(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 422 880**

(51) Int. CI.:

H04N 21/418 (2011.01)
H04N 21/4623 (2011.01)
H04N 5/913 (2006.01)
H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.03.2003 E 03704928 (5)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2013 EP 1495637**

(54) Título: **Método para almacenar de forma segura datos encriptados**

(30) Prioridad:

15.03.2002 CH 456022002

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.09.2013

(73) Titular/es:

NAGRAVISION SA (100.0%)
22, ROUTE DE GENÈVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

LE BUHAN, CORINNE;
BERTHOLET, PATRICK y
SASSELLI, MARCO

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para almacenar de forma segura datos encriptados

[0001] La presente solicitud se refiere al ámbito de los receptores/descodificadores de servicios con acceso condicional, en particular a los receptores que disponen de unidad de almacenamiento tales como los discos duros.

[0002] La evolución tecnológica en el ámbito de las capacidades de almacenamiento y de la rapidez de los discos magnéticos (disco duro) ha hecho que sea posible almacenar el contenido de emisión de vídeo para que el usuario acceda a éste en diferido.

[0003] Tales receptores son conocidos bajo la marca ReplayTV ® o Tivo ® y ofrecen almacenamientos de varias decenas de horas de transmisión digital. Sin embargo, estos receptores no están directamente integrados en los receptores/descodificadores de servicios con acceso condicional; en particular, el contenido se almacena sin protección particular en el disco, lo que hace imposible la recogida de los derechos de autor asociados al contenido, en caso de que el disco se duplicara después para fines de redistribución comercial.

[0004] A la inversa, en un sistema de televisión digital de pago, el flujo digital transmitido hacia estos receptores se encripta para poder controlar la utilización y definir las condiciones para tal utilización. Esta encriptación se realiza gracias a las palabras de control (Control Words) que se cambian a intervalos regulares (normalmente entre 5 y 30 segundos) para disuadir cualquier ataque que busque recuperar tal palabra de control.

[0005] Para que el receptor pueda desencriptar el flujo encriptado por estas palabras de control, éstas últimas se le envían independientemente del flujo en mensajes de control (ECM) encriptados por una clave propia del sistema de transmisión entre el centro de gestión (CAS) y el módulo de seguridad de la unidad de usuario. De hecho, las operaciones de seguridad se efectúan en una unidad de seguridad (SC) que habitualmente tiene forma de tarjeta inteligente, considerada inviolable. Esta unidad puede ser de tipo extraíble o estar directamente integrada en el receptor.

[0006] Durante la desencriptación de un mensaje de control (ECM), se verifica, en la unidad de seguridad (SC), que el derecho de acceso a la transmisión en cuestión está presente. Este derecho se puede gestionar a través de mensajes de autorización (EMM) que cargan tal derecho en la unidad de seguridad (SC). También son posibles otras opciones tales como el envío de claves de desencriptado.

[0007] Para el resto de la descripción, se denominará "evento" a un contenido de video, de audio (por ejemplo MP3) o de datos (programa de juego, por ejemplo) que es encriptado según el método conocido por las palabras de control, es decir con una clave que sólo es valida para una parte del contenido.

[0008] El reconocimiento de la utilización de tales eventos se basa hoy en día en el principio de la suscripción o de la compra unitaria. La suscripción permite definir un derecho asociado a uno o varios canales de difusión de estos eventos y permite al usuario obtener estos eventos en abierto si el derecho se encuentra en su unidad de seguridad.

[0009] Al mismo tiempo, es posible definir los derechos propios de un evento, tal como una película o un partido de fútbol. El usuario puede adquirir este derecho (compra, por ejemplo) y este evento será específicamente gestionado por este derecho. Este método se conoce bajo la denominación "pay-per-view" (PPV).

[0010] Un mensaje de control (ECM) no sólo contiene la palabra de control sino también las condiciones para que esta palabra sea devuelta al receptor/descodificador. Durante la desencriptación de las palabras de control, se verifica si un derecho asociado a las condiciones de acceso enunciadas en el mensaje se encuentra en la unidad de seguridad.

[0011] La palabra de control sólo se devuelve en abierto a la unidad de usuario cuando la comparación es positiva. Esta palabra de control se encuentra en un mensaje de control ECM que está encriptado por una clave de transmisión (TK).

[0012] Para que el derecho esté presente en la unidad de seguridad, debe ser cargado por un mensaje de gestión de derecho (EMM) que, por razones de seguridad, normalmente está encriptado por una clave diferente de la clave del derecho (RK).

[0013] Según una forma conocida de difusión de televisión de pago, los tres elementos siguientes son necesarios para desencriptar un contenido en un momento dado:

- el evento encriptado por una pluralidad de palabras de control
- los mensajes de control ECM
- el derecho correspondiente almacenado en la unidad de seguridad

[0014] Para el resto de la exposición, se denominará "claves de sistemas" al conjunto de las claves e informaciones ligadas a las claves de desencriptación que permiten el acceso al contenido. En una configuración conocida de televisión de pago, se trata de claves de transmisión para desencriptar los mensajes de control (ECM) y de claves de derecho para desencriptar los mensajes de derecho (EMM).

[0015] Según un esquema conocido, el contenido encriptado que se almacena en una unidad de almacenamiento tal como un disco duro está acompañado de al menos mensajes de control ECM.

[0016] Dado que la desencriptación a posteriori de los mensajes ECM puede suponer un problema, en particular debido al cambio de la clave de transmisión, se propone una primera solución en el documento EP 0 912 052, solución que implica la desencriptación de estos mensajes en la unidad de seguridad y la reencriptación antes del almacenamiento en el disco.

[0017] Esta solución resuelve el problema del período de vida útil de la clave de transmisión pero carga enormemente la unidad de seguridad en el momento de la grabación, sin saber si el contenido grabado se utilizará algún día. Además, una de las reglas fundamentales del sistema de seguridad es devolver a la unidad de usuario las palabras de control sólo si los derechos existen. En este caso, es muy probable que estos derechos no existan si se considera una compra por evento. El derecho será adquirido en el momento de la compra, que se puede hacer mucho más tarde, en el momento en el que el usuario decida visualizar este evento.

[0018] Este documento EP 0 912 052 no resuelve el problema del acceso al derecho porque en el momento de la compra, el mensaje de derecho EMM debe difundirse siempre para que sea cargado en la unidad de seguridad.

[0019] De este modo, la solución descrita en este documento sólo es aplicable para eventos difundidos para los cuales el derecho ya está presente en la unidad de seguridad para autorizar la desencriptación y la reencriptación del ECM.

[0020] Por lo tanto, supone un problema no resuelto cuando se almacenan eventos sin que se disponga del derecho en el momento del almacenamiento o cuando las condiciones de desencriptación varían entre el momento del almacenamiento y el momento del disfrute del evento por el usuario. Otro aspecto es la carga suplementaria requerida por la unidad de seguridad para esta desencriptación y reencriptación.

[0021] El documento EP-A-0 936 774 describe un sistema para la transmisión y la grabación de datos digitales encriptados que son difundidos por un centro de difusión, de la misma manera que los mensajes de gestión ECM y EMM. El objetivo de la invención descrito en este documento es impedir que los datos, una vez desencriptados, se puedan duplicar en copias piratas sin prohibir, no obstante, que un usuario legítimo grabe un contenido prepagado. Para ello, los datos digitales son encriptados con al menos una palabra de control cifrada por una primera clave asociada a la identidad de los datos transmitidos. Un dispositivo de grabación graba los datos encriptados así como los mensajes ECM, EMM. El mensaje ECM incluye la palabra de control cifrada mientras que el mensaje EMM incluye la primera clave cifrada por una segunda clave almacenada en un módulo de control de acceso. Gracias a esta segunda clave, este módulo es capaz de descifrar el EMM para obtener la primera clave, y después descifrar el ECM mediante esta primera clave para obtener la palabra de control que permite desencriptar los datos digitales grabados. El inconveniente de este sistema reside en el hecho de que presenta un nivel de seguridad insuficiente.

[0022] El objetivo de la presente invención es proponer un método de almacenamiento de un evento encriptado por palabras de control (CW) que garantice el acceso a este evento en cualquier momento, aunque ciertas claves del sistema hayan cambiado por razones de seguridad.

[0023] Este objetivo se alcanza mediante un método de almacenamiento de un evento encriptado por palabras de control (CW) en una unidad de recepción y de desencriptación conectada a una unidad de seguridad (SC), estas palabras de control (CW) y los derechos necesarios están contenidos en mensajes de gestión (ECM, EMM) encriptados por claves de sistemas (TK, RK), caracterizado por el hecho de que consiste en almacenar el evento encriptado así como los mensajes de control (ECM) en la unidad de almacenamiento y en almacenar en la unidad de almacenamiento las claves de sistema encriptadas (SK) por una clave local predeterminada almacenada en la unidad de seguridad (SC).

[0024] De este modo, la unidad de almacenamiento contiene todos los elementos que permiten en un momento dado visualizar este evento garantizando a la vez la seguridad inicialmente definida.

[0025] Según la invención, se utiliza una clave diferente para esta operación de almacenamiento de las claves de sistema, estas claves son necesarias para la desencriptación de los mensajes de control y para su funcionamiento, diferentes de las utilizadas en el marco habitual del sistema de recepción. Se dice que están predefinidas porque puede tratarse de un conjunto de claves que se utilizan según una indicación de fecha, por ejemplo. De este modo, se utilizará una clave para el mes de enero y otra para el mes de febrero; incluso una clave para los días pares y otra para los días impares. Esta indicación de fecha está incluida en el contenido y, por lo tanto, la clave adecuada podrá ser utilizada para desencriptar el conjunto de claves encriptadas SK.

[0026] En los sistemas conocidos de televisión de pago, los mensajes de gestión están compuestos por los mensajes de control (ECM) y los mensajes de derecho (EMM). La o las claves de transmisión (TK) que permiten desencriptar los mensajes de control (ECM) se cambian a intervalos regulares. Además, según el tipo de implantación elegido, es posible cambiar también la o las claves de derecho (RK) que se encargan de desencriptar los mensajes de derecho (EMM). Se precisa aquí que, según la implementación elegida, es posible utilizar más de una clave para desencriptar un mensaje de transmisión (ECM) o para desencriptar un mensaje de derecho (EMM).

[0027] En el momento de la encriptación de las claves de sistemas, es posible crear no sólo un bloque que contiene las claves de transmisión y las claves de derecho sino también dos bloques encriptados por la clave local, el primero contiene las claves de transmisión y el segundo contiene las claves de derecho.

[0028] De este modo, la solución propuesta por la presente invención es utilizar una clave particular (S1) que no se cambiará nunca y que, por lo tanto, garantiza que años más tarde sea posible acceder al evento encriptado.

[0029] En una forma de realización, se genera una clave de sesión AS aleatoriamente y se utiliza para encriptar las claves de sistemas. Antes de transferir las claves de sistemas, el módulo de seguridad encripta la clave de sesión por la clave local S1 y la transfiere a la unidad de almacenamiento. Esta forma de realización presenta la ventaja de que se pueden utilizar diferentes algoritmos para la encriptación de las claves de sistemas y para la clave de sesión, particularmente en términos de seguridad. La encriptación de las claves de sistemas será ejecutada por un algoritmo simétrico y la clave de sesión podrá ser encriptada por un algoritmo simétrico o asimétrico.

[0030] Según la invención, debido a que el cambio de las claves se puede producir durante la difusión del contenido encriptado, se propone entonces almacenar todas las claves de sistema activas durante la transmisión del contenido, es decir las claves en uso y las claves siguientes preparadas para la orden de cambio de claves. La unidad de seguridad dispone continuamente de la clave activa y de la clave futura.

[0031] Por razones evidentes de seguridad, la clave local que sirve para la encriptación de la clave de transmisión debe conservarse en la unidad de seguridad de cada receptor/descodificador y se pondrá especial atención a los medios de codificación (algoritmo, longitud de clave) para encriptar las claves de sistema.

[0032] La invención se comprenderá mejor gracias a la siguiente descripción detallada y que hace referencia a los dibujos anexos que se aportan a modo de ejemplo, en ningún caso limitativo, a saber:

- la figura 1 ilustra un descodificador que contiene una unidad de almacenamiento,
- la figura 2 ilustra los datos que están almacenados en la unidad de almacenamiento.

[0033] El descodificador (STB) ilustrado en la figura 1 recibe los datos de entrada de forma encriptada. Estos datos se memorizan en la unidad de almacenamiento HD y comprenden particularmente el evento considerado EV, los mensajes de control ECM y los mensajes de derecho EMM.

[0034] Según la invención, en tal operación de almacenamiento, la unidad de seguridad SC recibe los mensajes de control pero no los reenvía a la unidad de usuario. En cambio, esta unidad codifica las claves de sistema por una clave secreta S1 y este conjunto de claves de sistema encriptado SK se almacena en la unidad de almacenamiento.

[0035] Esta clave secreta S1 puede ser una clave propia, de este descodificador STB, propia de un grupo de descodificadores o una clave única para todos los descodificadores.

[0036] En el momento de la lectura, se implementa un mecanismo particular en la unidad de seguridad. De hecho, no es posible reemplazar las claves existentes por las contenidas en el conjunto SK. En tal caso, el funcionamiento normal del descodificador se alteraría.

[0037] Las claves contenidas en el conjunto formado por las claves de sistemas encriptadas SK se almacenan en una región particular propia de esta operación de lectura de informaciones almacenadas.

[0038] La unidad de seguridad debe ser capaz de duplicar sus funcionalidades y de utilizar una zona de la memoria diferente en la que se almacenarán estas claves pasadas.

[0039] Sabiendo que una u otra de estas claves de sistema puede cambiar, según una variante de la invención, este conjunto de claves SK se genera a intervalos regulares y se almacena en la unidad de almacenamiento HD.

[0040] En una variante de la invención, en especial cuando se desea evitar la encriptación del mismo contenido (las claves de sistema) con claves diferentes (la clave secreta S1 de cada descodificador) o hacer accesible la información desde el momento del cambio de claves, se agrega una parte aleatoria (padding) a las claves de sistema antes de la encriptación. Gracias a esta aleatoriedad, incluso durante un período en el que las claves no cambian, cada conjunto encriptado SK es diferente.

[0041] En otra variante de la invención, en particular cuando se quiere esconder la frecuencia de cambio de las claves de sistema, una información de período de validez, relacionada con la codificación de tiempo del contenido en sí (por ejemplo, del minuto 15 al minuto 18 de difusión del contenido), se añade al registro de cada conjunto encriptado SK. De este modo, éste último sólo es válido durante el período de validez que se le asocia así artificialmente y no durante el período de validez *de facto* de las claves de sistema que oculta.

[0042] En cuanto a la clave secreta S1, están previstas varias posibilidades en el marco de esta invención. La característica común es que esta clave es conocida desde el centro de gestión para poder regenerar una unidad de seguridad SC que se hubiera perdido o destruido. De hecho, ahora la clave se convierte en el elemento básico del acceso a los eventos almacenados y es imperativo que la destrucción de una unidad de seguridad no haga que los datos previamente almacenados sean irremediablemente inaccesibles.

[0043] En una variante con la clave S1 propia de un usuario, esta clave se puede generar en el momento de la personalización de la unidad de seguridad y almacenar en el centro de gestión junto al número único de la unidad.

[0044] La descripción de este método no se limita al ámbito de la televisión de pago, sino que se puede aplicar también al ámbito del almacenamiento de audio en formato MP3, por ejemplo.

[0045] Otro dominio de aplicación de la invención se refiere al almacenamiento de programas de ordenador o de juegos.

[0046] Según otra forma de realización de la invención, el contenido encriptado se desencripta gracias a las palabras de control que se envían desde la unidad de seguridad hacia el descodificador de forma encriptada. Esta configuración se describe en el documento WO 99/57901 y garantiza que estas palabras de control no podrán servir para otro descodificador.

[0047] La desencriptación de estas palabras se hace directamente en el circuito integrado que se encarga de desencriptar el contenido, de volverlo a encriptar después por una clave proporcionada también por la unidad de seguridad. Por lo tanto, el contenido se almacena en la unidad de almacenamiento del descodificador y es accesible por una sola clave.

[0048] Según esta configuración y en este modo de reencriptación, los datos en abierto no salen del circuito integrado especializado.

[0049] Por razones de seguridad, la clave utilizada para volver a encriptar el contenido se denomina clave de sesión porque se genera de una manera pseudoaleatoria cada vez que tal operación es necesaria.

[0050] Esta clave de sesión se encripta a continuación de la misma manera que las claves de sistemas y se almacena en la unidad de almacenamiento.

[0051] Con esta clave, es posible añadir condiciones de acceso a este contenido, condiciones que serán verificadas en el momento de la presentación de esta clave de sesión encriptada en la unidad de seguridad.

REIVINDICACIONES

1. Método de grabación de un contenido encriptado a través de palabras de control (CW) en una unidad de almacenamiento de una unidad de recepción y de desencriptación (STB) conectada a una unidad de seguridad (SC), estas palabras de control (CW), al igual que las condiciones necesarias para el acceso de este contenido se transmiten en mensajes de control (ECM) encriptados cada uno por una clave de transmisión (TK), los derechos adquiridos para acceder a este contenido se transmiten en mensajes de derecho (EMM) encriptados cada uno por una clave de derecho (RK), el contenido encriptado, al igual que los mensajes de control (ECM) encriptados y los mensajes de derecho (EMM) encriptados, se almacenan en la unidad de almacenamiento, **caracterizado por el hecho de que** consiste en almacenar en la unidad de almacenamiento las claves de transmisión (TK) de forma encriptada por una clave local predefinida (S1) contenida en la unidad de seguridad (SC) y diferente de las utilizadas en el marco habitual del sistema de recepción, así como las claves de derecho (RK) de forma encriptada por dicha clave local predefinida (S1).

2. Método según la reivindicación 1, **caracterizado por el hecho de que** una clave de sesión (AS) se genera aleatoriamente y se utiliza para encriptar las claves de transmisión (TK) y de derecho (RK), esta clave de sesión es encriptada por la clave local (S1) y almacenada con las claves de sistemas encriptadas.

3. Método según la reivindicación 1 o 2, **caracterizado por el hecho de que** la clave local (S1) se duplica en un centro de administración para poder generar una nueva unidad de seguridad (SC) en caso de necesidad.

4. Método según la reivindicación 1, **caracterizado por el hecho de que** las claves de transmisión (TK) y de derecho (RK) son encriptadas por la clave local (S1) para formar un bloque de sistema encriptado.

5. Método según la reivindicación 1, **caracterizado por el hecho de que** las claves de transmisión (TK) y de derecho (RK) son encriptadas por la clave local (S1) para formar dos bloques de sistema encriptados, uno contiene la o las claves de transmisión (TK) y el otro contiene la o las claves de derecho (RK).

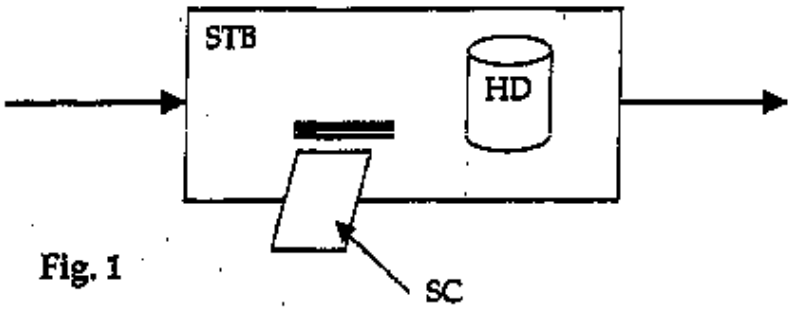

Fig. 1

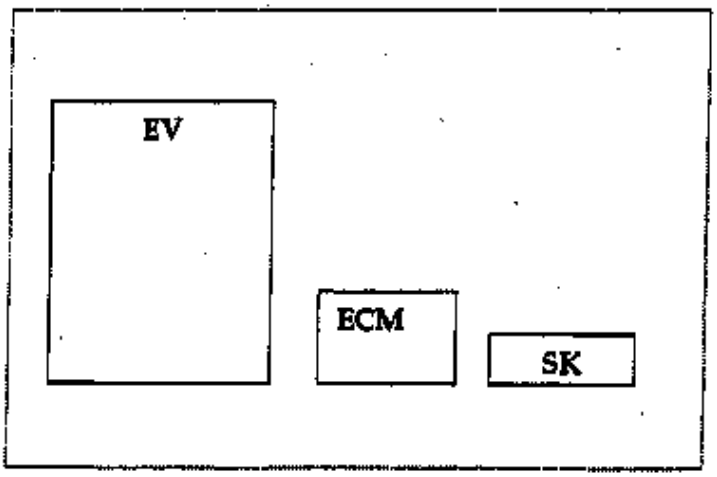

Fig. 2