(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 444 915**

(51) Int. CI.:

H04N 7/16 (2011.01)
H04N 21/258 (2011.01)
H04N 21/418 (2011.01)
H04N 21/442 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/6543 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.10.2002 E 02796829 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2013 EP 1438855**

(54) Título: **Método para verificar receptores de televisión con control de acceso y receptor correspondiente**

(30) Prioridad:

26.10.2001 FR 0113878

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.02.2014

(73) Titular/es:

NAGRA FRANCE SAS (100.0%)
28, rue du Colonel Pierre Avia
75015 PARIS, FR

(72) Inventor/es:

DAUVOIS, JEAN-LUC

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para verificar receptores de televisión con control de acceso y receptor correspondiente

Campo Técnico

[0001] La presente invención se refiere a un método para verificar receptores de televisión con control de acceso y un receptor que es capaz de ser verificado utilizando este método.

Estado de la técnica

[0002] En televisión con control de acceso, los datos para ser transmitidos se codifican primero utilizando un algoritmo de cifrado y los datos codificados luego se difunden en conjunto con mensajes de control de acceso. Los receptores de los abonados que se han abonado al abono apropiado, se cargan con información que constituye un derecho de acceso que les permite encontrar en los mensajes de control de acceso, la clave requerida para descodificar los datos transmitidos.

[0003] Como un ejemplo, el documento FR-A-2 448 625 describe un sistema que utiliza claves de abono Ci, que cambian aleatoriamente en intervalos relativamente largos en el rango de un mes, y una clave de servicio K, que también cambia aleatoriamente pero en cortos intervalos en el rango de unos cuantos minutos. Los datos se descodifican utilizando la clave de servicio K. Los mensajes de control de acceso Mi se obtienen de las claves de abono Ci y la clave de servicio K, utilizando un algoritmo que se define por las claves de abono Ci. En el equipo receptor de un abonado, la tarjeta chip o microcircuito ahí contenida se ha cargado con claves que corresponden a abonos a los cuales se ha abonado el abonado. El terminal asociado con la tarjeta contiene un circuito para obtener la clave de servicio K, que recibe los mensajes Mi y que tiene disponible la clave de abono Ci contenida en la tarjeta. Medios de descodificación luego recuperan los datos en la forma descodificada.

,

[0004] Aunque se proporciona satisfacción en muchos aspectos, esta tecnología tiene la inconveniencia de estar sujeta a fraude. Sin duda, un receptor puede ser modificado por una persona con destreza, culpable de fraude, que sea capaz de recibir un programa aunque el abonado no haya pagado el abono correspondiente. Para evitar este fraude (o reducirlo), se requeriría efectuar periódicamente verificaciones en el sitio del abonado, a fin de controlar la integridad de su receptor. Esto es difícilmente concebible por razones comerciales obvias.

[0005] La presente invención por lo tanto se dirige a resolver este problema.

[0006] En la publicación de la solicitud de patente internacional 01/111820 A1, se divulga un método para garantizar la integridad y autenticidad de los datos transmitidos entre un centro de gestión y una o varias unidades receptoras. Según este documento, el método consiste en calcular una información de control (Hx) representativa del resultado de una función llamada unidireccional y sin colisión, efectuada sobre todos o parte de los datos transmitidos y en transmitir el resultado al centro de gestión para su comprobación. Este método tiene una desventaja en el sentido de que el resultado, depende sólo del contenido de los datos, será el mismo para todo receptor que se someta a un control con base en los mismos datos. Esto abre la posibilidad de colaborar entre receptores para obtener un buen resultado, al mismo tiempo que permite al receptor llamado malintencionado dejar creer al centro de gestión que sus datos son íntegros y auténticos incluso cuando éste no es el caso.

Exposición de la invención

[0007] De acuerdo con la invención, la verificación de un receptor se ordena por el organismo difusor y se realiza por el propio receptor. Si la verificación revela que el receptor ha mantenido su integridad, entonces continua funcionando normalmente. En el caso opuesto, el funcionamiento se altera, en una forma u otra, por ejemplo por parada parcial o total.

[0008] De acuerdo con la invención, esto se logra como sigue:

A) - el difusor realiza cálculos definidos por uno o varios parámetros determinados;
- el difusor luego transmite a cada receptor los resultados de los cálculos que le conciernen, cada receptor almacena los diversos resultados;

B) - A fin de verificar un receptor específico, el difusor transmite a este receptor uno o varios parámetros determinados;
- el receptor luego realiza el cálculo y compara el resultado que obtiene con el resultado correspondiente que ha almacenado; en caso de diferencia, altera su funcionamiento en una forma apropiada, por ejemplo dejando de funcionar.

[0009] Cuando el receptor comprende un terminal y una tarjeta de chip, es de preferencia la tarjeta de chip la que almacena los resultados de los cálculos transmitidos por el difusor y el terminal realiza los cálculos pertinentes.

[0010] En una primera alternativa, el terminal transmite los resultados de su cálculo a la tarjeta; esta última compara este resultado con aquel que almacena y en caso de diferencia, altera el funcionamiento del receptor, por ejemplo no aceptando cooperar con el terminal.

[0011] En una segunda alternativa el terminal lee de la tarjeta entre los resultados aquél que corresponde al cálculo que ha realizado y compara este resultado con aquel que ha obtenido ella misma; en caso de diferencia, altera el funcionamiento del receptor, por ejemplo no aceptando cooperar con la tarjeta.

[0012] Los parámetros empleados pueden ser constituidos por un primer parámetro que corresponde a uno de los abonos y por un segundo parámetro constituido por una de las características de los receptores, por ejemplo el número de serie de su tarjeta de chip (que es único).

[0013] Los algoritmos de cálculo implementados pueden ser de cualquier tipo: estos pueden ser algoritmos de cifrado simétrico o asimétrico, o de tipo RSA, o el tipo HASH, o del tipo DES o de cualquier otro tipo.

[0014] El algoritmo de cálculo implementado en relación con un abono no es necesariamente el mismo que aquel implementado con los otros. Este algoritmo puede instalarse en el terminal al fabricar o cargarse por el difusor en el momento de la verificación.

[0015] La presente invención también se refiere a un receptor de televisión que es capaz de ser controlado de acuerdo con el método que se acaba de definir. Este receptor comprende un terminal y una tarjeta de chip que contiene derechos de acceso y se caracteriza porque:
- la tarjeta además contiene diversos resultados de cálculo,
- el terminal comprende medios capaces de realizar un cálculo determinado, utilizando uno o varios parámetros determinados,
- el receptor comprende medios para comparar los resultados del cálculo realizado por el terminal con el resultado correspondiente contenido en la tarjeta,
- el receptor comprende medios para alterar su funcionamiento en una forma apropiada en caso de una diferencia entre los dos resultados.

[0016] En una primera alternativa, los medios para comparar los resultados se ubican en la tarjeta, esta última siendo capaz de alterar el funcionamiento del receptor.

[0017] En una segunda alternativa, los medios para comparar los resultados se ubican en el terminal, este último es capaz de alterar el funcionamiento del receptor.

[0018] Uno de los parámetros puede corresponder a uno de los abonos y otro parámetro puede ser una de las características del receptor y por ejemplo el número de serie de la tarjeta.

Breve descripción de los dibujos

[0019] Las Figuras 1 a 3 cada una ilustra en forma esquemática, un receptor capaz de implementar el método de acuerdo con la invención.

Descripción detallada de formas de realización preferidas

[0020] Se considera que, a modo de ejemplo no limitativo, el algoritmo de cálculo es un algoritmo de cifrado de clave simétrica, que se refiere al número de serie de la tarjeta de chip. Estos algoritmos se utilizan actualmente en control de acceso, en particular para recuperar la clave de servicio (ver introducción). Nombramos A_{Ci} (NSj) el algoritmo que utiliza la clave Ci, en donde el índice i se refiere a los n diferentes abonos del sistema (i varía de 1 a n), y NSj representa el número de serie del receptor $j^{ésimo}$, el índice j identifica el receptor (j varía de 1 a p). El resultado de este cálculo se escribe Ri,j. Se considera que cada receptor tiene todas las n claves de abono Ci.

[0021] El difusor calcula, en un momento u otro, los np resultados Ri,j, i que varía de 1 a n y j de 1 a p. Solo n resultados corresponden a un receptor de rango determinado q (j=q), Ri,q correspondiendo a n claves de abono Ci (i de 1 a n).

[0022] A fin de realizar la verificación del receptor del rango q, el difusor selecciona una de las claves de abono entre n, digamos Ck, y ordena al receptor que realice el cálculo utilizando la clave Ck como parámetro. Este cálculo ha producido el resultado Rk, q cuando el difusor lo había efectuado. De esta manera calcula Act (NSq) y compara el resultado con aquél que ya se había recibido del difusor y que ha almacenado. Si se encuentra que los resultados son iguales, el receptor continua su funcionamiento normal. Si los resultados son diferentes entre sí, o si el receptor no puede incluso realizar el cálculo solicitado, entonces se ha producido una manipulación del receptor fraudulenta y el funcionamiento puede ser interrumpido.

[0023] La tabla 1 resume estas operaciones.

[0024] Esta tabla no indica qué medios del receptor realizan la comparación de los resultados. En la tabla II, se considera que la tarjeta se utiliza para esta tarea. En este caso, los resultados escritos en la tarjeta no son legibles por el terminal. La tabla III corresponde al caso en donde el terminal se utiliza para la comparación. En ambas tablas II y III, el índice q, que identifica el receptor, se ha omitido para simplificar las notaciones.

Tabla I

DIFUSOR	RECEPTOR j=q
• Calcula todo los Rij = A_{Ci} (NSj) (i de 1 a n) (j de 1 a p)	• Almacena Ci (i de 1 a n) Almacena Ri,q
• Transmite el receptor q Ci (i de 1 a n) Ri,q	• Calcula R'k,q= A_{CK} (Nsq) Compara R'k,q y Rk,
• Ordena al receptor q que calcule mientras que indica i=k, esto es $R_{k,q}$= A_{CK} (NSq)	

Tabla II

TARJETA DE CHIP	TERMINAL
Almacena Ci y Ri (i de 1 a n)	• Recibe comando para calcular con Ci determinado • Lee la tarjeta Ci y NS
Compara R'i con Ri	• Calcula R'1= A_{CI} (NS) • Transmite R'i a la tarjeta

Tabla III

TARJETA DE CHIP	TERMINAL
Almacena Ci y Ri	• Recibe la orden para calcular con Ci determinado • Lee en la tarjeta Ci y NS • Calcula R'i=A_{Ci} (NS) • Lee Ri en la tarjeta • Compara R'i con Ri

[0025] Como un ejemplo simple, puede considerarse que a cada receptor corresponde un abono. El difusor calcula los n resultados R_i. Un resultado Rq corresponde a un receptor de rango q, el resultado Rq corresponde a la clave de abono Cq y al algoritmo AC_q.

[0026] A fin de realizar la verificación de este receptor, el difusor ordena al receptor que realice el cálculo mientras que toma esta clave Cq como parámetro. Este cálculo ha producido el resultado Rq cuando el difusor lo ha realizado. El receptor de esta manera calcula AC_q (NSq) y compara el resultado obtenido con Rq que obtiene del difusor.

[0027] Se notará que de acuerdo con la invención, el terminal y la tarjeta de chip, son productos dinámicos en el sentido de que su contenido puede variar: en cualquier momento puede recibir nuevos derechos de acceso y nuevos resultados de cálculo.

[0028] El algoritmo de cálculo puede utilizar otras claves diferentes a las claves de abono, y por ejemplo claves diversificadas que se obtienen de una clave base combinada con el identificador de cada tarjeta de chip. En este caso, cada receptor realiza un cálculo con una clave que es específica al receptor. También, el algoritmo puede cambiarse o modificarse dinámicamente.

[0029] Cada una de las formas de realización del receptor correspondientes a las tablas I a III se ilustran en cada una de las figuras respectivas 1 a 3.

[0030] En la Figura 1 el receptor de televisión 1 es capaz de ser verificado por el método de acuerdo con una de las modalidades de la invención, comprende un terminal 2 y una tarjeta de chip 3 que contienen derechos de acceso referentes a abonos. La tarjeta además contiene diversos resultados de cálculo.

[0031] El terminal 2 comprende medios 4 capaces de realizar cualquiera de los cálculos de acuerdo con el método al utilizar uno o varios parámetros predeterminados.

[0032] El receptor 1 comprende medios 5 para comparar el resultado de cálculo realizado por el terminal 2 con el resultado correspondiente contenido en la tarjeta 3.

[0033] El receptor comprende medios 6 para alterar su funcionamiento en una forma apropiada en caso de una diferencia entre los dos resultados.

[0034] En la Figura 2, que muestra un receptor apto para realizar un modo de realización según la invención, los medios 5 para comparar el resultado de cálculo realizado por el terminal 2 con el resultado correspondiente contenido en la tarjeta 3, se ubican en la tarjeta 3, esta última es capaz de alterar el funcionamiento del receptor.

[0035] En la Figura 3, que muestra un receptor apto para realizar otro modo de realización según la invención, los medios 5 para comparar el resultado de cálculo realizado por el terminal 2 con los resultados correspondientes contenidos en la tarjeta 3, se ubican en el terminal 2, esta última es capaz de alterar el funcionamiento del receptor.

REIVINDICACIONES

1. Método para verificar receptores para sistema de televisión con control de acceso, en donde un difusor transmite los derechos de acceso correspondientes a los abonados que se hayan abonado a abonos con derechos de acceso correspondientes, los receptores almacenan estos derechos de acceso, este método **se caracteriza por el hecho de que**:

A) el difusor realiza, para cada receptor, una pluralidad de cálculos, cada cálculo estando parametrado por un primer parámetro que corresponde a uno de los abonos y un segundo parámetro constituido por una de las características del receptor,
- el difusor luego transmite a cada receptor los resultados de los cálculos que le conciernen,
- cada receptor almacena estos resultados,

B) para verificar un receptor particular:
- el difusor elige uno de los primeros parámetros que corresponden a uno de los abonos,
- el difusor ordena al receptor que efectúe uno de dichos cálculos indicando al receptor el parámetro elegido,
- el receptor realiza el cálculo tomando el parámetros elegido y un parámetro constituido por una de las características, creando así un resultado obtenido por el receptor,
el receptor,
- se realiza una comparación entre el resultado obtenido por el receptor y el resultado previamente almacenado,
- en caso de diferencia, el funcionamiento del receptor es interrumpido,

los cálculos realizados por el difusor y los receptores definidos por un algoritmo de cada cifrado cuya clave de cifrado depende de las claves de abono, este cifrado basándose en un número que depende de una de las características de cada receptor.

2. Método según la reivindicación 1, en el que, cada receptor que comprende un terminal y una tarjeta de chip, es la tarjeta la que almacena los derechos y los resultados que le transmite el difusor y es el terminal el que realiza el cálculo requerido por el difusor.

3. Método según la reivindicación 2, en el que:
- el terminal transmite el resultado de su cálculo a la tarjeta,
- la tarjeta compara el resultado transmitido por el terminal y el resultado correspondiente que ha recibido del difusor,
-en caso de diferencia, la tarjeta altera el funcionamiento del receptor.

4. Método según la reivindicación 2, en el que:
- el terminal lee en la tarjeta el resultado correspondiente al cálculo que realiza,
- el terminal compara el resultado de su cálculo con el resultado leído en la tarjeta,
- en caso de una diferencia, el terminal altera el funcionamiento del receptor.

5. Método según la reivindicación 1, en el que la clave de cifrado es una clave de abono.

6. Método según la reivindicación 1, en el que la característica cifrada es el número de serie de la tarjeta de chip utilizada en el receptor.

7. Receptor de televisión capaz de ser verificado utilizando el método según cualquiera de las reivindicaciones 1 a 6, este receptor comprende un terminal y una tarjeta de chip que contiene derechos de acceso que se refieren a abonos, este receptor se caracteriza por el hecho de que:
- la tarjeta además contiene diversos resultados de cálculo,
- el terminal comprende medios capaces de realizar uno cualquiera de estos cálculos utilizando un primer parámetro constituido por uno de los derechos de acceso contenidos en la tarjeta y un segundo parámetro constituido por una de las características del receptor,
- el receptor comprende medios para comparar el resultado de cálculo realizado por el terminal con el resultado correspondiente contenido en la tarjeta,
- el receptor comprende medios para alterar su funcionamiento en una forma apropiada en caso de una diferencia entre los dos resultados.

8. Receptor según la reivindicación 7, en el que los medios para comparar los resultados se ubican en la tarjeta, esta última es capaz de interrumpir el funcionamiento del receptor.

9. Receptor según la reivindicación 7, en el que los medios para comparar los resultados se ubican en el terminal, este último es capaz de interrumpir el funcionamiento del receptor.

10. Receptor según la reivindicación 7, en el que el segundo parámetro empleado para realizar el cálculo es el número de serie único de la tarjeta.

11. Tarjeta de chip para la utilización con un receptor de televisión, el receptor de televisión siendo capaz de ser verificado por el método según cualquiera de las reivindicaciones 1 a 6, la tarjeta de chip (3) conteniendo las claves de abono (Ci) y los resultados (Ri) de los cálculos realizados por el difusor, los cálculos refiriéndose al receptor.

12. Tarjeta de chip según la reivindicación 11, que comprende además unos medios para comparar (5) los resultados (Ri) de los cálculos realizados por el difusor en la tarjeta con los resultados de cálculos realizados por el receptor.

FIG. 1

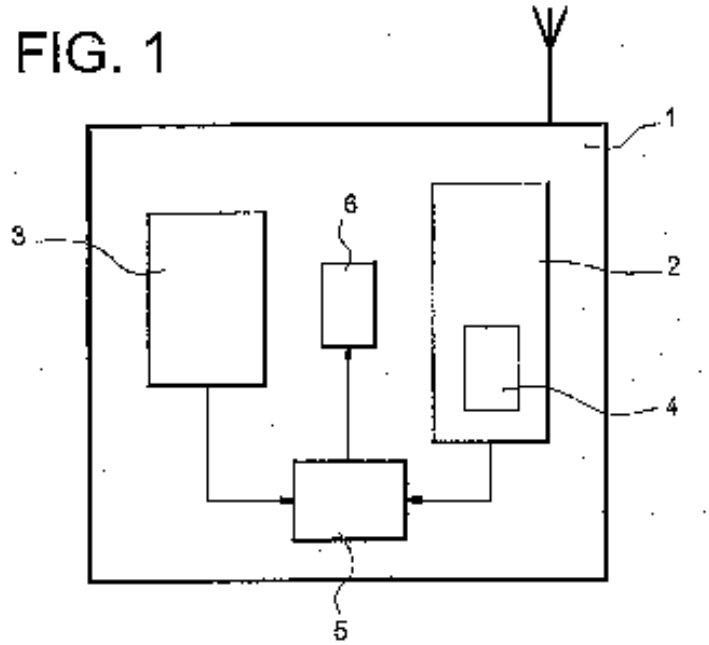
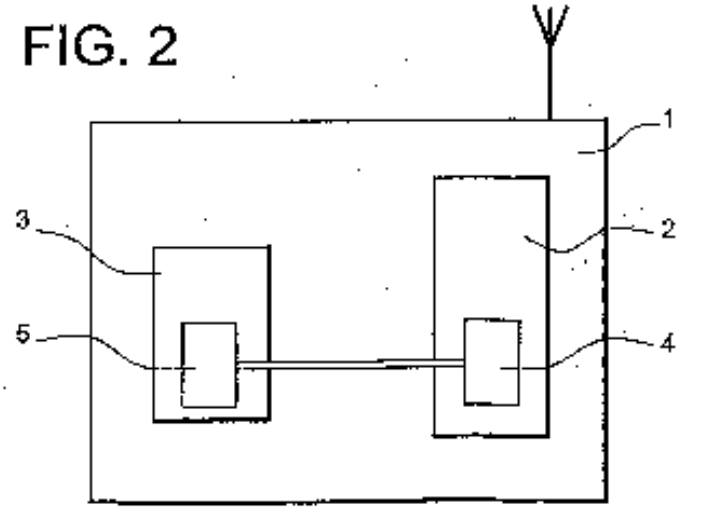


FIG. 2



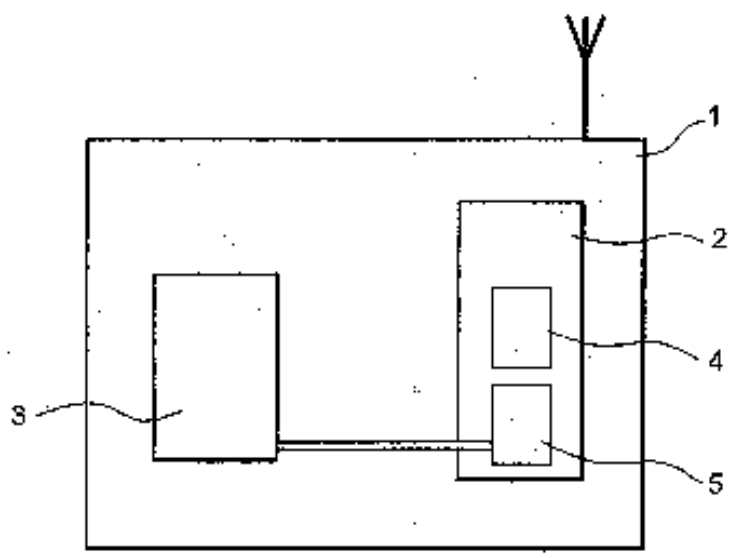


FIG. 3