(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 428 353**

(51) Int. CI.:

H04N 21/418 (2011.01)
H04N 21/2347 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/222 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.03.2003 E 03744838 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2013 EP 1491046**

(54) Título: **Encriptación selectiva de datos multimedia**

(30) Prioridad:

21.03.2002 DE 10212656

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.11.2013

(73) Titular/es:

SMARDTV S.A. (100.0%)
ROUTE DE GENÈVE 22
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

GENEVOIS, CHRISTOPHE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Encriptación selectiva de datos multimedia

[0001] La presente invención se refiere a un sistema de acceso condicional donde los datos multimedia digitalizados se transmiten en un flujo de transporte continuo de paquetes de datos sucesivos. La invención también se refiere a un método para producir un flujo de transporte corrupto o parcialmente codificado a partir de un flujo de transporte en abierto que contiene datos multimedia digitalizados en paquetes de datos sucesivos.

[0002] La seguridad de los datos es un aspecto importante en el comercio multimedia. Los sistemas de acceso condicional (CAS) principalmente se basan en la codificación de un flujo de transporte que contiene contenidos multimedia protegidos. En la emisión de vídeo digital ("DVB"), por ejemplo, sólo los abonados con un módulo de acceso condicional ("CAM") y una tarjeta de abonado válida (tarjeta inteligente "SSC") pueden descodificar un flujo de transporte codificado y obtener contenidos de TV en abierto para su aplicación a un aparato de TV. El módulo de acceso condicional debe tener la capacidad de procesar un flujo de MPEG en tiempo real a un índice de tratamiento de al menos aproximadamente 1,5 MB/seg, imponiendo así altas demandas de rendimiento en el hardware usado en el CAM.

[0003] En la patente estadounidense número 5 805 700, se describe un dispositivo para aplicar políticas basadas en la encriptación selectiva de datos de vídeo comprimidos. Las unidades de transferencia básica (BTU) de datos de vídeo comprimidos se encriptan selectivamente conforme a la política para degradar las imágenes de vídeo a un estado virtualmente inútil en caso de que los datos selectivamente encriptados se presentaran sin desencriptación. La política es de manera que sólo un número seleccionado de BTUs del número total de BTUs se encripta.

[0004] La presente invención proporciona un sistema de acceso condicional para datos multimedia que ofrece seguridad aceptable con demanda drásticamente reducida de rendimiento de hardware. Para las formas de realización específicas que incluyen circuitos de desencriptación dentro de una tarjeta inteligente de usuario, el nivel de seguridad de tal sistema es incluso superior que el de las convencionales.

[0005] Según la invención, un flujo de transporte selectivamente encriptado se forma a partir de un flujo de transporte de base mediante la detección de paquetes de datos particulares en el flujo de transporte de base, eliminando y encriptando los paquetes de datos particulares con una clave de encriptación de evento e insertando los paquetes de datos encriptados en el flujo de transporte de base restante en posiciones de inserción correspondientes a las posiciones originales de los paquetes de datos particulares en el flujo de transporte de base. Dado que sólo los paquetes de datos seleccionados se deben procesar para encriptación/desencriptación, la cantidad de procesamiento se ve drásticamente reducida.

[0006] Según una forma de realización específica de la invención, un flujo de transporte selectivamente encriptado se forma a partir de un flujo de transporte de base mediante la detección de paquetes de datos particulares en el flujo de transporte de base, eliminando y encriptando los paquetes de datos particulares con una clave de encriptación del evento e insertando los paquetes de datos encriptados en el flujo de transporte de base restante en posiciones de inserción por delante en el tiempo con respecto a las posiciones originales de los paquetes de datos particulares en el flujo de transporte de base.

[0007] En un aspecto de la invención, el flujo de transporte de base es un flujo de transporte en abierto, es decir, los datos no están codificados. Mediante la encriptación selectiva del flujo de transporte, se obtiene un alto nivel de seguridad, aunque el flujo de transporte de base esté en abierto, porque sólo los paquetes de datos seleccionados se deben desencriptar y la desencriptación se puede hacer con hardware de bajo rendimiento, tal como el que pueda contener una tarjeta inteligente (Smart Card), que es intrínsecamente segura.

[0008] En otro aspecto de la invención, el flujo de transporte de base es un flujo de transporte codificado, es decir, los datos están codificados conforme a una norma específica, tal como la norma DVB. Mediante la encriptación selectiva del flujo de transporte encriptado, se añade un alto nivel de seguridad al conseguido por codificación.

[0009] La invención usa el hecho de que en un flujo de datos multimedia comprimido típico, tal como un flujo MPEG, el contenido de paquetes de datos particulares se propagan a paquetes de datos sucesivos, es decir, los paquetes de datos sucesivos dependen del contenido de los paquetes de datos precedentes, de modo que mediante la encriptación sólo de paquetes de datos particulares, se ven afectados muchos paquetes de datos sucesivos, dando como resultado una codificación general suficiente del flujo de datos. Teniendo en cuenta los requisitos de hardware moderados, la desencriptación se puede realizar mediante las tarjetas inteligentes disponibles, que permiten una implementación de hardware donde la toda la seguridad reside en la tarjeta inteligente.

[0010] Además, debido a que la clave se puede cambiar frecuentemente y se puede usar un algoritmo de encriptación altamente eficaz tal como, por ejemplo, DES o 3DES, la seguridad en el sistema propuesto es suficiente para las necesidades particulares. Una posibilidad para mejorar la seguridad es usar un algoritmo de encriptación no pública.

[0011] Para el contenido multimedia de poco valor, o en un entorno de pago por evento, generalmente será suficiente enviar una clave de desencriptación de evento fija antes de la transmisión real del flujo de transporte selectivamente encriptado. Para el contenido multimedia de mayor valor, la clave de desencriptación de evento se puede cambiar frecuentemente. En un entorno DVB, por ejemplo, las claves de desencriptación de evento se pueden transmitir con los EMMs (mensaje de gestión de derechos) en el flujo de transporte. Se usará una clave de usuario disponible en la tarjeta inteligente del usuario (tarjeta de abonado) para desencriptar en los EMMs, las claves de desencriptación de evento. Otra posibilidad es tener la clave de desencriptación de evento disponible en una tarjeta inteligente mono evento, que se venderá a los usuarios.

[0012] En la forma de realización preferida de la invención, la clave de desencriptación de evento se transmite a un receptor autorizado provisto de un módulo de acceso condicional "ligero". Como se usa en este caso, "ligero" significa que el módulo de acceso condicional no incluirá necesariamente recursos de desencriptación o descodificación de hardware o de software, dado que la desencriptación se puede llevar a cabo en la tarjeta inteligente del usuario. El flujo de transporte selectivamente encriptado se transmite al receptor. El módulo de acceso condicional ligero detecta paquetes de datos encriptados, retira los paquetes de datos encriptados del flujo de transporte recibido, desencripta los paquetes de datos encriptados con la clave de desencriptación de evento e inserta los paquetes de datos desencriptados en el flujo de transporte recibido restante en las posiciones correspondiente a las posiciones originales respectivas de los paquetes de datos particulares dentro del flujo de transporte en abierto. Preferiblemente, los paquetes de datos encriptados se insertan en posiciones que se encuentran un número predeterminado de paquetes de datos hacia adelante de las posiciones originales respectivas.

[0013] Según otras formas de realización de la invención, sus características técnicas se pueden resumir en las siguientes declaraciones:

Declaración 1: un sistema de acceso condicional donde los datos multimedia digitalizados se transmiten en un flujo de transporte continuo de paquetes de datos sucesivos y donde un flujo de transporte selectivamente encriptado se forma a partir de un flujo de transporte de base mediante la detección de paquetes de datos particulares en el flujo de transporte de base, dicho sistema, caracterizado por el hecho de que los paquetes de datos particulares se retiran y se encriptan con una clave de encriptación de evento, dichos paquetes de datos encriptados se insertan en el flujo de transporte de base restante en posiciones de inserción que se encuentran por delante en el tiempo con respecto a las posiciones originales de los paquetes de datos particulares en el flujo de transporte de base.

Declaración 2: el sistema de la declaración 1, donde se proporciona una clave de desencriptación de evento a un receptor autorizado provisto del sistema de acceso condicional, el flujo de transporte selectivamente encriptado se transmite al receptor, el sistema de acceso condicional detecta paquetes de datos encriptados, retira los paquetes de datos encriptados del flujo de transporte recibido, desencripta los paquetes de datos encriptados con la clave de desencriptación de evento e inserta los paquetes de datos desencriptados en el flujo de transporte recibido restante en las posiciones correspondiente a las posiciones originales respectivas de los paquetes de datos particulares en el flujo de transporte de base.

Declaración 3: el sistema de la declaración 2, donde la clave de desencriptación de evento está provista en una tarjeta inteligente mono evento.

Declaración 4: el sistema de la declaración 2, donde la clave de desencriptación de evento está provista en una tarjeta inteligente de un periodo limitado.

Declaración 5: el sistema de la declaración 2, donde la clave de desencriptación de evento en un entorno DVB se transmite en EMMs específicos protegidos por una clave de encriptación de usuario, la clave de desencriptación de usuario correspondiente se proporciona en el CAS, en una tarjeta inteligente de usuario o en una SIM de usuario.

Declaración 6: el sistema de la declaración 2, donde el sistema de acceso condicional tiene una memoria de búfer para memorizar paquetes de datos en abierto mientras que un paquete de datos encriptados se desencripta.

Declaración 7: el sistema de la declaración 2, donde dichos paquetes de datos encriptados se insertan en posiciones que se encuentran un número predeterminado de paquetes de datos hacia adelante de las posiciones originales respectivas.

Declaración 8: el sistema de cualquiera de las declaraciones 2 a 7, donde dicho sistema de acceso condicional incluye una tarjeta inteligente con un conjunto de circuitos de desencriptación sobre la misma.

Declaración 9: el sistema de la declaración 8, donde la tarjeta inteligente es una tarjeta SIM.

Declaración 10: el sistema de cualquiera de las declaraciones precedentes, donde la clave de desencriptación se transmite a un receptor con el flujo de datos selectivamente encriptados.

Declaración 11: el sistema de cualquiera de las declaraciones 1 a 10, donde la clave de desencriptación de evento es una clave fija distribuida sobre la base de pago por evento.

Declaración 12: el sistema de la declaración 11, donde la clave de desencriptación de evento se transmite en una red GSM antes de un evento y se carga en una tarjeta SIM o tarjeta inteligente insertada en un lector de tarjeta SIM o de tarjetas inteligentes de un teléfono móvil.

Declaración 13: el sistema de cualquiera de las declaraciones precedentes, donde la clave de desencriptación de evento se proporciona encriptada con una clave de encriptación de usuario y una clave de desencriptación de usuario correspondiente también se proporcionada a un usuario autorizado.

Declaración 14: el sistema de cualquiera de las declaraciones precedentes, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera que incluye una interfaz común CI que a su vez tiene una interfaz de tarjeta inteligente SC para una tarjeta inteligente que tiene un conjunto de circuitos de encriptación sobre la misma.

Declaración 15: el sistema de cualquiera de las declaraciones 1 a 13, que comprende un codificador de cabecera para producir selectivamente un flujo de datos encriptados, el codificador de cabecera que incluye una interfaz común CI para un módulo de tarjeta PC que tiene un conjunto de circuitos de encriptación sobre la misma.

Declaración 16: el sistema de cualquiera de las declaraciones 1 a 13, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera incluye un ordenador personal PC con una interfaz para una tarjeta de chip que contiene una clave de encriptación de evento o una clave de encriptación de usuario, la encriptación se procesa en el PC.

Declaración 17: el sistema de cualquiera de las declaraciones 1 a 13, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera incluye un módulo codificador CI con una interfaz CI&TS (interfaz común y flujo de transporte) para un Set-Top-Box STB profesional.

Declaración 18: el sistema de cualquiera de las declaraciones 1 a 17 donde el flujo de datos de base es un flujo de datos en abierto.

Declaración 19: el sistema de cualquiera de las declaraciones 1 a 17 donde el flujo de datos de base es un flujo de datos codificado por DVB.

Declaración 20: el sistema de la declaración 17, donde el módulo codificador CI comprende además una interfaz de alta velocidad para un PC, un flujo de transporte de base se envía al PC vía la interfaz de alta velocidad para ser selectivamente encriptado por el PC o por un periférico del PC, dicho periférico del PC es uno de los siguientes:

- un lector de tarjetas inteligentes SCR para una tarjeta inteligente SC que tiene un conjunto de circuitos de encriptación sobre la misma;

- un módulo de encriptación PCMCIA que tiene un conjunto de circuitos de encriptación y que forma un SCR para una tarjeta inteligente de cabecera.

Declaración 21: el sistema de cualquiera de las declaraciones precedentes, donde dichos paquetes de datos particulares comprenden contenido del que dependen paquetes de datos sucesivos.

Declaración 22: el sistema de cualquiera de las declaraciones 3 a 21, donde el sistema de acceso condicional se introduce en un Set-Top-Box (STB) de usuario.

Declaración 23: el sistema de cualquiera de las declaraciones 3 a 21, donde dicho sistema de acceso condicional incluye una tarjeta PC con una interfaz común CI para conexión a un Set-Top-Box (STB) de usuario.

Declaración 24: el sistema de la declaración 22 o la declaración 23, donde dicho Set-Top-Box (STB) de usuario es capaz de detectar un nivel de encriptación actual del flujo de transporte y dirigir el flujo de transporte, conforme al nivel de encriptación detectado, a un conjunto de circuitos de desencriptación asociado con ese nivel de encriptación.

Declaración 25: el sistema de la declaración 22 o la declaración 23, donde el Set-Top-Box (STB) de usuario es capaz de detectar al menos algunos de los siguientes niveles de encriptación del flujo de transporte:

- Ninguno

- Sólo DVB

- Sólo encriptación selectiva;

y el Set-Top-Box (STB) es capaz de dirigir el flujo de transporte a al menos uno de los siguientes medios de desencriptación:

- Ninguno

- Un sistema de acceso condicional introducido en el Set-Top-Box (STB) capaz de manejar DVB sólo,

- Un sistema de acceso condicional introducido en el Set-Top-Box (STB) capaz de manejar la encriptación selectiva sólo,

- Un módulo de acceso condicional en la primera ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de manejar DVB sólo,

- Un módulo de acceso condicional en la primera ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de manejar la encriptación selectiva sólo,

- Un módulo de acceso condicional en la segunda ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de manejar DVB sólo,

- Un módulo de acceso condicional en la segunda ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de manejar la encriptación selectiva sólo,

- Una tarjeta inteligente (SC) en un lector de tarjetas inteligentes (SCR).

[0014] Otras ventajas y características de la invención se harán evidentes a partir de la siguiente descripción de las formas de realización preferidas con referencia a los dibujos. En los dibujos:

Las figuras 1 a 6 son diagramas de bloque con leyendas descriptivas para formas de realización diferentes de un equipamiento de cabecera para producir selectivamente flujos de datos encriptados que contienen datos multimedia digitalizados;

Las figuras 7 a 10 son diagramas de bloque con leyendas descriptivas para formas de realización diferentes de un equipamiento de usuario para descodificar selectivamente flujos de datos encriptados que contienen datos multimedia digitalizados;

La fig. 11 es un diagrama que ilustra una primera forma de realización de un método para producir un flujo de transporte corrupto o codificado a partir de un flujo de transporte en abierto por encriptación selectiva;

La fig. 12 es un diagrama que ilustra un método para producir un flujo de transporte en abierto a partir de un flujo de transporte corrupto o codificado producido con el método de la figura 11;

La fig. 13 es un diagrama que ilustra una segunda forma de realización de un método para producir un flujo de transporte corrupto o codificado a partir de un flujo de transporte en abierto por encriptación selectiva; y

La fig. 14 es un diagrama que ilustra una tercera forma de realización de un método para producir un flujo de transporte corrupto o codificado a partir de un flujo de transporte en abierto por encriptación selectiva, donde el flujo de transporte corrupto o codificado consiste en paquetes selectivamente encriptados y paquetes DVB codificados.

[0015] Con referencia ahora a la fig. 1, se muestra una primera forma de realización de un componente de cabecera para producir un flujo de transporte selectivamente encriptado que contiene datos multimedia digitales. Específicamente, el componente incluye un PC de cabecera (ordenador personal) 10 con una interfaz 12 para una SC (tarjeta inteligente) 14 y una interfaz de comunicación bidireccional de alta velocidad en serie 16 (p. ej. una interfaz 1394 o USB2). La SC 14 tiene un procesador interno con capacidad de codificación o encriptado y una memoria segura para almacenar una pluralidad de claves de usuario privadas. El componente de cabecera incluye además un STB (Set-Top-Box) profesional (transmisor) 18 que tiene CI (interfaz común) e interfaz de TS (flujo de transporte) 20 y un puerto RF 22 para conectar a un enlace satelital 24. El componente de cabecera incluye por último un módulo de interfaz 26 para establecer una

conexión en serie de alta velocidad entre la interfaz 20 de STB 18 y la interfaz 16 de PC 10. El módulo 26 es preferiblemente una tarjeta PC según la norma PCMCIA e incluye un microprocesador y una memoria, además de una interfaz CI y TS y una interfaz en serie de alta velocidad.

[0016] Con referencia a la fig. 11, para generar flujo de transporte selectivamente encriptado SETS a partir de un flujo de transporte de base BTS que consiste en paquetes de datos digitales sucesivos numerados 1, 2,... 13..., se extraen paquetes de datos seleccionados del BTS y se encriptan o codifican con el conjunto de circuitos de la SC 14, utilizando una "clave de evento". En la forma de realización de la fig. 1, el BTS es un flujo de transporte digital en abierto que consiste en paquetes de datos sucesivos y disponibles en el PC 10. En la fig. 11, el paso de encriptación o de codificación se denomina "codificación de paquete". Se debe entender que el flujo de transporte de base BTS puede ser un TS en abierto, como se indica en la fig. 11, o un flujo de transporte codificado y, en particular, un flujo de transporte codificado por DVB convencional.

[0017] Las claves usadas en el método de encriptación/codificación selectiva incluyen un par de claves de usuario y un par de claves de evento, como se indica en la fig. 1, y cada par de claves puede ser simétrico o asimétrico, como también se indica en la fig. 1. Las claves de usuario (clave de usuario 2) se almacenan en la memoria de la SC 14 en el caso de las claves privadas (pares de claves públicas y privadas). Las claves de usuario se transmiten con el EMM en un entorno DVB para desencriptar las claves de evento usadas para la encriptación/codificación selectiva.

[0018] En el siguiente paso, denominado "reenvío/inserción de paquete" en la fig. 11, los paquetes de datos codificados o encriptados se insertan en el flujo de transporte reenviado en posiciones que se encuentran por delante en el tiempo de las posiciones correspondientes en el BTS original. Por ejemplo, el paquete de datos codificado #2 se inserta entre el paquete de datos # -3 y el paquete de datos # -1 y ahora la posición disponible entre los paquetes de datos #1 y #3 se rellena con el paquete de datos codificado #5. Como resultado, se proporciona un flujo de transporte selectivamente encriptado SETS, o codificado, como se muestra en la fig. 11.

[0019] El SETS se comunica al STB 18 vía el módulo 26 para transmisión de difusión sobre enlace satelital 24, como se ha visto en la fig. 1.

[0020] Con referencia a la fig. 7, una primera forma de realización de un componente de usuario final se muestra para recuperación conforme al método ilustrado en la fig. 12, a partir de un flujo de transporte selectivamente encriptado, como se puede producir con el componente en la fig. 1 y conforme al método de la fig. 11, un flujo de transporte en abierto.

[0021] El componente de usuario mostrado en la fig. 7 incluye un módulo de tarjeta PC 30 denominado "módulo de cifrado selectivo", que incluye una interfaz CI & TS 32 (interfaz común e interfaz para flujo de transporte), un lector de tarjeta inteligente incorporado 34, un microprocesador con unidad de memoria 36 y un filtrado de paquete y lógica de inserción 38. El componente de usuario funciona con una tarjeta inteligente 40 que se inserta en el lector 34 y se denomina en la fig. 7 "tarjeta inteligente de pago por evento". Por supuesto, este es sólo uno de los muchos escenarios posibles en un entorno DVB protegido.

[0022] El módulo 30 se inserta en una ranura CI de un Set-Top-Box convencional que tiene la capacidad de recibir un flujo de transporte selectivamente encriptado/codificado, tal como el producido por el equipamiento en la fig. 1, que ha convertido el flujo de transporte encriptado/codificado en un flujo en abierto mediante el módulo 30, y que reenvía una señal de vídeo/audio a un aparato tal como un aparato de TV.

[0023] Con referencia a la fig. 12, se recibe un flujo de transporte selectivamente encriptado SETS y se extraen paquetes de datos encriptados para la desencriptación o descodificación por el conjunto de circuitos de la SC 40. La clave de usuario para este tipo de desencriptación se almacena en una memoria segura de SC 40. Este paso se denomina "descodificación de paquete" en la fig. 12. Como siguiente paso, los paquetes de datos descodificados se insertan en el flujo de transporte reenviado en ubicaciones correspondientes en tiempo a las posiciones originales en el flujo de transporte de base BTS. Como resultado, se obtiene un flujo de transporte en abierto CTS.

[0024] En esta forma de realización, la desencriptación selectiva se realiza con el conjunto de circuitos de la SC 40. Esto es posible debido a que la encriptación selectiva propuesta en este caso se puede abordar en el lado del usuario con un requisito de rendimiento de hardware moderado, como típicamente incorpora una tarjeta inteligente. En otras formas de realización de la invención, no obstante, la desencriptación selectiva se puede realizar mediante el conjunto de circuitos incorporado en el módulo 30 o el software/firmware que reside en el mismo.

[0025] Con referencia a las figuras 2 a 6, se muestran diferentes formas de realización del componente de cabecera, pero todas pueden tener la misma funcionalidad que en la fig. 1. Específicamente, la forma de realización de la fig. 2 funciona sin un PC, y la encriptación de los paquetes de datos seleccionados se realiza en el módulo 26, que es un lector de tarjetas inteligentes de tarjeta PC para SC 14. Alternativamente, la encriptación se puede realizar mediante un conjunto de circuitos en la SC 14, como se muestra en la fig. 3 donde la SC 14 tiene un codificador 29. La selección de los paquetes de datos que se van a encriptar se lleva a cabo bien mediante software ejecutado por un microprocesador 27 de 10 dentro del módulo 26, bien mediante un filtro de hardware incorporado en el módulo 26. En la fig. 4, el

codificador 29 se muestra como incorporado en el módulo 26. En la fig. 5, la funcionalidad del módulo 26 se incorpora en el STB 18, que está equipado con un lector de tarjetas inteligentes 13 para la SC 14. El codificador 29 se incorpora en la SC 14. En la fig. 6, la única diferencia con respecto a la fig. 5 es que el codificador 29 está incorporado en el STB 18.

[0026] Con referencia a la figura 8, se muestran detalles de la tarjeta inteligente de usuario (SC) 40 (véase la fig. 7). La SC 40 tiene una interfaz 35 que corresponde a la interfaz 34 del módulo 30. También tiene un descodificador de paquete privado 50 para la desencriptación de los paquetes de datos selectivamente encriptados y un microordenador 52 con un microprocesador y una memoria para almacenar una clave de evento, o una clave de usuario en caso de que se descargue una clave de evento con los EMMUs. En la fig. 8, se supone que la SC 40 es una "tarjeta inteligente de pago por evento".

[0027] Con referencia a las figuras 9 y 10, se muestran formas de realización diferentes del componente de usuario, pero todas pueden tener la misma funcionalidad que las de la fig. 7. Específicamente, en la forma de realización de la fig. 9, el componente de usuario incluye un Set-Top-Box (STB) de usuario 37 con una interfaz 39 para el módulo 30. El módulo 30 tiene incorporado un descodificador DVB convencional 41. En esta forma de realización, la desencriptación de los "paquetes de datos seleccionados" se realiza en la SC 40, mientras que la descodificación DVB se realiza en el módulo 30, que es un módulo de acceso condicional (CAM) mejorado para afrontar las necesidades de la encriptación selectiva de paquete de datos. En la forma de realización de la fig. 10, la funcionalidad del módulo 30 se ha incorporado en el STB 37, como se conoce por los sistemas de acceso condicional introducidos convencionales. Por consiguiente, STB 37 tiene una interfaz 53 para la SC 40. La desencriptación de los paquetes de datos selectivamente encriptados se sigue llevando a cabo mediante el conjunto de circuitos en la SC 40, es decir mediante el descodificador 50.

[0028] Tras haber descrito las formas de realización básicas, se hacen evidentes otras mejoras a partir de las figuras 13 y 14.

[0029] En la fig. 13, se muestra en detalle el procesamiento de un paquete de datos para la encriptación selectiva. Los paquetes de datos seleccionados en este caso para su encriptación son preferentemente aquellos cuyo contenido se propaga para suceder a los paquetes de datos en un flujo de transporte MPEG, de modo que se consigue un efecto de codificación relativamente potente con un porcentaje relativamente reducido de paquetes de datos encriptados. Este es un factor importante si la desencriptación de los paquetes de datos selectivamente encriptados se tiene que realizar en una tarjeta inteligente con capacidad de procesamiento intrínsecamente moderada, pero con un nivel de seguridad intrínsecamente alto.

[0030] En la Fig. 14, se ilustra la generación de un flujo de transporte parcialmente codificado por DVB y selectivamente encriptado. Como se ve fácilmente, todos los paquetes de datos diferentes de los paquetes de datos selectivamente encriptados se codifican por DVB. Específicamente, un contenido en abierto está parcialmente selectivamente encriptado y codificado parcialmente por DVB, las claves DVB se procesan a partir del contenido en abierto del paquete selectivamente encriptado.

[0031] De esta manera, se proporciona un flujo completamente codificado sin utilizar EMM para difundir claves DVB. El flujo codificado contiene las palabras de control (CW) que se procesan a partir de un paquete selectivamente encriptado que se ha desencriptado. El nivel de seguridad sigue siendo alto ya que esas palabras de control sólo podrían recuperarse si la "tarjeta de un evento" está disponible para desencriptar los paquetes selectivamente encriptados. Esta solución tiene la ventaja de que el flujo está completamente codificado y de que la difusión del contenido es independiente de los EMMs, de este modo independiente de las empresas de radiodifusión (como TPS, Canal +, etc.).

[0032] En la figura 14, se ilustra el proceso para obtener el flujo de codificación:

- paquetes que se van a encriptar selectivamente son sel 1, sel 2, sel 3

- paquetes que se van a codificar por DVB son 1.1,1.2,....,1.n,2.1,2.2,....,2.n,3.1, 3.2...

- CW(Sel i) es la palabra de control calculada a partir del contenido Sel i en abierto y que se usará para codificar los paquetes i.1,i.2,...,i.n

- tan pronto como CW (Sel i) se procesa, Sel i se encripta en la tarjeta inteligente de cabecera (por ejemplo)

- CW(Sel i) se alimenta al codificador DVB para procesar el codificado i.1,i.2,...,i.n

- Sel i encriptado se inserta por delante de i.1,i.2,.....,i.n

[0033] Cuando un usuario STB recibe el flujo codificado,

- éste enviará el paquete encriptado Sel i a la tarjeta inteligente,

- la tarjeta inteligente desencriptará Sel i,

- la tarjeta inteligente procesará CW(Sel i),

- Sel i se enviará al descodificador DVB,

- el descodificador DVB descodificará los paquetes i.1,i.2,...,i.n con Sel i.

REIVINDICACIONES

1. Sistema de acceso condicional donde los datos multimedia digitalizados se transmiten en un flujo de transporte continuo de paquetes de datos sucesivos y donde un flujo de transporte selectivamente encriptado se forma a partir de un flujo de transporte de base mediante la detección de paquetes de datos particulares en el flujo de transporte de base, dicho sistema está **caracterizado por el hecho de que** los paquetes de datos particulares se retiran y se encriptan con una clave de encriptación de evento, dichos paquetes de datos encriptados se insertan en el flujo de transporte de base restante en posiciones de inserción por delante en el tiempo con respecto a las posiciones originales de los paquetes de datos particulares en el flujo de transporte de base.

2. Sistema según la reivindicación 1, donde se provee una clave de desencriptación de evento para un receptor autorizado provisto del sistema de acceso condicional, el flujo de transporte selectivamente encriptado se transmite al receptor, el sistema de acceso condicional detecta paquetes de datos encriptados, retira los paquetes de datos encriptados del flujo de transporte recibido, desencripta los paquetes de datos encriptados con la clave de desencriptación de evento e inserta los paquetes de datos desencriptados en el flujo de transporte recibido restante en posiciones correspondientes a las posiciones originales respectivas de los paquetes de datos particulares en el flujo de transporte de base.

3. Sistema según la reivindicación 2, donde la clave de desencriptación de evento se provee en una tarjeta inteligente de un solo evento.

4. Sistema según la reivindicación 2, donde la clave de desencriptación de evento se provee en una tarjeta inteligente de un periodo limitado.

5. Sistema según la reivindicación 2, donde la clave de desencriptación de evento, en un entorno DVB, se transmite en EMMs específicos protegidos por una clave de encriptación de usuario, la clave de desencriptación de usuario correspondiente se provee en el CAS, en una tarjeta inteligente de usuario o en una SIM de usuario.

6. Sistema según la reivindicación 2, donde el sistema de acceso condicional tiene una memoria de búfer para almacenar paquetes de datos en abierto mientras se desencripta un paquete de datos encriptado.

7. Sistema según la reivindicación 2, donde dichos paquetes de datos encriptados se insertan en posiciones que se encuentran un número predeterminado de paquetes de datos por delante de las posiciones originales respectivas.

8. Sistema según cualquiera de las reivindicaciones 2 a 7, donde dicho sistema de acceso condicional incluye una tarjeta de chip con conjunto de circuitos de desencriptación sobre la misma.

9. Sistema según la reivindicación 8, donde la tarjeta inteligente es una tarjeta SIM.

10. Sistema según cualquiera de las reivindicaciones precedentes, donde la clave de desencriptación se transmite a un receptor con el flujo de datos selectivamente encriptados.

11. Sistema según cualquiera de las reivindicaciones 1 a 10, donde la clave de desencriptación de evento es una clave fija distribuida sobre una base de pago por evento.

12. Sistema según la reivindicación 11, donde la clave de desencriptación de evento se transmite en una red GSM antes de un evento y se carga en una tarjeta SIM o tarjeta inteligente insertada en un lector de tarjetas SIM o inteligentes de un teléfono móvil.

13. Sistema según cualquiera de las reivindicaciones precedentes, donde la clave de desencriptación de evento se provee encriptada con una clave de encriptación de usuario y también se provee una clave de desencriptación de usuario correspondiente a un usuario autorizado.

14. Sistema según cualquiera de las reivindicaciones precedentes, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera incluye una interfaz común CI que a su vez tiene una interfaz de tarjeta inteligente SC para una tarjeta inteligente que comporta un conjunto de circuitos de encriptación sobre la misma.

15. Sistema según cualquiera de las reivindicaciones 1 a 13, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera incluye una interfaz común CI para un módulo de tarjeta PC que comporta un conjunto de circuitos de encriptación sobre la misma.

16. Sistema según cualquiera de las reivindicaciones 1 a 13, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera incluye un ordenador personal PC con una interfaz para una tarjeta inteligente con una clave de encriptación de evento o una clave de encriptación de usuario, la encriptación se procesa en el PC.

17. Sistema según cualquiera de las reivindicaciones 1 a 13, que comprende un codificador de cabecera para producir el flujo de datos selectivamente encriptados, el codificador de cabecera incluye un módulo codificador CI con una interfaz CI&TS (interfaz común y flujo de transporte) para un Set-Top-Box STB profesional.

18. Sistema según cualquiera de las reivindicaciones 1 a 17, donde el flujo de datos de base es un flujo de datos en abierto.

19. Sistema según cualquiera de las reivindicaciones 1 a 17, donde el flujo de datos de base es un flujo de datos codificado por DVB.

20. Sistema según la reivindicación 17, donde el módulo codificador CI comprende además una interfaz de alta velocidad para un PC, un flujo de transporte de base se envía al PC vía la interfaz de alta velocidad para ser selectivamente encriptado por el PC o por un periférico del PC, dicho periférico del PC es uno de los siguientes:

- un lector de tarjetas inteligentes SCR para una tarjeta inteligente SC que tiene un conjunto de circuitos de encriptación sobre la misma;

- un módulo de encriptación PCMCIA que tiene un conjunto de circuitos de encriptación y que forma un SCR para una tarjeta inteligente de cabecera.

21. Sistema según cualquiera de las reivindicaciones precedentes, donde dichos paquetes de datos particulares se componen de contenido del cual dependen paquetes de datos sucesivos.

22. Sistema según cualquiera de las reivindicaciones 2 a 21, donde el sistema de acceso condicional se introduce en un Set-Top-Box (STB) de usuario.

23. Sistema según cualquiera de las reivindicaciones 2 a 21, donde dicho sistema de acceso condicional incluye una tarjeta PC con una interfaz común CI para la conexión a un Set-Top-Box (STB) de usuario.

24. Sistema según la reivindicación 22 o la reivindicación 23, donde dicho Set-Top-Box (STB) de usuario es capaz de detectar un nivel de encriptación actual del flujo de transporte y dirigir el flujo de transporte, conforme al nivel de encriptación detectado, hacia un conjunto de circuitos de desencriptación asociado con ese nivel de encriptación.

25. Sistema según la reivindicación 22 o la reivindicación 23, donde el Set-Top-Box (STB) de usuario es capaz de detectar al menos algunos de los siguientes niveles de encriptación del flujo de transporte:

- Ninguno
- DVB sólo
- Encriptación selectiva sólo;

y el Set-Top-Box (STB) es capaz de dirigir el flujo de transporte hacia al menos uno de los siguientes medios de desencriptación:

- Ninguno
- Un sistema de acceso condicional integrado en el Set-Top-Box (STB) capaz de tratar el DVB sólo,
- Un sistema de acceso condicional integrado en el Set-Top-Box (STB) capaz de tratar la encriptación selectiva sólo,
- Un módulo de acceso condicional en la primera ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de tratar el DVB sólo,
- Un módulo de acceso condicional en la primera ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de tratar la encriptación selectiva sólo,
- Un módulo de acceso condicional en la segunda ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de tratar el DVB sólo,
- Un módulo de acceso condicional en la segunda ranura de la interfaz común (CI) del Set-Top-Box (STB) capaz de tratar la encriptación selectiva sólo,
- Una tarjeta inteligente (SC) en un lector de tarjetas inteligentes (SCR).

26. Método para producir un flujo de transporte corrupto o parcialmente encriptado a partir de un flujo de transporte en abierto que contiene datos multimedia digitalizados en paquetes de datos sucesivos, donde un flujo de transporte selectivamente encriptado se forma a partir de un flujo de transporte en abierto mediante la detección de paquetes de datos particulares en el flujo de transporte en abierto, dicho método está **caracterizado por el hecho de que** los paquetes de datos particulares se retiran y se encriptan con una clave de encriptación de evento, dichos paquetes de datos encriptados se insertan en el flujo de transporte en abierto restante en posiciones de inserción que se encuentran por delante en el tiempo con respecto a las posiciones originales de los paquetes de datos particulares en el flujo de transporte en abierto.

Fig. 1: Componente de cabecera: STB profesional, CI para módulo I/F bidireccional de alta velocidad y PC con I/F de SC e I/F bidireccional de alta velocidad

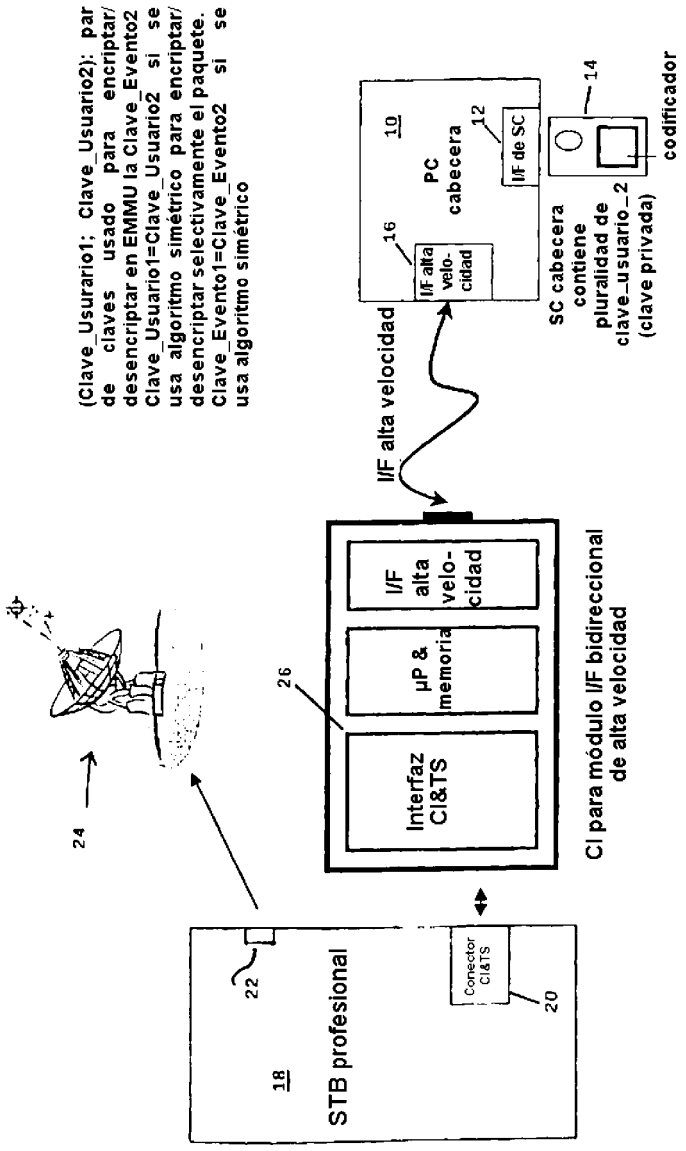


Fig. 2: Componente de cabecera: STB profesional, módulo CI que incluye SCR, encriptación por SC

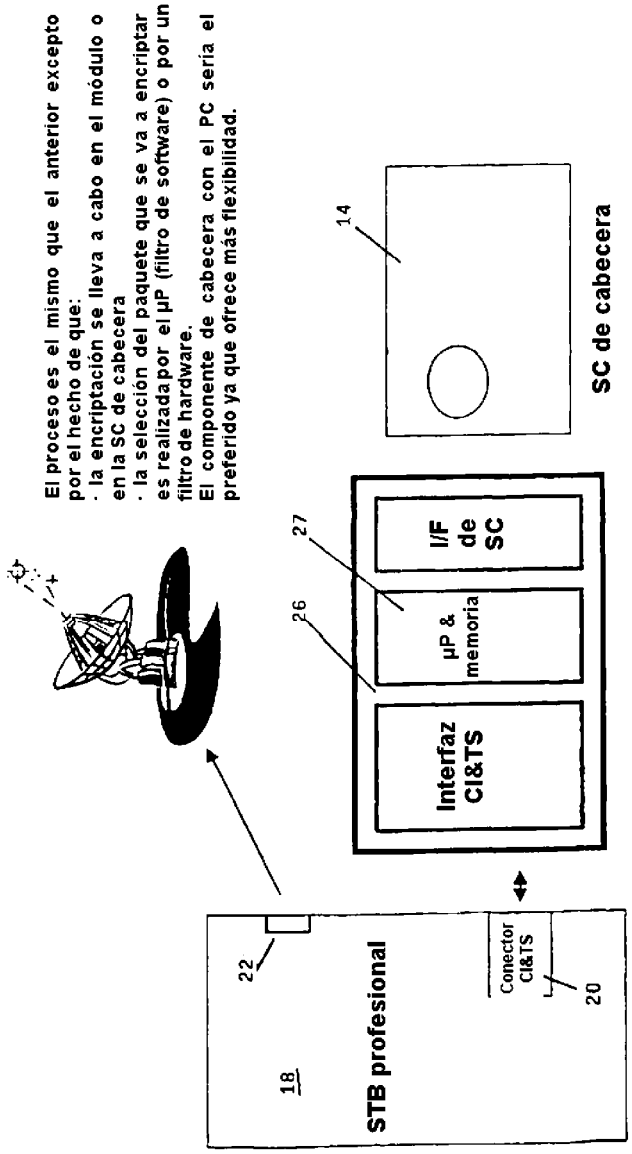


Fig. 3: Componente de cabecera: STB profesional, módulo CI que incluye SCR, encriptación por SC de cabecera

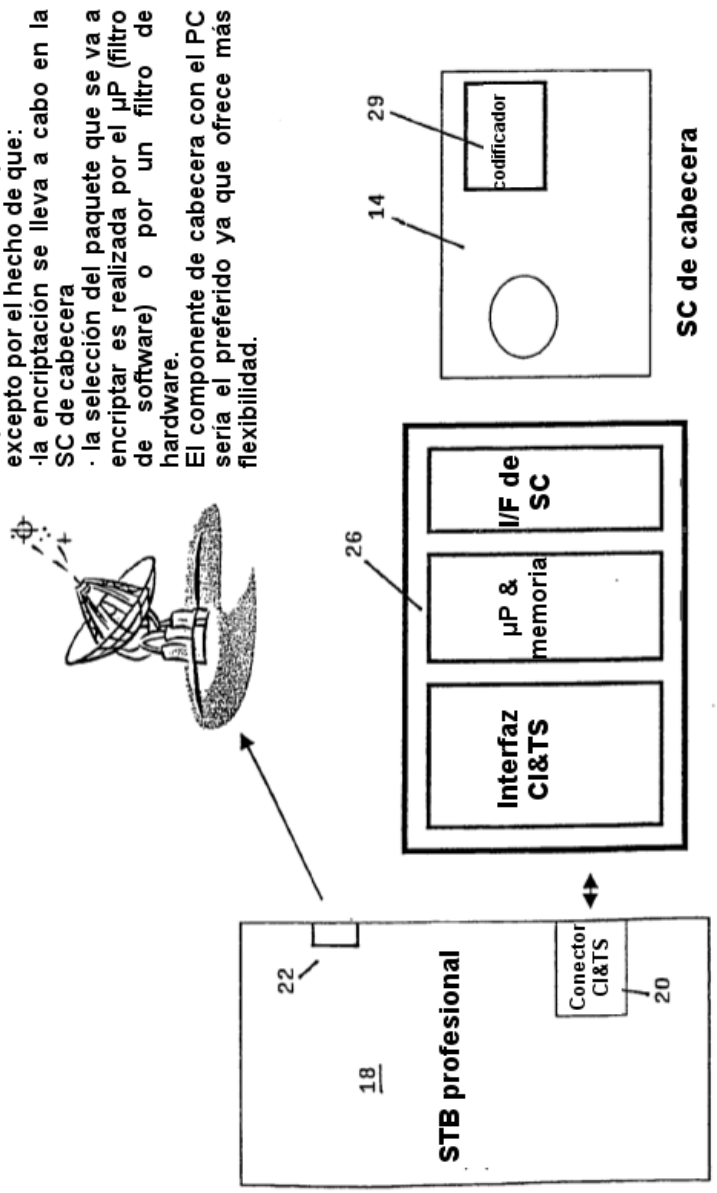


Fig. 4: Componente de cabecera: STB profesional, módulo CI que incluye SCR, encriptación por módulo

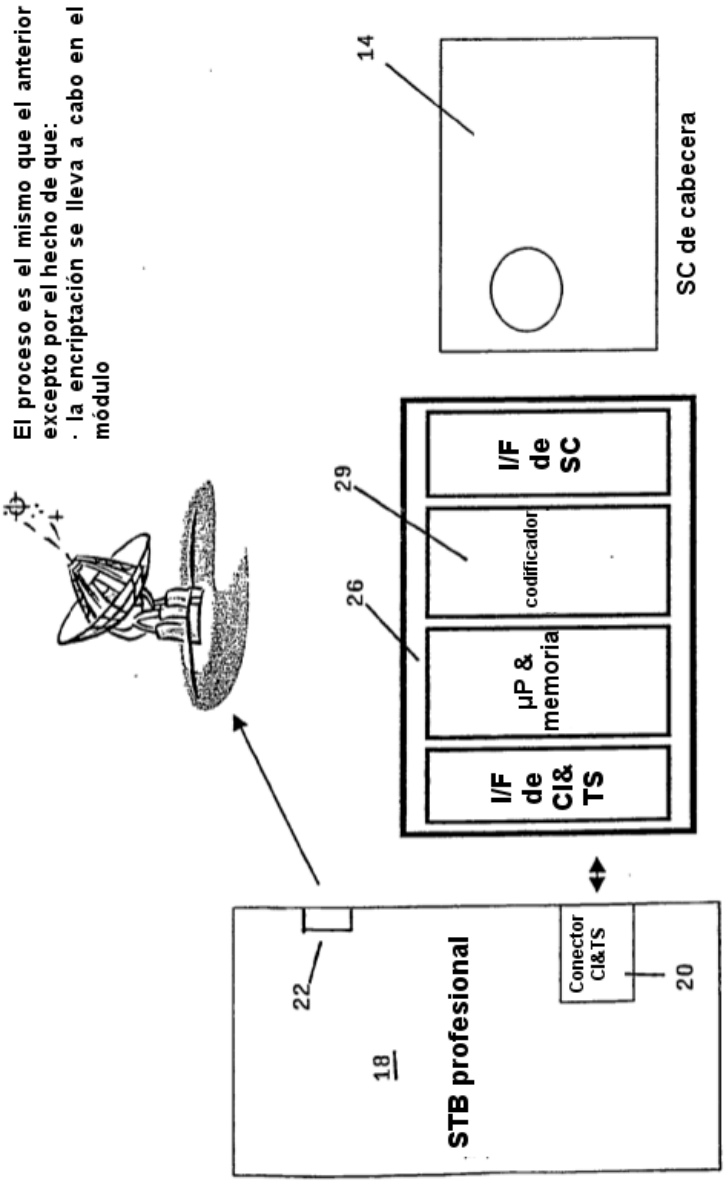


Fig. 5: Componente de cabecera: STB profesional que incluye SCR, encriptación por SC de cabecera

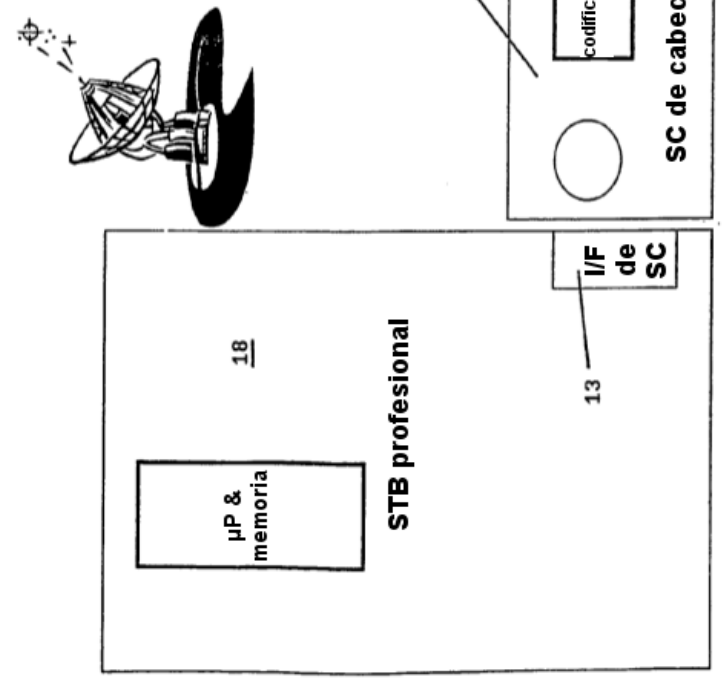


Fig. 6: Componente de cabecera: STB profesional que incluye SCR, encriptación por STB

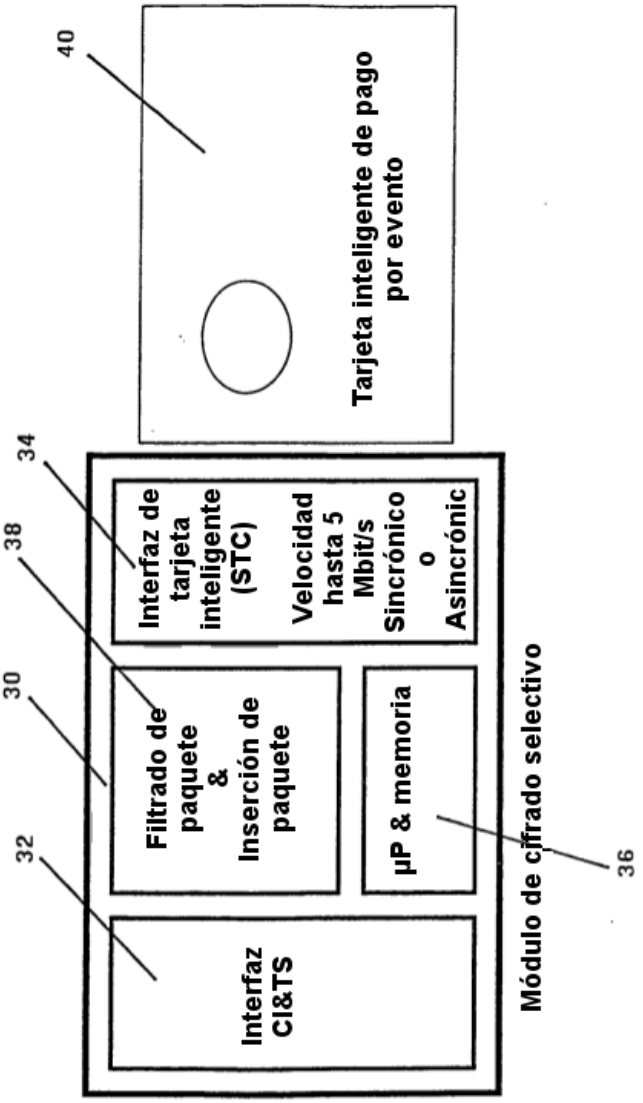


Fig. 7: Descodificador de usuario: STB + Módulo de cifrado selectivo + SC de usuario

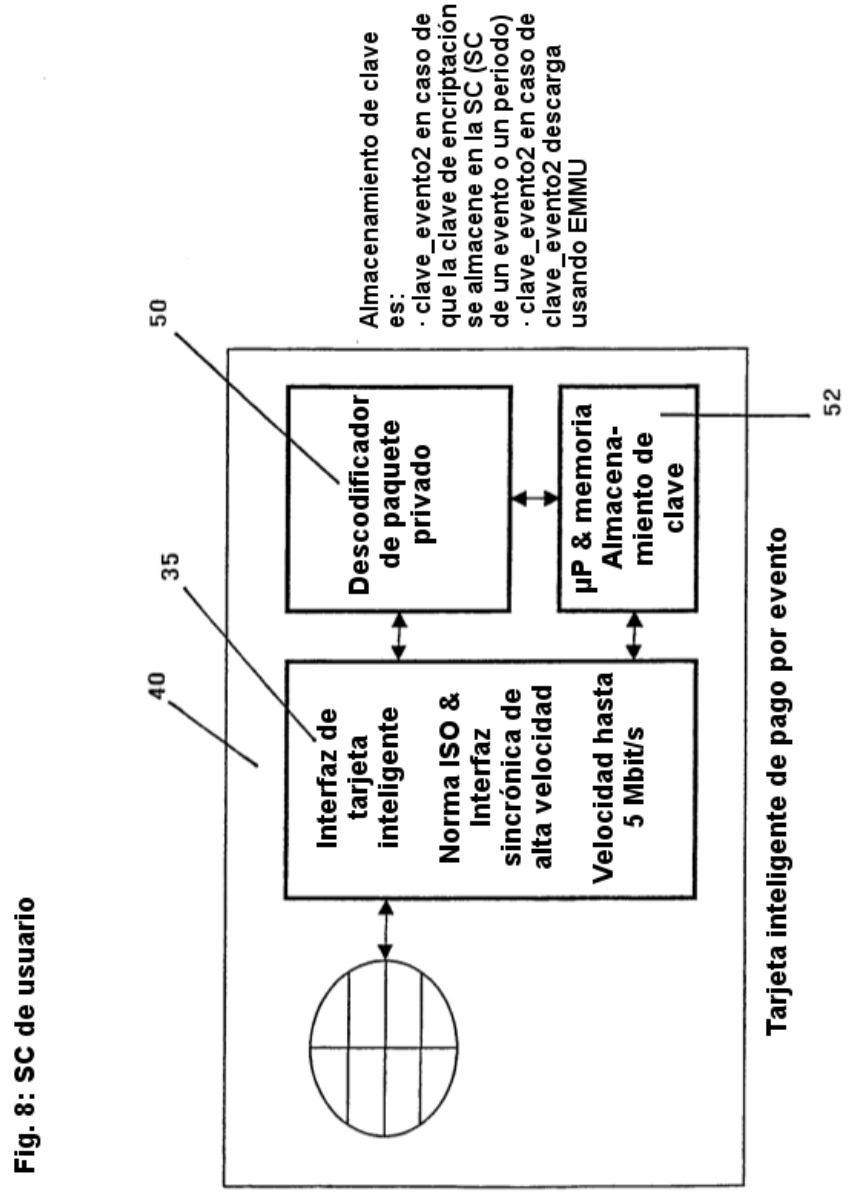


Fig. 8: SC de usuario

Fig. 9: Descodificador de usuario: STB de usuario, módulo actualizado de CI de DVB estándar y SC de usuario

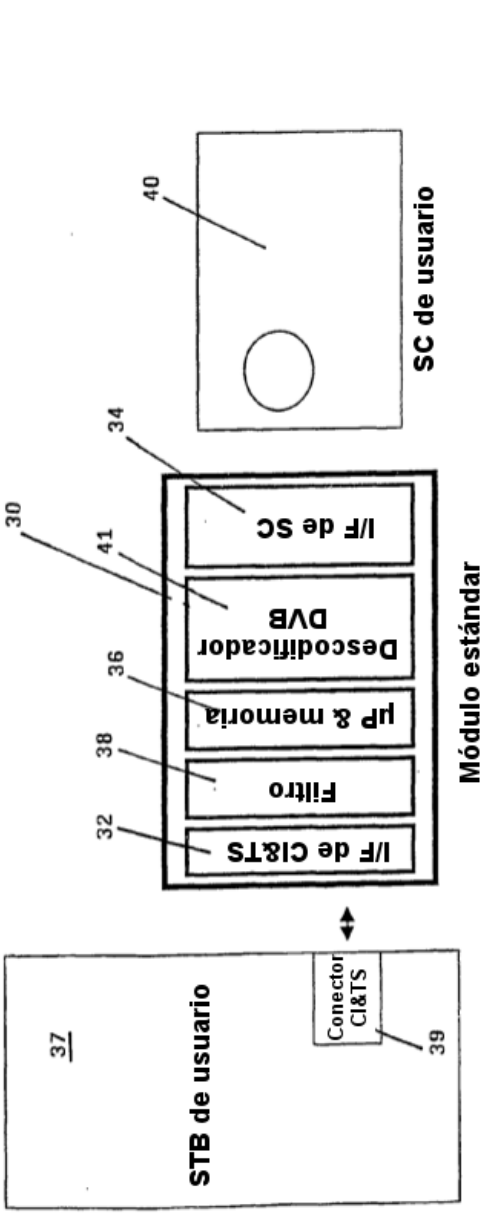


Fig. 10: Descodificador de usuario: STB de usuario que incluye SCR

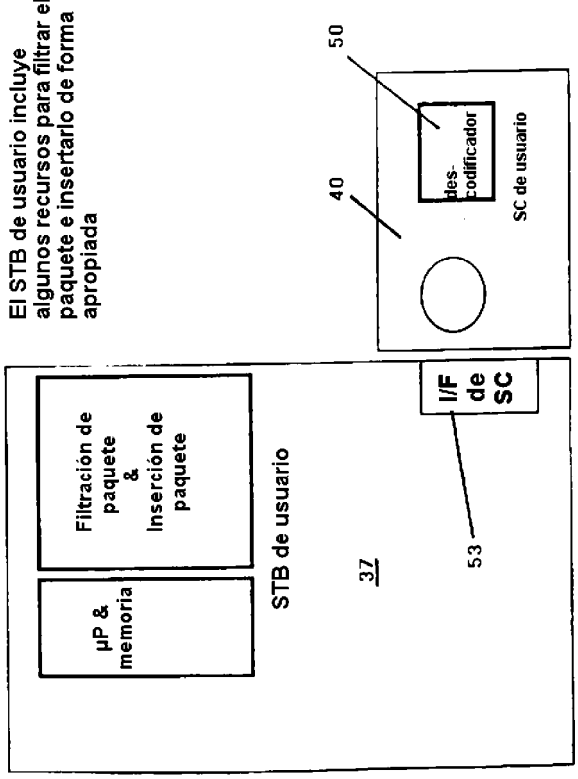


Fig 11 :

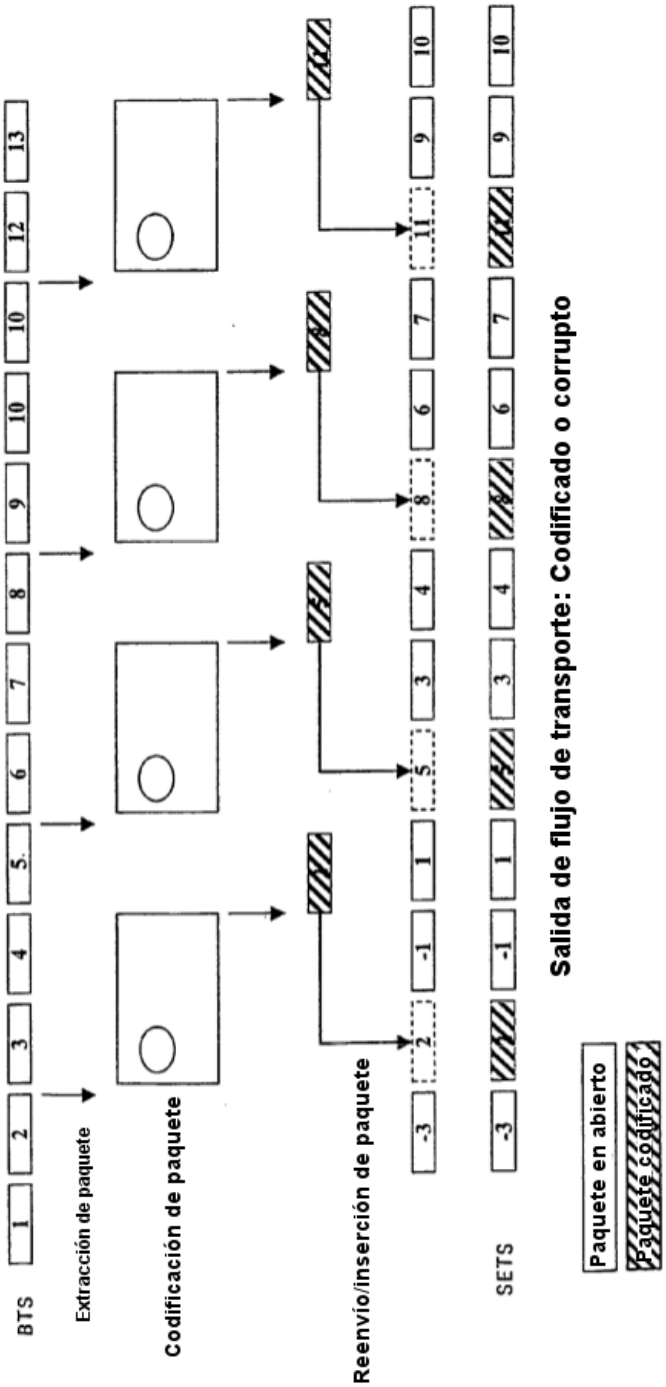

Entrada de flujo de transporte: en abierto
BTS
1
2
3
4
5.
6
7
8
9
10
10
12
13
Extracción de paquete
Codificación de paquete
Reenvío/inserción de paquete
-3
2
-1
1
5
3
4
8
6
7
11
9
10
SETS
-3
-1
1
3
4
6
7
9
10
Salida de flujo de transporte: Codificado o corrupto
Paquete en abierto
Paquete codificado

Fig 12 :

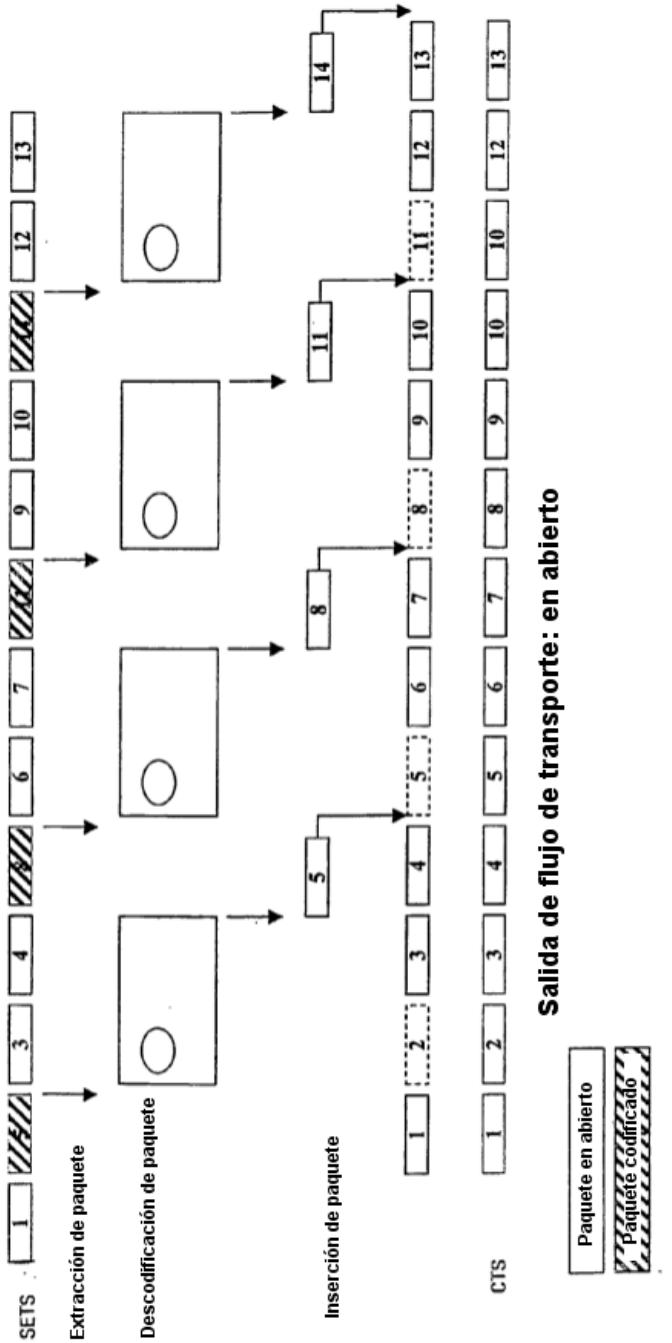

Entrada de flujo de transporte: codificado o corrupto
SETS
Extracción de paquete
Descodificación de paquete
Inserción de paquete
CTS
Salida de flujo de transporte: en abierto
Paquete en abierto
Paquete codificado

Fig. 13: encriptación de bits de signo del coeficiente AC & DC

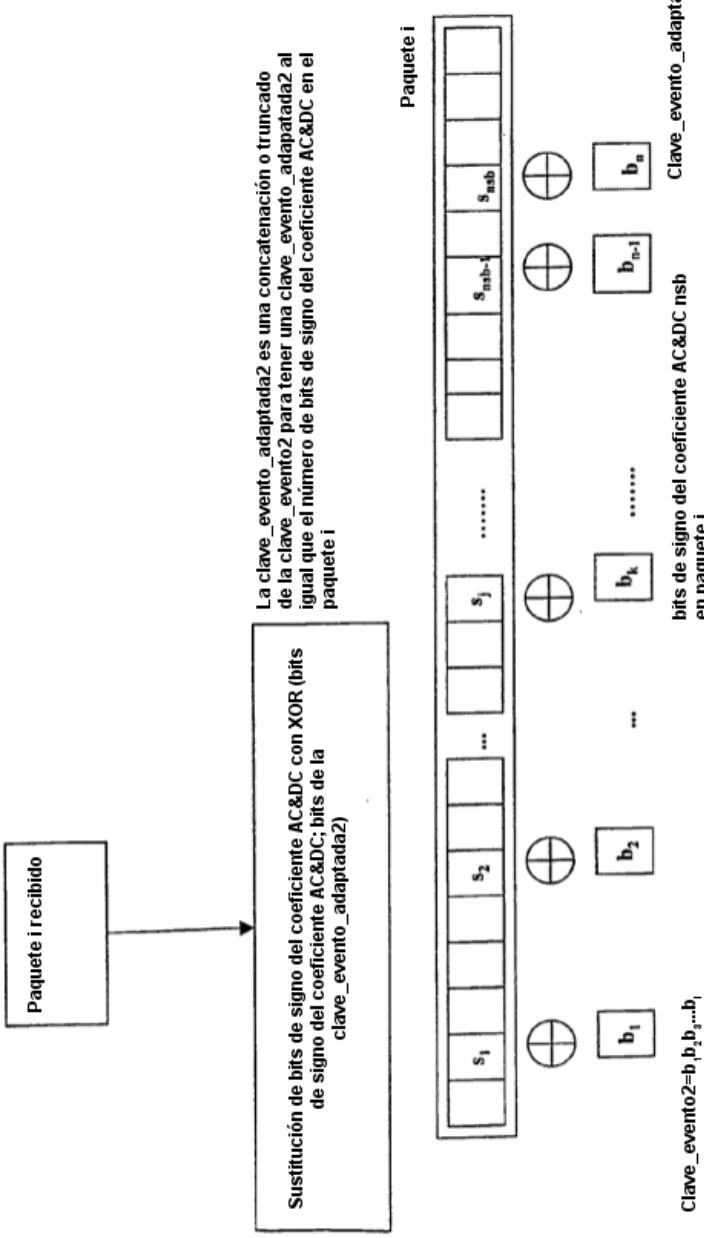
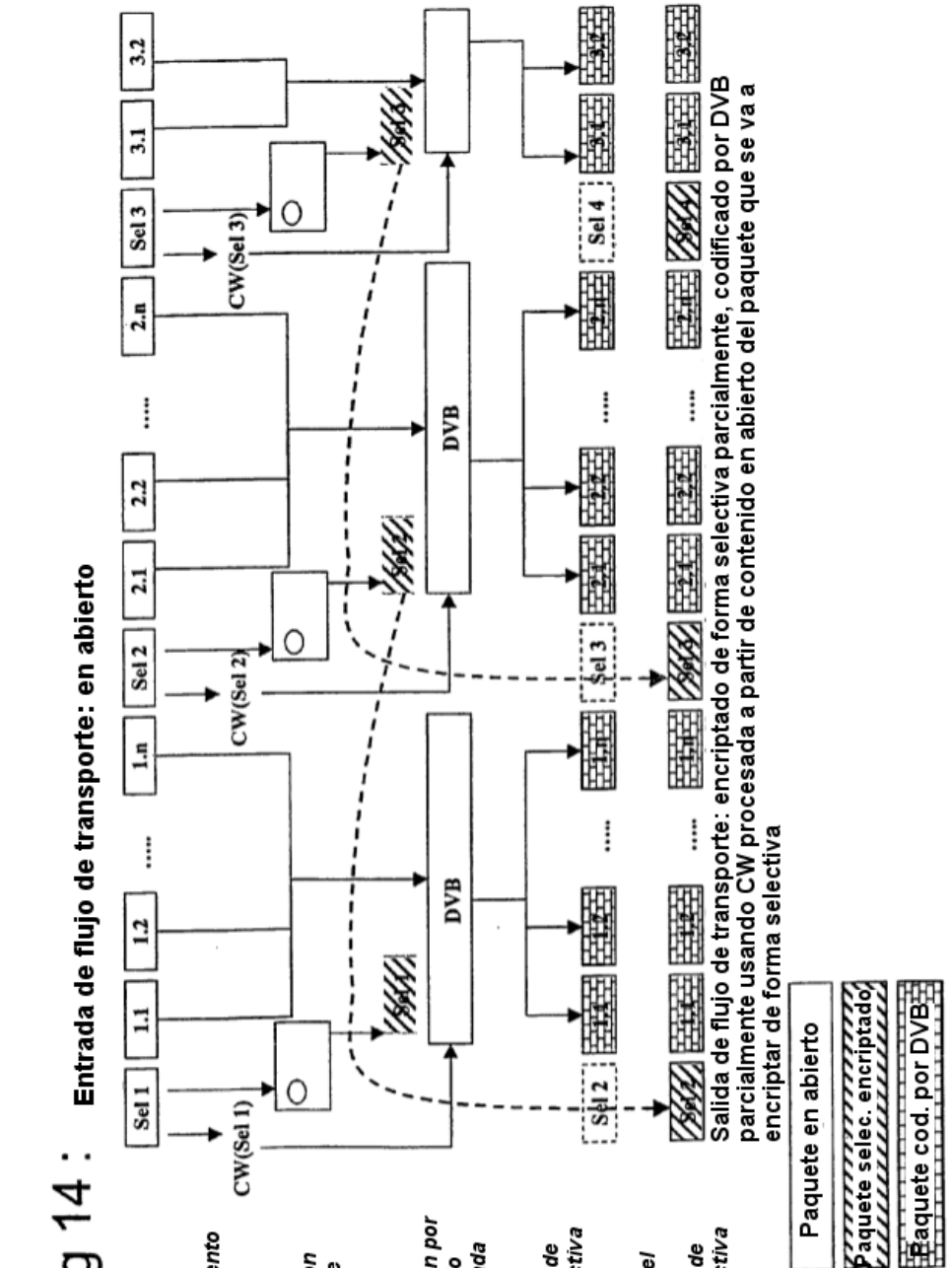


Fig 14 :


Entrada de flujo de transporte: en abierto
Sel 1
1.1
1.2
1.n
Sel 2
2.1
2.2
2.n
Sel 3
3.1
3.2
CW(Sel 1)
CW(Sel 2)
CW(Sel 3)
DVB
Sel 4
Procesamiento CW DVB
Encriptación selectiva de paquete
Codificación por DVB usando CW calculada sobre el paquete encriptado de forma selectiva anterior
Inserción del paquete encriptado de forma selectiva
Salida de flujo de transporte: encriptado de forma selectiva parcialmente, codificado por DVB parcialmente usando CW procesada a partir de contenido en abierto del paquete que se va a encriptar de forma selectiva
Paquete en abierto
Paquete selec. encriptado
Paquete cod. por DVB