(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 789**

(51) Int. CI.:

G06F 21/10 (2013.01)
H04N 21/436 (2011.01)
H04N 21/4408 (2011.01)
H04N 21/845 (2011.01)
H04N 21/418 (2011.01)
H04N 21/4367 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/658 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.03.2015 E 15159981 (8)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 3070629**

(54) Título: **Método y dispositivo para proteger un contenido multimedia descifrado antes de su transmisión a un dispositivo de consumo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.11.2019

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

FISCHER, JEAN-BERNARD

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Método y dispositivo para proteger un contenido multimedia descifrado antes de su transmisión a un dispositivo de consumo

Introducción

La presente solicitud se refiere a la protección de contenido multimedia de acceso condicional que un decodificador recibe y procesa. El decodificador se encarga de recibir el contenido multimedia protegido y de quitarle la protección para que el usuario pueda acceder al mismo.

Antecedentes de la invención

Los dispositivos de consumo, como decodificadores, computadoras, tabletas o cualquier dispositivo de procesamiento conectado a una pantalla, se encargan de recibir contenido multimedia protegido, eliminar la protección y transmitirlo desprotegido a dispositivos de consumo, como los televisores.

El contenido multimedia podría adquirir la forma de un vídeo, que generalmente se cifra mediante una clave única, que es la clave del contenido multimedia. El así denominado contenido multimedia cifrado se almacena en un servidor de gestión mientras se espera que el dispositivo de consumo inicie su solicitud.

Cuando el dispositivo de consumo, o el usuario del mismo, solicita un contenido multimedia, el mensaje que lo solicita contiene una identificación de dicho dispositivo de consumo. El centro de gestión puede, a continuación, preparar un mensaje seguro, que contiene la clave del contenido multimedia y que se cifra con una clave que pertenece al decodificador. El centro de gestión obtiene esa clave gracias a los datos de identificación proporcionados en el mensaje de solicitud. Esto significa que el centro de gestión almacena una clave personal para cada dispositivo de consumo y que obtiene la correcta gracias a los datos de identificación.

El mensaje seguro, cifrado mediante la clave personal, se envía al dispositivo de consumo. Este último descifra el mensaje seguro, obtiene la clave del contenido multimedia y lo descifra.

El dispositivo de consumo cuenta con medios de seguridad, por ejemplo, un módulo de seguridad, una tarjeta inteligente, un chip dedicado o un software ofuscado, para descifrar el contenido multimedia cifrado. Por lo tanto, manipulando la clave personal es muy difícil romper la seguridad del contenido multimedia cifrado. En algunos casos, el contenido multimedia se almacena de forma local y cuando está descifrado se vuelve a cifrar mediante una clave local. Por lo tanto, un atacante se centrará en el dispositivo de consumo para intentar obtener la clave local y poder conseguir el valioso contenido multimedia descifrado.

Si se trata de un portal de enlace doméstico, este recibe el contenido multimedia cifrado del proveedor y lo descifra utilizando sus propios medios de seguridad. Antes de transmitir el contenido multimedia al dispositivo de consumo, lo vuelve a cifrar mediante una clave local, que el portal de enlace doméstico y el dispositivo de consumo comparten. El nivel de protección de la clave local almacenada en el dispositivo de consumo es menor que en los medios de seguridad del portal de enlace doméstico, así que el atacante centrará sus esfuerzos en obtener la clave local del mismo.
Un ataque a la clave del contenido multimedia mientras se utiliza para descifrar el contenido es suficiente obtener todo el contenido descrifrado. Por lo tanto, el pirata solo necesita realizar un ataque por contenido, lo que significa un gran incentivo: incluso si tarda varios días en hackear la clave, vale la pena acceder a un contenido de alto valor. Además, dado que el contenido a menudo está disponible de forma gratuita desde la red de distribución de contenido (CDN), no tiene que redistribuir el contenido: simplemente puede redistribuir la clave del contenido multimedia y dejar que los destinatarios lo obtengan desde la CDN.

Los expedientes de invenciones anteriores US2012/0246462-A1, US2014/0281481-A1 y US2013/0227283-A1 revelan sistemas y métodos para contenido protegido y distribuido a través de una red y volver a cifrarlo para su uso local.

Breve descripción de la invención

Según una modalidad de la invención, se propone un método y un dispositivo para proteger un contenido multimedia descifrado antes de su transmisión a un dispositivo de consumo. Se propone un método para proteger un contenido multimedia cifrado mediante una clave del contenido multimedia, dicho método se lleva a cabo mediante un módulo

de seguridad integrado en un dispositivo de recepción y en conexión con un decodificador, dicho método consta de los pasos siguientes:

a. Recibir el contenido multimedia cifrado mediante una clave del contenido multimedia.
b. Recibir un mensaje seguro que contenga la clave del contenido multimedia, dicho mensaje se cifrará mediante una clave personal del módulo de seguridad.
c. Descifrar el mensaje seguro mediante la clave personal para obtener la clave del contenido multimedia.
d. Descifrar el contenido multimedia que ha sido cifrado mediante la clave del contenido multimedia.
e. Generar una clave local actual.
f. Cifrar una parte del contenido multimedia mediante la clave local actual, dicha parte define un fragmento.
g. Transmitir de forma segura la clave local actual al decodificador.
h. Transmitir el fragmento cifrado al decodificador.
i. Repetir los pasos de e) a h) para cada parte del contenido multimedia y modificar la clave local actual para cada fragmento diferente.

Según la solución propuesta, el contenido multimedia que entra en los medios de seguridad se cifra mediante una sola clave, que es la clave del contenido multimedia. Al salir del entorno seguro de los medios de seguridad, el contenido multimedia se cifra mediante diversas claves, cada una de las cuales se aplica a una parte del contenido multimedia, denominada fragmento.

Mediante la introducción de un dispositivo intermedio de alta seguridad (es decir, el módulo de seguridad) que descifra y vuelve a cifrar el contenido multimedia, simplemente compartir la clave del contenido multimedia (local) para volver a cifrarlo deja de ser una solución y el pirata tiene que volver a distribuir el contenido multimedia. Al cifrar fragmentos pequeños con claves diferentes, la complejidad de obtener miles de claves para descifrar el contenido hace que sea muy difícil para el pirata descifrar todo el contenido en un plazo de tiempo y coste razonables, de modo que se elimina el incentivo de hacerlo.

Breve descripción de las figuras

La presente invención se puede entender mejor gracias a las figuras adjuntas en las que:

- La figura 1 representa los dispositivos que reciben, descifran y vuelven a cifrar el contenido multimedia.
- La figura 2 muestra la transformación del contenido multimedia.
- La figura 3 muestra un chip seguro en el decodificador a cargo de descifrar los fragmentos.
- La figura 4 muestra el módulo de seguridad a cargo descifrar y volver a cifrar el contenido multimedia.

Descripción detallada

La figura 1 muestra los diferentes elementos que forman parte del proceso de recifrado. Un proveedor de contenido multimedia (MC) proporciona un dispositivo receptor que contiene un módulo de seguridad (SM). Un contenido multimedia, según la presente solicitud, es un contenido de audio o vídeo que representa un evento único, como una película, un espectáculo deportivo, un espectáculo o un documental. El proveedor puede enviar el contenido multimedia a través de diferentes medios de comunicación, como difusión, IP, cable, vía terrestre o cualquier tipo de red inalámbrica. El proveedor puede conectarse con un centro de gestión que maneja la autorización para acceder a los contenidos multimedia.

Como es bien sabido por los expertos en la materia, el módulo de seguridad se puede básicamente adquirir cuatro formas distintas. Una de estas formas es una tarjeta de microprocesador, una tarjeta inteligente o, más generalmente, un módulo electrónico (en forma de una llave, tarjeta de autorización, etc.). Dicho módulo generalmente es extraíble y se puede conectar al dispositivo receptor. La forma que cuenta con contactos eléctricos es la más utilizada (ISO 7816 o CAM), pero también se puede usar una conexión sin contactos, por ejemplo, del tipo ISO 14443, Bluetooth, wifi.

Una segunda forma conocida es la representada por una caja de circuito integrado dedicada (por ejemplo, un sistema sobre chip), que generalmente se coloca de forma fija e inamovible en el dispositivo receptor. Una alternativa consiste en un circuito montado en una base o en un conector, como un conector de módulo SIM.

Una tercera forma es que el módulo de seguridad esté integrado en el dispositivo receptor como un chip de silicio dedicado o como parte de un chip de silicio principal encargado del funcionamiento del dispositivo de recepción.

Una cuarta forma es que el módulo de seguridad no sea mediante hardware, sino que su función se implemente solamente en forma de software. Dado que los cuatro casos ejercen su función de forma idéntica, aunque el nivel de seguridad sea diferente, podemos decir que se trata de un módulo de seguridad independientemente de la forma en que se lleve a cabo su funcionamiento o de la forma que pueda adoptar.

El contenido multimedia (MC) se cifra previamente mediante una clave del contenido multimedia (MK) y se envía al dispositivo receptor. La clave del contenido multimedia puede ser una clave única para el módulo de seguridad (SM) específico y que cumpla la función de la clave personal. En otros casos, la clave del contenido multimedia (MK) se genera aleatoriamente y el contenido multimedia se cifra mediante la misma incluso antes de que el dispositivo receptor solicite el contenido multimedia (MC). En este caso, la clave del contenido multimedia (MK) se cifra con una clave personal (PK) del módulo de seguridad. Durante la solicitud del contenido multimedia (MC), el dispositivo receptor identifica el módulo de seguridad (SM), por ejemplo, transmitiendo su dirección única (UA).Basándose en esta información, el centro de gestión determina qué clave personal (PK) se almacena en el módulo de seguridad (SM) identificado.

La clave del contenido multimedia (MK) cifrada se envía al dispositivo receptor y pasa al módulo de seguridad (SM).El módulo de seguridad puede descifrar la clave del contenido multimedia cifrada u obtener la clave del contenido multimedia (MK).

Una vez que el dispositivo receptor recibe el contenido multimedia cifrado, este se transmite al módulo de seguridad para su procesamiento. La clave del contenido multimedia (MK) descifrada se utiliza para descifrar el contenido multimedia (MC). En ese momento, el contenido multimedia se vuelve a cifrar utilizando una clave local actual (K). Este esquema tiene la particularidad de que la clave local se aplica solo a una parte del contenido multimedia, que se define como un fragmento. El fragmento está formado preferiblemente por diversos paquetes de transporte (TS).Cada paquete tiene un encabezado que describe su contenido.

El tamaño de los fragmentos se puede elegir según diferentes parámetros, como el número de paquetes, la duración representada por la reproducción de un fragmento (por ejemplo, 10 segundos). El tamaño se puede establecer en el sistema de recifrado o puede variar mientras se generan los fragmentos.

El módulo de seguridad (SM) agrega un marcador en el encabezado de los paquetes para indicar qué clave local debe usarse para el paquete. La clave cambia para cada fragmento y el decodificador debe estar preparado con la siguiente clave cuando dicho cambio suceda.

La presente solicitud propone diversas soluciones para transmitir de manera segura la clave local.

En una primera modalidad, el mensaje enviado por el módulo de seguridad al decodificador contiene 2 claves, la clave impar y la clave par. El marcador en el encabezado del paquete indica qué clave debe utilizarse. En la parte inicial del nuevo fragmento, el mensaje enviado junto con el fragmento cifrado consta de la clave actual (por ejemplo, K1) y la siguiente clave (por ejemplo, K2). Cada vez que se define un nuevo fragmento, se envía un nuevo mensaje al decodificador que incluye la clave actual y la clave siguiente.

En una segunda modalidad, la siguiente clave local se envía justo antes de que comience el siguiente fragmento. El generador de claves genera la siguiente clave mientras la clave actual aún está en uso. La siguiente clave se cifra mediante la clave de transporte y se envía al decodificador.

En una tercera modalidad, la clave local cifrada se formatea en un paquete de claves que tiene un encabezado de paquete específico y se inserta en la transmisión de paquetes enviados al decodificador. Cuando cambia la clave local, se genera un nuevo paquete que contiene la nueva clave local y se inserta justo antes del paquete con esa nueva clave. En el decodificador, el paquete que contiene la nueva clave se procesa y la clave se carga en el módulo de descifrado del mismo decodificador, que ya está listo para procesar el siguiente paquete cifrado con la nueva clave.

Estas claves locales se cifran con una clave de transporte (TK). Esta clave puede ser una clave fija en el código del descodificador, en una memoria segura, o puede intercambiarse entre el módulo de seguridad y el descodificador antes de la transmisión de los fragmentos. En este último caso, la clave de transporte (TK) se genera durante un intercambio de números aleatorios para crear un canal seguro. Algunos protocolos seguros son SSL o Diffie-Helmann. La clave de transporte, una vez generada, se almacena en una memoria segura del decodificador y se elimina al finalizar la transmisión de todos los fragmentos.

Según una modalidad del presente método, el decodificador incluye una cascada de claves como se ilustra en la figura 3. El dispositivo receptor que contiene el módulo de seguridad (SM) puede solicitar a un centro de gestión el derecho para distribuir contenidos al decodificador. Para ello, el dispositivo receptor envía una solicitud que contiene la identificación del decodificador, en particular la identificación del chip seguro (SEC_CH) del decodificador. El centro de gestión (vinculado al proveedor) puede enviar al dispositivo receptor la clave secreta (SK) del chip seguro. La clave secreta se cifra mediante la clave personal (PK) del módulo de seguridad (SM) y el centro de gestión la envía.

El módulo de seguridad (SM) genera una clave de transporte (TK), por ejemplo, una clave generada aleatoriamente. A continuación, el módulo de seguridad cifra la clave de transporte (TK) mediante la clave secreta (SK) del chip seguro y la envía al decodificador. Este criptograma (TK) SK se carga en la cascada de claves del chip seguro (SEC_CH) para generar la clave de transporte (TK) con un módulo de descifrado adecuado (DECR).Una vez generada, la clave de transporte (TK) se aplica en otro módulo de descifrado (DECR).Una vez que se recibe la clave local cifrada (Kn), el decodificador aplica esta clave cifrada (Kn) TK a la segunda iteración de la cascada de claves para generar la clave local actual (Kn).

Según la primera y segunda modalidad descritas anteriormente, y para tener preparada la clave local cuando se cambia la clave, la clave actual Kn y la siguiente clave Kn+1 se cargan en el módulo de descifrado del decodificador. El chip seguro recibe la clave actual cifrada (Kn) TK y la siguiente clave (Kn +1) TK.Estos dos criptogramas se pasan al chip seguro para generar la clave actual (Kn) y la siguiente (Kn+1), gracias a la presencia de la clave de transporte (TK) obtenida de la descripción del primer módulo de descifrado (DECR).

El decodificador cuenta con un filtro (Fltr) para analizar el encabezado de los paquetes entrantes (CHn) Kn y para determinar si debe utilizarse la clave par o impar (ODD/EVEN). Esta información de par o impar (O/E) se pasa al módulo de descifrado final encargado de obtener el contenido multimedia descifrado (CHn).

La cascada de claves presentada anteriormente es parte de un chip seguro (SEC_CH) y fuera del chip no se puede acceder a los resultados intermedios de los módulos de descifrado (DECR).

En el dispositivo receptor, en particular en el módulo de seguridad (SM), se utiliza una clave local (K1) para cifrar un fragmento (CH1). La clave local actual está cifrada mediante la clave de transporte (TK) para generar el primer criptograma, que es la clave local actual (K1) TK cifrada. La siguiente clave cifrada (K2), que forma un segundo criptograma, se envía al decodificador, como mínimo antes de que la segunda clave K2 se utilice para cifrar el siguiente fragmento. Estos criptogramas se envían al decodificador para que el chip seguro los procese. En caso de que los criptogramas se envíen a través de un canal lógico diferente al decodificador (y no como un paquete adicional insertado en el flujo de envío de los paquetes), cada criptograma incluye además una indicación de si la clave cifrada es par o impar, lo que permite que el chip seguro cargue el criptograma en su entrada correcta. Esta información de par o impar concuerda con la información añadida al encabezado de los paquetes cifrados mediante el módulo de seguridad (SM).

En caso de que la clave K10 esté actualmente en uso, el aviso "par" se añade al encabezado del fragmento cifrado (CH10) K10.Las claves cifradas (K10) TK y (K11) TK se transmiten al chip seguro. El primer criptograma (K10) TK incluye el aviso "par" y el segundo criptograma (K11) TK incluye el aviso "impar". Como consecuencia, el módulo de descifrado final se carga con la clave par K10 y la clave impar K11.La información extraída del encabezado de los paquetes cifrados indica el estado "par" y la clave par K10 se carga en el módulo de descifrado. En el caso de que el módulo de seguridad (SM) cambie la clave, la siguiente clave K11 estará lista para usarse tan pronto como el filtro (Fltr) detecte un nuevo estado en el encabezado de los paquetes cifrados.

El chip seguro (SEC_CH) es parte del decodificador y tiene la clave secreta (SK) precargada, dicha clave es única para cada chip seguro. La clave está oculta en el interior del silicio y no se puede extraer. Cada chip seguro también está asociado con un número de identificación único (UIN) que se utiliza para identificar el decodificador (y particularmente el chip seguro) cuando el dispositivo receptor solicita la clave secreta (SK) al centro de gestión. Cuando se solicita la clave secreta (SK) de un decodificador dado, la solicitud también puede contener una identificación del módulo de seguridad (SM).El centro de gestión puede entonces autorizar o denegar la comunicación entre el dispositivo receptor y el decodificador enviando o no la clave secreta al dispositivo receptor.

Según una modalidad, la clave secreta (SK) no se envía al módulo de seguridad y nunca abandona la base de datos segura del centro de gestión. El módulo de seguridad (SM), a través del dispositivo receptor, solicita que se genere un criptograma (TK) SK, esta solicitud contiene la clave de transporte (TK) y la identificación del chip seguro (UIN). El centro de gestión, tras haber obtenido la clave secreta correspondiente basada en la identificación UIN, cifra la

clave de transporte recibida (TK) mediante la clave secreta (SK) obtenida. Este criptograma (TK) SK se envía al módulo de seguridad y se pasa al decodificador. Una vez el primer módulo de descifrado (DECR) lo descifra usando la clave secreta (SK), la clave de transporte (TK) está disponible para los siguientes módulos de descifrado. Cuando se solicita la clave de transporte de un decodificador dado, la solicitud también puede contener una identificación del módulo de seguridad (SM).El centro de gestión puede entonces autorizar o denegar la comunicación entre el dispositivo receptor y el decodificador enviando o no la clave secreta cifrada al dispositivo receptor.

La figura 4 muestra un módulo de seguridad adaptado para realizar el presente método. El módulo de seguridad se encarga de descifrar y volver a cifrar el contenido multimedia. Para tal fin, el módulo de seguridad (SM) cuenta con un primer módulo de descifrado (DEC1) encargado de descifrar la clave del contenido multimedia (MK) cifrada mediante la clave personal (PK) cargada en el módulo de seguridad. Este descifrado permite obtener la clave del contenido multimedia (MK), que el segundo módulo de descifrado (DEC2) utiliza. El contenido multimedia (MC) está formado por varios paquetes, por ejemplo, paquetes TS. Un paquete se carga en el módulo de descifrado (DEC2) y se descifra utilizando la clave del contenido multimedia (MK).Una vez descifrado, el paquete se pasa al módulo de cifrado (ENC2) para cifrarse con la clave local actual (Kn).El paquete cifrado se transfiere a continuación, a un módulo de marcado (MAK) que añade al encabezado del paquete la indicación par o impar (O/E) de la clave utilizada, creada por el generador de claves (KG).El paquete ya está listo para ser enviado al decodificador.

El módulo de seguridad (SM) cuenta, además, con un generador de claves (KG) para generar las claves locales K1, K2, K3, ..., Kn. Estas claves se utilizan para cifrar un paquete del contenido multimedia descifrado y se cambian según las reglas contenidas en el generador de claves (KG). Para estar preparado cuando se produzca un cambio de claves, el generador de claves (KG) genera la siguiente clave local, es decir, la clave que se usará para el siguiente fragmento. Tanto la siguiente clave local como la clave local actual (generada como la siguiente clave local durante el cifrado del fragmento anterior) se envían de forma segura al decodificador.

El módulo de seguridad contiene además un segundo módulo de cifrado (ENC2) para cifrar las claves locales Kn mediante la clave de transporte (TK).

Los paquetes cifrados (CHn), así como las claves locales cifradas (Kn) TK, se envían al decodificador.

El dispositivo de recepción, que cuenta con el módulo de seguridad, es preferiblemente un dispositivo doméstico, como un decodificador, un ordenador personal, o un portal de enlace doméstico.

REIVINDICACIONES

1. Un método para proteger un contenido multimedia (MC) cifrado mediante una clave del contenido multimedia (MK), dicho método se lleva a cabo mediante un módulo de seguridad (SM) integrado en un dispositivo de recepción y conectado con un decodificador, dicho método consta de los pasos siguientes:

a. Recibir el contenido multimedia (MC) cifrado (MK) mediante una clave del contenido multimedia (MK).
b. Recibir un mensaje seguro que contiene la clave del contenido multimedia (MK), dicho mensaje se cifra mediante una clave personal (PK) del módulo de seguridad (SM).
c. Descifrar el mensaje seguro mediante la clave personal (PK) para obtener la clave del contenido multimedia (MK).
d. Descifrar el contenido multimedia que ha sido cifrado mediante la clave del contenido multimedia.
e. Generar una clave local actual (K1, K2, K3, ...,Kn).
f. Cifrar una parte del contenido multimedia (MC) mediante la clave local actual, dicha parte se define como fragmento.
g. Transmitir de forma segura la clave local actual al decodificador.
h. Transmitir el fragmento cifrado ((CHn) Kn) al decodificador.
i. Repetir los pasos de e) a h) para cada parte del contenido multimedia y modificar la clave local actual para cada fragmento diferente,

Caracterizado porque: Los fragmentos vueltos a cifrar forman un flujo de paquetes y la transmisión segura de la clave local actual consta de los siguientes pasos:
j. Generar un nuevo paquete de claves locales que contiene la clave local actual cifrada.
k. Insertar el nuevo paquete de clave local en el flujo de paquetes justo antes de que se utilice la clave local actual para cifrar el paquete que contiene el contenido multimedia.

2. El método de la reivindicación 1, en el que el contenido multimedia está formado por un primer número de paquetes (cada paquete se descifra con la clave del contenido multimedia (MK) y se vuelve a cifrar con la clave local actual (Kn) antes de enviarse al decodificador) y un fragmento está formado por un segundo número de paquetes inferior al primer número de paquetes, para el que se aplica la misma clave local.

3. El método de la reivindicación 2, que consta de los siguientes pasos:

- Generar las claves locales (K1, K2, K3, ...,Kn).
- Definir la clave impar (K1, K3, K5, ...) y la clave par (K2, K4, K6, ...).
- Utilizar sucesivamente una clave par e impar como clave local actual.
- Marcar el encabezado del paquete que se ha vuelto a cifrar con una indicación que permita diferenciar si la clave es par o impar.

4. El método de cualquiera de las reivindicaciones 1, 2 o 3, que consta de los siguientes pasos:

- Generar la clave local siguiente, que va a utilizarse con el siguiente fragmento.
- Transmitir de forma segura la clave local actual y la siguiente clave local al decodificador.

5. El método de cualquiera de las reivindicaciones 1, 2, 3 o 4, en el que el decodificador cuenta con una clave secreta (SK), dicha clave local está cifrada mediante la clave secreta (SK) antes de transmitirse al decodificador.

6. El método de cualquiera de las reivindicaciones 1, 2, 3, 4 o 5, en el que el decodificador cuenta con una identificación del decodificador (UIN) y un chip seguro (SEC_CH) que almacena una clave secreta (SK) y que consta de los siguientes pasos:

- Transmitir mediante el módulo de seguridad (SM) una solicitud a un centro de gestión que contiene la identificación del decodificador (UIN) y una clave de transporte (TK) generada aleatoriamente.
- Obtener en el centro de gestión, utilizando la identificación del decodificador, la clave secreta (SK) de dicho decodificador.
- Cifrar la clave de transporte (TK) mediante la clave secreta (SK).
- Transmitir la clave de transporte cifrada al decodificador.
- Cargar la clave de transporte cifrada en el chip seguro del decodificador.
- Descifrar la clave de transporte cifrada en el chip seguro para obtener la clave de transporte (TK).

7. El módulo de seguridad (SM) es parte de un dispositivo de recepción e incluye una clave personal (PK) y:

- Un primer módulo de descifrado (DEC1) configurado para recibir y descifrar una clave del contenido multimedia (MK) cifrada mediante la clave personal (PK).
- Un segundo módulo de descifrado (DEC2) para recibir y descifrar un contenido multimedia (MC) cifrado mediante la clave del contenido multimedia (MK).
- Un generador de claves (KG) para crear varias claves locales (K1, K2, K3, ...,Kn).
- Un primer módulo de cifrado (ENC1) para cifrar las claves locales mediante una clave de transporte (TK).
- Un segundo módulo de cifrado (ENC2) para cifrar una parte del contenido multimedia descifrado mediante una de las claves locales, siendo dicha parte más pequeña que el contenido multimedia completo, de modo que varias claves se utilizarán para cifrar sucesivamente el contenido multimedia (MC).

Caracterizado porque: El módulo de seguridad está configurado para transmitir un flujo de paquetes con las partes que se han vuelto a cifrar, para generar un nuevo paquete de claves locales que contenga la clave local actual cifrada, e insertar el nuevo paquete de claves locales en el flujo de paquetes justo antes del local actual. La clave se utiliza para cifrar el paquete con el contenido multimedia.

8. Módulo de seguridad según la reivindicación 7, en el que, cada paquete cuenta con un encabezado, el módulo de seguridad cuenta, además, con un módulo de marcado (MAK) configurado para añadir un aviso de par o impar (O/E) al encabezado del paquete que indica la clave local utilizada.

9. Módulo de seguridad de la reivindicación 7 u 8, configurado además para:

- Generar la clave de transporte (TK).
- Enviar la clave de transporte (TK) a un centro de gestión junto con la identificación del decodificador de destino.
- Recibir la clave de transporte (TK) cifrada mediante una clave secreta (SK) del decodificador de destino.
- Transmitir la clave de transporte (TK) cifrada al decodificador.

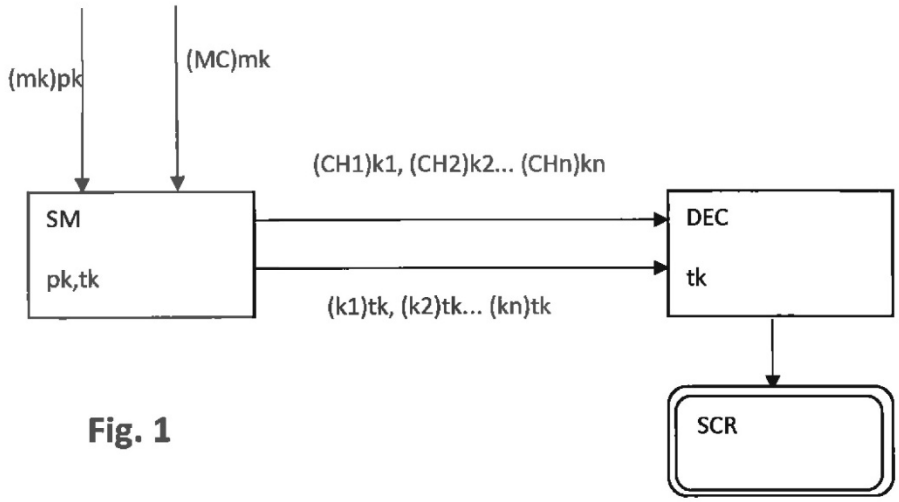

Fig. 1

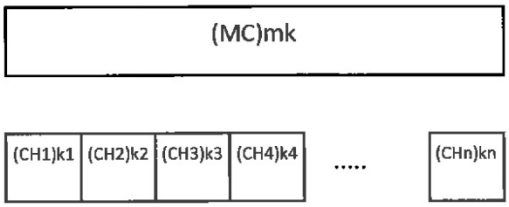

Fig. 2

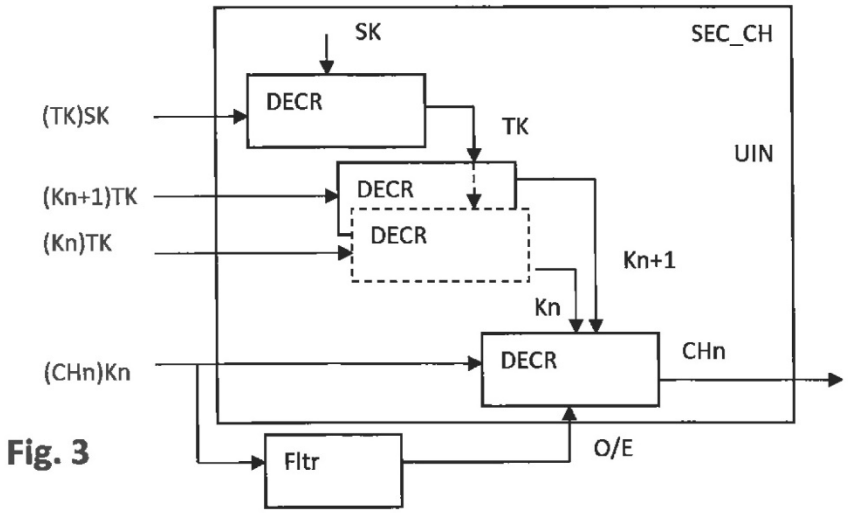

Fig. 3

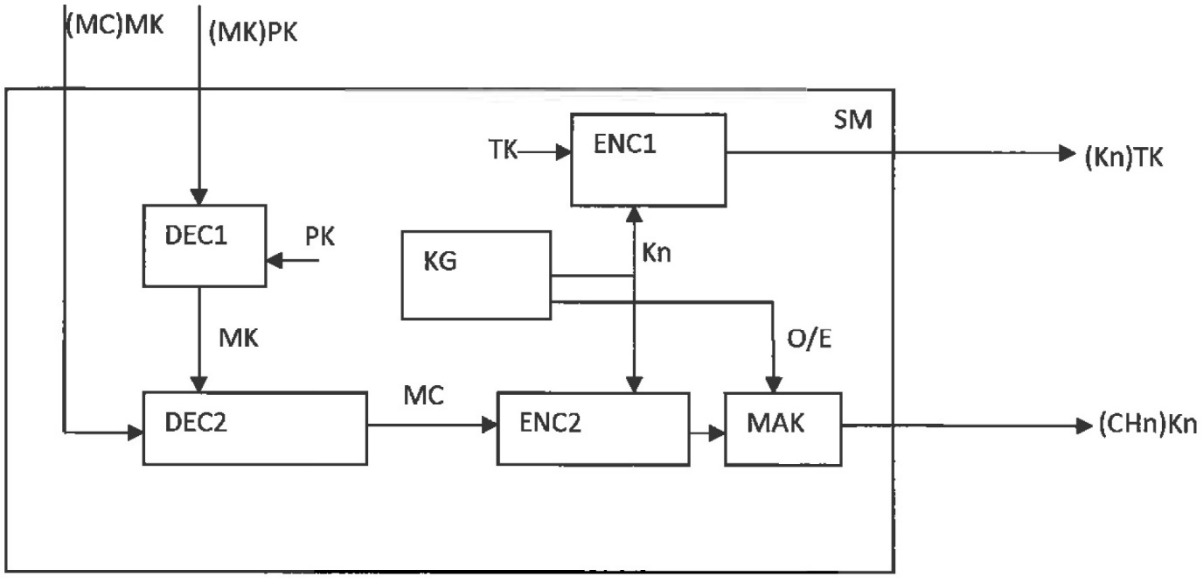
(MC)MK
(MK)PK
SM
TK
ENC1
(Kn)TK
DEC1
PK
KG
Kn
MK
O/E
MC
DEC2
ENC2
MAK
(CHn)Kn

Fig. 4