(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 724 703**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.07.2008 PCT/FR2008/051278**

(87) Fecha y número de publicación internacional: **29.01.2009 WO09013420**

(96) Fecha de presentación y número de la solicitud europea: **08.07.2008 E 08826503 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2019 EP 2168304**

(54) Título: **Verificación del código MAC sin revelación**

(30) Prioridad:

13.07.2007 FR 0705095

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.09.2019

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C 76, Route de la Demi-Lune
92057 Paris La Défense Cedex, FR

(72) Inventor/es:

CHIEZE, QUENTIN y
LEPORINI, DAVID

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Verificación del código MAC sin revelación

Sector de la técnica

La presente invención se refiere a la seguridad de los mensajes intercambiados entre entidades distantes, principalmente a la verificación de la autenticidad y/o la integridad de dichos mensajes. Se aplica ventajosamente pero no limitativamente al campo del acceso a contenidos multimedia protegidos.

Estado de la técnica

En este campo, en función de la naturaleza de una red de soporte de comunicación de contenidos multimedia y de un tipo de servicio ofrecido, los sistemas de protección de contenidos implementados pueden ser típicamente sistemas de control de acceso (o CAS, por *"Conditional Access Systems")* o también unos sistemas de gestión de derechos digitales (o DRM, por *"Digital Rights Management")*.
Unas aplicaciones típicas son por ejemplo:

- la emisión/recepción de datos multimedia difundidos en tiempo real (o *"TV live")*,
- o la lectura de datos multimedia almacenados por un grabador digital (frecuentemente basado en disco duro) del terminal a disposición de un usuario (o PVR por *"Personal Video Recorder")*,
- o también aplicaciones de vídeo bajo demanda (o VOD por *"Video On Demand")*.

La seguridad de dicho sistema se basa principalmente en la garantía (por tanto en la verificación) de la autenticidad y de la integridad de los mensajes de control de acceso.
Dichos mensajes pueden ser típicamente, en el contexto del control de acceso CAS, unos mensajes de control de acceso específicos, llamados *"mensajes EMM"* (por *"Entitlement Management Message"*) y *"mensajes ECM"* (por *"Entitlement Control Message"*). La descripción de la figura 1 dada a continuación explica un ejemplo de contexto de utilización de dichos mensajes.
Una presentación exhaustiva de los sistemas de control de acceso está accesible en el documento:
"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM", EBU REVIEW-TECHNICAL EUROPEAN BROADCASTING UNION. BRUSELAS, BE, n.º 266 21 de diciembre de 1995.

En el contexto de la gestión DRM, dichos mensajes pueden ser típicamente unas licencias. La descripción de la figura 2 dada a continuación explica un ejemplo de contexto de utilización de dichos mensajes.

En los sistemas de control de acceso (CAS) o también de gestión DRM, que implementan una criptografía simétrica de claves secretas, la redundancia criptográfica, transmitida con los mensajes de tipo EMM, ECM (para el control de acceso) o respectivamente de licencia, para garantizar la autenticidad y la integridad, se implementa clásicamente por medio de un código MAC (por *"Message Authentication Code"*).

La invención se aplica sin embargo en cualquier contexto en el que un atacante pueda tener acceso a un dispositivo que realice la verificación de un código de autentificación de un mensaje (o MAC por *"Message Authentication Code"*).

Se describe a continuación la intervención de una verificación MAC de ese tipo en el contexto del control de acceso CAS, y posteriormente en el contexto de la gestión DRM.

Contexto del control de acceso CAS

Los sistemas de control de acceso CAS funcionan frecuentemente según unos principios de arquitectura y una cinemática resumidos en la figura 1. Tal como se ilustra en la figura 1, la protección de un contenido tal como un programa audiovisual (o la protección de un componente de un programa de ese tipo) durante su transporte y el control de su acceso por parte de un abonado implementan, por una parte, una función de aleatorización/desaleatorización del programa y, por otra parte, una función de control del permiso de acceso del abonado que se apoya en una distribución de autorizaciones gestionadas a distancia por el operador.

La aleatorización 10

La aleatorización (referencia 10 de la figura 1) permite hacer ininteligible el programa durante su transporte pero puede sin embargo ser captado sin restricción. Pueden implementarse diversas soluciones de aleatorización/desaleatorización. Se trata de algoritmos de cifrado/descifrado propietarios o normalizados, elegidos según el contexto.

Con el fin de hacer la aleatorización impredecible y por tanto casi imposible la desaleatorización fortuita, los algoritmos de cifrado/descifrado utilizan una clave llamada comúnmente *"palabra de control"* (referencia CW por *"Control Word"* de la figura 1). Es habitual modificar el valor de la palabra de control de manera aleatoria, según unas estrategias variables elegidas según el contexto. Por ejemplo, una palabra de control puede modificarse cada 10 segundos, de manera clásica, en la televisión difundida o, en el extremo, con cada película únicamente por ejemplo en el contexto de VOD con particularización individual por abonado.

Un sistema de acceso condicional particularmente del presente Solicitante no incluye solución de aleatorización/desaleatorización pero es compatible con cualquier solución de aleatorización desde el momento en que pueda inicializarse mediante una palabra de control.

El control de acceso

La implementación de la aleatorización/desaleatorización particularizada por una palabra de control dinámica necesita que el aleatorizador y el desaleatorizador (referencia 11 de la figura 1) estén sincronizados con precisión en cuanto al valor de la palabra de control actual CW y en cuanto al instante de cambio de esta.

Además, el control por el operador del acceso al programa por parte de un usuario se efectúa condicionando el acceso a la palabra de control en la disponibilidad de una autorización *"comercial"*. El operador añade al programa una condición de acceso que debe cumplirse por el abonado para poder desaleatorizar este programa.

La transmisión de las palabras de control y la descripción de una condición de acceso son dos de las funcionalidades de un sistema de acceso condicional típico, particularmente del presente Solicitante. Se materializa mediante unos mensajes de control de acceso específicos, llamados *"mensajes ECM"*, calculados por el subsistema *"Explotación"* 12 de la figura 1. Estos mensajes ECM están destinados a ser tratados por el procesador de seguridad 13 que coopera con un terminal desaleatorizador 11 (llamado frecuentemente *"decodificador"* por un término equivocado). En la práctica, el procesador de seguridad 13 se materializa frecuentemente mediante una tarjeta de chips a disposición de un abonado y que coopera con el terminal 11.

En la parte de recepción, por tanto después del conjunto terminal - procesador de seguridad, se verifica un mensaje ECM en cuanto a su seguridad (autenticidad, integridad) y posteriormente se compara la condición de acceso con los títulos de acceso presentes en la memoria no volátil del procesador de seguridad. Si la condición de acceso se satisface por uno de estos títulos de acceso, el procesador de seguridad restituye mediante descifrado la palabra de control y la proporciona al terminal, permitiendo así la desaleatorización.

Gestión de los títulos de acceso

El abonado puede cumplir una condición de acceso a un programa si dispone de un título de acceso que satisface esta condición tal como un título de abono, la referencia de un programa adquirido por adelantado o en tiempo real u otros. Por supuesto, pueden participar otros criterios en la conformidad del abonado con una condición de acceso, tales como una referencia geográfica, un respeto de nivel moral u otros.

Los títulos de acceso o los medios para adquirir los títulos de acceso (por ejemplo unas *"fichas"* para un PPV impulsivo - por *"Pay Per View")* son por tanto gestionados por el operador e inscritos a continuación a distancia en la memoria no volátil (referencia 15) del procesador de seguridad 13 del abonado.

Las acciones a distancia por el operador sobre los títulos de acceso del abonado constituyen otro conjunto de funcionalidades del sistema de acceso condicional de la figura 1. Se materializan mediante unos mensajes de control de acceso específicos, llamados *"mensajes EMM"*, calculados por el subsistema *"Gestión"* (referencia 14) de la figure 1 y por el procesador de seguridad 13.

Seguridad criptográfica

Un sistema de control de acceso no satisface sin embargo su papel más que si no está comprometido o desviado. En particular, los mensajes destinados al sistema de recepción (mensajes ECM y EMM) no deben poder ser generados y aprovechados más que por unos dispositivos debidamente habilitados por el operador de servicio.

Esta restricción fundamental se asegura protegiendo los mensajes destinados al sistema de recepción mediante unas modalidades criptográficas que garantizan la integridad de estos mensajes, su autenticidad y la confidencialidad de los datos sensibles que puedan incluir. En particular, la autenticidad y la integridad de los mensajes están protegidas asociando a cada mensaje su propia redundancia criptográfica.

Estas modalidades criptográficas implementan unos algoritmos específicos parametrizados mediante unas claves. La modificación de los valores de las claves es un medio complementario para reforzar la seguridad del sistema. La actualización de estas claves se asegura mediante unos mensajes de gestión EMM específicos de la seguridad.

Tratamiento de los mensajes de control de acceso por el sistema de recepción

La mayoría de las soluciones operativas de sistemas de control de acceso se apoyan en un sistema de recepción compuesto por dos elementos:

- el terminal 11 que asegura principalmente la recepción de la señal que contiene el/los servicios, su demultiplexado, la desaleatorización y la decodificación de los componentes del servicio elegido por el usuario,

- el procesador de seguridad 13, que soporta las funciones de control de acceso con los tratamientos criptográficos asociados.

El procesador de seguridad 13 trata los mensajes EMM y ECM para controlar el acceso a los servicios, memorizar / gestionar / verificar los derechos de acceso a estos servicios, memorizar / gestionar / aprovechar los secretos criptográficos y aplicar a los mensajes recibidos los tratamientos y controles criptográficos de seguridad.

El terminal receptor 11 y el procesador de seguridad 13 dialogan mediante una interfaz frecuentemente de acuerdo con la norma ISO 7816.

En esta arquitectura, ciertas funciones vinculadas al control de acceso pueden tratarse por el terminal 11 en colaboración con el procesador de seguridad 13. Se trata principalmente de las funciones de selección de los mensajes ECM y EMM a tratar, de las funciones de diálogo con el usuario y de la comunicación con la parte del terminal que incluye un módulo de desaleatorización.

Este principio de arquitectura, en el que puede aplicarse la invención, se encuentra igualmente cuando se utiliza un módulo de control de acceso y de desaleatorización externo al terminal, de acuerdo por ejemplo con el módulo de interfaz común definido por la norma DVB (*"Digital Video Broadcast"*). Un módulo de ese tipo se considera naturalmente como formando parte de la descripción de la presente invención.

Contexto de la gestión DRM

Los sistemas de acción DRM actuales funcionan según los principios de arquitectura y de una cinemática resumidos en la figura 2 en la que:

- un servidor 21 asegura un formateo (o *"packaging"*) de un contenido multimedia al *"formato DRM"* y distribuye los contenidos protegidos (por ejemplo, en modo de gran difusión o *"streaming"* o de descarga individual),

- un servidor de licencias 22 permite la gestión y el control de las utilizaciones: una licencia (o RO por *"Rights Object"*) corresponde a la yuxtaposición de informaciones sobre el contenido, principalmente su identificador y eventualmente la clave criptográfica que permite desaleatorizarlo e informaciones sobre los permisos y limitaciones de uso del contenido (número de lecturas permitidas, derecho de grabación, fecha límite de utilización, duración de la utilización u otros),

- Un cliente DRM 23 sobre el terminal del cliente permite el acceso al contenido protegido y asegura el control de la licencia (incluso su renovación si es necesario) y

- Finalmente, un editor de contenido o *"player"* 24 más adelante que el cliente DRM 23 asegura la presentación o la reproducción del contenido en claro.

En la mayor parte de los sistemas de gestión DRM actuales, la licencia de utilización RO, encriptada gracias a la clave única propia del cliente DRM (muy frecuentemente obtenida según los mecanismos de infraestructura de clave pública o PKI), no es por tanto legible/válida más que para el cliente DRM 23 en cuestión. En otros términos, una licencia de utilización está estructuralmente vinculada a la *"identidad"* del terminal (en el que el cliente DRM 23 está integrado). La noción de *"identidad"* se entiende en este caso por la utilización de una clave de encriptado (secreta o privada) propia del terminal.

Un elemento importante de la licencia de utilización es el lenguaje de descripción de los derechos (o REL por *"Rights Expression Language"*), adosado a un diccionario de derechos, permite expresar las limitaciones/condiciones de los permisos particulares asociados a la utilización de un contenido.

Una presentación detallada del sistema DRM (por ejemplo OMA-DRM) está accesible en los documentos citados por el consorcio *"Open Mobile Alliance"*, tales como:

- "OMA DRM Approved Version 2.0 - 23" (marzo de 2007) o también

- "OMA DRM Specification V2.0 Draft Version 2.0 - 21" (junio de 2004).

Cálculo del código MAC

Un código MAC se calcula clásicamente a partir de una función E de cifrado por bloque de longitud L. Se trata de un cifrado por bloques y encadenado o *"CBC-MAC"* (CBC por *"Cipher Block Chaining"*). Además del mensaje M, de cualquier longitud, a proteger, esta función toma en la entrada una clave simétrica K y un vector de inicialización IV de longitud L. Los datos K y IV son compartidos por la cabeza de la red y por la parte terminal, siendo secreto el dato K y público el dato IV.

El cálculo del código MAC consiste entonces en la complementación de M en una longitud múltiplo de L, y posteriormente en la aplicación, al mensaje M' así obtenido, del cifrado en modo CBC. El código MAC del mensaje M es el último bloque cifrado así obtenido. Un algoritmo del cálculo realizado puede ser por tanto del tipo:

Temp2=IV

Para i yendo de 1 a n, hacer:

Temp1 = Temp2 XOR M'_i

Temp2 = E(K,Temp1)

Finalmente para

MAC = Temp2

en el que n es el número de bloques de longitud L.

El mensaje M' está por tanto constituido por la concatenación de estos n bloques y el código MAC obtenido es el siguiente:
MAC = E(K, M'_n XOR E(K, M'_{n-1} XOR ... E(K, M'_2 XOR E(K, M'_1 XOR IV))...)) Este procedimiento de cálculo del código MAC se representa en la figura 3, en la que se supone el mensaje M' constituido por la concatenación de n bloques (con n=4 en el ejemplo representado) de longitud L e indicados por M'_1, M'_2, M'_3 y M'_4.

Verificación del código MAC

Para asegurar la autenticidad y la integridad de un mensaje M, se verifica el código MAC recibido con este mensaje M.

Esta verificación del código MAC consiste básicamente en un nuevo cálculo de este código MAC, y posteriormente en la comparación del valor del código MAC así (re)calculado con el recibido con el mensaje M. Si estos valores son iguales, el mensaje recibido es auténtico e íntegro.

El nuevo cálculo, por una entidad receptora, del código MAC de un mensaje M, se realiza a partir del mensaje M, de la clave K y del vector de inicialización IV, según el mismo algoritmo que por la entidad emisora del mensaje M, es decir según el procedimiento ilustrado por la figura 3.

El documento US 202/071552 A1 describe un procedimiento de generación y de verificación de un código MAC de autentificación del mensaje.

Problemas planteados

El algoritmo clásico de verificación del código MAC de un mensaje, que se basa en un (re)cálculo del código MAC, provoca necesariamente la revelación, en y por la entidad receptora, del valor correcto del código MAC del mensaje considerado.
Esta revelación tiene lugar por supuesto en todos los casos, comprendidos en ellos aquellos en los que el mensaje considerado se ha recibido con un código MAC erróneo.
Esta revelación permite entonces (con la condición sin embargo de haber logrado previamente un ataque sobre el sistema que permita extraer el valor correcto del código MAC (re)calculado) plantear un mensaje de su elección con un código MAC arbitrario que tiene sin embargo la longitud L, para obtener el valor correcto del código MAC. El mensaje puede ser re-sometido a continuación, con este valor correcto del código MAC, al sistema receptor y por tanto ser tenido en cuenta por él.
Un ataque puede por ejemplo consistir en provocar perturbaciones *("glitches")* sobre el componente de manera que se recupere una imagen (o *"dump")* de la memoria volátil del sistema que contiene la memoria tampón (o *"buffer")* de cálculo del código MAC.
Un ataque de ese tipo puede realizarse en particular en cualquier contexto, principalmente en el de la televisión de pago difundida, en la que un atacante puede tener acceso a un dispositivo que realice la verificación del código MAC.

Un remedio para este inconveniente forzaría entonces a unos usuarios deshonestos (o *"piratas"*) a determinar hasta la clave y la función criptográfica de cifrado para acceder al código MAC, siendo por supuesto el coste de esta operación superior al del ataque antes citado.

Objeto de la invención

La presente invención se dirige a mejorar la situación proponiendo impedir la revelación del valor correcto del código MAC para un mensaje dado.
Propone con este fin un procedimiento, implementado mediante unos medios informáticos, de verificación de la autenticidad y/o la integridad de un mensaje transmitido, con una redundancia criptográfica, desde una entidad emisora hacia una entidad receptora.
En este procedimiento, la redundancia criptográfica es un código de autentificación de mensaje (o MAC) calculado a partir de al menos un primer cifrado, mediante una función de cifrado por bloque y con la ayuda de una clave, de una combinación de un vector de inicialización y de un primer bloque representativo de al menos una primera parte de datos del mensaje.

La clave de cifrado y el vector de inicialización tienen unos valores almacenados por las entidades emisora y receptora.
La verificación por la entidad receptora de la redundancia criptográfica que acompaña a un mensaje recibido incluye, en el sentido de la invención, las etapas:

a) aplicación a la redundancia criptográfica de al menos un primer descifrado, mediante una función de descifrado homóloga de la función de cifrado y con ayuda de la clave,

b) combinación de resultados de este primer descifrado en un primer bloque representativo de al menos una primera parte de datos del mensaje recibido,

c) comparación del resultado de la combinación de la etapa b) con el valor secreto almacenado por la entidad receptora y

d) decisión de aceptar el mensaje recibido como auténtico y/o íntegro en el caso de identidad de los valores comparados en la etapa c).

Las combinaciones antes citadas incluyen preferentemente la aplicación de la función booleana *"O exclusiva"* (o "*XOR*").

Ventajosamente, el cifrado por bloques involucra a más de un bloque y el cálculo del código de autentificación de mensaje incluye entonces al menos un segundo cifrado, por la función de cifrado y con la ayuda de la clave, de una combinación del resultado del primer cifrado y del segundo bloque representativo de una segunda parte de datos del mensaje.
Preferentemente, la etapa b) en el sentido de la invención incluye entonces además al menos las operaciones:

b1) aplicación, a la combinación entre el resultado del primer descifrado y el primer bloque, de al menos un segundo descifrado, por la función de descifrado y con ayuda de la clave y
b2) combinación del resultado de este segundo descifrado a un segundo bloque representativo de al menos una segunda parte de datos del mensaje recibido.

En el caso ventajoso de un cifrado por bloque que implique una pluralidad de bloques y en el que la función de cifrado sea de longitud de bloque L, el cálculo del código de autentificación del mensaje incluye:

- una transformación de un mensaje a enviar mediante la adición o supresión de datos para que el tamaño del mensaje transformado sea igual a nL, siendo n un entero superior o igual a 2, elegido,

- una división del mensaje transformado en n bloques sucesivos de longitud L, según una primera sucesión elegida,

- un primer cifrado de una combinación entre el vector de inicialización y un primer bloque de dicha primera sucesión y

- al menos un cifrado a continuación de la combinación entre el resultado del primer cifrado y un segundo bloque que sigue al primer bloque en la primera sucesión.

Preferentemente, las etapas a) y b) en el sentido de la invención incluyen entonces:

- una transformación de un mensaje recibido mediante la adición o supresión de datos para que el tamaño del mensaje transformado sea igual a nL,

- una división del mensaje transformado en n bloques sucesivos de longitud L, según una segunda sucesión elegida,

- una combinación entre un primer descifrado de la redundancia criptográfica recibida y un primer bloque de dicha segunda sucesión y

- al menos un descifrado a continuación de la combinación entre el resultado del primer descifrado y un segundo bloque que sigue al primer bloque en dicha segunda sucesión.

Ventajosamente, la invención implementa un cifrado el modo CBC (por *"Cipher Block Chaining"*), incluyendo entonces el cálculo del código de autentificación del mensaje:

- la aplicación al mensaje a emitir de una complementación en una longitud múltiplo de la longitud L para obtener un mensaje transformado constituido por una concatenación de n bloques cada uno de longitud L, siendo n un entero superior o igual a 2 y

- la aplicación al mensaje transformado de un cifrado por bloque en modo CBC. Preferentemente, el cálculo del vector de inicialización incluye entonces:

- una complementación del mensaje recibido en una longitud múltiplo de la longitud L para obtener un mensaje transformado constituido por una concatenación de n bloques cada uno de longitud L, siendo n un entero superior o igual a 2 y

- un descifrado por bloque, en modo CBC, del mensaje transformado.

Se señala sin embargo que el procedimiento puede aplicarse a cualquier algoritmo de verificación de código MAC por construcción invertible, de manera que verifique una propiedad sintáctica sobre el mensaje de origen (por ejemplo unos tratamientos designados por XCBC-MAC, OMAC, EMAC, u otros).

En una realización ventajosa, para el cálculo del código de autentificación de mensaje, el primer bloque de la primera sucesión antes citada es el resultado de la aplicación al mensaje de una función de sentido único.

El resultado de la aplicación de la función de sentido único se envía entonces con destino a la entidad receptora, con el mensaje, preferentemente en la forma de una concatenación:

- del resultado de la aplicación al mensaje de la función de sentido único y

- del mensaje en sí mismo.

La función de sentido único es preferentemente una función de ofuscación y el resultado de su aplicación es de longitud superior o igual a la longitud L.

Como complemento o como variante, en el caso en el que el mensaje es susceptible de ser transmitido por fragmentos, de la entidad emisora a la entidad receptora, la primera sucesión de bloques y la segunda sucesión de bloques están preferentemente invertidas, de manera que la entidad receptora pueda comenzar el cálculo del vector de inicialización a partir de la recepción de un primer fragmento del mensaje.

En el contexto del control de acceso (CAS), principalmente para unos datos televisuales, una aplicación del procedimiento se dirige a la verificación de la redundancia criptográfica que acompaña a los mensajes de control de acceso tales como principalmente los mensajes ECM y EMM.

En el contexto de la gestión de derechos digitales (DRM), principalmente de contenidos de audio y/o de vídeo, una aplicación ventajosa del procedimiento se dirige a la verificación de la redundancia criptográfica que acompaña a las licencias sobre dichos contenidos.

Descripción de las figuras

Aparecerán otras características y ventajas de la invención con el examen de la descripción detallada que sigue y de los dibujos adjuntos en los que:

- la figura 1, descrita anteriormente en el presente documento, ilustra esquemáticamente los principios de arquitectura de control de acceso CAS,

- la figura 2, descrita anteriormente en el presente documento, ilustra esquemáticamente los principios de arquitectura de la gestión DRM,

- la figura 3, descrita anteriormente en el presente documento, ilustra esquemáticamente un cálculo del código MAC, tal como se realiza en la técnica anterior también para la verificación de este código MAC,

- la figura 4 ilustra el cálculo, en el sentido de la invención, de un vector de inicialización para la retro-verificación del código MAC,

- la figura 5 ilustra el cálculo del código MAC de un mensaje prefijado por una función de sentido único que puede implementarse ventajosamente por una entidad emisora, en una realización de la invención,

- la figura 6 ilustra la retro-verificación de un código MAC calculado como se ilustra en la figura 5, con prefijación del mensaje mediante una función de sentido único, implementándose esta retro-verificación por una entidad receptora en el ejemplo representado,

- la figura 7 ilustra un cálculo invertido del código MAC que puede implementarse ventajosamente por una entidad emisora, en una realización de la invención,

- la figura 8 ilustra la retro-verificación invertida del código MAC calculado como se ilustra en la figura 7, implementándose esta retro-verificación invertida por una entidad receptora en el ejemplo representado,

- las figuras 9a y 9b comparan las implementaciones respectivas de la técnica anterior (figura 9a) y en el sentido de la invención (figura 9b).

Descripción detallada de la invención

La invención propone por tanto un perfeccionamiento para el mecanismo de verificación de mensajes, implementando este mecanismo unos códigos MAC. Permite en particular verificar el código MAC de un mensaje, sin precisamente (re)calcular el código MAC en sí mismo, para no poner en riesgo facilitar este último.
En el contexto presentado anteriormente con referencia a la figura 3, pero aplicado en el sentido de la invención, se (re)calcula no el código MAC sino el valor del vector de inicialización IV, a partir del mensaje recibido y de su valor de código MAC, así como de la clave K. Este (re)cálculo implementa en particular una función D de descifrado asociada a la función de cifrado E (figura 4).

Si el vector de inicialización IV (re)calculado es igual al utilizado por la entidad emisora para calcular el código MAC, entonces este código MAC recibido se diagnostica como correcto y por tanto el mensaje se determina como auténtico e íntegro.

Es suficiente entonces, para la implementación de la invención, que el valor correcto del vector de inicialización sea constante, de sintaxis predefinida o implícita. El atacante debe entonces elegir un valor correcto del vector de inicialización, para asociarle al valor recibido del código MAC, y posteriormente generar un mensaje sintácticamente correcto que podría ser sometido al sistema de control de acceso. Se demuestra sin embargo que la obtención, por el atacante, de un valor del vector de inicialización correcto puede hacerse tan improbable como el de generar un código MAC válido para un mensaje de su elección y que el conocimiento de los resultados intermedios que pudiera revelar el sistema de control de acceso no favorece al atacante en el objetivo de realizar esta generación del mensaje correcto.

Con referencia a la figura 4, bajo las mismas hipótesis y con las mismas notaciones que las de la figura 3, la retro-verificación del código MAC se basa en el (re)cálculo de un valor IV' del vector de inicialización, en el que MAC designa el código MAC transmitido.
De este modo, las entradas de la figura 4 son el código MAC y el mensaje M, mientras que la salida da un valor IV' del vector de inicialización a verificar, cuando las entradas de la figura 3, para el (re)cálculo y la verificación del código MAC en el sentido de la técnica anterior, eran el valor conocido IV del vector de inicialización y el mensaje M, mientras que la salida daba un valor de código MAC a verificar.
Con referencia a la figura 4, el cálculo, en el sentido de la invención, del valor IV' consiste entonces en la complementación de M en una longitud múltiplo de L, y posteriormente en la aplicación, al mensaje M así obtenido, del descifrado en modo CBC utilizando la función de descifrado D asociada a la función de cifrado E de la figura 3. El vector de inicialización es el último bloque cifrado así obtenido.

Un algoritmo correspondiente al tratamiento representado en la figura 4 en el sentido de la invención puede ser entonces del tipo:

Temp1 = MAC

Para i yendo de 0 a n-1, hacer:

Temp2 = D(K,Temp1)

Temp1 = Temp2 XOR M'_{n-i}

Finalmente para

IV' = Temp1

El valor del vector de inicialización obtenido viene entonces dado por:
IV' = M'_1 XOR d(k, M'_2 XOR ... D(K, M'_{n-1} XOR D(K, M'_n XOR D(K, MAC))) ...)

En la figura 4 se representa un ejemplo de este cálculo del vector de inicialización para retro-verificación del código MAC, el mensaje M' está por tanto constituido por la concatenación de n bloques (con n=4 en el ejemplo representado) de longitud L e indicados por M'_1, M'_2, M'_3 y M'_4.

El valor IV' obtenido es el que debiera utilizar la entidad receptora para calcular el MAC del mensaje recibido de manera que se obtenga el mismo valor que el transmitido por el emisor.
La retro-verificación del código MAC consiste a continuación en la comparación del valor IV' del vector de inicialización encontrado, con el valor IV compartido del valor de inicialización que, en principio, se ha utilizado por la entidad emisora para calcular el valor del código MAC transmitido con el mensaje recibido. Si estos valores son iguales, el mensaje recibido es auténtico e íntegro.

No obstante la comparación de las entradas y salidas de las figuras 3 y 4 dadas anteriormente, conviene indicar que la entidad emisora conserva un esquema similar al de la figura 3 para construir el código MAC. No obstante, se presentan en el presente documento a continuación unas mejoras de este esquema.

Se llama a continuación la operación *"retro-verificación del código MAC"*, en el sentido de la invención, que consiste en verificar el valor IV' del vector de inicialización. Esta verificación conducida por la entidad receptora es idéntica a la presentada en la figura 4. Consiste en (re)calcular el valor IV' del vector de inicialización en función del mensaje recibido y de su código MAC y en compararle con el valor esperado IV del vector de inicialización.

Una debilidad residual que presentaría *a priori* el tratamiento en el sentido de la invención es la revelación en el sistema de control de acceso de los valores correcto IV y (re)calculado IV' del vector de inicialización y por tanto su extracción posible por un atacante del sistema. De este modo:

- presentando al sistema un mensaje M de su elección con un código MAC arbitrario,
- extrayendo estos valores,
- y posteriormente sustituyendo el primer bloque M_1 de su mensaje por la magnitud: N = M_1 XOR IV' XOR IV, el atacante obtiene un mensaje [N M_2 ... M_n] que puede ser sometido con éxito al sistema con el código MAC arbitrario elegido, es decir en el que el (re)cálculo del vector de inicialización da el resultado IV esperado.
  La retro-verificación del código MAC sería entonces positiva y el mensaje recibido tenido entonces en cuenta.

Sin embargo, el resultado IV' del cálculo anterior al no estar *a priori* controlado por el atacante, el de la magnitud N no lo es inicialmente, de manera que es altamente improbable que la sintaxis del nuevo mensaje [N M_2... M_n] sea la de un mensaje válido.
El hecho de que los resultados de los cálculos del valor IV' y de la magnitud N no estén controlados, significa además que no se sabe modificar el código MAC arbitrario a la vista de los primeros resultados erróneos anteriores, para obtener un nuevo mensaje [N M_2... M_n] de sintaxis válida.

En cualquier caso, en una realización ventajosa, se ofrece la posibilidad de protegerse, como base, contra la debilidad residual descrita anteriormente.
Se prevé con este fin fijar el mensaje a enviar por la entidad emisora con el resultado de su propio tratamiento mediante una función de sentido único, tal como una función de ofuscación (o función criptográfica de sentido único).
Este prefijado puede ser:

- *"implícito"*: el prefijo no se tiene en cuenta más que para el cálculo del código MAC y su verificación a través del cálculo del valor IV' (llamada a continuación *"retro-verificación"*) ante la entidad receptora, pero no transmitido con el mensaje,
- o *"explícito"*: el prefijo se transmite entonces además con el mensaje y el código MAC.

La utilización de una función H de sentido único consiste en calcular:

- la magnitud H(M) || M, en la que " || " designa el operador de concatenación;

- el código MAC del mensaje concatenado así obtenido.

El mensaje M' = (M'_1, M'_2,..., M'_n) se obtiene por complementación (o *"padding"*) de la magnitud H(M) || M.
El cálculo del código MAC en sí mismo se realiza entonces a continuación de manera similar a la ilustrada en la figura 3.
Conviene señalar que la seguridad del tratamiento es reducida si la longitud de la expresión H(M) es inferior a la longitud L. Se elegirá ventajosamente una función de sentido único H para que la expresión H(M) sea de longitud superior o igual a la longitud L.

Se tiene en particular $M'_1 = H(M)$ en el caso en que la expresión H(M) es de longitud L. En este caso ventajoso, las longitudes del bloque pueden permanecer inalteradas y no tienen que ser modificadas añadiendo o suprimiendo datos. El cálculo del código MAC realizado es entonces del tipo:

Temp2 = E(K, IV XOR H(M))

Para i yendo de 2 a n, hacer:

Temp1 = Temp2 XOR M'_i

Temp2 = E(K,Temp1)

Finalmente para

MAC = Temp2

en la que n es el número de bloques de longitud L. El mensaje M' está constituido por la concatenación de estos bloques y el código MAC obtenido viene dado por:
$MAC = E(K, M'_n \text{ XOR } E(K, M'_{n-1} \text{ XOR } ... E(K, M'_2 \text{ XOR } E(K, M'_2 \text{ XOR } E(K, IV \text{ XOR } H(M))))...))$

Este cálculo del código MAC se ilustra en la figura 5, en la que se supone el mensaje M' constituido por la concatenación de n bloques (con n=5 en el ejemplo representado) de longitud L e indicados por $H(M)=M'_1$, M'_2, M'_3, M'_4 y M'_5.
La entidad emisora transmite a continuación:

- el valor del vector de inicialización IV, si es necesario el mensaje M en el modo de realización *"implícito"* antes citado y el código MAC así calculado;

- el valor del vector de inicialización IV, si es necesario la concatenación H(M) || M en el modo de realización *"explícito"* antes citado y el código MAC así calculado.

Por supuesto, los casos en los que la expresión H(M) es de longitud múltiplo de la longitud L son también ventajosos. En los otros casos, es útil un *"padding"* complementario.

Ante la entidad receptora, a continuación, la retro-verificación del código MAC dirigido a la verificación del valor IV' del vector de inicialización, sigue el mismo principio que el ilustrado en la figura 4. Consiste en recalcular el valor IV' del vector de inicialización en función del mensaje recibido y de su código MAC y en compararle con el valor esperado IV del vector de inicialización.
Un ejemplo de algoritmo de retro-verificación es entonces el siguiente:

Temp1 = MAC

Para i yendo de 0 a n-1, hacer:

Temp2 = D(K,Temp1)

Temp1 = Temp2 XOR M'_{n-i}

Finalmente para

IV' = H(M) XOR D(K, Temp1)

El valor del vector de inicialización obtenido es por tanto:
$IV' = H(M) \text{ XOR } D(K, M'_1 \text{ XOR } D(k, M'_2 \text{ XOR } ... D(K, M'_{n-1} \text{ XOR } D(K, M'_n \text{ XOR } D(K, MAC))) ...))$

Este cálculo del vector de inicialización para retro-verificación del código MAC se representa en la figura 6, en la que se supone el mensaje M' constituido por la concatenación de n bloques (n=4 en el ejemplo representado) de longitud L e indicados por M'_1, M'_2, M'_3 y M'_4.
En el presente documento, esta verificación se completa además por la verificación del resultado del tratamiento del mensaje por la función de sentido único H. Esta verificación se realiza de manera análoga a la conocida en la técnica anterior de un código MAC, por (re)cálculo de este resultado y comparación con el valor recibido. Si los dos valores son iguales, el mensaje es íntegro.
Esta segunda verificación impediría entonces a un atacante modificar el inicio del mensaje M como se ha expuesto anteriormente, quedando así superada la debilidad residual antes citada. En efecto, la modificación del inicio del mensaje M, incluso aunque en sí misma fuera correcta, implicaría otra modificación, no controlada por su parte, de la magnitud H(M).

Se describe a continuación una realización ventajosa en un contexto (frecuente en el control de acceso CAS o en la gestión de DRM) en el que un mensaje puede, por diferentes razones, ser transmitido en trozos.
Es entonces oportuno poder realizar la (retro-)verificación del código MAC del mensaje, a medida de su recepción y teniendo necesidad de no memorizar finalmente más que un resultado intermedio en lugar del conjunto de los trozos del mensaje ya recibidos.
Para tal fin, el código MAC del mensaje debe poder trasmitirse con su primer bloque, de manera que su (retro-)verificación pueda comenzar desde la recepción de este primer bloque. Se transmite así, típicamente, el código MAC seguido del mensaje, y posteriormente del vector de inicialización. Para una implementación ventajosa de la invención, es suficiente entonces invertir el orden de los bloques del mensaje antes de calcular el código MAC, para poder comenzar su (retro-)verificación a continuación simplemente partir del primer bloque.

El cálculo del código MAC a realizar está así invertido:

Temp2=IV

Para i yendo de 0 a n-1, hacer:

Temp1 = Temp2 XOR M'_{n-i}

Temp2 = E(K,Temp1)

Finalmente para

MAC = Temp2

en la que n es el número de bloques de longitud L. El mensaje M' está constituido por la concatenación de estos n bloques $M' = [M'_1 M'_2 ... M'_n]$ y el código MAC obtenido viene dado, en este caso, por:
$MAC = E(K, M'_1 \text{ XOR } E(K, M'_2 \text{ XOR } ... E(K, M'_{n-1} \text{ XOR } E(K, M'_n \text{ XOR } IV))...))$

mientras que habitualmente, viene dado por:
$MAC = E(K, M'_n \text{ XOR } E(K, M'_{n-1}, \text{XOR} ... E(K, M'_2 \text{ XOR } E(K, M'_1 \text{ XOR } IV))...))$

Este cálculo del código MAC se ilustra en la figura 7, en la que se supone el mensaje M' constituido por la concatenación de n bloques (n=4 en el ejemplo representado) de longitud L e indicados por M'_1, M'_2, M'_3 y M'_4.

La retro-verificación a realizar de un código MAC que ha sido calculado en el modo invertido descrito anteriormente puede seguir por ejemplo el algoritmo siguiente:

Temp1 = MAC

Para i yendo de 1 a n, hacer:

Temp2 = D(K,Temp1)
Temp1 = Temp2 XOR M'_i

Finalmente para

IV' = Temp1

El valor del vector de inicialización obtenido viene entonces dado por:
$IV' = M'_n \text{ XOR } D(K, M'_{n-1} \text{ XOR } ... D(K, M'_2 \text{ XOR } D(K, M'_1 \text{ XOR } D(K, MAC))) ...)$

Este cálculo del vector de inicialización para la retro-verificación invertido del código MAC se representa en la figura 8, en la que se supone el mensaje M' constituido por la concatenación de n bloques (n=4 en el ejemplo representado) de longitud L e indicados por M'_1, M'_2, M'_3 y M'_4.

Es posible combinar el modo de realización que se dirige a la utilización de una función de sentido único con el modo de realización que se dirige a la inversión del orden de los bloques.
La posición del resultado H(M) de la función de sentido único H puede transmitirse a una posición elegida cualquiera: como prefijo o también como sufijo, en el medio de los bloques, etc. Las posiciones como prefijo y sufijo son sin embargo preferidas.
En el caso *"explícito"* en el que el valor H(M) se transmite y verifica, con el fin de permitir el cálculo sobre la marcha de la recepción de los fragmentos de mensaje por la entidad receptora, el valor H(M) se transmite por la entidad emisora preferentemente al final (por tanto como prefijo como se representa en la figura 5) para ser tenido en cuenta por la entidad receptora justo antes de la operación de verificación relativa al código MAC recibido (es decir justo antes del cálculo que da el valor supuesto del vector de inicialización como se representa en la figura 6). En el caso *"implícito"*

en el que el valor H(M) se calcula por la entidad receptora, la posición del resultado H(M) se elige independientemente del hecho de que el orden de estos bloques esté invertido.

Por otra parte, se recomienda, para la implementación de la invención, algunas de las precauciones que siguen. Con referencia a la figura 3, cuando el código MAC era calculado por la entidad receptora como en el sentido de la técnica anterior, solo se utilizaba la función de cifrado E, mientras que en la verificación del vector de inicialización por la entidad receptora en el sentido de la invención (figura 4), se utiliza la función de descifrado D. Requiriendo la retro-verificación del código MAC el descifrado del código MAC transmitido, y posteriormente de los bloques sucesivos módulo un resultado por el operador XOR de cada etapa, es necesario entonces proteger al sistema contra un ataque que utilizara un módulo de cálculo de retro-verificación del código MAC como oráculo del descifrado, es decir la función de descifrado D para poder acceder a informaciones confidenciales que se habrían cifrado principalmente con la función E.

Un ataque de ese tipo consistiría en someter, al módulo de retro-verificación del código MAC, a un mensaje vacío, así como al criptograma de datos confidenciales, en lugar del código MAC, para poder extraer del sistema de verificación estos datos confidenciales en claro.
En el contexto de aplicación ventajosa de la difusión de contenidos multimedia protegidos mediante el sistema de CAS, estos datos confidenciales pueden ser típicamente la palabra de control de descifrado del contenido CW de la figura 1. En los contextos en los que la protección de los contenidos se realiza mediante el sistema de DRM (figura 2), estos datos confidenciales pueden ser típicamente la clave de descifrado del contenido.

Ventajosamente, se prevé, en este sentido, hacerlo de manera que las operaciones de descifrado implementadas para la retro-verificación del código MAC y para la supresión de la confidencialidad de las informaciones transportadas por el mensaje, sean diferentes.
Se podrá, con este fin y por orden de preferencia decreciente:

- compartimentar los algoritmos y las claves utilizadas para el tratamiento del código MAC, por un lado y para el de la confidencialidad, por otra parte, imponiendo dos algoritmos diferentes;

- utilizar la función criptográfica en modo de descifrado para el cálculo del código MAC y por tanto el modo de cifrado para la retro-verificación del código MAC, así como para el cálculo de la confidencialidad;

- o compartimentar los algoritmos y las claves utilizadas para el tratamiento del código MAC, por un lado y para el de la confidencialidad, por otra parte, imponiendo unas claves dedicadas diferentes.

De este modo, en términos más genéricos, en el caso en el que el mensaje a transmitir incluye unos datos confidenciales cifrados, la clave de descifrado K y/o la función de descifrado D utilizadas para la verificación de la redundancia criptográfica forman de ese modo unos medios preferentemente diferentes de los medios de descifrado de los datos confidenciales.

Las figuras 9a y 9b sintetizan muy esquemáticamente las diferencias de tratamiento entre los procedimientos en el sentido de la técnica anterior (figura 9a) y el procedimiento en el sentido de la invención (figura 9b).
En estas dos figuras 9a y 9b, las entidades emisoras (referenciadas respectivamente 91 y 95) juegan el mismo papel, a saber calcular, con la ayuda de medios tales como un procesador de cálculo PROC y de una memoria de trabajo (no representada), el código MAC a partir:

- del mensaje M a enviar,

- del vector de inicialización IV,

- y aplicando la clave K y la función E de cifrado.

Se mantendrá sin embargo en el espíritu que la entidad emisora 95 (figura 9b), en un modo de realización preferido de la invención, aplica una función de sentido único al mensaje M como se ha descrito anteriormente. A este respecto, la presente invención se dirige también a una entidad emisora 95 de ese tipo de mensajes M enviados cada uno con una redundancia criptográfica y que incluyen unos medios de cálculo PROC de un código de autentificación del mensaje que acompaña cada mensaje a enviar, de acuerdo con este modo de realización. La presente invención se dirige también a un programa informático, destinado a estar almacenado en memoria de la entidad emisora 95 y que incluye unas instrucciones para la implementación de este modo de realización, cuando se ejecutan por el procesador PROC de la entidad emisora 95. Se han dado anteriormente ejemplos de algoritmos de un programa de ese tipo.

Con referencia de nuevo a las figuras 9a y 9b, el mensaje M y el código MAC se envían a continuación con destino a una entidad receptora, por ejemplo *vía* una red 90. En los procedimientos de la técnica anterior (figura 9a), la entidad receptora 92 recalcula un código MAC', a partir del mensaje M recibido, del vector de inicialización IV y aplicando la clave K y la función E de cifrado. A continuación, la entidad receptora 92 compara el código MAC' así calculado con el código MAC recibido y decide que el mensaje recibido M es válido en caso de identidad entre los códigos comparados.

En un planteamiento diferente en el sentido de la invención, la entidad receptora 96 (figura 9b) calcula, con la ayuda de medios tales como un procesador de cálculo PROC y de una memoria de trabajo (no representada), un valor del vector de inicialización IV', a partir del mensaje M y del código MAC recibidos y aplicando la clave K y la función D de descifrado. A continuación, la entidad receptora 96 compara el valor IV' así calculado con un valor de referencia IV almacenado en memoria. La entidad receptora 96 decide entonces que el mensaje recibido M es válido en caso de identidad entre los valores comparados.
A este respecto, la presente invención se dirige también a una entidad receptora 96 (figura 9b) de mensajes recibidos cada uno con una redundancia criptográfica MAC y que incluye entonces unos medios, tales como el procesador PROC, de verificación de la redundancia criptográfica que acompaña un mensaje recibido M.

En una aplicación ventajosa de la invención en un sistema de control de acceso (CAS), la entidad receptora puede ser por ejemplo un desaleatorizador que recibe unos mensajes, por ejemplo del tipo EMM o ECM, con una redundancia criptográfica tal como código MAC. En este caso, el procesador de seguridad 13 (figura 1) de un sistema de ese tipo incluye unos medios (un procesador, una memoria de trabajo u otros) para la verificación de la redundancia criptográfica que acompaña a un mensaje recibido, de acuerdo con el procedimiento en el sentido de la invención. A este respecto, la presente invención se dirige también a un procesador de seguridad de ese tipo.

La presente invención se dirige también a un programa informático, destinado a estar almacenado en memoria de la entidad receptora 96 de la figura 9b o de un procesador de seguridad en el sentido de la invención y que incluye entonces instrucciones para la implementación del procedimiento en el sentido de la invención cuando se ejecutan por un procesador PROC de la entidad receptora o del procesador de seguridad. Se han dado anteriormente ejemplos de algoritmos de un programa de ese tipo.

REIVINDICACIONES

1. Procedimiento, implementado mediante unos medios informáticos, de verificación de la autenticidad y/o de la integridad de un mensaje (EMM, ECM; RO) transmitido, con una redundancia criptográfica (MAC), de una entidad emisora (10; 22) hacia una entidad receptora (11; 23),
procedimiento en el que la redundancia criptográfica es un código de autentificación de mensaje (MAC) calculado a partir de al menos un primer cifrado, mediante una función de cifrado (E) por bloque y con la ayuda de una clave (K), de una combinación (XOR) de un vector de inicialización (IV) y de un primer bloque (M'_1) representativo de al menos una primera parte de datos del mensaje,
la clave de cifrado (K) y el vector de inicialización (IV) tienen unos valores almacenados por las entidades emisora y receptora,
caracterizado por que la verificación por la entidad receptora de la redundancia criptográfica que acompaña a un mensaje recibido incluye las etapas:

a) aplicación a la redundancia criptográfica (MAC) de al menos un primer descifrado, mediante una función de descifrado (D) homóloga de la función de cifrado (E) y con ayuda de la clave (K),
b) combinación (XOR) de resultados de este primer descifrado en un primer bloque (M'_n) representativo de al menos una primera parte de datos del mensaje recibido,
c) comparación del resultado de la combinación de la etapa b) con el valor del vector de inicialización almacenado por la entidad receptora y
d) decisión de aceptar el mensaje recibido como auténtico y/o íntegro en el caso de identidad de los valores comparados en la etapa c).

2. Procedimiento según la reivindicación 1, en el que el cálculo del código de autentificación de mensaje (MAC) incluye al menos un segundo cifrado, por la función de cifrado (E) y con la ayuda de la clave (K), de una combinación (XOR) del resultado del primer cifrado y de un segundo bloque (M'_2) representativo de una segunda parte de datos del mensaje,
caracterizado por que la etapa b) incluye además al menos las operaciones:

b1) aplicación, a la combinación entre el resultado del primer descifrado y el primer bloque (M'_n), de al menos un segundo descifrado, por la función de descifrado (D) y con ayuda de la clave (K) y
b2) combinación (XOR) del resultado de este segundo descifrado a un segundo bloque (M'_{n-1}) representativo de al menos una segunda parte de datos del mensaje recibido.

3. Procedimiento según la reivindicación 2, en el que la función de cifrado (E) es de longitud de bloque L y el cálculo del código de autentificación de mensaje (MAC) incluye:

- una transformación de un mensaje (M) a enviar mediante la adición o supresión de datos para que el tamaño del mensaje transformado (M') sea igual a nL, siendo n un entero superior o igual a 2, elegido,
- una división del mensaje transformado (M') en n bloques sucesivos de longitud L, según una primera sucesión elegida,
- un primer cifrado de una combinación (XOR) entre el vector de inicialización (IV) y un primer bloque (M'_1; M'_4) de dicha primera sucesión y
- al menos un cifrado siguiendo la combinación (XOR) entre el resultado del primer cifrado y un segundo bloque (M'_2; M'_3) que sigue al primer bloque en la primera sucesión,

caracterizado por que las etapas a) y b) incluyen:

- una transformación de un mensaje recibido (M) mediante la adición o supresión de datos para que el tamaño del mensaje transformado (M') sea igual a nL,
- una división del mensaje transformado (M') en n bloques sucesivos de longitud L, según una segunda sucesión elegida,
- una combinación (XOR) entre un primer descifrado de la redundancia criptográfica recibida (MAC) y un primer bloque (M'_1) de dicha segunda sucesión y
- al menos un descifrado a continuación de la combinación (XOR) entre el resultado del primer descifrado y un segundo bloque (M'_2) que sigue al primer bloque (M'_1) en dicha segunda sucesión.

4. Procedimiento según la reivindicación 3, en el que el cálculo del código de autentificación de mensaje (MAC) incluye:

- la aplicación al mensaje a emitir (M) de una complementación en una longitud múltiplo de la longitud L para obtener un mensaje transformado (M') constituido por una concatenación de n bloques (M'_1, M'_2, M'_3, M'_4) cada uno de longitud L, siendo n un entero superior o igual a 2 y
- la aplicación al mensaje transformado (M') de un cifrado por bloque en modo CBC,

caracterizado por que el cálculo del vector de inicialización incluye:

- una complementación del mensaje recibido (M) en una longitud múltiplo de la longitud L para obtener un mensaje transformado (M') constituido por una concatenación de n bloques (M'_1, M'_2, M'_3, M'_4) cada uno de longitud L, siendo n un entero superior o igual a 2 y
- un descifrado por bloque, en modo CBC, del mensaje transformado (M').

5. Procedimiento según una de las reivindicaciones 3 y 4, **caracterizado por que**, para el cálculo del código de autentificación de mensaje (MAC), dicho primer bloque (H(M)), en la primera sucesión, es el resultado de la aplicación al mensaje (M) de una función de sentido único.

6. Procedimiento según la reivindicación 5, **caracterizado por que** el resultado de la aplicación de la función de sentido único se envía con destino a la entidad receptora, con el mensaje (M), en la forma de una concatenación (H(M)||M):

- del resultado de la aplicación al mensaje (M) de la función de sentido único y
- de dicho mensaje (M).

7. Procedimiento según una de las reivindicaciones 5 y 6, **caracterizado por que** la función de sentido único es una función de ofuscación y el resultado de su aplicación (H(M)) es de longitud superior o igual a la longitud L.

8. Procedimiento según una de las reivindicaciones 3 a 7, en el que el mensaje es susceptible de ser transmitido por fragmentos, de la entidad emisora a la entidad receptora,
caracterizado por que la primera sucesión de bloques (M'_4, M'_3, M'_2, M'_1) y la segunda sucesión de bloques (M'_1, M'_2, M'_3, M'_4) están invertidas y **por que** la entidad receptora comienza el cálculo del vector de inicialización a partir de la recepción de un primer fragmento del mensaje.

9. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** dichas combinaciones incluyen la aplicación de la función booleana "O *exclusiva* (XOR).

10. Procedimiento según una de las reivindicaciones anteriores, en el que el mensaje a transmitir incluye unos datos confidenciales (CW) cifrados, **caracterizado por que** la clave de descifrado (K) y/o la función de descifrado (D) utilizadas para la verificación de la redundancia criptográfica forman unos medios diferentes de los medios de descifrado de los datos confidenciales (CW).

11. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se aplica, en el contexto del control de acceso (CAS), principalmente para unos datos televisuales, en la verificación de la redundancia criptográfica que acompaña a los mensajes de control de acceso (ECM, EMM).

12. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado por que** se aplica, en el contexto de la gestión de derechos digitales (DRM), principalmente de contenidos de audio y/o de vídeo, en la verificación de la redundancia criptográfica que acompaña a las licencias sobre dichos contenidos (RO).

13. Entidad receptora de mensajes (EMM, ECM; RO) recibidos cada uno con una redundancia criptográfica (MAC), **caracterizada por que** incluye unos medios de verificación de la redundancia criptográfica que acompaña a un mensaje recibido, de acuerdo con el procedimiento según una de las reivindicaciones anteriores.

14. Procesador de seguridad en una entidad receptora de un sistema de control de acceso (CAS), recibiendo la entidad receptora unos mensajes (EMM, ECM) con una redundancia criptográfica (MAC), **caracterizado por que** el procesador de seguridad (13) incluye unos medios de verificación de la redundancia criptográfica que acompaña a un mensaje recibido, de acuerdo con el procedimiento según la reivindicación 11.

15. Programa informático, destinado a estar almacenado en la memoria de una entidad receptora según la reivindicación 13 o de un procesador de seguridad según la reivindicación 14, **caracterizado por que** incluye instrucciones para la implementación del procedimiento según una de las reivindicaciones 1 a 12 cuando se ejecutan por un procesador de dicha entidad receptora o dicho procesador de seguridad (13).

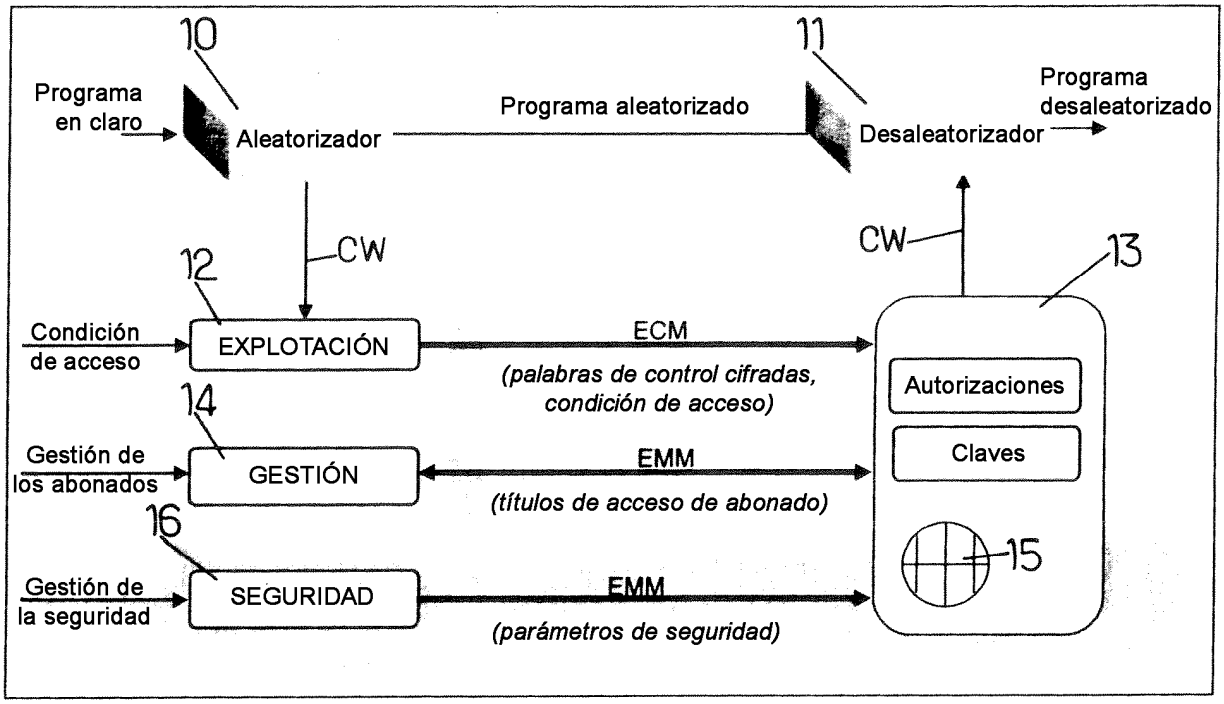
10
11
Programa en claro
Aleatorizador
Programa aleatorizado
Desaleatorizador
Programa desaleatorizado
CW
CW
12
13
Condición de acceso
EXPLOTACIÓN
ECM
(palabras de control cifradas, condición de acceso)
Autorizaciones
Claves
14
Gestión de los abonados
GESTIÓN
EMM
(títulos de acceso de abonado)
16
15
Gestión de la seguridad
SEGURIDAD
EMM
(parámetros de seguridad)

FIG.1.

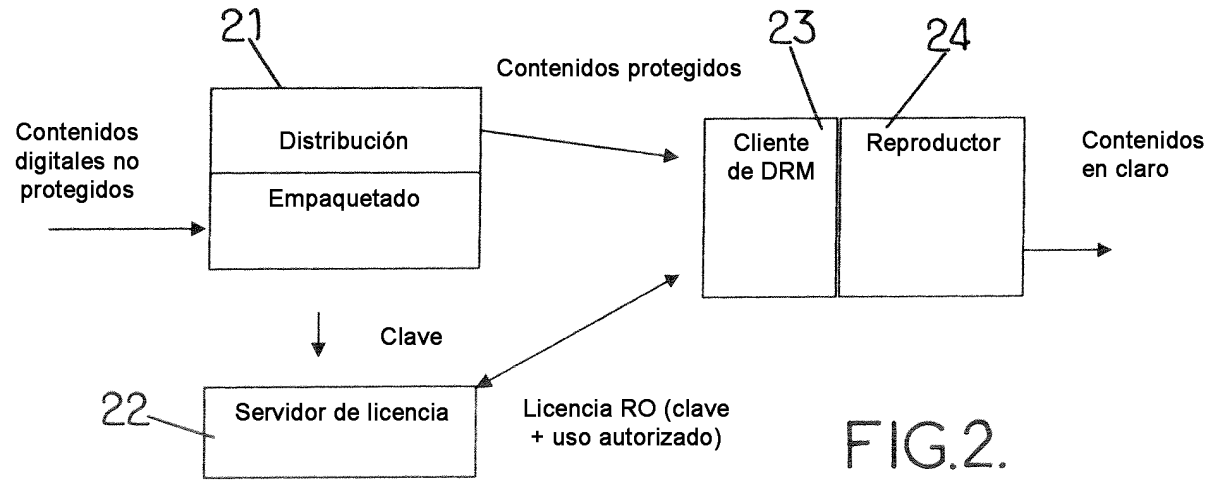
21
Contenidos protegidos
23
24
Contenidos digitales no protegidos
Distribución
Empaquetado
Cliente de DRM
Reproductor
Contenidos en claro
Clave
22
Servidor de licencia
Licencia RO (clave + uso autorizado)

FIG.2.

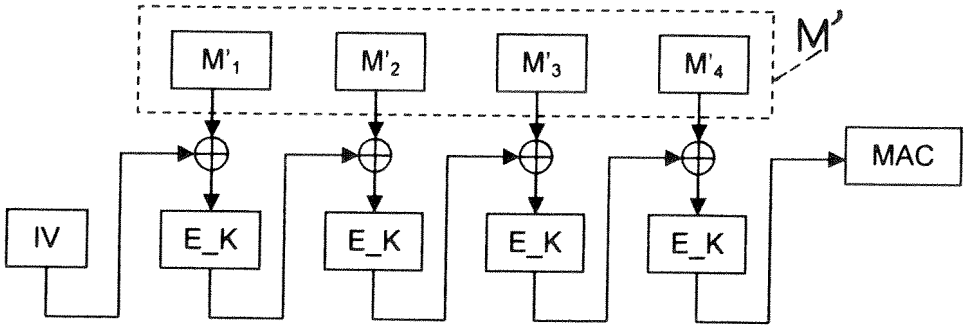

FIG.3.

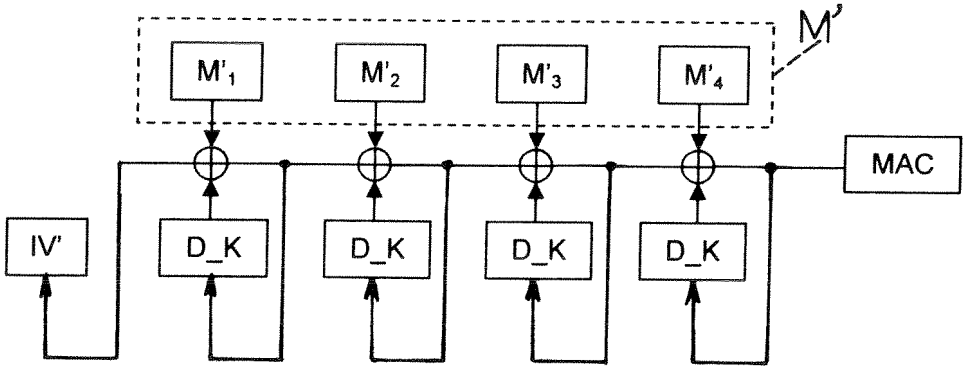

FIG.4.

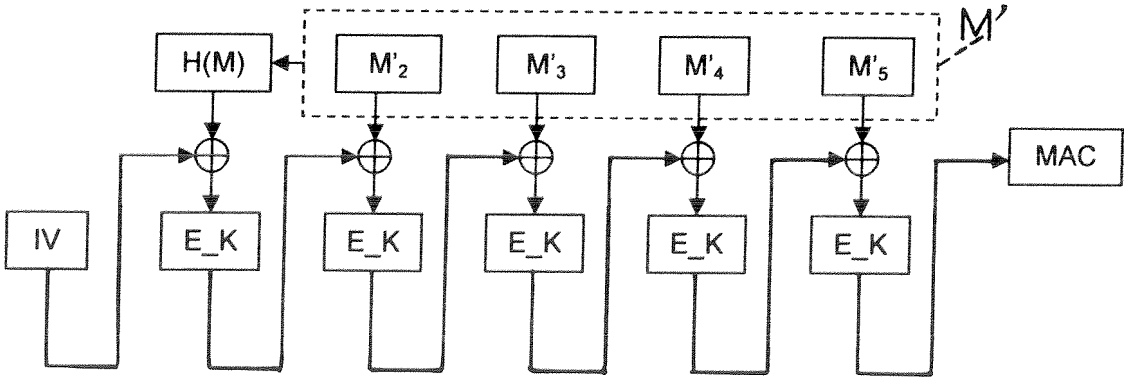

FIG.5.

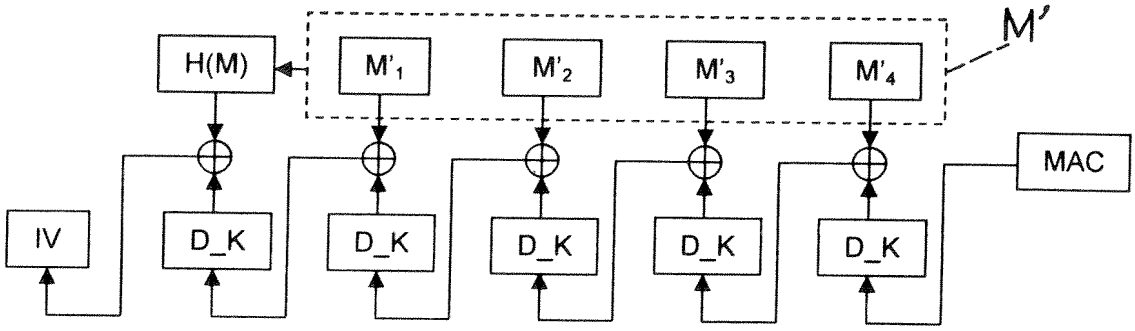

FIG.6.

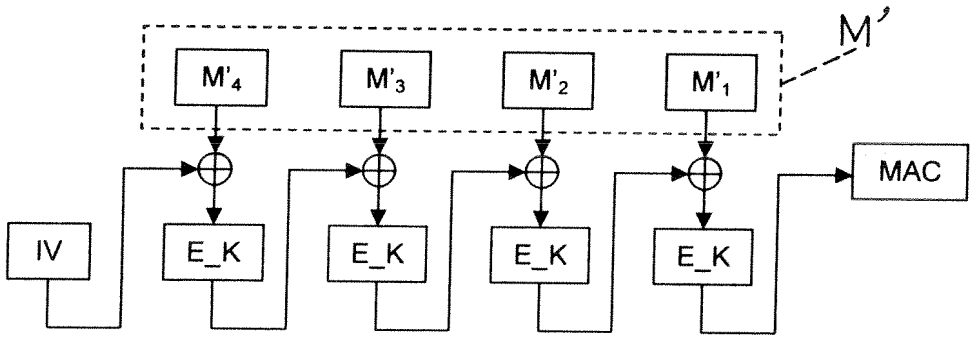

FIG.7.

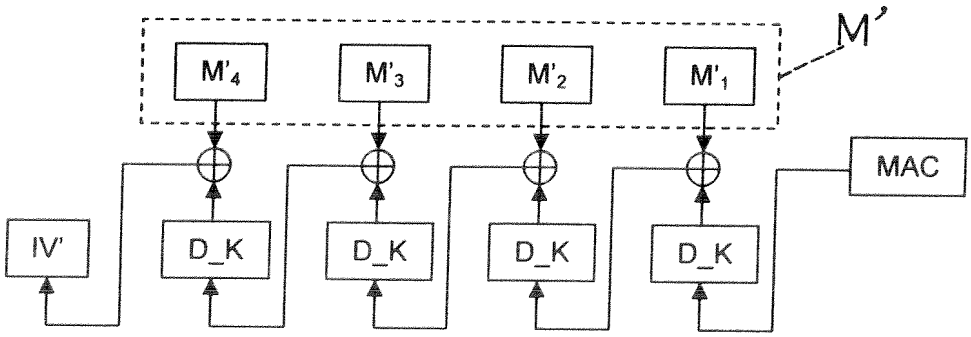

FIG.8.

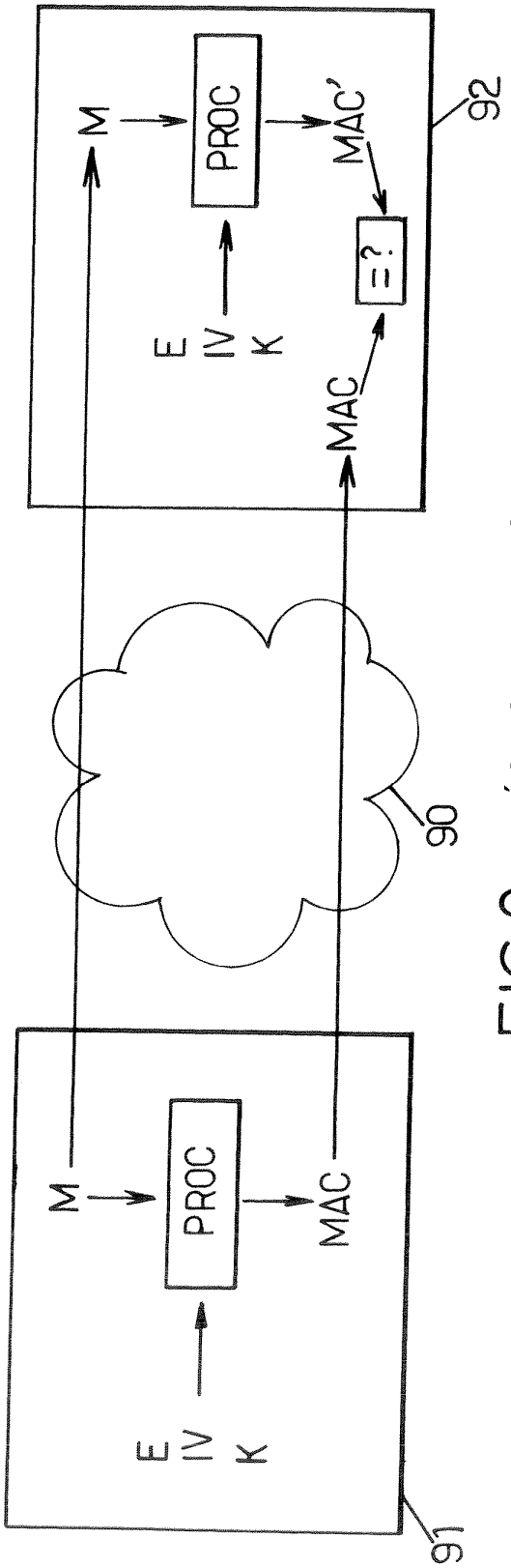

FIG.9a. (TÉCNICA ANTERIOR)

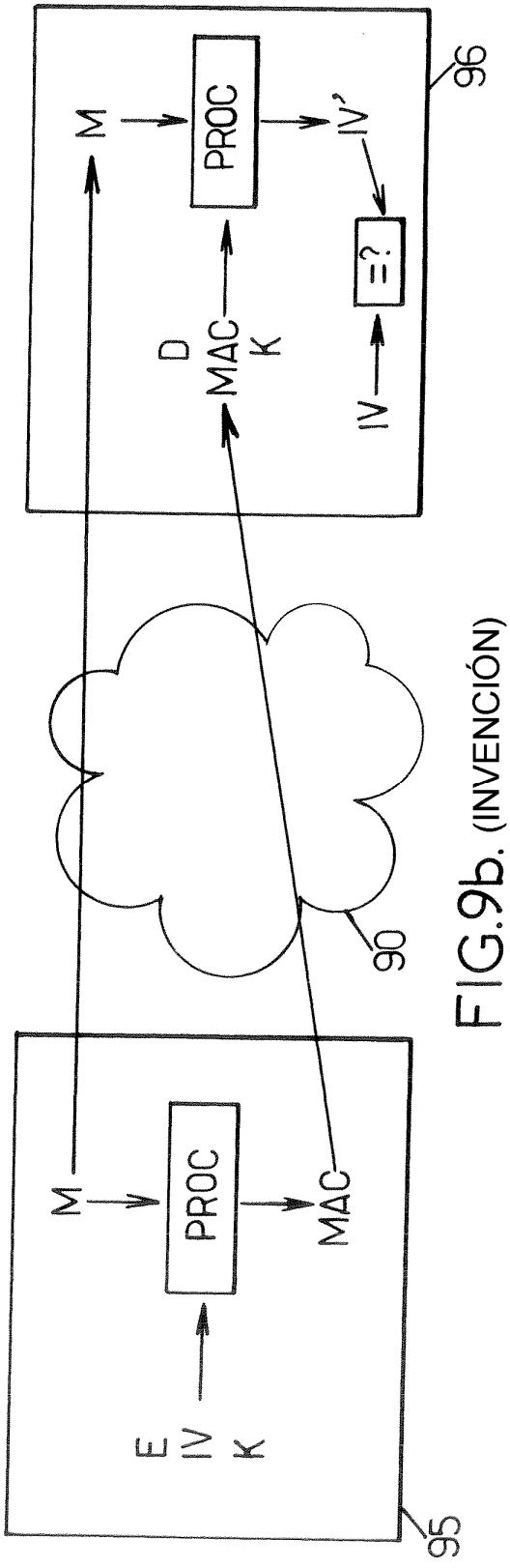

FIG.9b. (INVENCIÓN)