(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 611 313**

(51) Int. CI.:

H04N 21/258 (2011.01)
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04N 21/4623 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.08.2007 PCT/EP2007/058455**

(87) Fecha y número de publicación internacional: **21.02.2008 WO08020041**

(96) Fecha de presentación y número de la solicitud europea: **15.08.2007 E 07802621 (8)**

(97) Fecha y número de publicación de la concesión europea: **16.11.2016 EP 2052539**

(54) Título: **Método de revocación de módulos de seguridad utilizados para proteger mensajes transmitidos**

(30) Prioridad:

17.08.2006 EP 06119127

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.05.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
ROUTE DE GENÈVE 22-24
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

JUNOD, PASCAL

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de revocación de módulos de seguridad utilizados para proteger mensajes transmitidos

Introducción

[0001] La presente invención se refiere al dominio de la seguridad de módulos de seguridad, estos módulos estando destinados a contener información personal y secreta que permite el acceso a servicios o a prestaciones.

[0002] Esta invención se aplica más precisamente al dominio de la televisión de pago, en la cual un contenido se difunde de forma cifrada, el descifrado de este contenido estando autorizado en determinadas condiciones.

Estado de la técnica

[0003] De manera ampliamente conocida, para poder visualizar un evento de televisión de pago, como una película, un evento deportivo o un concurso, particularmente, se transmiten varios flujos con una unidad multimedia como destino, por ejemplo un descodificador.
Estos flujos son, particularmente, por una parte el fichero del evento en forma de un flujo de datos cifrados y, por otra parte, un flujo de mensajes de control que permite el descifrado del flujo de datos.
El contenido del flujo de datos se cifra a través de "palabras de control" (Control words = cw), renovadas regularmente.
El segundo flujo se denomina flujo ECM (Entitlement Control Message) y se puede formar de dos maneras diferentes.
Según una primera manera, las palabras de control son cifradas por una clave, denominada clave de transmisión TK, que habitualmente es propia del sistema de transmisión entre el centro de gestión y un módulo de seguridad asociado al receptor/descodificador.
La palabra de control se obtiene descifrando los mensajes de control mediante la clave de transmisión TK.

[0004] Según una segunda manera, el flujo ECM no contiene directamente las palabras de control cifradas, sino que contiene información que permite determinar las palabras de control.
Esta determinación de las palabras de control puede hacerse mediante diferentes operaciones, en particular por descifrado, este descifrado pudiendo llevar directamente a la palabra de control, lo que corresponde a la primera manera descrita anteriormente, pero el descifrado puede igualmente llevar a un dato que contiene la palabra de control, ésta debiendo ser aún extraída del dato.
En particular, el dato puede contener la palabra de control así como un valor asociado al contenido por difundir, y particularmente las condiciones de acceso a este contenido.
Otra operación que permite la determinación de la palabra de control puede utilizar, por ejemplo, una función hash de dirección única de esta información particularmente.

[0005] Las operaciones de seguridad generalmente se llevan a cabo en un módulo de seguridad asociado a la unidad multimedia o al descodificador.
Tal módulo de seguridad se puede realizar en particular según cuatro formas distintas.
Una de ellas es una tarjeta con microprocesador, una tarjeta inteligente o más generalmente un módulo electrónico (en forma de clave, de etiqueta de identificación,...). Tal módulo es habitualmente desmontable y conectable al descodificador.
La forma con contactos eléctricos es la más utilizada, pero no se excluye una conexión sin contacto, por ejemplo de tipo ISO 14443.

[0006] Una segunda forma conocida es la de un encapsulamiento de circuito integrado colocado, habitualmente de manera definitiva e inamovible, en la caja del descodificador.
Una variante está constituida por un circuito instalado sobre una base o conector como un conector de módulo SIM.

[0007] En una tercera forma, el módulo de seguridad está integrado en un encapsulamiento de circuito integrado que también tiene otra función, por ejemplo, en un módulo de descodificación del descodificador o el microprocesador del descodificador.

[0008] En una cuarta forma de realización, el módulo de seguridad no se realiza en forma material, sino que su función se efectúa únicamente en forma de software.
Dado que, en los cuatro casos, aunque el nivel de seguridad difiere, la función es idéntica, se hablará de módulo de seguridad sea cual sea la manera de realizar su función o la forma que puede tomar este módulo.

[0009] Durante el descifrado de un mensaje de control (ECM), se verifica, en el módulo de seguridad, que el derecho para acceder al contenido considerado está presente.
Este derecho se puede gestionar a través de mensajes de autorización (EMM = Entitlement Management Message) que cargan dicho derecho en el módulo de seguridad.

[0010] La difusión de datos numéricos con acceso condicional se divide esquemáticamente en tres módulos.
El primer módulo está a cargo del cifrado de los datos numéricos por las palabras de control cw y de la transmisión de estos datos.

[0011] El segundo módulo prepara los mensajes de control ECM que contienen las palabras de control cw, así como las condiciones de acceso, y los transmite a los usuarios.

[0012] El tercer módulo, por su parte, prepara y transmite los mensajes de autorización EMM que están a cargo de definir los derechos de recepción en los módulos de seguridad conectados a los receptores.

[0013] Mientras que los dos primeros módulos generalmente son independientes de los destinatarios, el tercer módulo gestiona el conjunto de los usuarios y transmite las informaciones a un usuario, a un grupo de usuarios o a todos los usuarios.

[0014] Uno de los métodos para eludir la seguridad, que es ciertamente pesado pero realizable, consiste en analizar el contenido de un módulo de seguridad autorizado (ingeniería inversa) con el fin de imitar la parte de seguridad (descifrado de los mensajes) mientras que se crea un corto circuito en la parte de verificación de los derechos.
De este modo, es posible realizar un "clon" de un módulo de seguridad auténtico.
Dicho clon dispondrá, por lo tanto, de la clave de transmisión, lo que le permitirá descifrar las palabras de control cw contenidas en los mensajes de control ECM.
Como los derechos no se verifican en este clon, funcionará como el original en lo que respecta a los medios de descifrado sin que sea necesario, no obstante, disponer de los derechos para realizar este descifrado.

[0015] En un sistema de televisión de pago, es posible cambiar de clave de transmisión.
Para esto se pueden utilizar dos métodos en principio.
El primero consiste en transmitir la nueva clave de transmisión a todos los descodificadores.
Éstos pueden entonces actualizarse de manera que, en cuanto la nueva clave es utilizada, pueden descifrar los eventos.
Este tipo de actualización no permite excluir un descodificador clonado porque podrá recibir igualmente los mensajes de actualización, ya que dispone de las claves de descifrado aferentes.

[0016] Como cada módulo de seguridad comprende al menos una clave única, el segundo método consiste en transmitir la nueva clave de transmisión en un mensaje codificado por esta clave única.
En ese caso, el número de mensajes es como mínimo igual al número de módulos de seguridad instalados con el fin de renovar individualmente esta clave de transmisión.
Se sabe que, si un módulo está fuera de servicio, (es decir si el aparato huésped no es alimentada), no recibirá tal mensaje y ya no podrá ofrecer al usuario los servicios a los cuales tendría legitimo derecho una vez el aparato huésped sea reiniciado.
Para evitar eso, cuando se envía un mensaje destinado a un módulo, este mensaje se repite un gran número de veces con el fin asegurar que su destinatario lo haya recibido bien.

[0017] Debido al ancho de banda limitado disponible y para asegurar que cada abonado haya recibido bien la nueva clave, es necesario transmitir el mensaje bastante antes de que esta nueva clave sea utilizada, por ejemplo repitiendo un mes antes cada mensaje a diferentes horas del día.

[0018] De ahí en adelante, el poseedor de un módulo clon acudirá al técnico que le ha proporcionado dicho clon y que dispone de medios para extraer la nueva clave de transmisión de un módulo auténtico.
Una vez la clave sea proporcionada, por ejemplo por Internet, todos los clones pueden ser actualizados incluso antes de que la nueva clave sea activada.
De esta manera, los clones siempre permanecen operativos.

[0019] De esto resulta que el envío de claves de transmisión tanto por transmisión global como individual presenta inconvenientes y no permite eliminar un módulo clonado.

Breve descripción de la invención

[0020] De este modo, el objetivo de la presente invención es proponer un método para impedir el uso abusivo de datos con acceso condicional, en particular mediante clones de módulos de seguridad cuya seguridad ha sido comprometida.

[0021] Este objetivo se alcanza mediante un método de revocación de módulos de seguridad destinados a recibir mensajes de seguridad transmitidos a una pluralidad de módulos de seguridad, dichos módulos de seguridad que comprenden al menos una clave personal, este método que comprende las etapas, previamente a la revocación, de:

- división del conjunto de los módulos de seguridad en al menos dos grupos,
- determinación, para cada grupo, de una clave asimétrica que comprende una clave pública y una pluralidad de claves privadas diferentes,

- carga de una clave privada por módulo de seguridad,
- preparación con el fin del envío de un mensaje de seguridad por grupo, dicho mensaje estando encriptado por la clave pública de dicho grupo;

donde la revocación consiste en las etapas siguientes:

- envío a cada miembro del mismo grupo que el módulo de seguridad por revocar, a excepción del o de los módulos de seguridad por revocar, de una nueva clave privada correspondiente a la clave pública de otro grupo, cada clave privada estando encriptada por la clave personal de dicho módulo de seguridad.

[0022] Un ejemplo de generación de las claves asimétricas de grupo utiliza el sistema de Boneh-Franklin (Dan Boneh, Matthew K. Franklin: An Efficient Public Key Traitor Tracing Scheme. CRYPTO 1999: 338-353).
Para una clave pública es posible generar una pluralidad de claves privadas, cada una de las cuales permite desencriptar el mensaje encriptado por la clave pública.

[0023] Esto nos permite colocar una clave diferente en cada módulo de seguridad enviando un número limitado de mensajes diferentes.

Breve descripción de las figuras

[0024] La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere a los dibujos anexos que se proporcionan a modo de ejemplo en ningún caso limitativo, en los cuales:

- la figura 1 ilustra esquemáticamente un emisor y un receptor de televisión de pago,
- la figura 2 ilustra la distribución en 4 grupos que comprenden cada uno 3 módulos de seguridad,
- la figura 3 ilustra la distribución de los grupos después de la revocación de un módulo de seguridad.

Descripción detallada

[0025] En el dominio de la transmisión de mensajes de seguridad, preparados y enviados desde un centro de gestión CG a una pluralidad de unidades multimedia STB, se debe hacer frente al compromiso del direccionamiento global, ya sea el mismo mensaje para todas las unidades, o el direccionamiento individual, ya sea un mensaje para cada unidad.

[0026] En el primer caso, el sistema es rápido porque un solo mensaje permite, por ejemplo, cambiar la clave de transmisión.
Esta clave es la que codifica los mensajes que contienen las palabras de control cw.

[0027] Se puede imaginar las consecuencias del segundo caso si hace falta transmitir regularmente las informaciones a cada módulo de seguridad.

[0028] Por esta razón, la solución según la invención es dividir el conjunto de los módulos de seguridad en grupos, cada grupo pudiendo contener varias centenas de módulos.
Según una variante, cada grupo comprende 256 miembros.
De este modo, 1 millón de abonados representa aproximadamente 4000 grupos, por lo tanto, 4000 mensajes para renovar la clave de transmisión o actualizar una programa de seguridad.

[0029] El centro de gestión CG envía los mensajes de seguridad a las unidades multimedia STB.
Estas unidades STB comprenden medios de seguridad SC, ilustrados en la figura 1 por una tarjeta inteligente enchufable.

[0030] Durante la personalización de un tal módulo de seguridad, se colocan claves secretas propias en cada módulo.
Cada módulo de seguridad lleva un número de identificación UA que permitirá rastrear las claves secretas introducidas en un módulo.

[0031] El centro de gestión CG dispone de una base de datos con, para cada módulo de seguridad, la lista de las claves personales.

[0032] La puesta en grupo puede hacerse ya sea con la personalización del módulo (en general antes de la entrega) o durante la puesta en circulación en el sitio.
Según nuestra invención, una clave o una información es necesaria para acceder a los servicios controlados por el centro de gestión.
Esto puede ser una etapa complementaria e independiente a la gestión de los derechos.
El hecho de que la clave o la información sea accesible a todos los módulos de seguridad no significa que los servicios sean accesibles a los abonados que disponen de estos módulos de seguridad.

[0033] Como se ha indicado anteriormente, un módulo de seguridad se asigna a un grupo, por ejemplo el grupo GrA.

Esta asignación puede hacerse o bien durante la inicialización del módulo, o bien mediante el envío de la clave privada personal correspondiente al grupo GrA.
El envío de esta clave se protege por la encriptación de dicha clave por una de las claves personales del módulo de seguridad.
Según el ejemplo de la figura 2, los módulos de seguridad SC1A, SC2A y SC3A forman parte de este grupo GrA.
Las informaciones secretas son encriptadas por la clave KGrA en el centro de gestión CG y descifradas gracias a cada clave privada en los módulos de seguridad.

[0034] De la misma manera, otros grupos GrB, GrC o GrD también comprenden módulos de seguridad SC..B, SC..C o SC..D.

[0035] Así, el conjunto de los módulos de seguridad recibe las informaciones secretas necesarias para el buen funcionamiento del sistema de acceso condicional mediante el envío de tantos mensajes diferentes como grupos existentes.
Se debe señalar que esto no excluye la repetición de los mensajes en el caso de que los descodificadores no dispongan de vía de retorno.
El centro de gestión repetirá los mensajes según una frecuencia convenida, por ejemplo 1 vez al día a las horas seleccionadas aleatoriamente.

[0036] Cuando se detecta un clon de módulo de seguridad, por ejemplo si un tal módulo ha sido comprometido por la extracción de las claves, la clave privada personal se encontrará en todos los clones.

[0037] Una vez se conoce un clon, es posible determinar cuál es el módulo de seguridad que ha sido comprometido por la comparación de la clave privada de este módulo clon con las claves privadas almacenadas en el centro de gestión.
El centro de gestión guarda una copia de la clave privada cargada en cada módulo de seguridad.
Según nuestro ejemplo, el módulo por revocar es el módulo SC1A.
El grupo GrA, por lo tanto, desaparecerá porque ya no es posible enviar los mensajes secretos encriptados por la clave pública KGrA.
Antes de detener el envío de los mensajes encriptados por la clave de grupo KGrA, todos los módulos de seguridad, a excepción del módulo de seguridad corrompido, deberán cambiar de grupo.

[0038] En el ejemplo de la figura 3, el módulo de seguridad SC2A se desplaza al grupo B, el módulo SC2A se desplaza al grupo D. Esta operación se realiza mediante el envío de la clave de grupo de su nuevo destino.
Esta clave de grupo es encriptada por una clave personal del módulo de seguridad con el fin de que este mensaje sólo pueda ser interpretado por el módulo de seguridad afectado.
Una vez que el grupo comprometido ha sido vaciado de sus miembros no corruptos, el envío de los mensajes con la clave del grupo A es interrumpido.
En este momento, todos los clones dejan ser operativos porque ya no pueden recibir las informaciones secretas.

[0039] El desplazamiento de los miembros no revocados a otros grupos se puede hacer ya sea hacia grupos existentes, ya sea mediante la creación de un nuevo grupo.

[0040] La pertenencia a un grupo se realiza como se ha indicado mediante la presencia de una clave privada única generada en un sistema de clave asimétrica de claves privadas múltiples.
Según una forma de realización, también se incluye un identificador de grupo con el fin de filtrar los mensajes relativos a este grupo de los otros mensajes.
Las informaciones secretas son encriptadas por la clave pública de dicho grupo, y a éstas se agrega el identificador de grupo.
Esto evita desencriptar el mensaje y darse cuenta de que su contenido es aleatorio porque no se ha utilizado la clave correcta.
El identificador es preferiblemente testado por el aparato huésped que ha recibido esta información por parte del módulo de seguridad.
Un mensaje sólo se transmite al módulo de seguridad si contiene el identificador del módulo de seguridad.

[0041] Las informaciones secretas pueden tomar varias formas y se transmiten por un mensaje de seguridad.
El documento WO0156287 describe un método para combinar informaciones para la obtención de la palabra de control.
Las informaciones secretas podrían ser o bien la palabra de control maestra que será combinada con las palabras de control cw contenidas en los mensajes de control, o bien la clave para descodificar el mensaje que contiene la palabra de control maestra.

[0042] En otra forma de realización, las informaciones secretas representan la clave de transmisión.
Esta clave sirve para descodificar los mensajes de control ECM y extraer las palabras de control.
Esta clave de transmisión es cambiada, por ejemplo, todos los meses.

[0043] En la práctica, cuando se produce un cambio de clave de transmisión por ejemplo, el envío de la nueva clave a todos los módulos de seguridad puede llevar tiempo.
Los módulos de seguridad, por lo tanto, dispondrán de dos informaciones secretas, una corriente y la otra lista para tomar el relevo.
En el caso de la clave de transmisión, el encabezamiento del mensaje de control contendrá una indicación que permite saber cuál es la clave de transmisión que se ha de utilizar.
Un sistema sencillo es definir una clave de transmisión par y una clave de transmisión impar.
El mensaje de control ECM contendrá un bit para definir la paridad y, por lo tanto, la clave que se ha de utilizar.

[0044] Con el fin de evitar dar tiempo a terceros maliciosos para recobrar la información secreta, está previsto, según la invención, encriptar la información secreta mediante una clave de liberación.
Esta clave es global y se utiliza sea cual sea el grupo del módulo de seguridad.
Así, cada módulo de seguridad recibirá un mensaje encriptado por la clave de su grupo y encriptado por una clave global.
Lo inverso también es posible, a saber, que las informaciones secretas sean encriptadas por la clave global y luego por la clave de grupo.

[0045] Poco antes de la puesta en servicio de la información secreta, por ejemplo la clave de transmisión, el centro de gestión CG envía un mensaje, que contiene la clave global, encriptado según uno de los modos descritos anteriormente.
En este momento, cada módulo será capaz de disponer de la información secreta que le permite procesar las informaciones de seguridad correspondientes.

REIVINDICACIONES

1. Método de revocación de módulos de seguridad destinados a recibir mensajes de seguridad transmitidos a una pluralidad de módulos de seguridad, dicho módulo de seguridad que comprende al menos una clave personal, este método que comprende las etapas, previamente a la revocación, de:

- división del conjunto de los módulos de seguridad en al menos dos grupos,
- determinación, para cada grupo, de una clave asimétrica que comprende una clave pública y una pluralidad de claves privadas diferentes que permiten descodificar un mensaje encriptado por la clave pública,
- carga de una de dichas claves privadas por módulo de seguridad, donde cada módulo recibe una clave privada diferente, dichas claves privadas correspondientes a la clave pública de dicho grupo,
- transmisión de un mensaje de seguridad por grupo, dicho mensaje estando encriptado por la clave pública de dicho grupo;

donde la revocación consiste en las etapas siguientes

- envío a cada miembro del mismo grupo que el módulo de seguridad por revocar, a excepción del o de los módulos de seguridad por revocar, de una nueva clave privada correspondiente a la clave pública de otro grupo, cada clave privada estando encriptada por la clave personal de dicho módulo de seguridad, **caracterizado por el hecho de que** los módulos de seguridad contienen una clave común, **por el hecho de que** el contenido del mensaje de seguridad es sobreencriptado con una clave de liberación, dicha clave de liberación es encriptada por la clave común de los módulos de seguridad y es transmitida poco antes de la puesta en servicio del contenido del mensaje de seguridad.

2. Método de revocación según la reivindicación 1, utilizado en un sistema de televisión de pago en el cual el flujo de datos audio/vídeo se encripta a través de palabras de control (CW), estas últimas siendo transmitidas en mensajes de control (ECM), dichos mensajes siendo encriptados por una clave de transmisión, **caracterizado por el hecho de que** el mensaje de seguridad contiene la clave de transmisión necesaria para el descifrado de los mensajes de control (ECM).

3. Método de revocación según la reivindicación 1, utilizado en un sistema de televisión de pago en el cual el flujo de datos audio/vídeo se encripta a través de palabras de control (CW), estas últimas siendo transmitidas en mensajes de control (ECM), dichos mensajes siendo encriptados por una clave de transmisión, **caracterizado por el hecho de que** el mensaje de seguridad contiene una clave de sobreencriptado de las palabras de control (CW).

4. Método de revocación según la reivindicación 1, **caracterizado por el hecho de que** el mensaje de seguridad contiene actualizaciones del software de dicho módulo de seguridad,

5. Método de revocación según las reivindicaciones 1 a 4, **caracterizado por el hecho de que** los miembros de un grupo revocado se reasignan a grupos existentes diferentes, a excepción del o de los módulos de seguridad por revocar.

6. Método de revocación según las reivindicaciones 1 a 4, **caracterizado por el hecho de que** los miembros de un grupo revocado se reasignan a un nuevo grupo, a excepción del o de los módulos de seguridad por revocar.

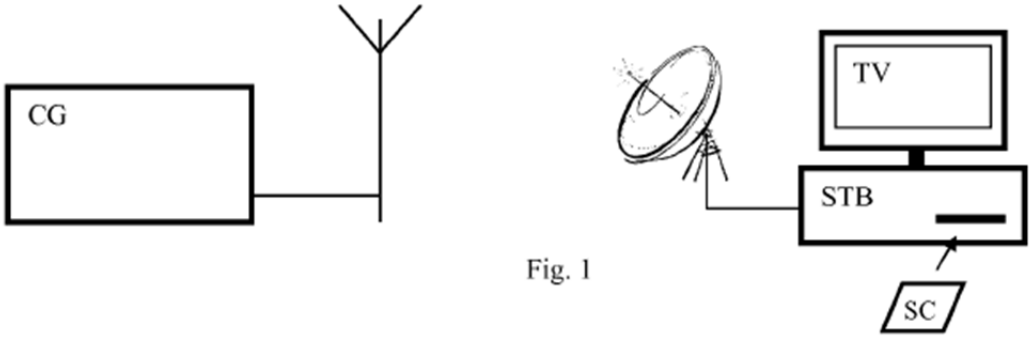

Fig. 1

KGrA	KGrB	KGrC	KGrD	KGrE
SC1A	SC1B	SC1C	SC1D	SC1E
SC2A	SC2B	SC2C	SC2D	SC2E
SC3A	SC3B	SC3C	SC3D	SC3E

Fig. 2

KGrA	KGrB	KGrC	KGrD	KGrE
SC1A	SC1B	SC1C	SC1D	SC1E
	SC2B	SC2C	SC2D	SC2E
	SC3B	SC3C	SC3D	SC3E
	SC2A		SC3A	

Fig. 3