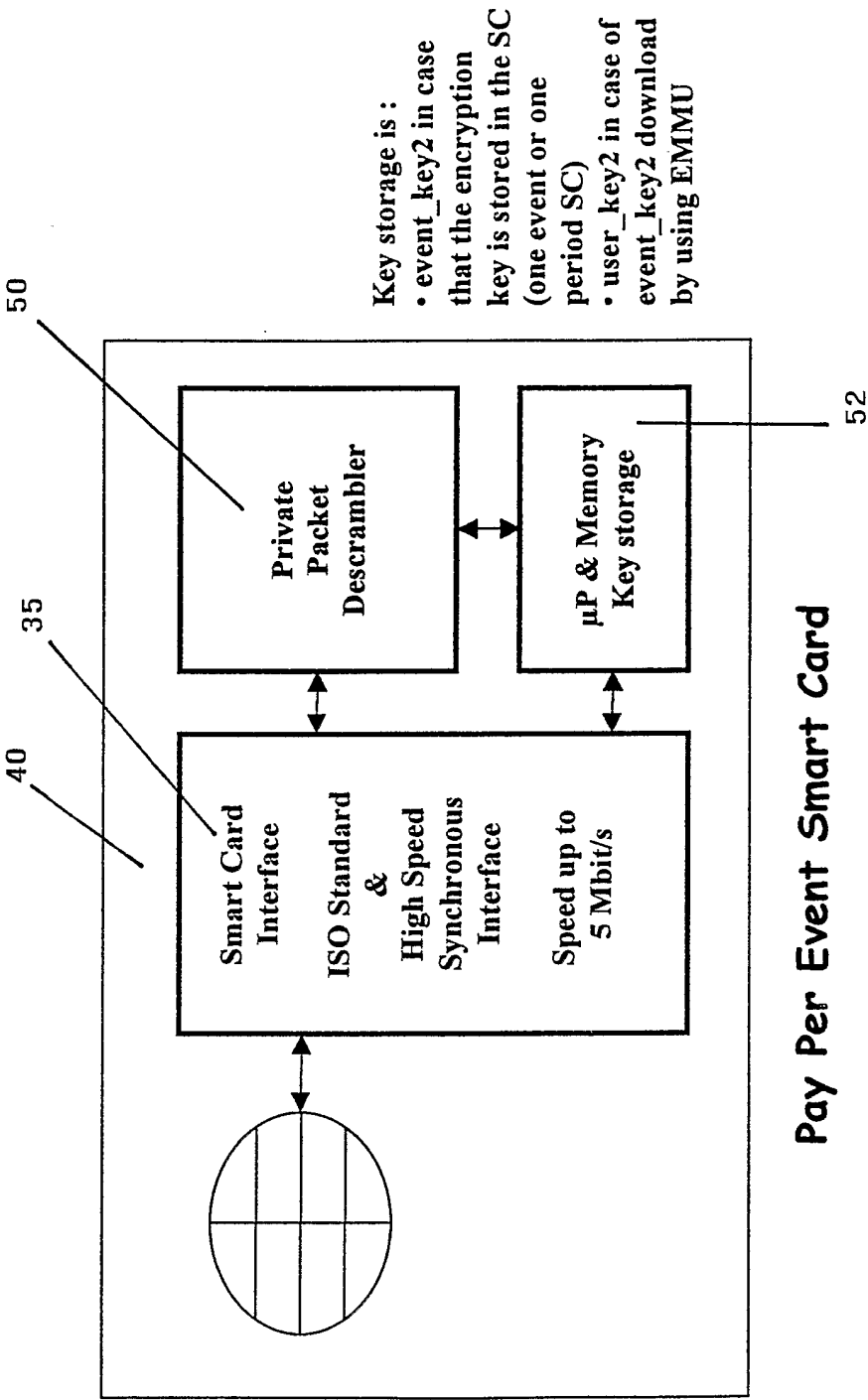


Fig 9 : User decoder : User STB, standard DVB CI updated module and user SC

- The process is the same as the previous one except that
- decryption is performed in a standard module updated to be able to cope with standard DVB scrambling and selective encryption
 - selective decryption is still performed by the user SC

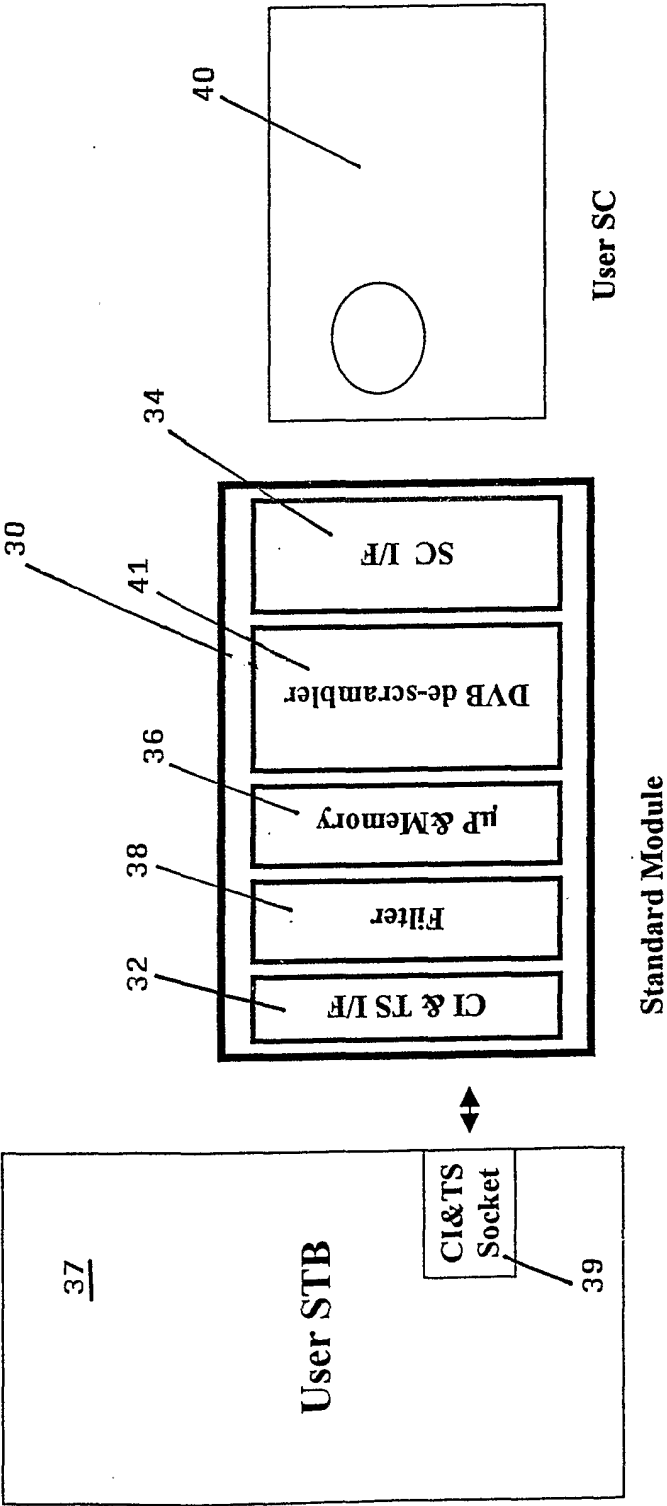


Fig 10 : User decoder : User STB including SCR

The User STB includes some resources to filter the packet and to insert it properly

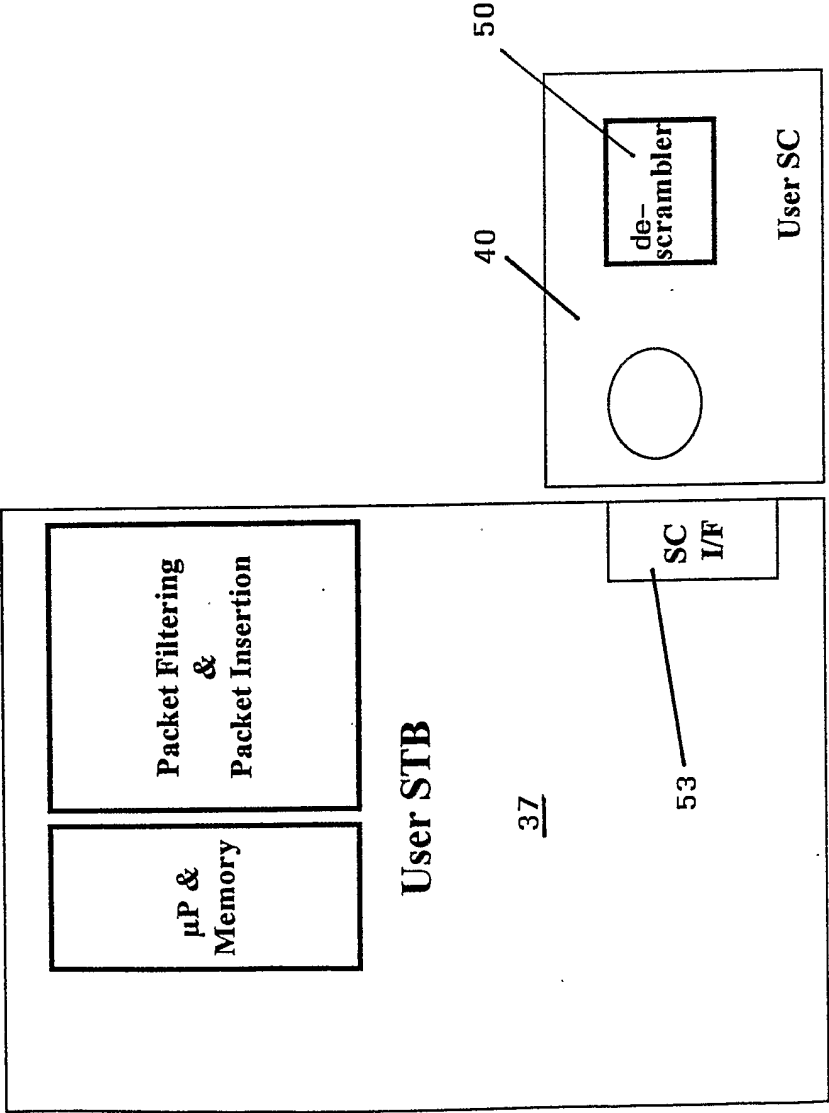


Fig 11 :

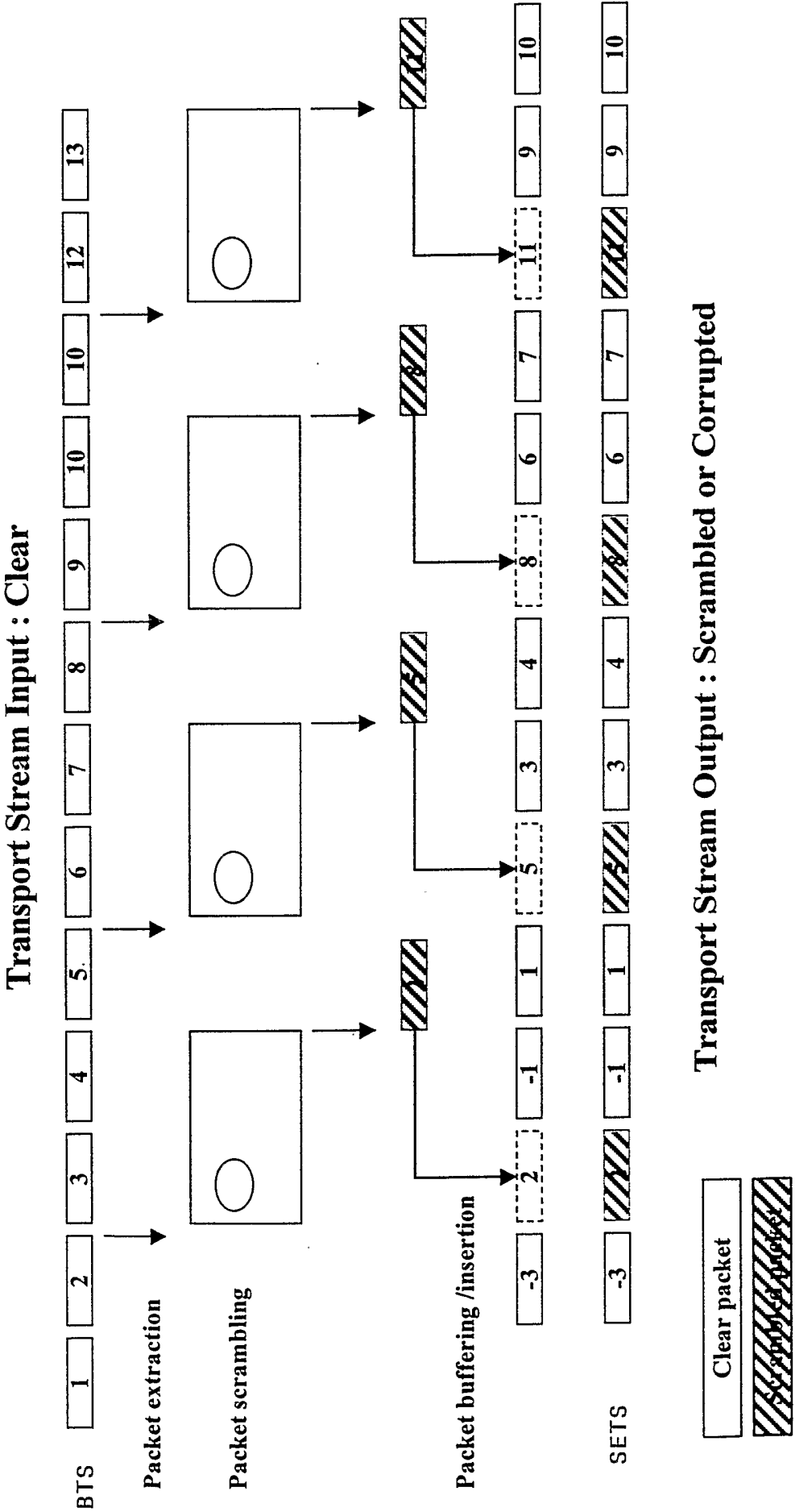


Fig 12 :

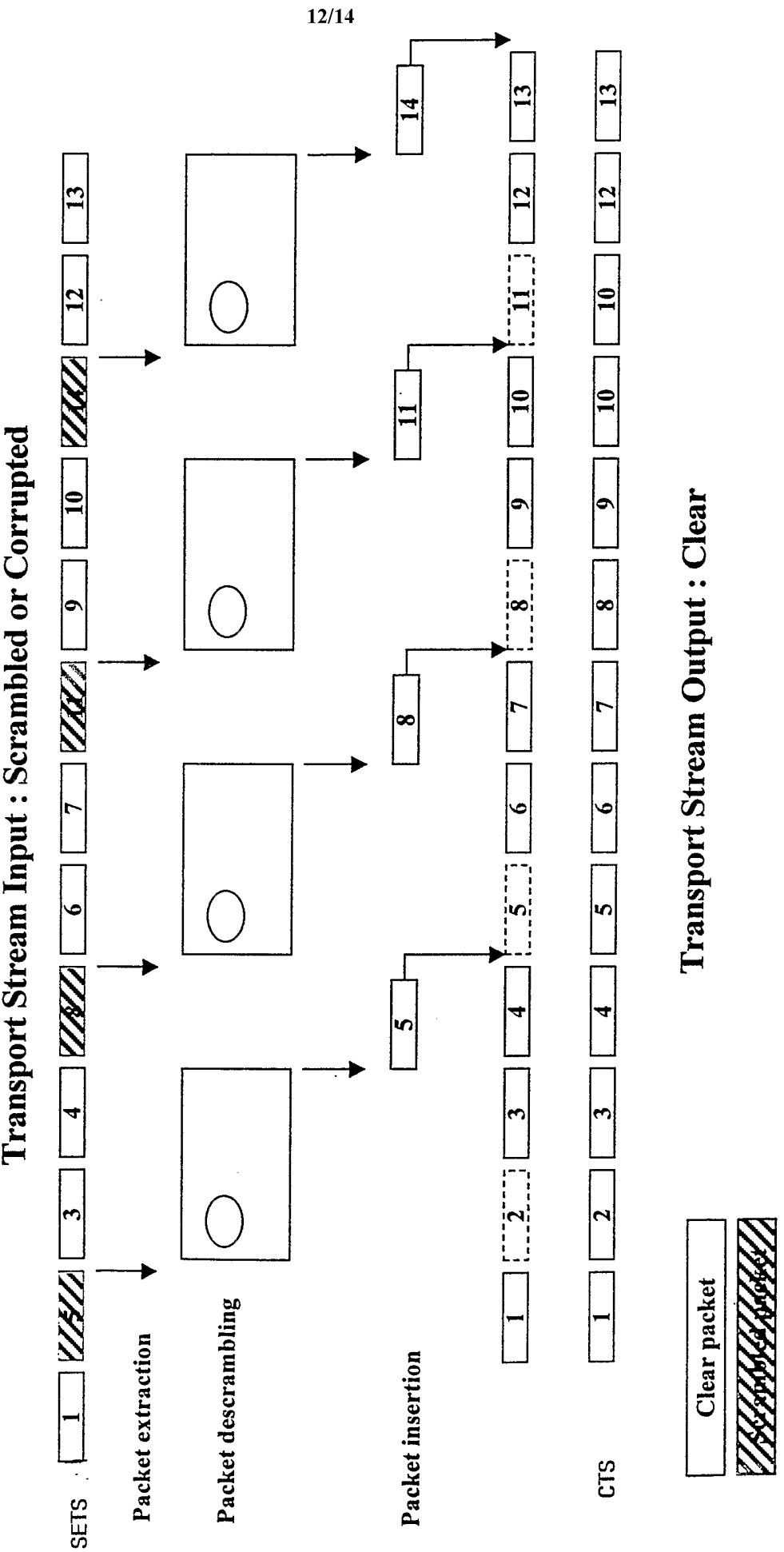


Fig 13 :AC & DC coefficients' sign bits encryption

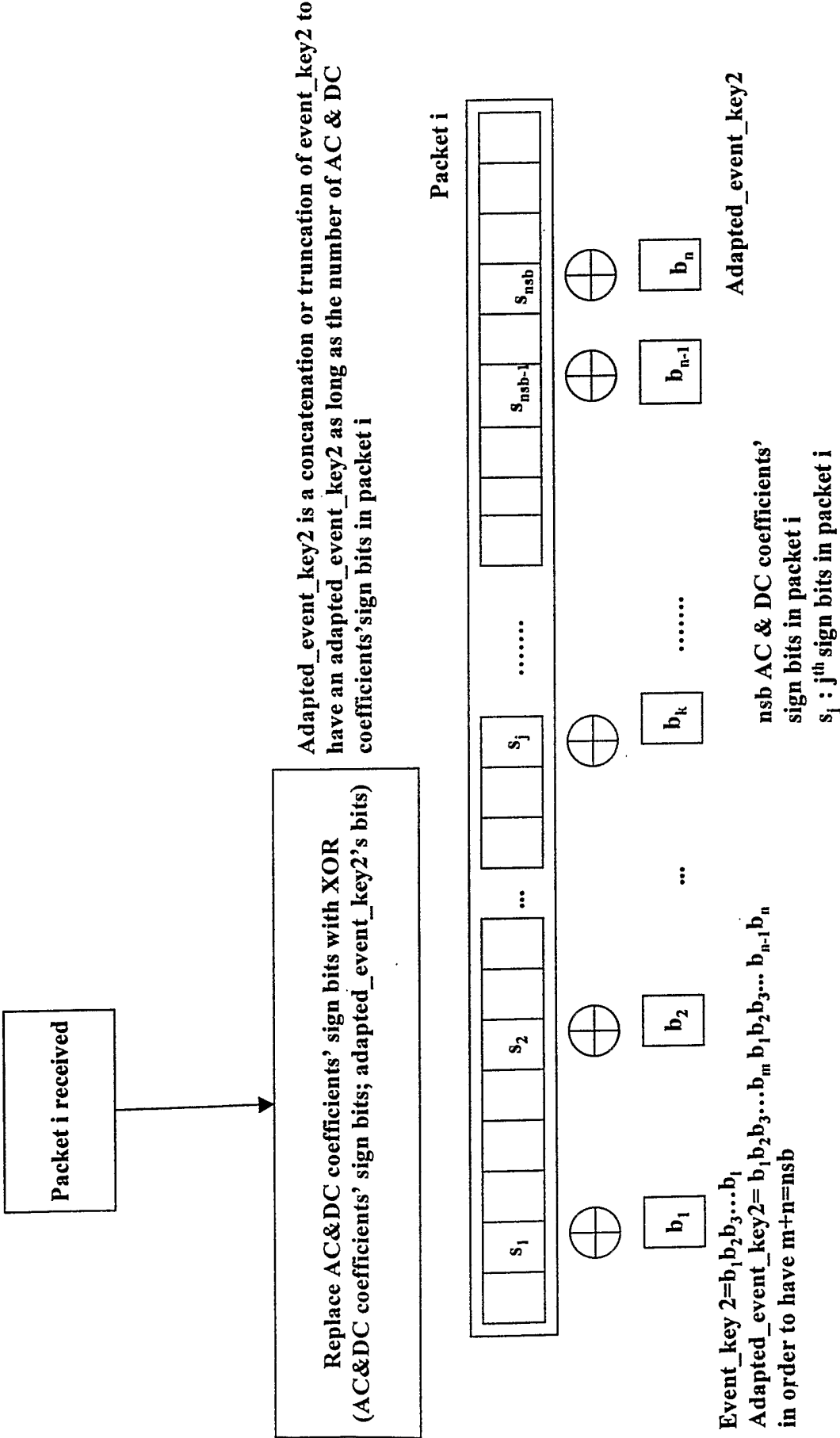


Fig 14 :

Transport Stream Input : Clear

