(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 697 612**

(51) Int. CI.:

H04N 21/4385 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4408 (2011.01)
H04N 21/4623 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.07.2014 PCT/EP2014/064332**

(87) Fecha y número de publicación internacional: **22.01.2015 WO15007549**

(96) Fecha de presentación y número de la solicitud europea: **04.07.2014 E 14734841 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.09.2018 EP 3022940**

(54) Título: **Método para la protección de claves de desciframiento en un descodificador y descodificador para la aplicación de este método**

(30) Prioridad:

19.07.2013 EP 13177287

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2019

(73) Titular/es:

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

(72) Inventor/es:

MACCHETTI (IT), MARCO;
PERRINE, JÉRÔME;
SERVET, PATRICK y
HUNACEK, DIDIER

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para la protección de claves de desciframiento en un descodificador y descodificador para la aplicación de este método

Campo técnico

[0001] La presente solicitud se refiere al dominio de la adquisición condicional de datos digitales, tales como los datos difundidos en el marco de la televisión de pago, y en particular atañe a la protección de las claves de descifrado de contenidos digitales, principalmente de contenidos de audio/vídeo.

Estado de la técnica

[0002] Un contenido, por ejemplo de tipo audio/vídeo (A/V), es encriptado por claves denominadas palabras de control (CW - *Control Word*) que cambian regularmente, normalmente cada minuto. El contenido encriptado de este modo a continuación se transmite a los receptores según un modo de difusión, es decir, el mismo contenido es recibido por una pluralidad de receptores.

[0003] Las palabras de control son encriptadas por una clave de transmisión (TK) que cambia a una frecuencia mucho más baja, por ejemplo cada mes. Una palabra de control encriptada se coloca en un mensaje de autorización (ECM -*Entitlement Control Message*) acompañada de las condiciones de descifrado. Estas condiciones describen los derechos que debe poseer el receptor para ser autorizado a acceder al contenido. Estos derechos se transmiten regularmente en forma cifrada al receptor mediante mensajes de gestión de derechos (EMM - *Entitlement Management Message*). Los mensajes de autorización ECM y los mensajes de gestión de derechos EMM forman un conjunto de mensajes de datos DT que se unen al contenido encriptado para formar un flujo de transporte (TS - *Transport Stream*) enviado con los receptores como destino.

[0004] La oferta propuesta a los abonados de televisión de pago comprende muchos canales (CH1, CH2, CH3, etc..) cada uno de los cuales están encriptados según una o varias claves particulares. Esto es necesario debido a que un abonado puede suscribirse a un abono para un canal sin tener derecho a beneficiarse de los otros canales.

[0005] Los mensajes de autorización ECM se encriptan con una clave propia del sistema de gestión (CAS - *Conditional Access System*) habitualmente asociado a la cabecera de red (*Headend*) del cual proviene el flujo de transporte. El receptor del abonado comprende, entre otros, una unidad criptográfica protegida (SM - *Security Module*) a cargo de descodificar estos mensajes y un descodificador (STB - *Set-Top-Box*) que descifra el contenido encriptado con el fin de poder visualizar dicho contenido. El sistema de gestión transmite estos mensajes ECM en forma encriptada a la unidad criptográfica a cargo de descodificar estos mensajes, gestiona las autorizaciones y, según los derechos del abonado, transmite al descodificador las informaciones necesarias para la desencriptación de las señales de vídeo y audio.

[0006] Los resultados de la desencriptación por la unidad criptográfica son precisamente las palabras de control CW. Estas palabras de control guiarán al descodificador y el abonado podrá así beneficiarse en abierto de las informaciones transmitidas.

[0007] Como se ha indicado anteriormente, estas palabras de control se cambian regularmente con el fin de impedir que un pirata calcule estas informaciones de control mediante un ordenador potente y se beneficie gratuitamente de la prestación sometida a pago. Por esta razón, estas palabras de control se cambian en un intervalo habitualmente regular, período que normalmente es de 1 a 20 segundos. A este período se le llama criptoperiodo.

[0008] Los mensajes de autorización ECM se envían con una frecuencia mucho más elevada que el criptoperiodo, por ejemplo cada 100 milisegundos. Esto es indispensable, por un lado, cuando se pone en servicio el descodificador y, por otro lado, cuando se cambia de canal (CH1, CH2, CH3, etc ...).

[0009] En efecto, para poder visualizar la emisión deseada, las palabras de control son necesarias para la desencriptación de las señales. Es difícil imaginar que se tenga que esperar 5 segundos delante de la pantalla para que la imagen en abierto aparezca.

[0010] En el segundo caso, como las palabras de control son propias de cada canal, se debería esperar al final del criptoperiodo para recibir el mensaje de autorización que permite la desencriptación de las señales del nuevo canal. De la misma manera que antes, no se puede tolerar un retraso de varios segundos cuando se realiza un cambio de canal.

[0011] Por esta razón, en la práctica, los mensajes de autorización ECM se envían a una frecuencia comprendida entre 5 y 20 por segundo.

[0012] De este modo, una vez que el descodificador ha recibido la palabra de control, puede descodificar el contenido de audio/vídeo. Un descodificador actualmente puede procesar más de un flujo de audio/vídeo encriptado a la vez. Este puede ser el caso de una función PIP (*Picture-In-Picture*), el registro de un flujo y el visionado de otro, o el visionado simultáneo de varios flujos en una misma pantalla (mosaico de imágenes proveniente de varios canales diferentes) o en varias pantallas. Con este fin, el descodificador podrá procesar en paralelo varios flujos y, por lo tanto, debe disponer de varias palabras de control a la vez.

[0013] Otra explicación de la presencia de varias palabras de control con respecto a varios canales es la velocidad de cambio de canal. En efecto, es deseable que este cambio se haga en el tiempo más corto posible y según un modo particular, aunque el descodificador pueda procesar uno o dos flujos simultáneamente, el descodificador puede almacenar 10 o 20 palabras de control en un tiempo determinado. La unidad criptográfica a cargo de procesar los ECM extrae las palabras de control de una pluralidad de canales y las envía al descodificador aunque este último no esté a cargo de descodificar este contenido. Esto permite que esté inmediatamente lista la palabra de control cargada en el descodificador en cuanto el usuario solicita un cambio de canal.

[0014] Aunque durante un tiempo determinado solo una palabra de control esté activa, el descodificador debe disponer de la palabra de control actual y de la palabra de control siguiente. Con este fin, el contenido encriptado comprende una indicación para identificar la palabra de control (ODD, EVEN).

[0015] En función de lo anterior, es evidente que un descodificador memorizará un gran número de palabras de control, o bien para un uso simultáneo, o bien para estar preparado en caso de cambio de canal, o bien para una combinación de estos dos modos. De este modo, puede descodificar tres canales simultáneamente y almacenar las palabras de control para los 30 canales posibles que el usuario puede recibir. Cada canal representa dos palabras de control.

[0016] Como la unidad criptográfica está protegida de manera satisfactoria, hay terceros maliciosos que tienen interés en interceptar las palabras de control transmitidas por la unidad criptográfica. Por esta razón, se han propuesto soluciones como se describe en la patente EP 1078524. Se realiza una encriptación sobre las palabras de control por la unidad criptográfica antes de su transmisión al receptor. El receptor y la unidad criptográfica comparten una clave única, lo que permite emparejar estos dos elementos. Un mensaje interceptado entre estos dos elementos no se puede utilizar por otro receptor, puesto que la clave de emparejamiento es única.

[0017] Una vez que ha llegado al receptor, el mensaje se desencripta por la clave de emparejamiento y la palabra de control se almacena en abierto en una memoria protegida del receptor.

[0018] El documento WO 2006/044547 trata sobre los plazos que requiere un descodificador cuando, a partir de un flujo de transporte encriptado, debe cambiar de un canal a otro para satisfacer la solicitud de un usuario que desea pasar de una cadena de televisión a otra. Este documento divulga el uso de una memoria tampón (búfer) en la cual se almacenan temporalmente palabras de control con el fin de reducir el plazo de espera entre el momento en el que el usuario selecciona otro canal y el momento en el que el contenido de este nuevo canal se visualiza en abierto en la pantalla de televisión. Dentro de la memoria tampón, las palabras de control se renuevan constantemente según el principio de una pila de palabras de control de la cual las palabras de control antiguas se retiran sucesivamente para ser reemplazadas por nuevas. Esta memoria tampón la gestiona un gestor de palabras de control. Para poder reducir el tiempo necesario para el cambio, este documento sugiere particularmente almacenar en la memoria tampón no solo las palabras de control utilizadas para restituir las cadenas mostradas en un momento dado por el televisor, sino también las palabras de control de las otras cadenas, a saber, las cadenas que no están siendo vistas ni grabadas en ese momento. Este documento sugiere finalmente que las palabras de control almacenadas en la memoria tampón lo estén en forma cifrada por una clave propia de un canal protegido que conecta el gestor de palabras de control con el módulo de seguridad del cual estas palabras de control se extraen de los mensajes ECM. Cuando se cambia de una cadena a otra, las palabras de control relativas al nuevo canal serán descifradas por el gestor mediante la clave que está asociada al canal protegido entre este gestor y el módulo de seguridad. Luego, se transmitirán a la unidad de desaleatorización apropiada con el fin de que esta última pueda proceder al descifrado del nuevo canal de audio/vídeo.

[0019] La invención citada en el documento US 2012/0257749 tiene como objetivo reforzar la seguridad de las palabras de control mejorando la eficacia y la velocidad de las operaciones de verificación previas a la desaleatorización de un flujo de audio/vídeo protegido. Con este propósito, el método sugerido en este documento se centra esencialmente en las verificaciones de condiciones de acceso efectuadas sucesivamente por dos dispositivos de acceso condicional sobre un mensaje ECM. Así, esta invención propone modificar los mensajes de control ECM de manera que cada ECM esté estructurado para que un primer mensaje ECM1 encapsule un segundo mensaje ECM2 en lugar de la palabra de control normalmente contenida en el primer mensaje ECM1. De este modo, este documento sugiere una doble verificación de las condiciones de acceso por el acondicionamiento sucesivo de dos dispositivos con acceso condicional, uno para el ECM1, el otro para el ECM2, antes de que se restituya la palabra de control contenida en el segundo mensaje ECM2.

Breve descripción de la invención

[0020] La presente solicitud trata de la cuestión de la seguridad de las claves de descifrado (CW) almacenadas en el descodificador. El descodificador según la invención forma parte del receptor y habitualmente está en forma de un circuito especializado que integra numerosas funciones tales como la gestión del receptor, la visualización de los menús, la gestión de la grabación. Se trata de un conjunto de componentes especializados de los cuales uno es un microprocesador que integra en una pieza de silicio una función de descodificador. Este componente dispone de memoria interna y puede acceder a los programas o datos almacenados en una memoria externa.

[0021] Generalmente, las palabras de control se almacenan en una memoria interna dedicada a este fin. Es necesario que las palabras de control estén disponibles muy rápidamente en el momento de un cambio de criptoperiodo. Aunque esta memoria sea de difícil acceso, los ataques de *software* o por *glitch*, láser o desbordamiento de búfer han dado resultados positivos.

[0022] Por esta razón, se propone proteger el descodificador mediante la encriptación de las palabras de control a la espera de ser utilizadas.

[0023] Por lo tanto, se propone un método para proteger las palabras de control almacenadas, en una memoria, dentro de un descodificador a cargo de descodificar al menos un contenido de audio/vídeo protegido por dichas palabras de control. El descodificador comprende un gestor de claves conectado, a través de un canal protegido, a un módulo de seguridad a cargo de enviar las palabras de control al descodificador en forma cifrada, al menos una unidad de desaleatorización a cargo de descifrar el contenido de audio/vídeo, y un registro de palabras de control administrado por el gestor de claves. Según la invención, este método comprende las etapas siguientes:

- cargar, para cada unidad de desaleatorización en un directorio de claves administrado por el gestor, de una clave de emparejamiento (PK) que, por una parte, está referenciada por un identificador (ID) que la asocia a la unidad de desaleatorización a la que está dedicada únicamente y, por otra parte, es conocida por esta unidad de desaleatorización,

- recepción por el gestor de claves de al menos una palabra de control (CW) cifrada por el módulo de seguridad, esta palabra de control (CW) que también está referenciada por una indicación (D) que permite identificar la unidad de desaleatorización a la que está destinada,

- desciframiento, por el gestor de claves, de esta palabra de control a través de una clave de descifrado propia del canal protegido,

- identificación, en el directorio, de la clave de emparejamiento cuyo identificador (ID) corresponde a la indicación de destino (D) asociada a la palabra de control, y luego

- ciframiento de esta palabra de control con ayuda de la clave de emparejamiento así identificada, y

- almacenamiento en el registro, de manera cronológica y referenciada, de la palabra de control (cifrada por la clave PK) de manera que cualquier palabra de control específica requerida por una unidad de desaleatorización pueda ser retirada del registro con el fin de ser descifrada por esta unidad de desaleatorización y utilizada por esta última para descodificar dicho contenido de audio/vídeo (o al menos una parte de este contenido).

[0024] La presente solicitud propone igualmente un descodificador para la aplicación de este método según cualquier forma de realización de este último. El descodificador, segundo objeto de la presente invención, comprende un gestor de claves conectado, a través de un canal protegido, a un módulo de seguridad a cargo de enviar palabras de control (CW) al descodificador en forma cifrada, al menos dos unidades de desaleatorización a cargo de descifrar cada una un contenido de audio/vídeo cifrado por una parte de las palabras de control, y un registro de palabras de control administrado por el gestor de claves. Este último está configurado además para descifrar las palabras de control recibidas del módulo de seguridad y para almacenarlas en el registro en forma cifrada. Según la invención, este descodificador comprende igualmente:

- una memoria para almacenar al menos un directorio de claves administrado por el gestor y configurado para clasificar una pluralidad de claves de emparejamiento (PK), donde cada clave de emparejamiento está referenciada por un identificador (ID) que la asocia de manera única a una de las unidades de desaleatorización del descodificador,

- un módulo de referenciación que permite referenciar cada palabra de control (CW) por una indicación (D) que identifica a la unidad de desaleatorización, a la que esta palabra de control está destinada, en función de un canal de audio/vídeo del cual se extrae cada palabra de control.

[0025] Según la invención, el gestor de claves también está configurado para poder identificar, en el directorio, la clave de emparejamiento cuyo identificador (ID) corresponde a la indicación de destino (D) que referencia la palabra de control, y para cifrar esta última con ayuda de la clave de emparejamiento así identificada. Finalmente, el registro está configurado para almacenar las palabras de control (cifradas por la clave PK) de manera cronológica y referenciada.

Breve descripción de las figuras

[0026] La presente invención se comprenderá mejor gracias a las explicaciones basadas en las figuras, en las cuales:

- la figura 1 ilustra los principales componentes participantes en la invención en un descodificador,
- la figura 2 ilustra los intercambios que se producen entre diferentes elementos de este descodificador.

Descripción detallada

[0027] La figura 1 ilustra un descodificador 10, en particular los elementos de este descodificador útiles para la comprensión de la invención. El descodificador 10 recibe, en forma de flujo de transporte TS, flujos de audio/vídeo encriptados por palabras de control CW.

[0028] En la presente descripción, así como en las figuras anexas, se destacará que el cifrado (también denominado encriptación) de un flujo o de cualquier dato se designará incluyendo este dato entre corchetes. De este modo, en la figura 1, el flujo de transporte TS cifrado por palabras de control se designa como [TS]cw. Este flujo de transporte normalmente está constituido por paquetes de datos dentro de una señal difundida por la cabecera de red (*headend*) hacia una pluralidad de descodificadores 10, por ejemplo por vía satélite o terrestre (hertziana), por una red alámbrica (teléfono fijo, internet, cable) o por una red inalámbrica (telefonía móvil u otra red de difusión).

[0029] Como los paquetes de datos han sido multiplexados por la cabecera de red para que la información que contienen pueda ser enviada por un solo soporte de transmisión (flujo de transporte TS), esta señal compuesta debe ser desensamblada por un demultiplexor 11 a su entrada en el descodificador 10 para poder recuperar cada canal de audio/vídeo CH1, CH2, CH3, etc ... que contiene. Cada uno de estos canales (aún cifrados) incluye datos de audio (por ejemplo, varios canales de audio), datos de video, así como datos de control (ECM; EMM) y otras informaciones (metadatos). Como se esquematiza en la figura 1, los datos de audio/vídeo ([A/V]) de cada canal a continuación se separan de los otros datos (*Data*), en particular los datos de control ([DT]), por un dispositivo de selección 12 (SD - *Sorting Device*). Estos datos de audio/vídeo se cifran mediante palabras de control CW contenidas en los mensajes ECM que forman parte de los datos de control DT. Estos últimos también son cifrados por una clave de transmisión TK.

[0030] El descodificador 10 comprende además un gestor de claves 20 (KMG - *Key Manager*) conectado, a través de un canal protegido 25, a un módulo de seguridad 30 (SM - *Security Module*). Este último está a cargo de enviar, en forma cifrada, las palabras de control al descodificador 10 después de haber verificado que los derechos, administrados por los mensajes EMM, también están presentes en el entorno del usuario (en particular en el módulo de seguridad).

[0031] Tal módulo de seguridad 30 se puede realizar en particular según cuatro formas de realización distintas. Una de ellas es una tarjeta con microprocesador, una tarjeta inteligente o, más habitualmente, un módulo electrónico (con forma de llave, de tarjeta, ...). Dicho módulo generalmente es desmontable, conectable al receptor y considerado inviolable. El intercambio de datos entre el descodificador y el módulo de seguridad que está asociado a él se hace habitualmente por medio de un contacto físico (contacto eléctrico de un puerto de comunicación). Sin embargo, no se excluye prever, entre estas dos entidades, un intercambio de datos a través de una conexión sin contacto, por ejemplo de tipo ISO 15443.

[0032] Una segunda forma de realización conocida es la de un circuito integrado colocado, habitualmente de manera definitiva e inamovible, en la caja del receptor (descodificador). Una variante está constituida por un circuito instalado sobre un zócalo o un conector, como un conector de módulo SIM.

[0033] Según una tercera forma de realización, el módulo de seguridad puede estar integrado, dentro del receptor, en un órgano que también tiene otra función, por ejemplo en el microprocesador del descodificador.

[0034] Según una cuarta forma de realización, el módulo de seguridad no se realiza en forma material, sino que su función se efectúa en forma de *software*, únicamente.

[0035] Aunque el nivel de seguridad difiere entre estos casos, la función en sí misma es idéntica, de manera que se hablará de módulo de seguridad sea cual sea la manera de realizar este módulo. En las cuatro formas descritas

anteriormente, el módulo de seguridad posee medios (memoria, unidad central) para almacenar y ejecutar un programa interno. Este programa permite efectuar diferentes operaciones de seguridad, tales como verificar los derechos, efectuar desciframientos, activar un módulo para efectuar las operaciones criptográficas, etc.

[0036] Si se comprueba la presencia de los derechos requeridos para poder acceder al contenido de audio/vídeo de una cadena (CH1, CH2, CH3, etc ...), el módulo de seguridad 30 extrae las palabras de control CW de los mensajes ECM, después de haberlas descifrado mediante la clave de transmisión TK, y luego las reencripta utilizando una clave única SK (*Secret Key*), que además solo la conoce el gestor de claves 20 y que es por lo tanto propia del canal protegido 25 establecido entre estas dos entidades 20, 30.

[0037] Para poder descifrar las palabras de control reencriptadas por el módulo de seguridad, el gestor de claves 20 comprende un módulo criptográfico 23 (CRYP - *Cryptographie Module*). Así, esta unidad 23 está configurada para poder descifrar particularmente las palabras de control recibidas del módulo de seguridad 30 mediante la clave única SK.

[0038] Volviendo a los elementos principales que componen el descodificador 10, se destaca que este último comprende al menos una unidad de desaleatorización 14 (DSC - *Descrambling unit*) a cargo de descifrar el contenido de audio/vídeo encriptado [A/V] recibido del dispositivo de selección 12 correspondiente.

[0039] El descodificador 10 integra igualmente un registro 15 (REG - *Register*) de palabras de control que se administra por el gestor 20. Tal y como se ilustra con la línea discontinua de la figura 1, este registro 15 (o tabla de las palabras de control) podría formar parte del gestor 20.

[0040] El descodificador 10, preferiblemente el gestor de claves 20 de este descodificador, comprende igualmente una memoria para almacenar un directorio 22 de claves (DIR - *Directory*). Esta memoria o este directorio está configurado para clasificar una pluralidad de claves de emparejamiento (PK - *Pairing Key*). Este directorio 22 está destinado a ser administrado por el gestor 20.

[0041] Entre los componentes de este descodificador, se mencionará también un módulo de referenciación 24 (RFM - *Referencing module*) que permite referenciar cada palabra de control (CW) por una indicación (D) que identifica la unidad de desaleatorización 14 a la que esta palabra de control está destinada en función de la identidad (CH1, CH2, CH3, etc ...) de un canal de audio/vídeo del cual se extrae cada palabra de control.

[0042] Finalmente, el descodificador también puede contener al menos un generador 18 de números aleatorios que, como se describirá más adelante en la descripción, se podrá utilizar para generar claves de emparejamiento PK. Al igual que el registro 15, este generador de números aleatorios también podría formar parte del gestor 20. Alternativamente, tal generador 18 podría estar integrado o asociado a cada unidad de desaleatorización 14.

[0043] Tal y como se ilustra en la figura 1, el directorio 22 y/o el módulo de referenciación 24 forman parte preferiblemente del gestor 20. Este último integra finalmente una unidad central 26 (CPU - *Central Processing Unit*) útil para la gestión de diferentes órganos que están incluidos o se pueden incluir en el gestor de claves 20.

[0044] Se observará que el número de unidades de desaleatorización 14 (en este caso, tres) representadas en la figura 1 se da a modo de ejemplo en ningún caso limitativo. El descodificador 10 comprende al menos una unidad de desaleatorización 14, preferiblemente al menos dos unidades 14, cada una a cargo de descifrar uno de los flujos de audio/vídeo multiplexados. El número de unidades de desaleatorización se puede multiplicar de manera que se pueda procesar en paralelo tanto flujo de audio/vídeo como sea necesario.

[0045] Para seguir con la descripción de los principales componentes del descodificador que son necesarios para la comprensión de la invención, las etapas del método propuesto por esta invención se describirán a continuación con mayor detalle.

[0046] En su primero objeto, la invención se refiere a un método para proteger las palabras de control CW dentro del propio descodificador 10.

[0047] La primera etapa de este método tiene como objetivo cargar, para cada unidad de desaleatorización 14, una clave de emparejamiento PK en el directorio de claves 22. Esta clave de emparejamiento PK está referenciada por un identificador ID que la asocia a la unidad de desaleatorización a la que está dedicada únicamente. De este modo, habrá tantas claves de emparejamiento PK como unidades de desaleatorización 14. Tal y como se ilustra en la figura 1, la clave de emparejamiento PK1, a saber, la identificada por el identificador ID1, se dedica a la unidad de desaleatorización DSC1, a saber, a la unidad de desaleatorización 14 que también lleva el identificador 1. La asociación de la clave de emparejamiento PKn al identificador correspondiente IDn se puede realizar de diferentes maneras, por ejemplo a través de un registro (es decir una tupla o una estructura de datos informáticos) que contiene precisamente estos dos elementos. Así, el directorio 22 comprenderá tantos registros como claves PK, y cada uno de estos registros comprenderá al menos dos datos, a saber la clave PKn y el identificador IDn que está asociado a esta. Alternativamente, la asociación de la clave de emparejamiento PKn al identificador IDn

se podría obtener mediante varios directorios 22 o subdirectorios, cada uno de ellos identificado por un identificador IDn y comprendiendo la clave PKn correspondiente.

[0048] Además, cada clave de emparejamiento PK es conocida por la unidad de desaleatorización 14 a la que está dedicada. Así, cada clave de emparejamiento PK es conocida únicamente por un conjunto formado por el gestor de claves 20 y la unidad de desaleatorización 14 para la que esta clave está reservada. La transmisión de esta clave de emparejamiento PK del gestor 20 a la unidad de desaleatorización 14, o viceversa, puede hacerse normalmente durante una fase de inicialización previa a cualquier restitución en abierto del contenido de audio/vídeo.

[0049] La segunda etapa del método se realiza principalmente dentro del gestor de claves 20. Esta segunda etapa tiene como objetivo recibir al menos una palabra de control CW transmitida, en forma cifrada, por el módulo de seguridad 30. Para ello, cada palabra de control CW se cifra por la clave secreta SK que es conocida únicamente por el descodificador 10 (en particular por el gestor de claves 20 de este descodificador) y por el módulo de seguridad 30 asociado a este descodificador 10.

[0050] Según la invención, la palabra de control CW recibida del módulo de seguridad 30 está referenciada por una indicación D que permite identificar la unidad de desaleatorización a la que está destinada. Esta indicación D puede ser el identificador ID de la unidad de desaleatorización 14. Según una forma de realización preferida, esta indicación está situada dentro del descodificador 10 (a saber en un entorno local en casa del usuario) de tal manera que el flujo de datos DT, que contiene particularmente los mensajes de control ECM y, por lo tanto, las palabras de control CW, no tenga necesidad de ser modificado o personalizado. De este modo, el flujo de transporte TS sigue siendo un flujo ordinario, es decir, un flujo cuya estructura es conocida en el estado de la técnica y las normas vigentes. Ventajosamente, el descodificador 10 descrito en la presente invención, por lo tanto, sigue siendo compatible con tal flujo de transporte TS.

[0051] En la forma de realización preferida de la invención, la referenciación de las palabras de control CW por la indicación D la efectúa el módulo de referenciación 24. Este último está conectado a cada dispositivo de selección 12 por una vía dedicada al transporte de los datos DT de un canal de audio/vídeo. Así, el módulo de referenciación es capaz de asociar un identificador a cada paquete de datos, en particular a cada ECM, procedente de cada canal (CH1, CH2, CH3). Por ejemplo, los ECM procedentes del canal CH1 serán referenciados por la indicación D1, los procedentes del canal CH2 por la indicación D2 y los del canal CH3 por la indicación D3. Como cada palabra de control está comprendida dentro de un mensaje ECM, se vuelve a asociar, dentro del descodificador, una indicación D a las palabras de control en función de la identificación de un canal de audio/vídeo del cual cada palabra de control podrá ser extraída por medio de un mensaje ECM.

[0052] Después de haber extraído la palabra o palabras de control CW de cada ECM, el módulo de seguridad 30 es capaz de remitir a cada palabra de control la indicación D que había sido dispuesta en el mensaje ECM cuya palabra de control se ha extraído. Una vez remitida a la palabra de control en cuestión, la indicación D se puede mantener en abierto o cifrarse mediante la clave secreta SK. Preferiblemente, la palabra de control CW y su indicación de destino D serán cifradas en una operación mediante la clave secreta SK por el módulo de seguridad 30. Sea cual sea la manera de funcionar, el canal (de audio/vídeo) de cada palabra de control permanece identificable por el gestor de claves 20, incluso después de que estas palabras de control hayan sido procesadas por el módulo de seguridad 30.

[0053] La tercera etapa del método consiste en descifrar la palabra de control recibida del módulo de seguridad por el gestor de claves. Para ello, el gestor utilizará la clave secreta SK que es propia del canal protegido 25 establecido entre estas dos entidades. En caso de que la palabra de control CW y la indicación D asociada se hayan cifrado en un bloque por el módulo de seguridad mediante la clave secreta SK, la operación de descifrado de la palabra de control por el gestor 20 permite igualmente recobrar en abierto la indicación D asociada a la palabra de control en cuestión.

[0054] La cuarta etapa tiene como fin identificar, en el directorio 22, la clave de emparejamiento PK cuyo identificador ID corresponde a la indicación D asociada a la palabra de control CW recibida del módulo de seguridad. Esta operación la efectúa el gestor 20, por ejemplo recorriendo los registros memorizados en el directorio 22 para buscar cuál es el registro que lleva el identificador ID correspondiente a la indicación D de la palabra de control. Una vez que el gestor ha identificado el registro deseado, es capaz de conocer la clave de emparejamiento PK que está asociada a la unidad de desaleatorización 14 a la que esta palabra de control está destinada.

[0055] La quinta etapa consiste en cifrar esta palabra de control utilizando la clave de emparejamiento PK así identificada. Este cifrado puede ser ejecutado, por ejemplo, por el módulo criptográfico 23 del gestor 20.

[0056] En la sexta etapa, la palabra de control es almacenada a continuación, en esta nueva forma cifrada, dentro del registro 15 por el gestor 20. Este almacenamiento se efectúa de manera cronológica y referenciada de manera que toda palabra de control específica requerida por una unidad de desaleatorización pueda ser retirada de dicho

registro con el fin de ser descifrada y utilizada por esta unidad de desaleatorización para descodificar una parte de dicho contenido de audio/vídeo.

[0057] El carácter cronológico de este almacenamiento puede ser obtenido memorizando las palabras de control en un orden particular, particularmente en el orden de llegada al flujo de transporte. Este orden corresponde al orden en el que deberán ser utilizadas por la unidad de desaleatorización para descifrar el contenido de audio/vídeo. Un apilamiento sucesivo de las palabras de control procesadas por el gestor permite respetar la cronología de estas palabras de una manera muy sencilla. Alternativamente, también sería posible asociar un índice temporal a cada palabra de control almacenada en el registro 15. Dicho índice podría adoptar la forma de un valor incrementado en una unidad para cada nueva palabra de control almacenada. El índice temporal también podría adoptar la forma de una marca de tiempo determinada por un reloj que, por ejemplo, se puede dedicar específicamente a este fin.

[0058] El carácter referenciado del almacenamiento de las palabras de control cifradas en el registro 15 se puede obtener de la misma manera que ya se ha descrito para referenciar las claves de emparejamiento PK en el directorio 22. Así, como se muestra en la figura 1, cada palabra de control cifrada por medio de una clave de emparejamiento PK particular se puede almacenar en un registro que incluye la indicación D relativa al destino de esta palabra de control $[CW]_{PK}$. Como esta indicación D permite o bien identificar el canal CH1, CH2, CH3 asociado a esta palabra de control, o bien identificar la unidad de desaleatorización 14 que deberá utilizarla, de este modo se identifica debidamente el destino de cada palabra de control del registro 15.

[0059] Ventajosamente, el cifrado y el descifrado de las palabras de control $[CW]_{PK}$ mediante la clave de emparejamiento PK se efectúa localmente dentro del descodificador, excluyendo el módulo de seguridad de este último. Así, la protección de estas palabras de control es una protección que es única para cada descodificador y que solo concierne a este. En este punto, el módulo de seguridad ya no es necesario para que se asegure la desaleatorización del contenido de audio/vídeo por las unidades de desaleatorización 14. Además, gracias al directorio 22 en el que se pueden almacenar varias claves de emparejamiento PK, esta forma de realización permite atribuir una protección particular a cada unidad de desaleatorización 14 del descodificador 10. Por lo tanto, incluso en el caso de que una de las claves PK haya sido descifrada por una persona malintencionada, esta persona permanecería incapaz de poder descifrar los contenidos de audio/vídeo de todos los otros canales del flujo de transporte TS. El nivel de protección proporcionado por este método se encuentra, por lo tanto, ventajosamente reforzado.

[0060] Además, el cifrado de las palabras de control CW mediante la clave de emparejamiento PK lo efectúa ventajosamente un solo módulo criptográfico 23 para el conjunto de las unidades de desaleatorización 14 con las que cuenta el descodificador. Ya que esta operación puede ser centralizada, los recursos informáticos del descodificador se encuentran racionalizados.

[0061] Además, la memoria que alberga el registro 15 permite almacenar ventajosamente un gran número de palabras de control. El almacenamiento de estas últimas en este registro puede, por lo tanto, ser un almacenamiento de duración más o menos larga. De hecho, el criterio que determina la duración de este almacenamiento no depende del tamaño de la memoria que alberga el registro, como es habitual en el caso de las memorias de tipo memoria tampón (búfer). En el presente caso concreto, la palabra de control puede quedarse en el registro 15 al menos mientras no sea utilizada por la unidad de desaleatorización a la que está dedicada.

[0062] Ventajosamente, la presente invención permite proteger plenamente el acceso a las palabras de control en el propio descodificador 10. De este modo, todas las vías por las cuales transitan las palabras de control son vías protegidas, porque ninguna palabra de control utiliza una vía en forma no protegida. Así, aunque una persona malintencionada intentara extraer las palabras de control durante su tránsito entre el gestor 20 y cualquiera de las unidades de desaleatorización 14 del descodificador, no sería capaz de utilizar los datos extraídos. Gracias a la protección de todas las vías por las cuales transitan las palabras de control dentro del descodificador, también es posible separar físicamente el gestor 20 o el registro 15 de las unidades de desaleatorización 14. Esto permite aportar una flexibilidad bienvenida en la composición de los descodificadores y particularmente garantizar el acondicionamiento más adecuado de sus componentes.

[0063] También de manera ventajosa, la presente invención sugiere almacenar, en el registro 15, las palabras de control y no los mensajes ECM. Esta manera de hacer permite optimizar los recursos informáticos, particularmente el espacio de la memoria y la rapidez de restitución de la palabra de control en la unidad de desaleatorización que hace la solicitud en el momento de desciframiento del contenido de audio/vídeo. En efecto, los mensajes ECM contienen indicaciones relativas a los derechos que deben poseer los usuarios (descodificadores). Una vez procesadas por el módulo de seguridad, por lo tanto, es oportuno separarse de estas indicaciones que se han convertido en superfluas y conservar solo los datos esenciales en el descodificador para que en cualquier momento pueda descifrar el contenido de audio/vídeo. Así, al liberarse el almacenamiento de los mensajes ECM, se prescinde también de tener que memorizar las claves de transmisión TK que permiten descifrar los ECM. Sabiendo además que estas claves de transmisión cambian regularmente, también se evita tener que asegurar la gestión temporal de estas claves de transmisión.

[0064] Con el fin de optimizar más el tiempo de procesamiento de las palabras de control por el algoritmo criptográfico encargado de cifrarlas o de descifrarlas, se otorgará preferencia a la elección de una clave simétrica como tipo de clave de emparejamiento PK. Además, también se otorgará preferencia al uso de algoritmos rápidos para reducir en lo posible el tiempo necesario para el cifrado/descifrado de una sencilla palabra de control.

[0065] También ventajosamente, el recurso al directorio 22 permite almacenar una pluralidad de claves de emparejamiento PK, cada una debidamente identificada y reservada a una de las unidades de desaleatorización 14 del descodificador. El recurso a este directorio permite, por lo tanto, aportar una protección específica a las diferentes palabras de control en función de su destino o del canal del cual han salido. La pluralidad de claves de emparejamiento PK permite incrementar el grado de seguridad aplicado para proteger el acceso al conjunto de las palabras de control dentro del mismo del descodificador.

[0066] Gracias a la presente invención, se observará que las unidades de desaleatorización 14 solo están encargadas de efectuar las operaciones de desencriptación en el momento del tratamiento del flujo o flujos de audio/vídeo. En efecto, estas operaciones pretenden en primer lugar descifrar las palabras de control mediante la clave de emparejamiento PK y, en segundo lugar, descifrar al menos una parte del contenido de audio/vídeo por medio de la palabra de control que acaba de ser descifrada. Estas dos operaciones sucesivas pueden, por lo tanto, ser efectuadas por una parte por la misma entidad (unidad de desaleatorización) y por otra parte de manera consecutiva de manera que nunca haya una interrupción entre el momento en el que la palabra de control se descifra y el momento en el que se utiliza en el intervalo de tiempo del criptoperíodo. De este modo, cualquier riesgo de sustracción de una palabra de control en abierto por una persona malintencionada se reduce a cero, puesto que su obtención y su uso en abierto se efectúan de manera consecutiva dentro de la misma entidad.

[0067] El descifrado de las palabras de control $[CW]_{PK}$ en la unidad de desaleatorización 14 se efectúa, tal y como se ilustra en la figura 1, dentro de un módulo de descifrado 13 de esta unidad 14. La unidad de desaleatorización y su módulo de descifrado están estrechamente conectados y se encuentran preferiblemente en la misma zona en la parte de silicio de un componente electrónico. De naturaleza monolítica, tal unidad debería romperse físicamente para poder acceder a sus circuitos internos, en particular a su módulo de descifrado 13. Sin embargo, una vez destruida, esta unidad ya no es capaz de descifrar palabras de control.

[0068] Debido a su estructura, el registro 15 se puede colocar en un ambiente menos protegido. Tal y como se ilustra esquemáticamente en la figura 1, el registro 15 de las palabras de control preferiblemente está accesible a toda unidad de desaleatorización 14 del descodificador 10. Así, cuando una unidad de desaleatorización 14 requiera una nueva palabra de control (para poder continuar con el descifrado del contenido de audio/vídeo después del vencimiento de un criptoperiodo), ésta puede acceder por sí misma al registro 15 para extraer la próxima palabra de control que está destinada a ella, a saber aquella cuya indicación D corresponda al identificador ID que la designa. Alternativamente, la unidad de desaleatorización 14 puede enviar una solicitud al registro 15 (o al gestor de claves 20) para señalar que necesita recibir la próxima palabra de control relativa a ella. Gracias al identificador ID que, por ejemplo, puede estar asociado a la solicitud (para determinar la unidad de desaleatorización demandante) y a la indicación D de cada palabra de control, el registro (o el gestor de claves) puede a continuación buscar la próxima palabra de control de esta unidad y transmitírsela en respuesta a su solicitud. En ambos supuestos, cada palabra de control requerida por cualquier unidad de desaleatorización se transmite como está almacenada en el registro, a saber en forma cifrada (por medio de la clave de emparejamiento PK específica de esta unidad).

[0069] Si es preciso, la unidad de desaleatorización 14 también podría almacenar, por ejemplo en un registro local que le es propio, una reserva de palabras de control (por ejemplo, la palabra de control actual y la palabra de control siguiente) en previsión de su uso. En tal caso, se considerará que la unidad de desaleatorización 14, su registro local así como su módulo de descifrado 13 forman entonces una entidad monolítica.

[0070] Según una forma de realización, el descodificador 10 comprende al menos dos unidades de desaleatorización 14 capaces de procesar flujos de audio/vídeo encriptados según algoritmos diferentes. Por ejemplo, una primera unidad de desaleatorización es de tipo DVB-CSA y otra es de tipo AES. El mensaje de control ECM, que contiene la palabra de control CW, también contiene una indicación de qué tipo de algoritmo y, por lo tanto, de unidad de desaleatorización está previsto. Esta indicación (D) se almacena en el registro 15 con la palabra de control $[CW]_{PK}$.

[0071] De ahí en adelante es posible (pero no necesario) utilizar una clave de cifrado diferente por tipo de unidad de desaleatorización. De hecho, el gestor 20 puede disponer de más de un directorio 22 de claves de emparejamiento, por ejemplo una para la unidad de desaleatorización DVB-CSA y otra para la unidad de desaleatorización AES. Gracias a la indicación (D) remitida sobre la palabra de control, el gestor 20 puede seleccionar la clave de emparejamiento PK de la unidad de desaleatorización 14 en cuestión y encriptar la palabra de control CW con esta clave PK.

[0072] Se debe señalar que, en caso de que las unidades de desaleatorización 14 se puedan identificar en función de su tipo, la indicación (D) descrita anteriormente se puede reemplazar por la simple detección del formato (o tipo) de la palabra de control. Una palabra de control para un cifrado de tipo DVB-CSA puede ser de tamaño diferente que una palabra de control para un cifrado AES. Esto permite al gestor 20 seleccionar la clave de emparejamiento PK apropiada para la unidad de desaleatorización en cuestión.

[0073] La figura 2 ilustra el funcionamiento dinámico del conjunto de los principales elementos del descodificador representados en la figura 1. Para ello, esta figura se presenta en forma de un diagrama que, globalmente, se lee de arriba abajo y de izquierda a derecha. Los principales elementos del descodificador útiles para la comprensión de este funcionamiento se representan en la primera línea superior. El funcionamiento dinámico de este conjunto de elementos se describe por una sucesión de etapas identificadas por flechas en tono gris y numeradas de 1 a 9. Estas etapas definen dos fases distintas. La primera fase está formada por las etapas (1), (1') y (1"). La segunda fase comprende las etapas (2) a (9) que, como ilustra esquemáticamente la flecha de forma rectangular que las rodea, están destinadas a repetirse para cada palabra de control CW.

[0074] La primera fase tiene el fin de cargar la clave de emparejamiento PK. Esta carga se realiza, por una parte, en el directorio 22 del gestor 20 y, por otra parte, en el módulo de descifrado 13 de la unidad de desaleatorización 14 a la que esta clave de emparejamiento PK está dedicada. Varios escenarios son posibles:

- La clave de emparejamiento PK se carga de manera permanente durante una fase de inicialización del descodificador. Durante la fabricación del descodificador, o durante una fase de preparación del descodificador para un operador determinado o un cliente determinado, el descodificador 10 se coloca en modo de prueba y una clave de emparejamiento PK se genera (o bien por el equipo de prueba, o bien por el procesador del descodificador) y se transmite al directorio 22 y al módulo de descifrado 13 de la unidad de desaleatorización 14. Esta clave de emparejamiento PK se almacena para toda la vida del descodificador hasta se inicie un nuevo modo de prueba.

- La clave de emparejamiento PK se carga cada vez que se enciende el descodificador. Para ello, una clave de emparejamiento PK se genera aleatoriamente, por medio del generador 18, por el gestor 20 o por el módulo de descifrado 13, y se transmite a la otra entidad, a saber respectivamente al módulo de descifrado 13 o al gestor 20. El gestor 20 transfiere también esta clave PK al directorio 22 con el fin de su almacenamiento. La clave de emparejamiento PK se genera aleatoriamente por el generador aleatorio 18. De hecho, este último puede estar asociado o bien al gestor 20, o bien a cada unidad de desaleatorización 14, en particular estar integrado en el módulo de descifrado 13 de cada una de estas unidades. Este generador 18 puede ser una verdadera fuente de números aleatorios, una fuente de números pseudoaleatorios, incluso una mezcla de datos físicos del descodificador, tales como temperatura, fecha, tiempo de reacción del mando a distancia. La generación de esta clave de emparejamiento PK se ilustra en la figura 2 por la etapa (1). Las etapas (1') y (1") ilustran la compartición de esta clave de emparejamiento PK respectivamente entre el gestor 20, en particular el directorio 22, y la unidad de desaleatorización 14, en particular el módulo de descifrado 13 de esta unidad. Se debe señalar que el canal entre estas dos entidades 20,14 está protegido (segundo canal protegido), es decir, que una clave de sesión es negociada entre estas dos entidades, por ejemplo utilizando el algoritmo de Diffie-Hellman. Otro medio de asegurar la protección de tal canal podría consistir en recurrir a medios materiales. Por ejemplo, el bus en el que transitan los intercambios ente las entidades 20 y 14 podría ser un bus privado accesible únicamente por estas dos entidades.

[0075] Las etapas (1), (1') y (1"), por lo tanto, se pueden formular de la siguiente manera:

- (1) generación de una clave de emparejamiento PK por el gestor 20 o por la unidad de desaleatorización 14,

- atribución, a dicha clave de emparejamiento PK, del identificador ID propio de la unidad de desaleatorización 14 a la que la clave de emparejamiento PK está asociada de manera única,

- (1'), (1") transmisión de la clave de emparejamiento PK así referenciada entre el gestor de claves 20 y la unidad de desaleatorización 14 de manera que esta clave de emparejamiento PK sea conocida por estas dos entidades.

[0076] Según una forma de realización, el número aleatorio generado por una de las dos entidades 14, 20 (por medio del generador 18) se aplica a continuación a una función criptográfica contenida en la entidad en cuestión e inicializada por una clave de personalización. Esta clave se inicializa durante una fase de inicialización previa. De este modo, es posible personalizar cada descodificador o grupo de descodificadores con un valor particular de clave de personalización. La función criptográfica puede ser del tipo de un solo sentido (función *Hash*). El resultado de la función criptográfica produce la clave de emparejamiento PK. Aunque el generador de número aleatorio se haya visto comprometido y genere siempre el mismo valor, el hecho de modificar este valor por la función

criptográfica proporcionará una clave de emparejamiento que será diferente de un descodificador (o de un grupo de descodificadores) a otro.

[0077] La etapa (1) para generar la clave de emparejamiento PK puede comprender, por lo tanto, las subetapas siguientes:

- obtención de un número aleatorio por medio de un generador 18 de números aleatorios, de una fuente de números pseudoaleatorios, de una mezcla de datos físicos del descodificador 10, tales como temperatura, fecha o tiempo de reacción del usuario,

- aplicación de este número aleatorio a una función criptográfica contenida en el descodificador e inicializada por una clave de personalización para obtener la clave de emparejamiento PK.

[0078] La segunda fase de la figura 2 ilustra las etapas (2) a (9) iniciadas en el descodificador para procesar y gestionar cada palabra de control CW, desde su recepción por el módulo de seguridad, hasta su uso por una de las unidades de desaleatorización 14. En cuanto el gestor 20 recibe una palabra de control $[CW]_{SK}$, la envía (2) al módulo criptográfico 23. Este último, gracias a la clave secreta SK, la descifra (3) y luego la reencripta inmediatamente (4) gracias a la clave de emparejamiento PK apropiada que ha podido ser identificada en el directorio 22, o bien por la unidad central 26, o bien directamente por el módulo criptográfico 23. La identificación de esta clave de emparejamiento PK se puede obtener estableciendo una correspondencia entre el identificador ID asociado a la clave PK y la indicación D de destino que referencia la palabra de control. Una vez cifrada mediante la clave de emparejamiento PK, el módulo criptográfico 23 envía (5) la palabra de control $[CW]_{PK}$ al registro 15 de las palabras de control. Esta palabra de control se podrá almacenar en él bajo esta nueva forma cifrada al menos mientras no se utilice.

[0079] Cuando cualquiera de las unidades de desaleatorización 14 necesita una palabra de control para poder descifrar una nueva parte del contenido de audio/vídeo que está descodificando, la solicita (6) al registro 15 (por ejemplo, mediante el gestor 20 si este registro no es autónomo) transmitiendo por ejemplo una solicitud RQ. Para obtener la próxima palabra de control que está reservada para ella, esta solicitud va acompañada de la identidad de la unidad de desaleatorización 14, de manera que el registro 15 (o el gestor 20 que gestiona este registro) pueda identificar cuál es la unidad de desaleatorización 14 en cuestión entre todas las unidades de desaleatorización con las que cuenta el descodificador 10. Normalmente, la solicitud puede contener una información (ID o D) que permite asegurar esta identificación. Una vez que la palabra de control $[CW]_{PK}$ apropiada se ha transmitido (7) en respuesta a la solicitud de la unidad de desaleatorización (o ha sido obtenida por esta unidad si ésta tiene acceso directamente al registro 15), a continuación es descifrada (8) por el módulo de descifrado 13 mediante la clave de emparejamiento PK dedicada a la unidad de desaleatorización 14. Una vez descifrada, la palabra de control CW se transmite (9) al núcleo de la unidad de desaleatorización 14 en vista de ser utilizada como clave de descifrado para descodificar la parte del contenido de audio/vídeo procesada por esta unidad.

[0080] El segundo objeto de la invención trata sobre el descodificador 10 para la aplicación del método descrito anteriormente, según cualquiera de las variantes propuestas. Este descodificador, por lo tanto, estará a cargo de descodificar al menos un contenido audio/visual protegido por palabras de control CW. Tal y como se ilustra en la figura 1, este descodificador 10 comprende un gestor de claves 20 conectado, a través de un canal protegido 25, a un módulo de seguridad 30 a cargo de enviar palabras de control CW a dicho descodificador en forma cifrada. Comprende igualmente al menos dos unidades de desaleatorización 14 a cargo de descifrar cada una un contenido de audio/vídeo cifrado por una parte de dichas palabras de control CW, y un registro 15 de palabras de control administrado por dicho gestor 20. Este último está configurado para descifrar las palabras de control CW recibidas de dicho módulo de seguridad 30 y para almacenarlas en el registro 15 en forma cifrada.

[0081] Según la invención, este descodificador 10 comprende además:

- una memoria para almacenar un directorio de claves 22 administrado por el gestor 20 y configurado para clasificar una pluralidad de claves de emparejamiento PK, donde cada clave de emparejamiento PK está referenciada por un identificador ID que la asocia de manera única a una de las unidades de desaleatorización 14 del descodificador,

- un módulo de referenciación 24 que permite referenciar cada palabra de control CW por una indicación D que identifica la unidad de desaleatorización 14 a la que esta palabra de control se destina en función del canal de audio/vídeo del que se extrae cada palabra de control. Cada canal de audio/vídeo se puede identificar o bien por un identificador, o bien en función de su recorrido dentro del descodificador. Así, cada canal saliente del demultiplexor 11 (o de cada dispositivo de selección 12) se puede detectar y etiquetar con una etiqueta particular.

[0082] El gestor 20 también está configurado por una parte para identificar, en el directorio 22, la clave de emparejamiento PK cuyo identificador ID corresponde con la indicación de destino D que referencia toda palabra

de control CW y, por otra parte, para cifrar esta palabra de control CW con ayuda de la clave de emparejamiento PK así identificada. El cifrado de la palabra de control con ayuda de la clave de emparejamiento PK se efectuará, por ejemplo, mediante un módulo criptográfico 23 integrado en el gestor 20.

[0083] Finalmente, el registro 15 está configurado para que las palabras de control $[CW]_{PK}$, cifradas por la clave de emparejamiento PK, se puedan almacenar en él de manera cronológica y referenciada.

[0084] En una forma de realización, el registro 15 se vuelve directamente accesible a cualquier unidad de desaleatorización 14 del descodificador 10. Esto se puede hacer posible por ejemplo dotando al registro 15 de una vía de acceso (bus e interfaz de comunicación) que lo conecta directamente a cada unas de las unidades de desaleatorización.

[0085] Con el fin de asegurar la transferencia en secreto de la clave de emparejamiento PK del módulo criptográfico 23 al módulo de descifrado 13, o viceversa, el descodificador 10 puede estar configurado además para poder establecer un segundo canal protegido, reservado para este fin, entre el gestor 20 y las unidades de desaleatorización 14. Alternativamente, el descodificador 10 podría comprender, para cada unidad de desaleatorización 14, un bus privado accesible únicamente al gestor de claves 20 y a la unidad de desaleatorización 14 en cuestión.

[0086] Según una forma de realización, el descodificador 10 puede comprender un generador 18 de números aleatorios que se puede comunicar con cada una de las unidades criptográficas 14. Así, estas últimas serán capaces de obtener cada una una clave de emparejamiento PK que depende de un número aleatorio procedente del generador 18. Tal clave de emparejamiento PK se podría obtener, por ejemplo, aplicando a este número aleatorio una función criptográfica inicializada por una clave de personalización.

[0087] Aunque los objetos de la presente invención hacen referencia a un contenido, flujo o canal de tipo audio/vídeo (o audio/visual), se comprenderá que contenidos, flujos o canales de otro tipo se podrían considerar perfectamente. Estos otros tipos podrían hacer referencia a datos de imagen (fotográficos), a datos de audio (musicales), a otros datos multimedia (juegos) y a datos de cualquier otra naturaleza (programas informáticos, textos, valores digitales, etc ...). Así, se comprenderá que el adjetivo "de audio/vídeo" o "audio/visual" que califica los términos contenido, flujo o canal en el presente documento es accesorio y posee por lo tanto un carácter particular que se podría generalizar por el adjetivo digital.

REIVINDICACIONES

1. Método para proteger palabras de control (CW) dentro de un descodificador (10) a cargo de descodificar al menos un contenido digital protegido por dichas palabras de control, dicho descodificador (10) que comprende un gestor de claves (20) conectado, a través de un canal protegido (25), a un módulo de seguridad (30) a cargo de enviar dichas palabras de control (CW) a dicho descodificador (10) en forma cifrada, al menos una unidad de desaleatorización (14) a cargo de descifrar el contenido digital, y un registro (15) de palabras de control (CW) administrado por dicho gestor (20), método que comprende las etapas siguientes:

- la carga, para cada unidad de desaleatorización (14) en un directorio de claves (22) administrado por dicho gestor (20), de una clave de emparejamiento (PK) que, por una parte, está referenciada por un identificador (ID) que la asocia a la unidad de desaleatorización (14) a la que se dedica únicamente y, por otra parte, es conocida por esta unidad de desaleatorización,
- la recepción por dicho gestor de claves (20) de al menos una palabra de control (CW) cifrada por el módulo de seguridad (30), dicha palabra de control (CW) que también está referenciada por una indicación (D) que permite identificar la unidad de desaleatorización (14) a la que está destinada,
- el desciframiento, por el gestor de claves (20), de dicha palabra de control (CW) mediante una clave de descifrado (SK) propia de dicho canal protegido (25),
- la identificación, en dicho directorio (22), de la clave de emparejamiento (PK) cuyo identificador (ID) corresponde a la indicación de destino (D) asociada a dicha palabra de control (CW), y después
- el ciframiento de esta palabra de control (CW) con ayuda de la clave de emparejamiento (PK) así identificada, y
- el almacenamiento, en dicho registro (15) de manera cronológica y referenciada, de la palabra de control (CW) así cifrada con ayuda de la clave de emparejamiento (PK), de manera que toda palabra de control específica solicitada por una unidad de desaleatorización (14) pueda ser retirada de dicho registro (15) con el fin de ser descifrada y utilizada por esta unidad de desaleatorización para descodificar una parte de dicho contenido digital.

2. Método según la reivindicación 1, **caracterizado por el hecho de que** dicho descodificador (10) comprende al menos dos unidades de desaleatorización (14).

3. Método según la reivindicación 1 o 2, **caracterizado por el hecho de que** la asociación de dicha indicación de destino (D) a dichas palabras de control (CW) se efectúa en dicho descodificador (10), en función de la identificación de un canal digital del cual cada palabra de control se extrae en del descodificador.

4. Método según cualquiera de las reivindicaciones precedentes, **caracterizado por el hecho de que** dicho registro (15) de las palabras de control es accesible a cualquier unidad de desaleatorización (14) del descodificador (10).

5. Método según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** cada palabra de control (CW) solicitada por cualquier unidad de desaleatorización (14) es transmitida tal como está almacenada en dicho registro (15), a solicitud de este último, por dicho gestor de claves (20).

6. Método según la reivindicación 1, **caracterizado por el hecho de que** dicha clave de emparejamiento (PK) se carga en el dicho directorio de claves (22) por el gestor de claves (20) al final de las etapas siguientes:

- generación de una clave de emparejamiento (PK) por el gestor de claves (20) o por la unidad de desaleatorización (14),
- atribución, a dicha clave de emparejamiento (PK), de dicho identificador (ID) propio de la unidad de desaleatorización (14) a la que esta clave de emparejamiento (PK) está asociada de manera única,
- transmisión de la clave de emparejamiento (PK) entre el gestor de claves (20) y la unidad de desaleatorización (14) para que dicha clave de emparejamiento (PK) sea conocida por el gestor de claves (20) y por la unidad de desaleatorización (14) a la que esta clave está dedicada.

7. Método según la reivindicación 6, **caracterizado por el hecho de que** dicha clave de emparejamiento (PK) se genera por las etapas siguientes:

- obtención de un número aleatorio por medio de un generador (18) de números aleatorios, de una fuente de números pseudoaleatorios o de una mezcla de datos físicos del descodificador (10) tales como temperatura, fecha o tiempo de reacción de un usuario,
- aplicación de dicho número aleatorio a una función criptográfica contenida en el descodificador (10) e inicializada por una clave de personalización para la obtención de dicha clave de emparejamiento (PK).

8. Método según la reivindicación 6 o 7, **caracterizado por el hecho de que** la transmisión de dicha clave de emparejamiento (PK) entre el gestor de claves (20) y dicha unidad de desaleatorización (14) se realiza dentro de un segundo canal protegido.

9. Método según la reivindicación 6 o 7, **caracterizado por el hecho de que** la transmisión de dicha clave de desaleatorización (PK) entre el gestor de claves (20) y dicha unidad de desaleatorización (14) se realiza en un bus privado accesible únicamente por dicho gestor (20) y dicha unidad de desaleatorización (14).

10. Método según la reivindicación 1, **caracterizado por el hecho de que** dicha clave de emparejamiento (PK) se carga en dicho directorio de claves (15) de manera permanente durante una fase de inicialización previa a toda restitución en abierto de dicho contenido digital.

11. Descodificador (10) para la aplicación del método según cualquiera de las reivindicaciones 1 a 10, que comprende un gestor de claves (20) conectado, a través de un canal protegido (25), a un módulo de seguridad (30) a cargo de enviar palabras de control (CW) a dicho descodificador en forma cifrada, al menos dos unidades de desaleatorización (14) a cargo de descifrar cada una un contenido digital cifrado por algunas de dichas palabras de control (CW), y un registro (15) de palabras de control administrado por dicho gestor de claves (20), dicho gestor de claves (20) que también está configurado para descifrar las palabras de control (CW) recibidas de dicho módulo de seguridad (30) y para almacenarlas en dicho registro (15) en forma cifrada, **caracterizado por el hecho de que** comprende además:

- una memoria para almacenar un directorio (15) de claves administrado por dicho gestor (20) y configurado para clasificar una pluralidad de claves de emparejamiento (PK), donde cada clave de emparejamiento (PK) está referenciada por un identificador (ID) que la asocia de manera única a una de dichas unidades de desaleatorización (14) del descodificador (10),
- un módulo de referenciación (24) que permite referenciar cada palabra de control (CW) por una indicación (D) que identifica la unidad de desaleatorización (14) a la que esta palabra de control (CW) se destina en función de un canal digital del que se extrae cada palabra de control (CW),

donde dicho gestor de claves (20) está configurado además para poder identificar, en dicho directorio (22), la clave de emparejamiento (PK) cuyo identificador (ID) corresponde a la indicación de destino (D) que referencia dicha palabra de control (CW), y cifrar esta palabra de control (CW) con ayuda de la clave de emparejamiento (PK) así identificada, y
donde dicho registro (15) está configurado para almacenar, de manera cronológica y referenciada, cada palabra de control (CW) cifrada por unas de dichas claves de emparejamiento (PK).

12. Descodificador (10) según la reivindicación 11, **caracterizado por el hecho de que** dicho registro (15) de palabras de control está accesible directamente a cualquier unidad de desaleatorización (14) del descodificador.

13. Descodificador (10) según la reivindicación 11 o 12, **caracterizado por el hecho de que** está configurado para poder establecer un segundo canal protegido reservado a la transmisión de una clave de emparejamiento (PK) entre el gestor (20) y cada una de dichas unidades de desaleatorización (14).

14. Descodificador (10) según la reivindicación 11 o 12, **caracterizado por el hecho de que** comprende, para cada unidad de desaleatorización (14), un bus privado accesible únicamente al gestor de claves (20) y a dicha unidad de desaleatorización (14) para la transmisión de la clave de emparejamiento dedicada a esta unidad de desaleatorización.

15. Descodificador (10) según una de las reivindicaciones 11 a 14, **caracterizado por el hecho de que** comprende un generador (18) de números aleatorios que puede comunicarse con cada una de las unidades criptográficas (14) para que estas últimas puedan obtener cada una una clave de emparejamiento (PK) aplicando a un número aleatorio, procedente de dicho generador (18), una función criptográfica inicializada por una clave de personalización.

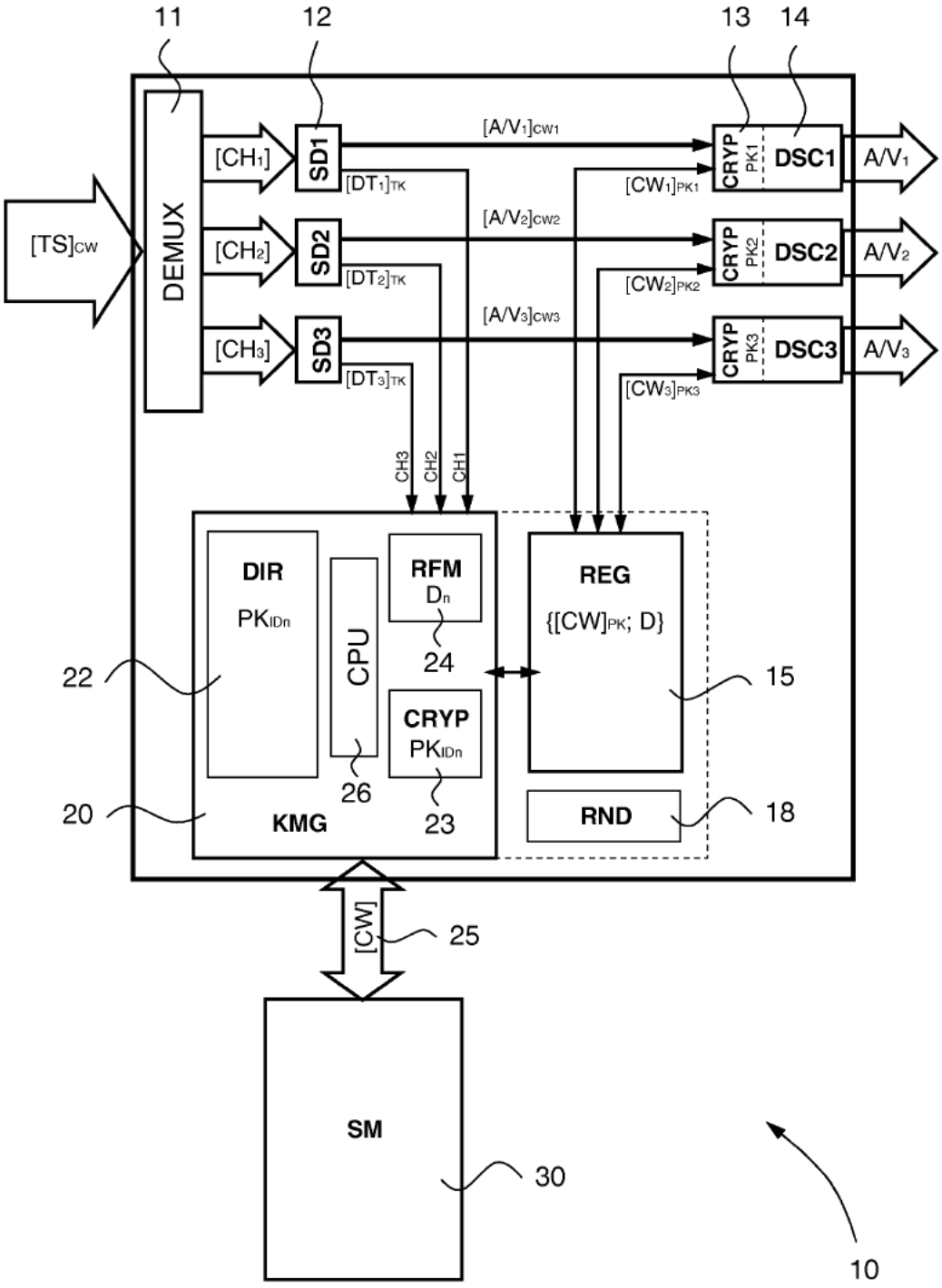
11
12
13
14
[TS]CW
DEMUX
[CH1]
[CH2]
[CH3]
SD1
SD2
SD3
[DT1]TK
[DT2]TK
[DT3]TK
[A/V1]CW1
[A/V2]CW2
[A/V3]CW3
[CW1]PK1
[CW2]PK2
[CW3]PK3
CRYP PK1
CRYP PK2
CRYP PK3
DSC1
DSC2
DSC3
A/V1
A/V2
A/V3
CH3
CH2
CH1
DIR
PKIDn
CPU
RFM
Dn
24
CRYP
PKIDn
26
23
KMG
REG
{[CW]PK; D}
RND
22
20
15
18
[CW]
25
SM
30
10

Fig. 1

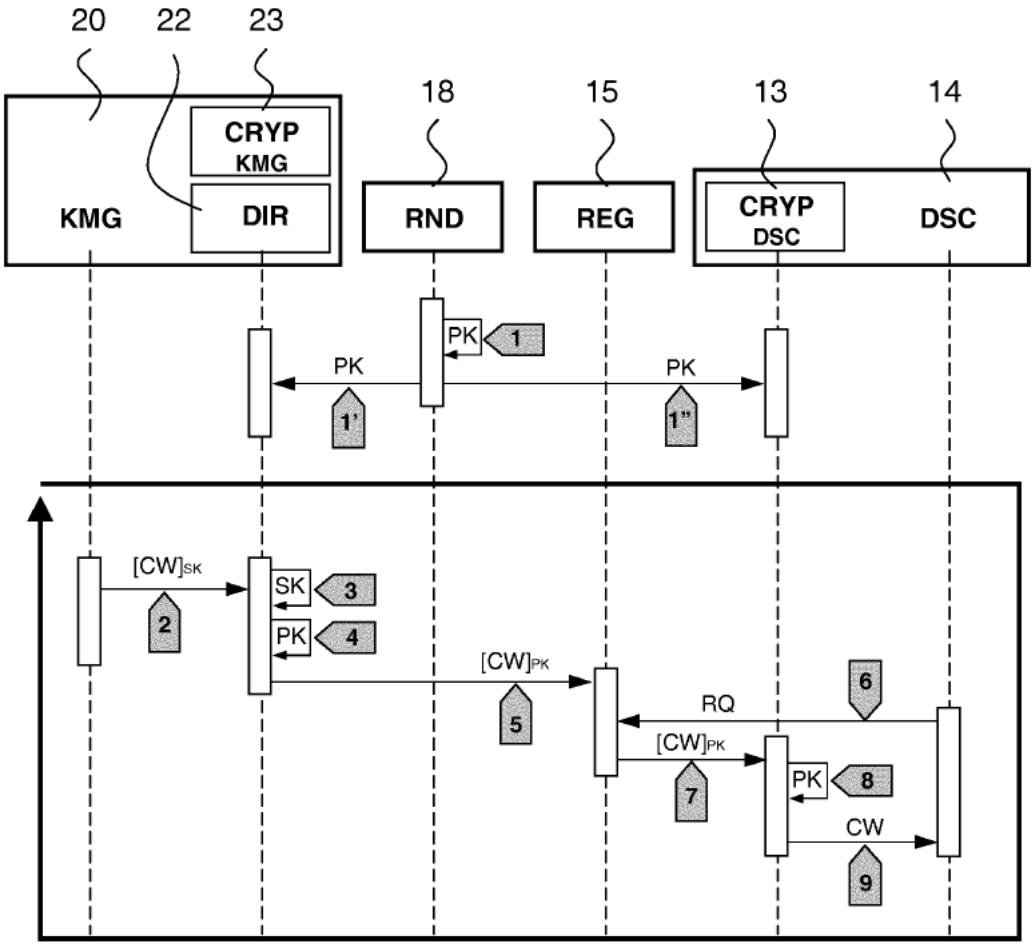
20
22
23
18
15
13
14
CRYP
KMG
KMG
DIR
RND
REG
CRYP
DSC
DSC
PK
1
PK
1'
PK
1"
[CW]SK
2
SK
3
PK
4
[CW]PK
5
RQ
6
[CW]PK
7
PK
8
CW
9

Fig. 2