(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 434 326**

(51) Int. CI.:

H04N 21/418 (2011.01)
H04N 21/4367 (2011.01)
H04N 7/16 (2011.01)
H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.02.2005 E 05716737 (1)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2013 EP 1730961**

(54) Título: **Gestión dinámica de tarjetas inteligentes**

(30) Prioridad:

11.03.2004 EP 04290656

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.12.2013

(73) Titular/es:

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

(72) Inventor/es:

MAILLARD, MICHEL y
LE FLOCH, DOMINIQUE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Gestión dinámica de tarjetas inteligentes

Antecedentes de la invención

Campo de la invención

[0001] En general, la invención tiene que ver con módulos de seguridad portátiles adaptados para descodificar información audiovisual codificada.

Estado de la técnica

[0002] La transmisión de datos encriptados es bien conocida en el campo de los sistemas de TV de pago, donde normalmente se difunde información audiovisual codificada a través de emisores terrestres, satélite o mediante una red de cable, a un número de abonados, cada uno de los cuales posee un descodificador o receptor/descodificador capaz de descodificar la información audiovisual codificada para su posterior visionado.

[0003] En un sistema típico, la información audiovisual codificada se puede descodificar utilizando una palabra de control. Para tratar de mejorar la seguridad del sistema, la palabra de control es modificada más o menos cada diez segundos. Cada 10 segundos, cada abonado recibe, en un ECM (Mensaje de control de titularidad), la palabra de control necesaria para descodificar la información audiovisual codificada y así permitir el visionado de la transmisión.

[0004] La palabra de control se encripta por una clave de explotación y se transmite en formato encriptado en el ECM. La información audiovisual codificada y la palabra de control encriptada son recibidas por un descodificador que, en el caso de un abonado, tiene acceso a la clave de explotación almacenada en un módulo de seguridad portátil, como por ejemplo una tarjeta inteligente, insertada en el descodificador. La palabra de control encriptada es desencriptada por la tarjeta inteligente utilizando la clave de explotación. La tarjeta inteligente transmite la palabra de control al descodificador. La información audiovisual codificada es descodificada utilizando la palabra de control desencriptada por el descodificador. El descodificador es lo suficientemente potente como para proporcionar una descodificación a tiempo real de la información audiovisual codificada.

[0005] La clave de explotación es modificada periódicamente, por ejemplo cada mes. El descodificador recibe mensualmente un EMM (Mensaje de gestión de titularidad), que se transmite en la tarjeta inteligente. El EMM contiene la clave de explotación en formato codificado. Una clave de grupo asignada a la tarjeta inteligente se habilita para descodificar la clave de explotación codificada.

[0006] El descodificador, por lo tanto, manda regularmente mensajes de comando a la tarjeta inteligente.

[0007] El mensaje de comando puede ser un ECM, es decir, el descodificador transmite a la tarjeta inteligente una palabra de control en formato encriptado. La tarjeta inteligente desencripta la palabra de control que utiliza la clave de explotación.
La transmisión de la palabra de control normalmente tiene lugar cada 10 segundos.

[0008] Si un espectador cambia de un primer canal a un segundo canal, el descodificador transmite a la tarjeta inteligente una segunda palabra de control en formato encriptado después de transmitir la primera palabra de control en formato encriptado. La primera palabra de control y la segunda palabra de control corresponden respectivamente al primer canal y al segundo canal. La tarjeta inteligente puede, por lo tanto, recibir Mensajes de Control de Titularidad con más frecuencia en lugar de cada 10 segundos debido al cambio de canales.

[0009] El mensaje de comando también puede ser un EMM, es decir, el descodificador transmite a la tarjeta inteligente una clave de explotación en formato codificado, o cualquier otro mensaje de comando que procede del descodificador.

[0010] La FIG. 1 ilustra esquemáticamente una tarjeta inteligente según un diseño anterior. La tarjeta inteligente 11 se activa por la recepción de un mensaje, por ejemplo un Mensaje de control de titularidad ECM_n de un descodificador (no representado): el descodificador da las órdenes y la tarjeta inteligente 11 las obedece. Una unidad de procesamiento 12 de la tarjeta inteligente sólo ejecuta los mensajes de comando recibidos desde el descodificador. La tarjeta inteligente 11 consta de una memoria de parámetros, por ejemplo una EEPROM 13, en la que los parámetros son almacenados. La unidad de procesamiento 12 puede controlar que los parámetros almacenados en la EEPROM 13 sean correctos. Los parámetros pueden ser, por ejemplo el tamaño de los Mensajes de Control de Titularidad que han de ser recibidos. La unidad de procesamiento puede controlar que el Mensaje de control de titularidad ECM_n tenga un tamaño apropiado antes de desencriptar una palabra de control encriptada contenida en el Mensaje de control de titularidad ECM_n.

[0011] Una tarjeta inteligente está pensada generalmente para la comunicación con un único descodificador. No obstante, un usuario fraudulento puede intentar configurar un servidor entre una única tarjeta inteligente y una pluralidad

de descodificadores. El servidor puede ser un divisor que comunica con la pluralidad de descodificadores directamente, por ejemplo a través de un cable eléctrico. El servidor también puede ser un Servidor de palabra de control que comunica con la pluralidad de descodificadores a través de una red, por ejemplo una red de internet.

[0012] La FIG. 2 ilustra esquemáticamente un ejemplo de la configuración de un divisor según un diseño anterior .

[0013] Un primer descodificador 24A recibe de forma continua la primera información audiovisual codificada $E_{CW1}(m_1)$ correspondiente a un primer canal. Un segundo descodificador 24B recibe de forma continua una segunda información audiovisual codificada $E_{CW2}(m_2)$ correspondiente a un segundo canal. El primer descodificador 24A y el segundo descodificador 24B permiten, respectivamente, una descodificación a tiempo real de la primera información audiovisual codificada $E_{CW1}(m_1)$ y de la segunda información audiovisual codificada $E_{CW2}(m_2)$.

[0014] La primera información audiovisual codificada $E_{CW1}(m_1)$ y la segunda información audiovisual codificada $E_{CW2}(m_2)$ son respectivamente descodificadas utilizando una primera palabra de control CW1 almacenada en una primera memoria 25A del primer descodificador 24A y una segunda palabra de control CW2 almacenada en una segunda memoria 25B del segundo descodificador 24B.

[0015] En cada criptoperiodo, es decir, cada 10 segundos, por ejemplo, el primer descodificador 24A y el segundo descodificador 24B reciben respectivamente, un primer Mensaje de control de titularidad ECM1 y un segundo Mensaje de control de titularidad ECM2.

[0016] En una configuración de divisor, el primer descodificador 24A y el segundo descodificador 24B transmiten, respectivamente, el primer Mensaje de control de titularidad ECM1 y el segundo Mensaje de control de titutlaridad ECM2 a un servidor único, por ejemplo un divisor 22, durante un único criptoperiodo.

[0017] El divisor 22 remite uno de los Mensajes de Control de Titularidad transmitidos, por ejemplo ECM1, a un módulo de seguridad portátil único, por ejemplo una tarjeta inteligente 21. Usando una clave de explotación almacenada en una memoria de tarjeta inteligente 26, la tarjeta inteligente puede desencriptar la palabra de control correspondiente, por ejemplo CW1, en la recepción del Mensaje de control de titularidad (ECM1) remitido. La palabra de control correspondiente CW1 es transmitida al divisor 22. Una vez el divisor 22 recibe la palabra de control transmitida CW1, el divisor 22 remite un Mensaje de control de titularidad diferente entre los Mensajes de Control de Titularidad transmitidos, por ejemplo ECM2, a la tarjeta inteligente 21. La tarjeta inteligente desencripta la palabra de control correspondiente, por ejemplo CW2, en la recepción del Mensaje de control de titularidad remitido (ECM2). La palabra de control correspondiente CW2 es transmitida al divisor 22.

[0018] El divisor 22 remite las palabras de control desencriptadas CW1 y CW2, respectivamente, al primer descodificador 24A y al segundo descodificador 24B.

[0019] El servidor permite que una pluralidad de descodificadores descodifiquen la información audiovisual codificada con una única tarjeta inteligente.

[0020] Resumiendo, un abonado posee generalmente un único módulo de seguridad portátil, por ejemplo una tarjeta inteligente. No obstante, un servidor configurado por un usuario fraudulento, por ejemplo un divisor o un Servidor de palabra de control, permite a una pluralidad de descodificadores descodificar información audiovisual codificada con una única tarjeta inteligente. Por lo tanto, es posible para el abonado facilitar el acceso de uno o más usuarios desautorizados que no posean una tarjeta inteligente a la información audiovisual dirigida al abonado.

[0021] Es necesario un método que permita desalentar el uso de un servidor configurado como un divisor . No obstante, un abonado regular que posea un descodificador que se comunique directamente con una tarjeta inteligente no debería tener ningún problema.

[0022] Un primer método puede consistir en la implementación de un software de ralentización en tarjetas inteligentes, donde el software de ralentización permite ralentizar el procesamiento de cada tarjeta inteligente. Las tarjetas inteligentes pueden, por lo tanto, no ser capaces de desencriptar más de una palabra de control durante un criptoperiodo, por ejemplo en 10 segundos.

[0023] Un segundo método puede consistir en la emisión de Mensajes de Control de Titularidad en criptoperiodos más cortos, por ejemplo cada 3 segundos.

[0024] Tanto el primer método como el segundo permiten restringir el procesamiento a un único ECM por criptoperiodo. Como consecuencia, el servidor, por lo general, no podrá sincronizar comunicaciones entre una pluralidad de descodificadores y una única tarjeta inteligente. Sólo un único descodificador podrá funcionar correctamente con una única tarjeta inteligente.

[0025] No obstante, si un abonado regular posee un único descodificador y cambia de un canal a otro a una velocidad relativamente alta, la tarjeta inteligente tampoco podrá desencriptar una pluralidad de ECM recibidos por criptoperiodo. El abonado regular debe, por lo tanto, evitar cambiar entre la variedad de información audiovisual ofrecida. Por lo general, es posible que desaparezca la imagen de la pantalla del abonado regular al cambiar de canal aunque el usuario sea un abonado regular. El documento EP 0 866 613 describe un receptor/descodificador que está programado sólo para aceptar Mensajes de Control de Titularidad (EMM) actuales si ha recibido al menos un EMM procedente de un periodo anterior del calendario. Cuando éste es recibido, se usa para comprobar los derechos actuales en el receptor/descodificador. Este método impide que un abonado original obtenga los derechos de forma fraudulenta mediante la desconexión de un descodificador (antes de que un mensaje de autorización pueda actualizar la memoria del descodificador para evitar la desencriptación) y la reconexión del descodificador (para así ser confundido con un nuevo abonado que ha obtenido legitimamente esos derechos).

Resumen de invención

[0026] En un primer aspecto, la invención proporciona un método para asegurar un módulo de seguridad portátil que se usa con un elemento de descodificación, el módulo de seguridad portátil y el elemento de descodificación permiten descodificar la información audiovisual codificada. El método comprende en el modulo de seguridad portátil el procesamiento de los Mensajes de Control de Titularidad (ECM) recibidos en el módulo de seguridad portátil para permitir la descodificación de la información audiovisual codificada. El método comprende además el análisis de una secuencia de ECM en el módulo de seguridad portátil; la secuencia de ECM constaría de un nuevo ECM y un ECM recibido previamente, los ECM de la secuencia se recibirían en el módulo de seguridad portátil en momentos diferentes, y el análisis se realizaría cuando se recibe el nuevo ECM. El registro de errores se incrementa durante el análisis con un resultado determinado extraído del análisis y de la aplicación de una penalización al módulo de seguridad portátil, que depende del valor del registro de errores, mediante la introducción de un tiempo muerto en el procesamiento para así ralentizar el mismo.

[0027] En una primera implementación, los ECM se sustituyen con Mensajes de Gestión de Titularidad (EMM).

[0028] En una segunda implementación, el tiempo muerto tiene una duración que depende del valor del registro de errores.

[0029] En una tercera implementación, la duración del tiempo muerto es más corta que el valor de un tiempo máximo. El valor de un tiempo máximo es lo suficientemente alto como para evitar que el módulo de seguridad portátil procese más de un Mensaje de control de titularidad durante un único criptoperiodo.

[0030] En una cuarta implementación, cada Mensaje de control de titularidad contiene un identificador de canal.
El identificador de canal se asocial a un canal determinado.
El análisis de la secuencia de ECM comprende la comparación del identificador de canal del nuevo ECM y el identificador de canal del ECM previo.

[0031] En una quinta implementación, cada Mensaje de control de titularidad consta de una primera palabra de control encriptada y una segunda palabra de control encriptada. La primera palabra de control permite descodificar la información audiovisual codificada durante un primer criptoperiodo y la segunda palabra de control permite descodificar la información audiovisual codificada durante un segundo criptoperiodo diferente del primer criptoperiodo. El análisis de la secuencia de ECM comprende la comparación de una segunda palabra de control del ECM previo con una primera palabra de control del nuevo ECM.

[0032] En una sexta implementación, el análisis de la secuencia de ECM comprende la comparación de un contenido determinado correspondiente a un primer ECM de la secuencia de ECM con un segundo contenido determinado perteneciente a un segundo ECM de la secuencia de ECM.

[0033] En una séptima implementación, se introduce un tiempo muerto de reinicio para reiniciar cada procesamiento de los Mensajes de control de titularidad. El tiempo muerto de reinicio tiene una duración que depende de un número de Mensajes de Control de Titularidad recibidos en el módulo de seguridad portátil después del reinicio. La duración es igual al valor de un primer tiempo de reinicio durante un primer procesamiento, que ocurre inmediatamente después del reinicio. El valor de un primer tiempo de reinicio es inferior al valor de un tiempo máximo.

[0034] En una octava implementación, la naturaleza de un reinicio posterior se evalúa según un grupo intermedio de mensajes de comando intermedio. El grupo intermedio comprende los mensajes de comando recibidos después de un reinicio previo al reinicio posterior.

[0035] En una novena implementación, se contabiliza el número de los ECM intermedios. El número de los ECM intermedios se compara con el número de umbral de reinicios. El resultado de la comparación permite evaluar la naturaleza del reinicio posterior. El registro de errores de reinicio se incrementa con el reinicio posterior si el si éste se considera sospechoso. El módulo de seguridad portátil se bloquea si el registro de error de reinicio tiene un valor superior al umbral de errores de reinicio.

[0036] Preferentemente, el módulo de seguridad portátil será una tarjeta inteligente y el elemento de descodificación un descodificador.

[0037] En un segundo aspecto, la invención proporciona un módulo de seguridad portátil que se usa con un elemento de descodificación, en el que el módulo de seguridad portátil y el elemento de descodificación permiten descodificar información audiovisual codificada. El módulo de seguridad portátil consta de sistemas de recepción para recibir Mensajes de Control de Titularidad (ECM) y sistemas de procesamiento para procesar un ECM recibido en el módulo de seguridad portátil permitiendo así la descodificación de la información audiovisual codificada . El módulo de seguridad portátil consta además de una memoria de mensajes de comando en la que un ECM recibido en un momento anterior puede ser almacenado, y de medios de análisis que permiten analizar una secuencia de ECM, la secuencia de ECM consta de un nuevo ECM y un ECM previo, los ECM de la secuencia se reciben en el módulo de seguridad portátil en momentos diferentes, y el análisis se realiza cada vez que se recibe un nuevo ECM. El módulo de seguridad portátil consta además sistemas de comparación con los que comparar el nuevo ECM y el ECM previo de la secuencia de ECM, un registro de errores, sistemas de incrementado para incrementar el registro de errores dependiente del resultado de la comparación, y sistemas de ralentización que permiten introducir un tiempo muerto con cada procesamiento, con el objeto de ralentizar el procesamiento.

[0038] En una décima implementación, los sistemas de ralentización también permiten introducir un tiempo muerto de reinicio con cada procesamiento después del reinicio. El tiempo muerto de reinicio tiene una duración que depende del número de procedimientos que tienen lugar después del reinicio. La duración es igual al valor de un primer tiempo muerto de reinicio que tiene lugar durante un primer procedimiento inmediatamente posterior al reinicio.

[0039] En una decimoprimera implementación, el módulo de seguridad portátil consta además de un registro de recuento que permite almacenar varios ECM intermedios. Los ECM intermedios se reciben en el módulo de seguridad portátil después de un reinicio previo. El módulo de seguridad portátil consta además de un indicador. El indicador tiene un valor que depende de un resultado de la comparación del registro de recuento con el número máximo de reinicios. El registro de errores de reinicio aumenta dependiendo del valor del indicador durante un reinicio posterior. Los sistemas de bloqueo permiten bloquear el módulo de seguridad portátil según el valor del registro de errores de reinicio.

[0040] En una decimosegunda implementación, los ECM se sustituyen por Mensajes de Gestión de Titularidad (EMM).

[0041] En un tercer aspecto, la invención proporciona un software que se usa dentro de un módulo de seguridad portátil. El software permite implementar el método del primer aspecto de la invención.

[0042] En un cuarto aspecto, la invención proporciona un método para asegurar un módulo de seguridad portátil. El método comprende la descarga de un software durante el proceso de fabricación de acuerdo con el tercer aspecto de la presente invención.

[0043] En un quinto aspecto, la invención proporciona un método para asegurar un módulo de seguridad portátil. El método comprende la descarga de un software de acuerdo con el tercer aspecto de la presente invención. La descarga comprende la recepción en el módulo de seguridad portátil de al menos un mensaje de configuración del elemento de descodificación.

[0044] Otros aspectos y ventajas de la invención se harán evidentes mediante la siguiente descripción y reivindicaciones anexas.

Breve descripción de dibujos

[0045] La FIG. 1 ilustra esquemáticamente un ejemplo de una tarjeta inteligente según el estado de la técnica.

[0046] La FIG. 2 ilustra esquemáticamente un ejemplo de la configuración de un divisor según el estado de la técnica.

[0047] La FIG. 3 ilustra un ejemplo de un módulo de seguridad portátil según la presente invención.

[0048] La FIG. 4 ilustra un ejemplo de un algoritmo que es ejecutado por una tarjeta inteligente según la presente invención.

[0049] Las FIG. 5A y FIG. 5B ilustran un ejemplo de una secuencia de mensajes de comando recibidos por un módulo de seguridad portátil según la presente invención.

[0050] La FIG. 6A ilustra una posible secuencia de valores del registro de errores en un módulo de seguridad portátil según la presente invención.

[0051] La FIG. 6B ilustra una posible secuencia de valores de la duración de un tiempo muerto en un módulo de seguridad portátil según la presente invención.

[0052] La FIG. 6C ilustra un ejemplo de una secuencia de valores de la duración de un tiempo muerto de un módulo de seguridad portátil según la presente invención.

[0053] La FIG. 7 ilustra un ejemplo de un algoritmo que se implementa en un módulo de seguridad portátil según la presente invención.

Descripción detallada

[0054] Visión de conjunto de la invención

[0055] La FIG. 3 ilustra un ejemplo de un módulo de seguridad portátil según la presente invención. Un módulo de seguridad portátil 31, por ejemplo una tarjeta inteligente, está pensado para ser usado con un elemento de descodificación (no representado), por ejemplo un descodificador. El módulo de seguridad portátil y el elemento de descodificación permiten descodificar información audiovisual codificada. El módulo de seguridad portátil 31 recibe una pluralidad de mensajes, por ejemplo Mensajes de control de titularidad. El módulo de seguridad portátil permite procesar cada Mensaje de control de titularidad recibido ECM_{n+1} para extraer una palabra de control CW_{n+1} que será enviada al descodificador.

[0056] Como ocurre con el módulo de seguridad portátil del estado de la técnica, la tarjeta inteligente 31 según la presente invención puede comprender una unidad de procesamiento 32 que sólo procesa los Mensajes de Control de Titularidad u otros mensajes recibidos en el módulo de seguridad portátil. El módulo de seguridad portátil 31 puede constar de una memoria de parámetros, por ejemplo una EEPROM 33, en la que se almacenan los parámetros. La unidad de procesamiento 32 puede comprobar que los parámetros almacenados en la EEPROM 33 sean correctos.

[0057] El módulo de seguridad portátil 31 de la presente invención consta de sistemas de análisis 35 para analizar secuencias de mensajes de comando (CM_{n+1} CM_n). Los mensajes de comando de la secuencia (CM_{n+1} , CM_n) se reciben en el módulo de seguridad portátil 31 en momentos diferentes.

[0058] Normalmente, el análisis es llevado a cabo cada vez que se recibe un nuevo mensaje de comando CM_{n+1}. La secuencia mensajes de comando comprende el nuevo mensaje de comando CM_{n+1} y un mensaje de comando previo CM_n, que pueden, por ejemplo, ser recibidos justo antes del nuevo mensaje de comando CM_{n+1}. La secuencia de mensajes de comando puede comprender además al menos otro mensaje de comando.

[0059] El análisis puede comprender la comparación de un contenido determinado de los mensajes de comando de la secuencia de mensajes de comando (CM_{n+1} , CM_n). El registro de errores 37 se puede incrementar con un resultado determinado extraído de la comparación.

[0060] La tarjeta inteligente de la presente invención permite, por lo tanto, extraer información, por ejemplo un valor del registro de errores 37, siempre que la información extraída tenga relación con los mensajes de comando que son recibidos antes que el nuevo mensaje de comando CM_{n+1}. Se podrá aplicar una penalización a la tarjeta inteligente 31 dependiente de un valor del registro de errores 37. Tal método, según la presente invención, permite evitar, a diferencia del primer y el segundo método, perjudicar a un abonado regular - que posea un único descodificador cuando cambia de un canal a otro a una velocidad relativamente alta.

[0061] La tarjeta inteligente 31 puede constar además de una memoria 36 de mensajes de comando en la que al menos se puede almacenar un mensaje de comando entre los mensajes recibidos consecutivamente. La memoria 36 de mensajes de comando puede ser diferente a una unidad central de procesamiento 34 que comprende la unidad de procesamiento 32 y ,medio de análisis 35.

[0062] De forma alternativa, la memoria de mensajes de comando puede constituir, por ejemplo, una parte de los medios de análisis: Por lo general, la memoria de mensajes de comando puede ser un único registro de los medio de análisis o de otros medios de procesamiento cualquiera.

[0063] Los medios de análisis 35 pueden ser un dispositivo de hardware diferente de la unidad de procesamiento 32, como se representado en la FIG. 3. Preferentemente, los medios de análisis son un software de análisis que se implementa en la tarjeta inteligente. La unidad central de procesamiento consta de un software de procesamiento y un software de análisis.

[0064] La FIG. 4 ilustra un ejemplo de un algoritmo que es ejecutado por una tarjeta inteligente según la presente invención.
La tarjeta inteligente recibe un mensaje. El mensaje recibido puede ser un mensaje de comando, por ejemplo un ECM, un EMM, o cualquier otro mensaje determinado. Cuando se recibe un nuevo mensaje de comando CM_{n+1} (caja 401),

se realiza un análisis de una secuencia de mensajes de comando. Por lo general, el nuevo mensaje de comando CM_{n+1} se compara con un mensaje de comando CM_n recibido en un momento anterior (caja 402). La comparación del nuevo mensaje de comando CM_{n+1} con el mensaje de comando CM_n recibido en un momento anterior puede consistir en la comparación de una parte determinada de cada mensaje de comando (CM_n, CM_{n+1}), por ejemplo un identificador. La comparación también puede consistir en la comparación de una información extraída de cada mensaje de comando (CM_n, CM_{n+1}), por ejemplo una palabra de control desencriptada por la tarjeta inteligente.

[0065] El registro de errores “error_reg” se puede incrementar dependiendo del resultado de la comparación (caja 403). El algoritmo comprende además la introducción de un tiempo muerto τ con cada procesamiento de los Mensajes de control de titularidad recibidos en la tarjeta inteligente (caja 404). Tal penalización de tiempo muerto τ permite ralentizar la tarjeta inteligente. En el método de la presente invención, el tiempo muerto τ tiene una duración que depende del valor del registro de errores “error_reg”. Por lo general, la duración del tiempo muerto τ aumenta con el valor del registro de errores “error_reg”.

[0066] En caso de una configuración de divisor, la tarjeta inteligente recibe más de un ECM por criptoperiodo. La tarjeta inteligente procesa cada ECM recibido para permitir la descodificación de la información audiovisual codificada. No obstante, si el análisis detecta un problema en cada criptoperiodo, por ejemplo cada 10 segundos, el registro de errores “error_reg” puede tener un valor relativamente alto. El tiempo muerto τ, por lo tanto, tiene una duración relativamente alta, que puede evitar que la tarjeta inteligente procese más de un ECM en cada criptoperiodo, interrumpiendo así la descodificación de una pluralidad de programas audiovisuales emitidos con una única tarjeta inteligente.

[0067] En caso de que un abonado regular posea un sistema de descodificación regular, este podrá generar, cuando cambie de un canal a otro, un incremento del registro de errores “error reg”. Como consecuencia, se introduce el tiempo muerto τ como una penalización, pero éste tiene una duración relativamente corta. Este tiempo muerto τ de corta duración permite que la tarjeta inteligente procese un único ECM regular desde un único descodificador durante un criptoperiodo. El método según la presente invención sólo interrumpe la descodificación mediante una configuración no autorizada, por ejemplo la configuración de divisor.

[0068] El valor del tiempo muerto τ se puede almacenar en una memoria RAM. Si, en caso de tratarse de una configuración no autorizada, la descodificación es interrumpida, un usuario desautorizado podrá reiniciar la tarjeta inteligente, para restablecer el valor del tiempo muerto τ y permitir una descodificación normal. El algoritmo puede, por lo tanto, comprender que el valor del tiempo τ muerto aumente como consecuencia de la introducción de un tiempo muerto de reinicio τ_reset (caja 406) con el reinicio de la tarjeta inteligente (caja 405). El tiempo muerto de reinicio τ_reset puede tener una duración que depende del número de ECM recibidos en la tarjeta inteligente después del renicio. En un primer procesamiento inmediatamente posterior al renicio, la duración del tiempo muerto de reinicio τ_reset puede ser igual a un primer valor de tiempo de reinicio que sea relativamente alto. De esta manera, el usuario desautorizado que reinicia la tarjeta inteligente no puede obtener la descodificación regular.

[0069] Además de la ralentización de la tarjeta inteligente, la aplicación de una penalización puede entrañar el bloqueo de la tarjeta inteligente. Como la tarjeta inteligente analiza mensajes de comando previos, es posible adaptar la penalización mediante la introducción de un tiempo muerto relativamente corto cuando se bloquea la tarjeta.

[0070] Además, un pirata informático puede hackear la tarjeta inteligente con un elevado número de mensajes de ataque para extraer parámetros esenciales. En el estado de la técnica, la tarjeta inteligente no permite proporcionar el análisis de la secuencia de mensajes de comando. Gracias al análisis de la secuencia de los mensajes de comando recibidos con anterioridad, el método de la presente invención permite detectar dicho ataque. Los mensajes de ataque pueden ser relativamente similares y el registro de errores “error_reg” puede tener un valor relativamente alto si se realiza un análisis adecuado. Las penalizaciones aplicadas a la tarjeta inteligente, por ejemplo la introducción del tiempo muerto τ o el bloqueo de la tarjeta inteligente, puede ralentizar o parar el ataque.

[0071] Análisis de una secuencia de ECM

[0072] Las FIG. 5A y FIG. 5B ilustran un ejemplo de una secuencia de mensajes de comando recibidos por un módulo de seguridad portátil según la presente invención. La secuencia ilustrada comprende dos Mensajes de Control de Titularidad .
La secuencia de mensajes de comando de la FIG. 5A es recibida por un módulo de seguridad portátil, por ejemplo una tarjeta inteligente, usada en una configuración regular. La secuencia de mensajes de comando de la FIG. 5B se recibe por una tarjeta inteligente usada en una configuración de divisor, o por una tarjeta inteligente usada en una configuración regular si abonado regular cambia de un canal determinado *i* a un segundo canal *j* mucho después de la recepción de un Mensaje de control de titularidad ECM_n previo.

[0073] Los Mensajes de Control de Titularidad (54_n, 54_{n+1}) de las FIG. 5A y FIG. 5B comprenden una primera palabra de control encriptada (52_n, 52_{n+1}). La tarjeta inteligente permite desencriptar la primera palabra de control encriptada (52_n, 52_{n+1}). La primera palabra de control CW_i [1] extraída del Mensaje de control de titularidad ECM_n previo permite una descodificación de la información audiovisual codificada de un canal determinado *i* durante un primer criptoperiodo.

[0074] En una primera implementación de la presente invención, los Mensajes de Control de Titularidad (54_n, 54_{n+1}) comprenden además una segunda palabra de control encriptada (53_n, 53_{n+1}). La tarjeta inteligente permite desencriptar la segunda palabra de control encriptada (53_n, 53_{n+1}). La segunda palabra de control CW_i [2] extraída del Mensaje de control de derecho de titularidad ECM_n permite una descodificación de la información audiovisual codificada de un canal determinado *i* durante un segundo criptoperiodo diferente al primer criptoperiodo. El segundo criptoperiodo puede seguir inmediatamente al primer criptoperiodo.

[0075] Con una configuración regular, como se ilustra en la FIG. 5A, si el abonado regular sólo ve programas de ese canal determinado, la segunda palabra de control CW_i [2] extraída del Mensaje de control de titularidad ECM_n previo es similar a la primera palabra de control CW_i [2] del nuevo Mensaje de control de derecho de titularidad ECM_{n+1}.

[0076] En el caso de cambiar de canal con frecuencia entre la recepción del Mensaje de control de titularidad ECM_n previo y la recepción de un Mensaje de control titularidad ECM'_{n+1} posterior, como se ilustra en la FIG. 5B, la tarjeta inteligente recibe como un Mensaje de control de titularidad el Mensaje de control de titularidad ECM'_{n+1}, que se une al segundo canal *j* que es diferente del canal determinado *i*. La segunda palabra de control CW_i [2] extraída del Mensaje de control de titularidad ECM_n previo es, por lo tanto, diferente a la primera palabra de control CW_j [1] del nuevo Mensaje de control de titularidad ECM'_{n+1}.

[0077] En caso de tratarse de una configuración de divisor, como se ilustra en la FIG. 5B, la tarjeta inteligente recibe Mensajes de Control de Titularidad de una pluralidad de descodificadores, cada uno de los cuales permite descodificar un flujo de información audiovisual codificada de un canal correspondiente. Si, por ejemplo, el divisor permite que la tarjeta inteligente se comunique con dos descodificadores, es posible que los dos canales correspondientes sean diferentes en la misma medida en que usuarios diferentes pueden no estar siempre viendo los mismos programas de TV.

[0078] Si los canales correspondientes son diferentes, las palabras de control que permiten descodificar la información audiovisual codificada de cada canal correspondiente son diferentes. Por lo tanto, la segunda palabra de control CW_i [2] extraída del Mensaje de control de titularidad ECM_n previo es diferente a la primera palabra de control CW_j [1] del nuevo Mensaje de control de titularidad ECM'_{n+1}.

[0079] En la primera implementación, un análisis de la secuencia de mensajes de comando consiste, por ejemplo, en la comparación de la segunda palabra de control extraída del Mensaje de control de tituralidad previo con la primera palabra de control del nuevo Mensaje de control de titularidad. Tal análisis puede ser realizado con cada recepción de un nuevo Mensaje de control de titularidad, o periódicamente.

[0080] El Mensaje de control de titularidad previo al que el Mensaje de control de titularidad nuevo es comparado puede ser recibido justo antes del nuevo Mensaje de control de titularidad. De forma alternativa, en caso de que se produzca una corriente doble, el Mensaje de control de titularidad previo puede ser elegido según un orden predeterminado.

[0081] En una segunda implementación de la presente invención que también aparece ilustrada en las FIG. 5A y 5B, los Mensajes de Control de Titularidad recibidos (54_n, 54_{n+1}) comprenden un identificador de canal (51_n, 51_{n+1}). El identificador de canal 51_n del Mensaje de control de titularidad 54_n previo se une al canal determinado que la primera palabra de control CW_i [1] permite descodificar.

[0082] Con una configuración regular, como se ilustra en la FIG. 5A, si el abonado regular no cambia de canal con frecuencia entre la recepción del Mensaje de control de titularidad ECM_n previo y la recepción de un Mensaje de control de titularidad ECM_{n+1} nuevo, solo la información audiovisual codificada del canal determinado es descodificada. El identificador de canal 51_n del Mensaje de control de titularidad ECM_n previo es, por lo tanto, similar al identificador de canal 51_{n+1} del nuevo Mensaje de control de titularidad ECM_{n+1}.

[0083] En el caso de cambiar de canal con frecuencia entre la recepción del Mensaje de control de titularidad ECM_n previo y la recepción de otro Mensaje de control de titularidad ECM'_{n+1} posterior, como se ilustra en la FIG. 5B, la tarjeta inteligente recibe como un Mmensaje de control de titularidad el Mensaje de control de titularidad $_{n+1}$ que se une al segundo canal *j* que es diferente del canal determinado *i*. El identificador de canal 51_n del Mensaje de control de derecho de titularidad ECM_n previo es, por lo tanto, diferente del identificador de canal 51_{n+1} del nuevo Mensaje de control de titularidad ECM'_{n+1}.

[0084] Si se trata de una configuración de divisor, también ilustrada en la FIG. 5B, la tarjeta inteligente puede recibir Mensajes de Control de Titularidad asociados por lo menos dos canales diferentes, como se explica en un párrafo anterior. De esta manera, el identificador de canal 51_n del Mensaje de control de titularidad ECM_n previo es diferente del identificador de canal 51_{n+1} del nuevo Mensaje de control de titularidad ECM'_{n+1}.

[0085] En la segunda implementación, el análisis de la secuencia de mensajes de comando consiste, por ejemplo, en la comparación del identificador de canal del Mensaje de control de titularidad previo con identificador de canal del nuevo Mensaje de control de titularidad. Tal análisis se puede realizar con cada recepción de un nuevo ECM, o periódicamente. El Mensaje de control de titularidad previo con el que se compara el Mensaje de control de titularidad nuevo puede ser recibido justo antes que el nuevo Mensaje de control de titularidad.

[0086] En un caso de una corriente doble, la segunda implementación permite detectar si no se ha producido ningún cambio de identificador de canal en la configuración regular y al menos un cambio de identificador de canal en la configuración de divisor. En esta última configuración, durante un criptoperiodo, la tarjeta inteligente recibe al menos:

[0087] - un primer ECM A asociado a un primer descodificador y a una primera corriente;

[0088] - un segundo ECM A' asociado al primer descodificador y a una segunda corriente;

[0089] - un tercer ECM B asociado a un segundo descodificador y a la primera corriente;

[0090] - un cuarto ECM B' asociado al segundo descodificador y a la segunda corriente.

[0091] El primer ECM, el segundo ECM, el tercer ECM y el cuarto ECM se puede recibir en el siguiente orden: A, A', B, B'.
El análisis detecta al menos un cambio de identificador de canal. El análisis detecta al menos tres cambios de identificador de canal si el ECM, el segundo ECM, el tercer ECM y el cuarto ECM se reciben en el siguiente orden: A, B, A', B'.

[0092] En caso de una corriente doble en la configuración regular sin cambiar de canal, solo se reciben el primer ECM A y el segundo ECM A' y no se detecta ningún cambio de identificador de canal. En este último caso, un método según la primera implementación de la presente invención detecta un cambio entre la segunda palabra de control del Mensaje de control de titularidad previo y la primera palabra de control del nuevo Mensaje de control de titularidad. Es preciso tener en cuenta la corriente doble en el análisis: el Mensaje de control de derecho de titularidad previo se elige según un orden predeterminado. La segunda implementación permite evitar tal precaución.

[0093] No obstante, si un pirata informático hackea la tarjeta inteligente con un número elevado de Mensajes de Control de Titularidad de ataque que sean relativamente similares, el método según la primera implementación permite detectar un elevado número de cambios entre la segunda palabra de control del Mensaje de control de titularidad previo y la primera palabra de control del nuevo Mensaje de control de titularidad. El método de la segunda implementación puede que no detecte ningún cambio en los identificadores de canal.

[0094] Como se ilustra en las FIG. 5A y FIG. 5B, los Mensajes de control de derecho de titularidad pueden comprender tanto el identificador de canal (51_n, 51_{n+1}) como la segunda palabra de control encriptada (53_n, 53_{n+1}). Tanto la comparación de la primera implementación como la comparación de la segunda implementación pueden realizarse como un análisis de la secuencia de mensajes de comando.

[0095] El análisis se puede realizar en cualquiera de los otros mensajes recibidos en la tarjeta inteligente, por ejemplo EMM o mensajes de reinicio. El análisis puede consistir en la comparación de un contenido determinado, por ejemplo un identificador de canal, o una información extraída, por ejemplo una palabra de control, de dos mensajes de comando. Si el contenido determinado/información extraída comparados son diferentes, el registro de errores puede ser incrementado. Se puede aplicar una penalización dependiente de un valor del registro de errores. La aplicación de una penalización por lo general comprende la introducción de un tiempo muerto con cada procesamiento de un Mensaje de control de titularidad.

[0096] Gestión de tiempos muertos

[0097] La FIG. 6A ilustra una posible secuencia de valores de un registro de errores en un módulo de seguridad portátil según la presente invención.

[0098] La FIG. 6B ilustra una posible secuencia de valores de la duración de un tiempo muerto en un módulo de seguridad portátil según la presente invención. La secuencia de tiempo muerto de la FIG. 6B corresponde a la secuencia de registro de errores de la FIG. 6A.

[0099] Ambas secuencias tienen la función de varios Mensajes de Control de Titularidad recibidos después de un reinicio.

[0100] Las secuencias ilustradas se pueden observar en una configuración de divisor, o cuando el abonado regular cambia con frecuencia de canal. Un análisis de los Mensajes de Control de Titularidad recibidos permite detectar diferencias en la comparación de un contenido determinado/información extraída de los Mensajes de Control de Titularidad recibidos consecutivamente. Por lo tanto, durante una primera fase 61 posterior al reinicio, el registro de errores aumenta regularmente, por ejemplo con cada recepción de un Mensaje de control de derecho de titularidad.

[0101] En el ejemplo ilustrado en las FIG. 6A y FIG. 6B, el tiempo muerto tiene una duración igual a cero si el valor del registro de errores es más pequeño que el valor de umbral mínimo C_min_thr, para evitar perjudicar al abonado regular que cambia de un canal a otro canal.

[0102] Durante una segunda fase 62, el valor del registro de errores se iguala con el umbral mínimo C_min _thr; la duración del tiempo muerto es, por lo tanto, no nulo y aumenta con el valor del registro de errores. No obstante, la duración del tiempo muerto sigue siendo más corta que un valor de tiempo máximo τ_max correspondiente a un valor de umbral máximo C_max_thr del registro de errores. El valor de tiempo máximo τ_max es lo suficientemente alto como para evitar que la tarjeta inteligente procese más de un Mensaje de control de titularidad durante un único criptoperiodo. En caso de que se produzca una corriente doble, donde un descodificador determinado manda un número concreto de Mensajes de Control de Titularidad en cada criptoperiodo, el valor de tiempo máximo τ_max tiene un valor lo suficientemente alto como para evitar el procesamiento del número concreto de Mensajes de Control de Titularidad desde una pluralidad de descodificadores. Por regla general, es posible que la tarjeta inteligente sólo procese un número concreto de Mensajes de Control de Titularidad por criptoperiodo.

[0103] Si el tiempo muerto tiene una duración que iguala sustancialmente a la del valor de tiempo máximo, la tarjeta inteligente no permite la descodificación de una pluralidad de información audiovisual codificada por una pluralidad de descodificadores. Al menos un usuario desautorizado, o un abonado que comparte su tarjeta inteligente con el(los) usuario(s) desautorizado(s), puede ver que le desaparezca la imagen de la pantalla.

[0104] Un abonado regular que cambia a menudo de un canal a otro canal puede provocar un aumento del tiempo muerto y que desaparezca la imagen de la pantalla durante un criptoperiodo tras cambiar nuevamente de canal. Es probable que el abonado regular atribuya la desaparición de la imagen de la pantalla a un problema de difusión y, como consecuencia, trate de ver otro canal,aumentando así el valor del registro de errores. En el ejemplo que se ilustra en la FIG. 6A, el valor del registro de errores puede estar siempre por debajo de un valor máximo C_max, para evitar castigar en exceso la tarjeta inteligente. No obstante, parámetros como el valor de tiempo máximo τ_max o el valor de umbral mínimo C_min_thr etc. pueden ser elegidos de forma legal para evitar que desaparezca la imagen de la pantalla en el caso de los abonados regulares.

[0105] El registro de errores puede seguir aumentando durante una tercera fase 63 incluso cuando la duración del tiempo muerto es igual al valor de tiempo máximo T_max, particularmente en el caso de la configuración de divisor.

[0106] El registro de errores puede estar basado en un principio circular: los aumentos prematuros que se generan por Mensajes de Control de Titularidad antiguos son eliminados. Por ejemplo, un registro circular con un tamaño determinado se puede utilizar para evaluar el registro de errores. Cada vez que se realiza el análisis, los valores binarios del registro circular son desplazados hacia la izquierda. El valor binario ubicado anteriormente en el extremo izquierdo del registro circular, por lo tanto, se elimina. Un valor binario nuevo que depende del resultado del análisis se escribe ahora en el hueco del extremo derecho del registro circular. Por lo general, se escribe un ' 1' si se detectan diferencias en la comparación de un contenido determinado/información extraída de los Mensajes de Control de Titularidad analizados, y un ' 0' si no se detectan diferencias.

[0107] El registro de errores puede tener un valor igual a la suma de los valores binarios del registro circular. El valor del registro de errores es, por lo tanto, siempre más pequeño o igual a un máximo que corresponde al tamaño del registro circular: si es igual, todas las ubicaciones del registro circular se rellenan con un ' 1'. El máximo puede ser el valor máximo C_max representado en la FIG. 6A.

[0108] El valor del registro de errores también puede disminuir si no se vuelven a detectar diferencias en la comparación de un contenido determinado/información extraída de los Mensajes de Control de Titularidad analizados, como se representa en la FIG. 6A. La dismunición puede deberse a varias cuestiones. En el caso de una configuración de divisor, los usuarios desautorizados pueden apagar sus descodificadores. Es posible que el abonado regular ya no cambie de canal etc.

[0109] De forma alternativa, el registro de errores puede ser un único número entero que se incrementa o disminuye dependiendiendo del resultado del análisis de la secuencia de mensajes de comando.

[0110] Mientras el valor del registro de errores sea superior al umbral de disminución, por ejemplo el valor de umbral máximo C_max_thr, la duración del tiempo de muerto permanecerá igual al valor de tiempo máximo T_max.

[0111] Cuando, en una cuarta fase 64, el valor de registro de errores es más pequeño que el valor de umbral máximo C_max_thr, la duración del tiempo muerto empieza a disminuir.

[0112] En el caso de una configuración de divisor, si el usuario desautorizado mantiene su descodificador en la tercera fase 63, la duración del tiempo muerto permanece en el valor de tiempo máximo τ_max. Si el usuario desautorizado apaga su descodificador en la cuarta fase 64, el registro de errores comienza a incrementarse de nuevo (secuencia no representada).

[0113] El usuario desautorizado también puede reiniciar la tarjeta inteligente en la tercera fase para restablecer el valor de la duración del tiempo muerto. El valor de la duración del tiempo muerto y el valor del registro de errores puede de hecho ser almacenado en una memoria no permanente que se elimina al reiniciar.

[0114] La FIG. 6C ilustra un ejemplo de una secuencia de valores de la duración del tiempo muerto de un módulo de seguridad portátil según la presente invención. La secuencia está representada como una función de varios Mensajes de Control de Titularidad recibidos después de un reinicio. A diferencia de la secuencia de ejemplo ilustrada en la FIG. 6B, la secuencia de ejemplo de la FIG. 6C tiene un valor no nulo inmediatamente después del reinicio. Se puede introducir un tiempo muerto de reinicio con cada procesamiento de un Mensaje de control de titularidad después del reinicio. El tiempo muerto de reinicio tiene una duración que depende del número de Mensajes de Control de Titularidad recibidos en la tarjeta inteligente después del reinicio. La duración del tiempo muerto de reinicio es igual a un primer valor de tiempo de reinicio τ_reset_max en un primer procesamiento inmediatamente posterior al reinicio y disminuye con el número de Mensajes de Control de Titularidad recibidos.

[0115] La introducción del tiempo muerto de reinicio y la introducción del tiempo muerto puede implementarse en un programa de software único: el total de un tiempo muerto puede ser igual a la suma del tiempo muerto de reinicio que se puede leer en una EEPROM y del tiempo muerto que se evalúa en un registro circular almacenado en una memoria no permanente.

[0116] El procesamiento de una tarjeta inteligente, por lo tanto, se ve ralentizado por el tiempo muerto de reinicio cuando se produce un reinicio.

[**0117]** El primer valor de tiempo de reinicio τ_reset_max es preferiblemente inferior que el valor de tiempo máximo τ_max del tiempo muerto, para evitar perjudicar a un abonado regular después de un reinicio regular, por ejemplo un reinicio debido a un apagón.

[0118] Como el primer valor de tiempo de restablecimiento τ_reset_max es inferior que el valor de tiempo máximo τ_max, un usuario desautorizado puede tratar de reiniciar la tarjeta inteligente cada vez que la descodificación de la información audiovisual codificada no funcione correctamente. Un pirata informático puede incluso provocar un reinicio de la tarjeta inteligente más o menos en cada criptoperiodo, para permitir una descodificación correcta o con el fin de realizar un ataque .

[0119] Bloqueo de tarjeta inteligente

[0120] La FIG. 7 ilustra un ejemplo de un algoritmo que es implementado en un módulo de seguridad portátil según la presente invención. El algoritmo de la FIG. 7 permite evaluar la naturaleza de otro reinicio posterior según un grupo intermedio de mensajes de comando intermedios. El grupo intermedio comprende una secuencia de mensajes de comando, por ejemplo Mensajes de control de titularidad, recibidos después de un reinicio previo al reinicio posterior .

[0121] Cuando se recibe un mensaje en la tarjeta inteligente, la tarjeta inteligente evalúa si el mensaje es un ECM o no (caja 71). Si el mensaje es un ECM, la tarjeta inteligente procesa el Mensaje de control de titularidad, por ejemplo la tarjeta inteligente desencripta una palabra de control encriptada comprendida en el Mensaje de control de titularidad. Varios mensajes de comando intermedios son contabilizados a través del aumento de un registro de recuento nb_ECM después cada procesamiento (caja 72).

[0122] El número de mensajes de comando intermedios es comparado con el umbral de reinicio nb_ECM_min (caja 73). El resultado de la comparación permite evaluar la naturaleza del reinicio posterior: si el registro de recuento nb_ECM iguala el umbral de reinicio nb_ECM_min, un indicador que tiene un valor NOK, por ejemplo ' 0', después de cada restablecimiento (caja 75) se fija en el valor OK, por ejemplo ' 1' (caja 74).

[0123] Si el registro de recuento nb_ECM es superior al de umbral de reinicio nb_ECM_min, el indicador ya tendría un valor OK. Si el registro de recuento nb_ECM es inferior al umbral de reinicio nb_ECM_min, el indicador tiene un valor NOK. El valor del indicador, por lo tanto, indica si el número de mensajes de comando intermedios es superior al umbral de reinicio nb_ECM_min o no. El valor del indicador se almacena en una memoria permanente. Cuando tiene lugar un

reinicio posterior (caja 76), el valor del indicador es leído y comparado con el valor NOK (caja 77).

[0124] Si el indicador tiene un valor favorable (OK), es decir si la tarjeta inteligente ha recibido más Mensajes de Control de Titularidad que el umbral de reinicio nb_ECM_min desde el reinicio previo, el reinicio posterior se evalúa como regular. El indicador es reiniciado al valor NOK de nuevo (caja 75) y la tarjeta inteligente espera la recepción de un mensaje nuevo (caja 78). Se procesa cada ECM nuevo (caja 72) y el indicador mantiene el valor NOK hasta que el umbral de reinicio nb_ECM_min de Mensajes de Control de Titularidad se recibe y se procesa, como se describe en un párrafo anterior .

[0125] Si el valor del indicador es NOK, es decir el número de mensajes de comando intermedios es más pequeño que el umbral de reinicio nb_ECM min desde el reinicio previo, el reinicio posterior se evalúa como sospechoso. El registro de errores de reinicio nb_reset_off aumenta (caja 79) y su valor es comparado con un umbral de errores de reinicio reset_max (caja 710).

[0126] Si el valor del registro de errores de reinicio nb_reset_off iguala el umbral de errores de reinicio reset_max, la tarjeta inteligente es bloqueada (caja 711). Si el valor del registro de errores de reinicio nb_reset_off es inferior al umbral de errores de reinicio reset_max, la tarjeta inteligente espera la recepción de mensaje (caja 78) y además cuenta los mensajes de comando intermedios. El valor del registro de errores de reinicio nb_reset_off puede no ser superior al umbral de errores de reinicio reset_max, ya que la tarjeta inteligente se bloquea cuando el valor del registro de errores de reinicio nb_reset_off iguala el umbral de errores de restablecimiento reset_max.

[0127] Tal algoritmo permite penalizar a un usuario desautorizado que reinicia la tarjeta inteligente cada vez que la información audiovisual codificada se descodifica de forma incorrecta, o que reinicia automáticamente la tarjeta inteligente tras un pequeño número de criptoperiodos.

[0128] Este algoritmo también permite bloquear una tarjeta inteligente que recibe órdenes de ataque con un reinicio entre ellas.

[0129] Parámetros como el umbral de errores de reinicio reset_max, el número umbral de reinicio nb_ECM_min etc. pueden tener valores adecuados que se adaptan a posibles comportamientos de un abonado regular, de un usuario desautorizado y de un pirata informático.

[0130] Cualquier otro algoritmo para administrar penalizaciones pueden ser aplicado a la tarjeta inteligente: por ejemplo, la tarjeta inteligente puede bloquearse cuando el valor del registro de errores alcanza un valor límite, que ha de ser superior al valor de umbral máximo C_max_thr.

[0131] El análisis de la secuencia de mensajes de comando puede consistir preferiblemente en la comparación de un Mensaje de control de titularidad nuevo con un Mensaje de control de tutoralidad previo. De forma alternativa, los EMM, los mensajes de reinicio, o cualquier otro mensaje recibido en la tarjeta inteligente pueden ser analizados. El análisis de la secuencia de mensajes de comando también puede consistir en el recuento de varios mensajes de comando intermedios entre dos reinicios para evaluar la naturaleza de un reinicio previo.

[0132] El análisis ha de ser ser preferiblemente una combinación del análisis descrito anteriormente: por ejemplo, cada Mensaje de control de titularidad se compara con un Mensaje de control titularidad previo y se contabiliza el número de Mensajes de Control de Titularidad entre dos reinicios, para fortalecer la seguridad de la tarjeta inteligente. Otro ejemplo de combinación del análisis anteriormente descrito consiste en la comparación de cada nuevo ECM con un ECM previo, cada EMM nuevo con un EMM previo, y cada nuevo mensaje de comando con un mensaje de comando previo. Los ECM, los EMM y los otros mensajes de comando se podrán contar para evaluar los reinicios. Preferiblemente se implementarán tres sistemas de recuento diferentes, para facilitar la completa comprensión de un comportamiento del usuario y, como consecuencia, aplicar la penalización adecuada.

[0133] Preferiblemente, la penalización que se aplica en la tarjeta inteligente permitirá interrumpir el procesamiento de los ECM. La penalización también permite interrumpir el procesamiento de un EMM, la recepción de mensajes en la tarjeta inteligente, o cualquier otra acción de la tarjeta inteligente.

[0134] El alcance de la presente invención también comprende un software que permite implementar el método según la presente invención.

[0135] El software podrá descargarse durante el proceso de fabricación del módulo de seguridad portátil. De forma alternativa, se recibirá al menos un mensaje de configuración en el módulo de seguridad portátil si ya está siendo usado por un abonado, permitiendo así descargar el software. El alcance de la presente invención cubre ambos métodos.

REIVINDICACIONES

1. Método para asegurar un módulo de seguridad portátil que se usa junto a un elemento de descodificación, de tal manera que el módulo de seguridad portátil y el elemento de descodificación permiten descodificar información audiovisual codificada que se organiza en una pluralidad de canales; el método comprende:
el procesamiento en el módulo de seguridad portátil de los Mensajes de Control de Titularidad (ECM) recibidos en dicho módulo para permitir la descodificación de la información audiovisual codificada;
el método se caracteriza además por el hecho comprender además:
el análisis (402) en el módulo de seguridad portátil de una secuencia de ECM, que comprende un nuevo ECM y un ECM previo recibido; los ECM de la secuencia se recibirían en el módulo de seguridad portátil en momentos diferentes, el análisis se realizaría en el momento de la recepción del nuevo ECM y determina si el nuevo ECM y el ECM previo pertenecen a un canal diferente;
en un evento positivo, el aumento del registro de errores durante el análisis;
la aplicación de una penalización al módulo de seguridad portátil dependiendo del valor del registro de errores mediante la introducción de un tiempo muerto en el procesamiento para ralentizar el procesamiento (404).

2. Método según la reivindicación 1, donde el tiempo muerto tiene una duración que depende del valor del registro de errores (404).

3. Método según la reivindicación 1 o 2, donde la duración del tiempo muerto es más corta que un valor de tiempo máximo;
el valor de tiempo máximo es lo suficientemente alto como para evitar que el módulo de seguridad portátil (31) procese más de un ECM durante un único criptoperiodo.

4. Método según cualquiera de las reivindicaciones 1 a 3, donde:
cada ECM (54_n, 54_{n+1}) comprende un identificador de canal (51_n, 51_{n+1}), el cual se asocia a un canal determinado;
el análisis de la secuencia de ECM comprende la comparación del identificador de canal 51_{n+1} del nuevo ECM 54_{n+1} y el identificador de canal 51_n del ECM 54_n previo.

5. Método según cualquiera de las reivindicaciones 1 a 3, donde:
cada ECM (54_n, 54_{n+1}) comprende una primera palabra de control encriptada (52_n, 52_{n+1}) y una segunda palabra de control encriptada (53_n .53_{n+1});
la primera palabra de control permite descodificar la información audiovisual codificada durante un primer criptoperiodo;
la segunda palabra de control permite descodificar la información audiovisual codificada durante un segundo criptoperiodo inmediatamente posterior al primer criptoperiodo;
el análisis de la secuencia de ECM comprende la comparación de una segunda palabra de control 53_n del ECM 54_n previo con una primera palabra de control 52_n del nuevo ECM 54_{n+1}.

6. Método según cualquiera de las reivindicaciones 1 a 5, que comprende además:
la introducción, durante un reinicio, de un tiempo muerto de reinicio con cada procesamiento de los ECM, donde:
el tiempo muerto de reinicio tiene una duración que depende del número ECM recibidos en el módulo de seguridad portátil después del reinicio, si dicha duración es igual a un primer valor de tiempo de reinicio en un primer procesamiento inmediatamente posterior al reinicio el primer valor de tiempo de reinicio es inferior al valor de tiempo máximo.

7. Método según cualquiera de las reivindicaciones 1 a 6, que comprende además:
una evaluación de la naturaleza de un reinicio posterior según un grupo intermedio de ECM intermedios, que comprende los ECM recibidos después de un reinicio previo anterior al reinicio posterior .

8. Método según la reivindicación 7, que comprende además: el recuento del número de ECM intermedios (72); la comparación del número de ECM intermedios con el umbral de reinicio (73), donde el resultado de la comparación permite evaluar la naturaleza de un reinicio posterior; el aumento del registro de errores de reinicio durante un reinicio (79) si el reinicio es evaluado como sospechoso; el bloqueo del módulo de seguridad portátil (711) si el registro de errores de reinicio tiene un valor superior al umbral de errores de reinicio.

9. Módulo de seguridad portátil (31) que se usa con un elemento de descodificación, donde el módulo de seguridad portátil y el elemento de descodificación permiten descodificar información audiovisual codificada que se organiza en una pluralidad de canales; el módulo de seguridad portátil comprende:
sistemas de recepción para recibir Mensajes de Control de Titularidad (ECM);
sistemas de procesamiento (32) para procesar un ECM recibido en módulo de seguridad portátil para permitir la descodificación de la información audiovisual codificada;
el módulo de seguridad portátil que se caracteriza además por el hecho de que comprende:
una memoria de mensajes de comando (36) en la que se puede almacenar al menos un identificador perteneciente a un canal concreto de un ECM (ECM_n) recibido
sistemas de análisis (35) para analizar una secuencia de ECM, que comprende un nuevo ECM y un ECM previo recibido; los ECM de la secuencia serían recibidos en el módulo de seguridad portátil en momentos diferentes, y el

análisis se realizaría con cada recepción de un nuevo ECM (ECM_{n+1}); sistemas de comparación para determinar si el ECM y el ECM previo pertenecen a un canal diferente; un registro de errores (37); sistemas de incremento para incrementar el registro de errores cuando ambos ECM están relacionados con un canal diferente; medios de retraso para introducir un tiempo muerto con cada procesamiento para ralentizar el mismo.

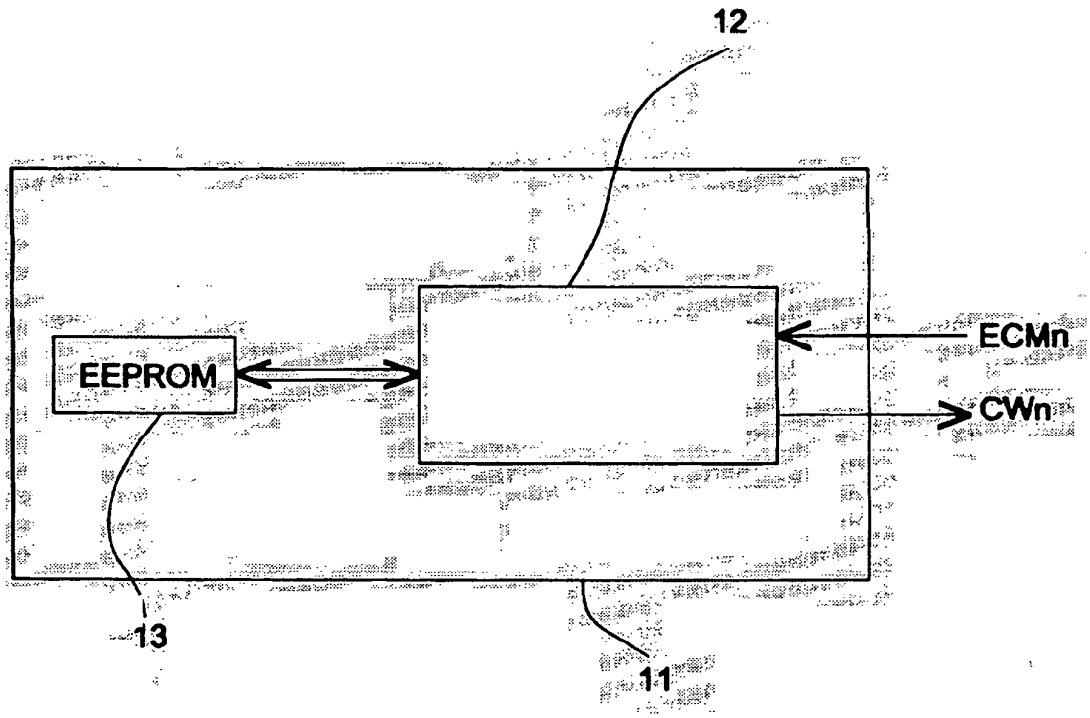
10. Módulo de seguridad portátil (31) según la reivindicación 9, donde: los sistemas de retraso también permiten introducir un tiempo muerto de reinicio con cada procesamiento después del reinicio; el tiempo muerto de reinicio tiene una duración que depende del número de procesamientos que tienen lugar después del reinicio, la duración es igual a un primer valor de tiempo de reinicio en un primer procesamiento inmediatamente posterior al reinicio.

11. Módulo de seguridad portátil (31) según las reivindicaciones 9 o 10, que comprende además: un registro de recuento que permite memorizar varios ECM intermedios, que se reciben en el módulo de seguridad portátil después de un reinicio previo; un indicador, cuyo valor depende del resultado de la comparación del registro de recuento con el umbral de reinicio; un registro de errores de reinicio que aumenta dependiendo del valor del indicador en caso de reinicio; sistemas de bloqueo para bloquear el módulo de seguridad portátil según el valor del registro de errores de reinicio.

12. Módulo de seguridad portátil según cualquiera de las reivindicaciones 9 a 11, donde la determinación de que dos ECM pertenecen al mismo canal se basa en un identificador de canal extraído del ECM.

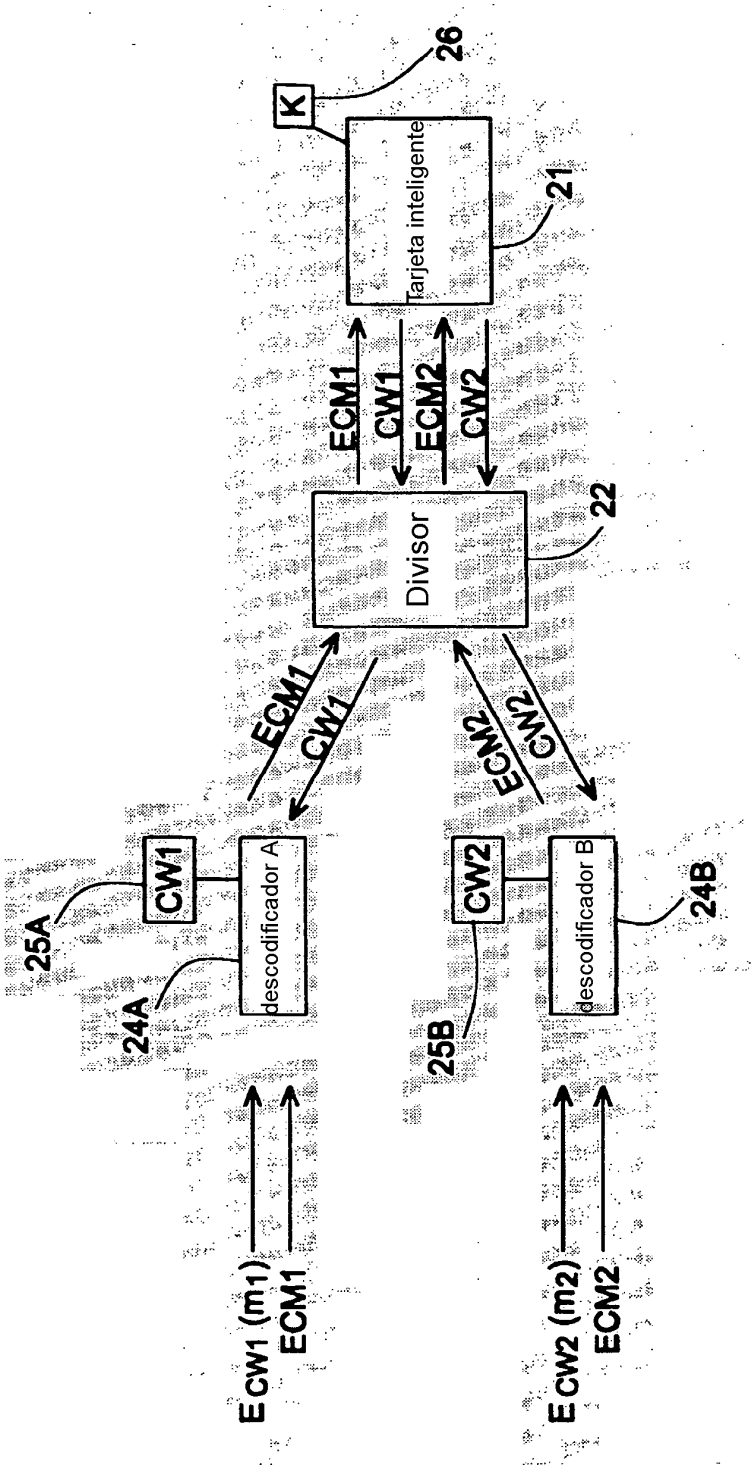
13. Módulo de seguridad portátil según cualquiera de las reivindicaciones 9 a 11, donde la determinación de que dos ECM pertenecen al mismo canal se basa en palabra de control extraída del ECM.

14. Programa informático que se usa dentro de un módulo de seguridad portátil, donde el programa informático implementa el método según cualquiera de las reivindicaciones 1 a 8.



Estado de la técnica

FIG.1



Estado de la técnica

FIG.2

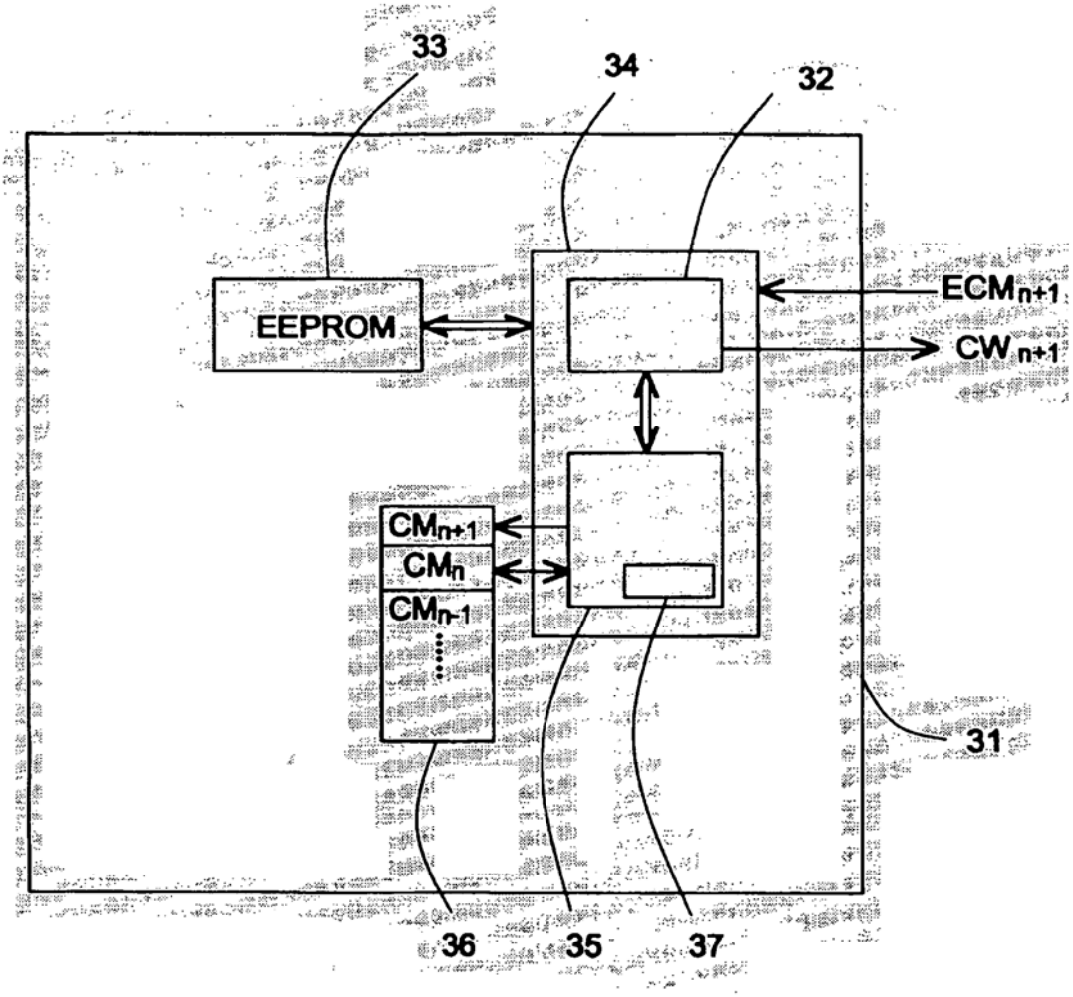


FIG.3

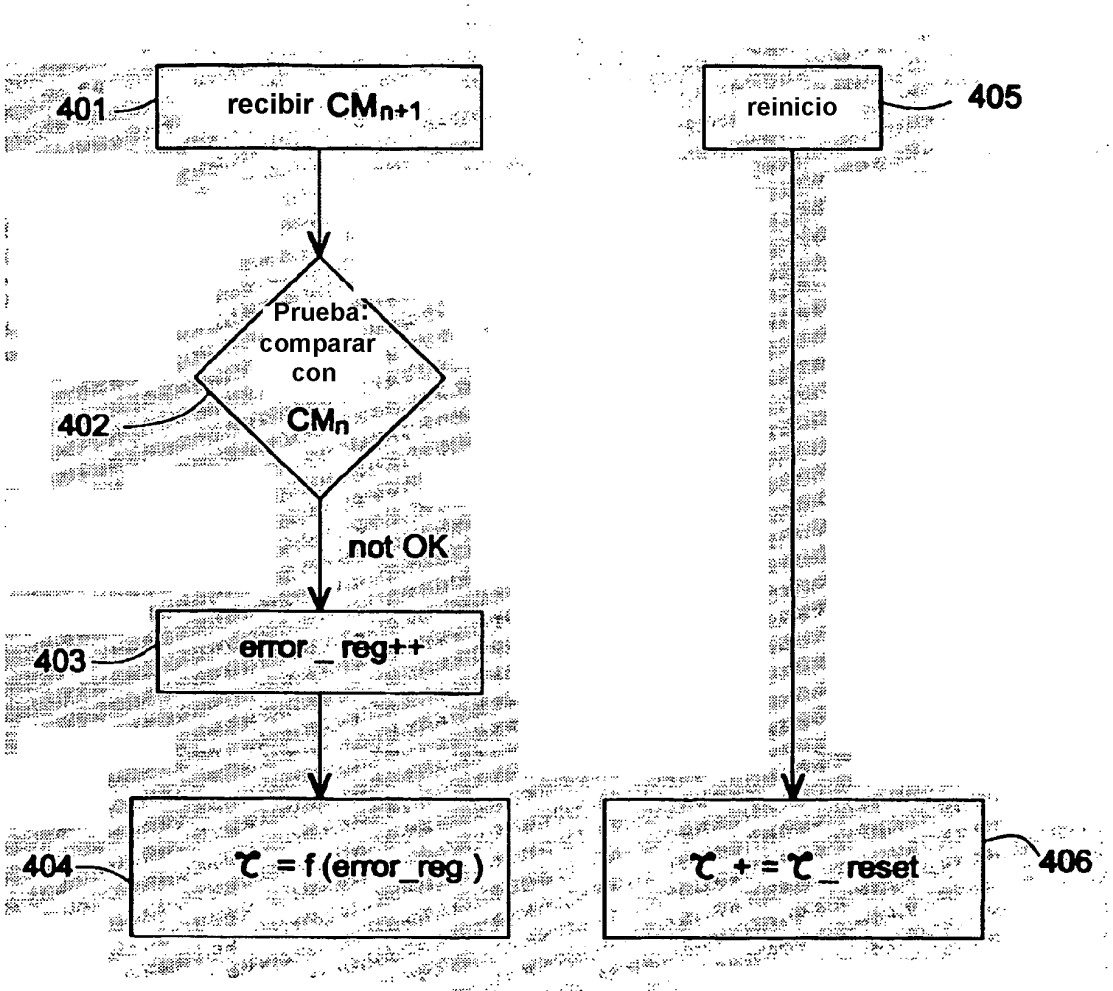

401
recibir CM_{n+1}
reinicio
405
Prueba: comparar con CM_n
402
not OK
403
error_reg++
404
τ = f (error_reg)
τ += τ _reset
406

FIG.4

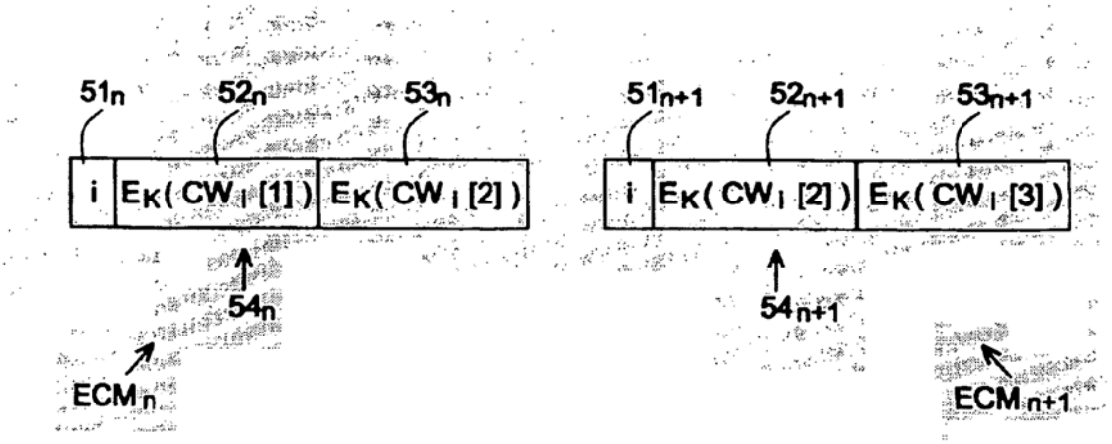

51n
52n
53n
i
EK(CW i [1])
EK(CW i [2])
54n
ECM n
51n+1
52n+1
53n+1
i
EK(CW i [2])
EK(CW i [3])
54n+1
ECM n+1

FIG.5A

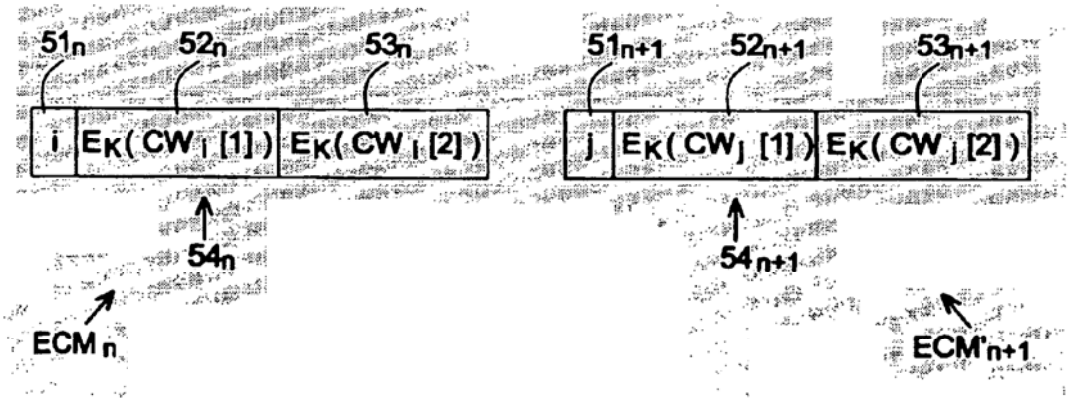

51n
52n
53n
i
EK(CW i [1])
EK(CW i [2])
54n
ECM n
51n+1
52n+1
53n+1
j
EK(CW j [1])
EK(CW j [2])
54n+1
ECM'n+1

FIG.5B

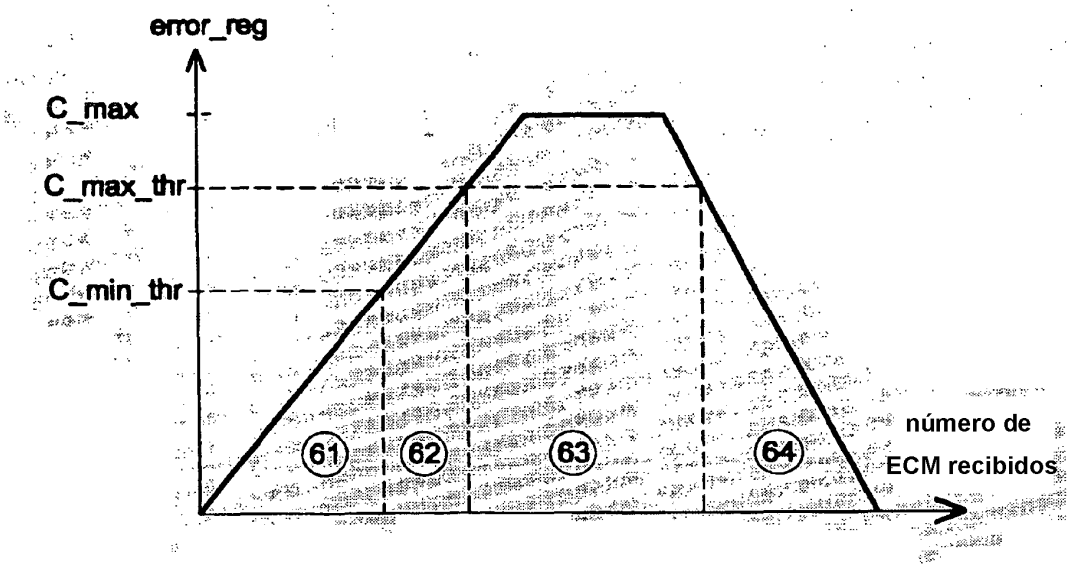

error_reg
C_max
C_max_thr
C_min_thr
61
62
63
64
número de
ECM recibidos

FIG.6A

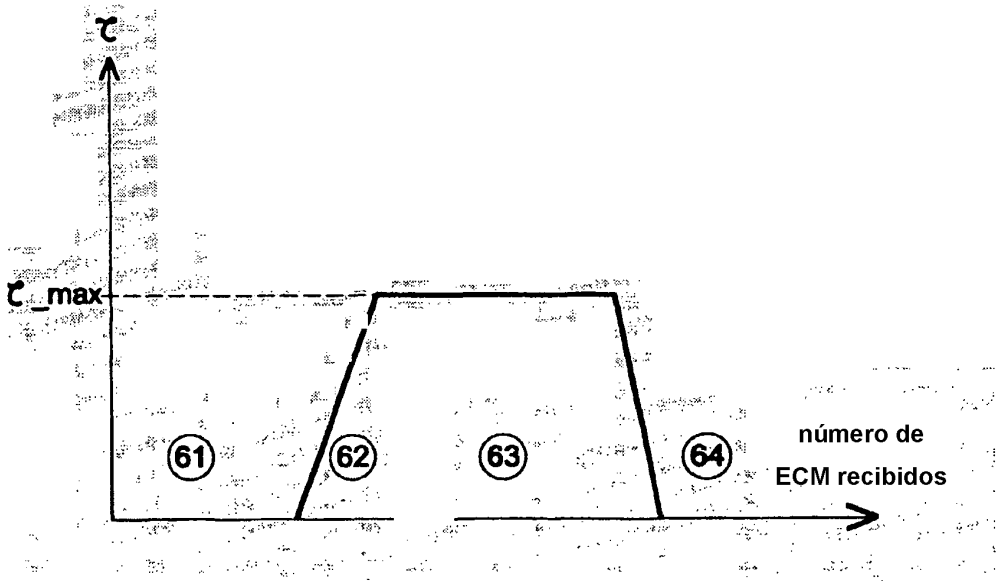

τ
τ_max
61
62
63
64
número de
ECM recibidos

FIG.6B

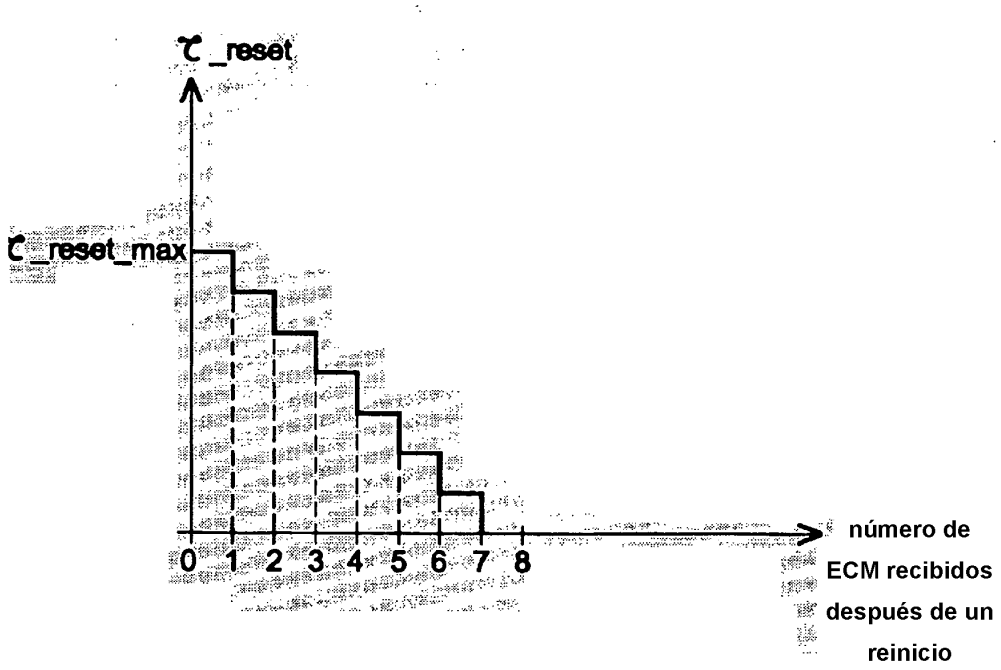

τ_reset
τ_reset_max
0
1
2
3
4
5
6
7
8
número de ECM recibidos después de un reinicio

FIG.6C

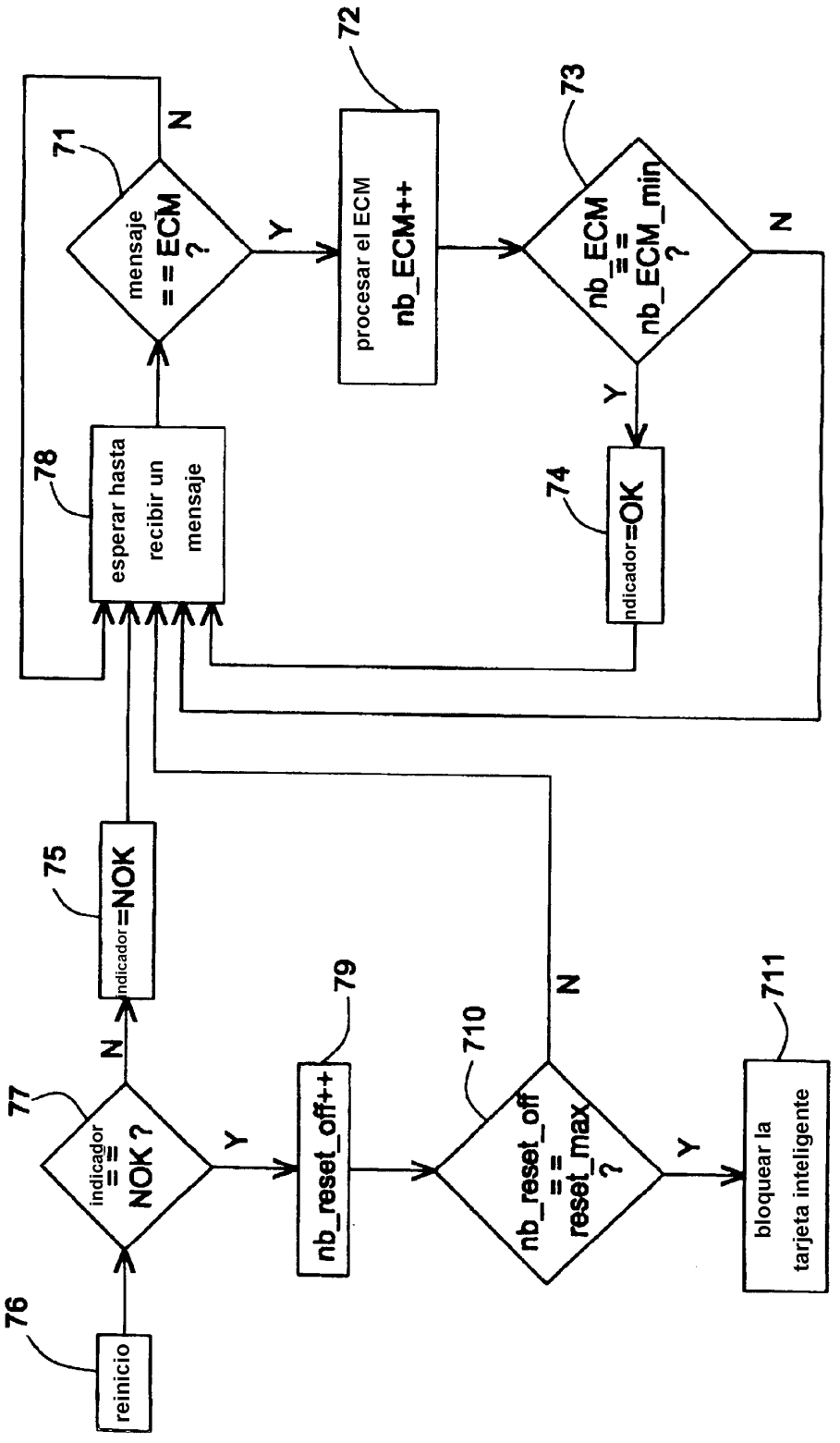

76
reinicio
77
indicador == NOK ?
N
Y
75
indicador=NOK
78
esperar hasta recibir un mensaje
71
mensaje == ECM ?
N
Y
72
procesar el ECM
nb_ECM++
73
nb_ECM == nb_ECM_min ?
N
Y
74
indicador=OK
79
nb_reset_off++
710
nb_reset_off == reset_max ?
N
Y
711
bloquear la tarjeta inteligente

FIG.7