(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 693 064**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2011 PCT/EP2011/073148**

(87) Fecha y número de publicación internacional: **05.07.2012 WO12089542**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2011 E 11802707 (7)**

(97) Fecha y número de publicación de la concesión europea: **15.08.2018 EP 2659613**

(54) Título: **Procedimiento de transmisión y de recepción de un contenido multimedia**

(30) Prioridad:

29.12.2010 FR 1061339

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.12.2018

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
92057 Paris La Défense, FR

(72) Inventor/es:

HAMON, VINCENT y
DUBROEUCQ, GILLES

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento de transmisión y de recepción de un contenido multimedia

La invención se refiere a un procedimiento de transmisión y de recepción de un contenido multimedia. La invención se refiere igualmente a un procedimiento de generación de mensajes ECM y a un procedimiento de recepción de mensajes ECM. La invención se refiere finalmente a un emisor, un terminal de recepción y un soporte de registro de informaciones para la implementación de estos procedimientos.

La invención se aplica en particular al campo del control de acceso para el suministro de programas multimedia de pago tales como la televisión de pago.

En esta descripción, se designa más específicamente por “contenido multimedia” a un contenido de audio y/o visual destinado a ser restituido en una forma directamente perceptible y comprensible por un ser humano. Típicamente, un contenido multimedia corresponde a una sucesión de imágenes que forman una película, una emisión de televisión o publicidad. Un contenido multimedia puede ser igualmente un contenido interactivo tal como un juego.

Para asegurar y someter la visualización de los contenidos multimedia a ciertas condiciones, como la suscripción de un abono de pago por ejemplo, los contenidos multimedia se difunden en forma encriptada y no en claro. En la presente descripción, el canal se dice “encriptado” cuando el contenido multimedia difundido en este canal está encriptado.

Más precisamente, cada contenido multimedia se divide en una sucesión de criptoperiodos. Durante toda la duración de un criptoperiodo, las condiciones de acceso al contenido multimedia encriptado permanecen sin cambios. En particular, durante toda la duración de un criptoperiodo, el contenido multimedia se encripta con la misma palabra de control. En general, la palabra de control varía de un criptoperiodo a otro.

Además, la palabra de control es generalmente específica de un contenido multimedia, siendo extraída esta última aleatoriamente o seudo-aleatoriamente. De ese modo, si en un instante dado, se difunden simultáneamente N contenidos multimedia, en N canales, existen N palabras de control diferentes e independientes empleadas cada una para encriptar uno de estos contenidos multimedia.

En este caso, los términos “encriptar” y “cifrar” se consideran como sinónimos. Es lo mismo para los términos “desencriptar” y “descifrar”.

El contenido multimedia en claro corresponde al contenido multimedia antes de que este sea encriptado. Este puede convertirse directamente en compresible para un ser humano sin tener que recurrir a operaciones de desencriptado y sin que su visualización esté sometida a ciertas condiciones.

Las palabras de control necesarias para desencriptar los contenidos multimedia se transmiten de manera sincronizada con los contenidos multimedia. Por ejemplo, las palabras de control necesarias para desencriptar el t-ésimo criptoperiodo se reciben por cada terminal durante el (t-1)-ésimo criptoperiodo. Para ello, por ejemplo, las palabras de control se multiplexan con el contenido multimedia encriptado.

Para asegurar la transmisión de las palabras de control, estas se transmiten a los terminales en la forma de criptogramas contenidos en unos mensajes ECM (Entitlement Control Message). Se designa en este caso por “criptograma” una información insuficiente por sí misma para encontrar la palabra de control en claro. De ese modo, si se intercepta la transmisión de la palabra de control, el único conocimiento del criptograma de la palabra de control no permite encontrar la palabra de control que permita desencriptar el contenido multimedia.

Para encontrar la palabra de control en claro, es decir la palabra de control que permita desencriptar directamente el contenido multimedia, esta debe combinarse con una información secreta. Por ejemplo, el criptograma de la palabra de control se obtiene cifrando la palabra de control en claro con una clave de explotación y un algoritmo de cifrado. En este caso, la información secreta es la clave de explotación utilizada y/o un algoritmo de descifrado que permita descifrar el criptograma.

La información secreta debe preservarse en lugar seguro. Para ello, ya se ha propuesto almacenar la información secreta en un procesador de seguridad tales como una tarjeta de chips o incluso una tarjeta virtual. Por “tarjeta virtual” se designa un componente de software que comprende un conjunto de recursos entre los que está:

- el código ejecutable de un algoritmo de cifrado o de descifrado, y
- el código ejecutable de un analizador sintáctico para localizar un criptograma de una palabra de control en el interior de un mensaje ECM o el código ejecutable de un constructor sintáctico para construir un mensaje ECM, y
- eventualmente unos títulos de acceso,
- eventualmente una clave de explotación utilizada como parámetro del algoritmo de cifrado o de descifrado.

Un código ejecutable es un código directamente adecuado para ser ejecutado por un interpretador o máquina virtual de un nivel inferior implementado en un microprocesador. El algoritmo de cifrado o de descifrado y el analizador sintáctico forman típicamente un programa ejecutable o varios programas ejecutables.

En lo que sigue, se designa por “tarjeta virtual madre” una tarjeta virtual utilizada para calcular un mensaje ECM. Se designa por “tarjeta virtual hija” una tarjeta virtual utilizada para tratar un mensaje ECM recibido. Se dice que una tarjeta virtual madre y una tarjeta virtual hija están “asociadas” una a la otra si la tarjeta virtual hija permite tratar con éxito un mensaje ECM recibido, calculado con ayuda de la tarjeta virtual madre.

En este contexto, un procedimiento de transmisión y de recepción de un contenido multimedia en el que cada criptoperiodo CP_t está encriptado con ayuda de una palabra de control CW_t respectiva, conocido por el solicitante incluye:

- el cifrado, por un emisor, de la palabra de control CW_t con ayuda de una clave de explotación y de un código ejecutable de un algoritmo de cifrado contenidos en una tarjeta virtual madre para obtener un criptograma CW_t*,
- la generación de un mensaje ECM que incorpora el criptograma CW_t* con ayuda de un código ejecutable y un constructor sintáctico contenido en la tarjeta virtual madre y la transmisión de este mensaje ECM a un terminal,
- la recepción por el terminal del mensaje ECM, la localización de la posición del criptograma CW_t* en el mensaje ECM con ayuda de un código ejecutable de un analizador sintáctico, y posteriormente el descifrado del criptograma CW_t* con ayuda de una clave de explotación de un algoritmo de descifrado, estando contenidos en el código ejecutable del analizador sintáctico y del algoritmo de descifrado en una tarjeta virtual hija asociada a la tarjeta virtual madre, y el desencriptado del criptoperiodo CP_t del contenido multimedia encriptado con ayuda de la palabra de control descifrada CW_t.

La utilización de tarjetas virtuales permite sustituir a menor coste y rápidamente informaciones secretas en los terminales. Por ejemplo, la sustitución de una tarjeta virtual permite modificar el algoritmo de cifrado y de descifrado utilizado cuando se descubre un fallo de seguridad. Sin embargo, la utilización de una tarjeta virtual en sí misma no aporta ganancia de seguridad con relación a la utilización de una tarjeta de chips.

Del estado de la técnica se conocen igualmente:

- FR2922393A1,
- EP1320006A1,
- WO2009/112966A2, y
- US2009/080648A1.

La invención se dirige a incrementar la seguridad de los procedimientos de transmisión y de recepción de un contenido multimedia que utilice tarjetas virtuales.

La invención trata así sobre un procedimiento de transmisión y de recepción de un contenido multimedia de acuerdo con la reivindicación 1.

En el procedimiento presentado anteriormente, cambiando como mínimo cada dos horas de tarjetas virtuales madre e hija, se aumenta la variedad de las claves y de los algoritmos empleados lo que complica la recuperación de la información secreta por un usuario ilícito, y la compartición de esta información con otros usuarios piratas. En particular, en el procedimiento anterior, se hace más difícil la recuperación ilícita de informaciones secretas, no solamente por el cambio frecuente de la clave de explotación, sino también por el cambio frecuente del algoritmo de cifrado y/o del constructor sintáctico. Por ejemplo, la recuperación ilícita de la clave de explotación se hace más difícil porque cambiando el constructor sintáctico, se modifican el formato del mensaje ECM y, por ejemplo, el emplazamiento de esta clave en un mensaje ECM. De esa manera se hace más difícil para un pirata informático extraer correctamente de un mensaje ECCM el criptograma de esta clave. El cambio del algoritmo de cifrado hace la recuperación ilícita de la única clave de explotación inútil porque es necesario también recuperar el algoritmo de cifrado o de descifrado a utilizar con esta clave. Se incrementa por tanto la cantidad de informaciones a recuperar ilícitamente para desencriptar correctamente un contenido multimedia y, al mismo tiempo, se incrementa igualmente la frecuencia de renovación de estas informaciones. El trabajo de los piratas informáticos se hace por tanto más complejo y se incrementa por tanto la seguridad del procedimiento de transmisión y de recepción de contenidos multimedia.

Los modos de realización de este procedimiento pueden incluir la característica de la reivindicación dependiente.

Los modos de realización de este procedimiento presentan además la ventaja siguiente:

- la utilización combinada de un algoritmo de cifrado o de descifrado y de un constructor sintáctico permite cifrar una palabra de control y hacer variar el formato del mensaje ECM (por ejemplo la localización del criptograma de la palabra de control en el mensaje ECM), de manera que se hace más complejo para un usuario ilícito el descifrado de este mensaje ECM.

La invención se refiere igualmente a un procedimiento de generación de mensajes ECM de acuerdo con la reivindicación 3.

Los modos de realización de este procedimiento pueden incluir una o varias de las características de las reivindicaciones dependientes.

Los modos de realización de este procedimiento incluyen además las siguientes ventajas:

- cuando se transmite el identificador de la tarjeta virtual en un mensaje ECM, puede acelerarse la frecuencia de cambio de una tarjeta virtual por otra tarjeta virtual,
- cuando las tarjetas virtuales madre están previamente registradas se minimiza el tiempo de conmutación entre una tarjeta virtual madre precedente y una nueva tarjeta virtual madre, a nivel del emisor,
- cuando la tarjeta virtual madre se selecciona seudo-aleatoriamente, se aumenta la seguridad del procedimiento haciendo difícil para un usuario ilícito prever por adelantado cuál será la tarjeta virtual hija asociada a utilizar para descifrar un próximo criptograma, y
- las tarjetas virtuales hija están previamente registradas, se minimiza el tiempo de conmutación entre una tarjeta virtual hija precedente y una nueva tarjeta virtual hija, a nivel del terminal.

La invención se refiere igualmente a un procedimiento de recepción de acuerdo con la reivindicación 8.

Los modos de realización de este procedimiento pueden incluir una o varias de las características de las reivindicaciones dependientes.

Los modos de realización de este procedimiento incluyen además las ventajas siguientes:

- cuando el procedimiento comprende el mecanismo de instrucciones adicionales tal como se ha presentado más arriba, se asegura aún más el procedimiento.

La invención se refiere finalmente a un soporte de registro de informaciones, que incluye instrucciones para la ejecución de uno de los procedimientos presentados anteriormente, cuando estas instrucciones se ejecutan por un calculador electrónico.

La invención se refiere igualmente a un emisor de acuerdo con la reivindicación 13.

La invención se refiere finalmente a un terminal de recepción de acuerdo con la reivindicación 14.

Surgirán claramente otras características y ventajas de la invención de la descripción que se realiza en el presente documento a continuación, a título indicativo y en ningún caso limitativo, con referencia a los dibujos adjuntos, en los que:

- la figura 1 es una ilustración esquemática de un sistema de emisión y recepción de contenidos multimedia encriptados,
- la figura 2 es una ilustración esquemática de un módulo de cálculo para el sistema de emisión de la figura 1,
- la figura 3 es una ilustración esquemática de un circuito integrado para el sistema de emisión de la figura 1,
- las figuras 3a, 3b y 3c son ilustraciones esquemáticas de bases de datos y de una tabla de registros previos en memorias del circuito integrado de la figura 3,
- la figura 4 es una ilustración esquemática de una tarjeta virtual madre y de una tarjeta virtual hija asociadas,
- la figura 5 es un organigrama de un procedimiento de transmisión de un contenido multimedia encriptado en el sistema de la figura 1, y
- la figura 6 es un organigrama de un procedimiento de recepción de un contenido multimedia encriptado en el sistema de la figura 1.

En estas figuras, se utilizan las mismas referencias para designar los mismos elementos.

En lo que sigue de la presente descripción, no se describen en detalle las características y funciones bien conocidas para el experto en la materia.

Además, la terminología utilizada es la de los sistemas de acceso condicional a contenidos multimedia. Para más informaciones sobre esta terminología, el lector puede referirse al documento siguiente: “Functional Model of Conditional Access System”, EBU Review, Technical European Broadcasting Union, Bruselas, BE, n.º 266, 21 de diciembre de 1995.

La figura 1 representa un sistema 2 de emisión y de recepción de contenidos multimedia encriptados. En este caso, los contenidos multimedia están linearizados. Por “contenido multimedia linearizado” se designa un contenido multimedia para el que el usuario no controla el instante de transmisión. Por ejemplo, un contenido multimedia corresponde a una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

Los contenidos multimedia en claro se generan por una o varias fuentes 4 y se transmiten a un dispositivo 6 de difusión. El dispositivo 6 difunde los contenidos multimedia simultáneamente hacia una multitud de terminales de recepción a través de una red 8 de transmisión de informaciones. Los contenidos multimedia difundidos están temporalmente sincronizados entre sí para, por ejemplo, respetar una rejilla preestablecida de programas.

La red 8 es típicamente una red de transmisión de informaciones a gran distancia tal como la red de internet o una red por satélites o cualquier otra red de difusión tal como la utilizada para la transmisión de la televisión digital terrestre (TDT).

Para simplificar la figura 1, solo se representan tres terminales 10 a 12 de recepción.

El dispositivo 6 comprende un codificador 16 que codifica los contenidos multimedia que recibe. El codificador 16 trata unos contenidos multimedia digitales. Por ejemplo, este codificador funciona de acuerdo con la norma MPEG2 (Moving Picture Expert Group – 2) o la norma UIT-T H264.

Los contenidos multimedia denominados comprimidos así obtenidos se dirigen hacia una entrada 20 de un encriptador 22. El encriptador 22 encripta cada contenido multimedia comprimido para condicionar su visualización a ciertas condiciones tales como la compra de un título de acceso por los usuarios de los terminales de recepción. Los contenidos multimedia encriptados se restituyen en una salida 24 conectada a la entrada de un multiplexor 26. El encriptador 22 encripta cada contenido multimedia comprimido con ayuda de una palabra de control $CW_{i,t}$ que se le proporciona por un generador de palabras de control $CW_{i,t}$ 32. Típicamente, el encriptado está de acuerdo con una norma tal como la norma DVB-CSA (Digital Video Broadcasting – Common Scrambling Algorithm), ISMA Cryp (Internet Streaming Media Alliance Cryp), SRTP (Secure Real-time Transport Protocol), AES (Advanced Encryption Standard), etc.

El generador 32 se programa para:

- generar una palabra de control $CW_{i,t}$, y
- transmitir una palabra de control generada al encriptador 22 y a un sistema 28.

En este ejemplo, el generador 32 genera seudo-aleatoriamente una palabra de control $CW_{i,t}$. En este caso, el generador 32 está comprendido en el multiplexor 26.

En lo que sigue, el índice i es un identificador del canal en el que se difunde el contenido multimedia encriptado y el índice t es un número de orden que identifica el criptoperiodo encriptado con esta palabra de control.

El sistema 28 es más conocido bajo el acrónimo CAS (Conditional Access System). El sistema 28 se programa para:

- generar un criptograma $CW^*_{i,t}$ de una palabra de control $CW_{i,t}$ transmitida por el generador 32, y
- generar para cada canal i un mensaje $ECM_{i,t}$ (Entitlement Control Message) que contiene al menos el criptograma $CW^*_{i,t}$ de la palabra de control $CW_{i,t}$ utilizada por el encriptador 22 para encriptar el criptoperiodo t del canal i.

Los mensajes $ECM_{i,t}$ y los contenidos multimedia encriptados se multiplexan por el multiplexor 26 antes de transmitirse en la red 8.

El sistema 28 se detalla más adelante con referencia a la figura 2.

El mensaje ECM que contiene la palabra de control $CW_{i,t}$ se indica por $ECM_{i,t}$ en lo que sigue de la descripción en la que:

- el índice i identifica el canal, y
- el índice t es el número de orden que identifica la posición temporal de este mensaje ECM con relación a los otros mensajes ECM diferentes emitidos para desencriptar el canal i.

En este caso, el índice t identifica igualmente el criptoperiodo $CP_{i,t}$ desencriptable con ayuda de la palabra de control $CW_{i,t}$ contenida en el mensaje $ECM_{i,t}$. El índice t es único para cada criptoperiodo $CP_{i,t}$.

El mismo identificador i se inserta en todos los mensajes $ECM_{i,t}$ que contienen un criptograma $CW^*_{i,t}$ para el desencriptado de los contenidos multimedia difundidos en este canal i. A título de ilustración, en este caso, el desencriptado y el multiplexado de los contenidos multimedia está de acuerdo con el protocolo DVB-Simulcrypt (ETSI TS 103 197). En este caso, el identificador i puede corresponder a un par “channel ID/stream ID” único en el que se envían todas las solicitudes de generación de mensajes ECM para este canal.

En el ejemplo, los terminales 10 a 12 son idénticos. También, en lo que sigue solo se describe más en detalle el terminal 10.

El terminal 10 se describe aquí en el caso particular en el que este es capaz de desencriptar un único canal i a la vez. Con este fin, el terminal 10 incluye una única línea 60 de desencriptado que permite el desencriptado del canal i. Por ejemplo, la línea 60 desencripta el canal i para presentarlo en un visualizador 84.

Por ejemplo el visualizador 84, es un televisor, un ordenador o incluso un teléfono fijo o móvil, en este caso, el visualizador es un televisor.

La línea 60 comprende un receptor 70 de contenidos multimedia difundidos. Este receptor 70 se conecta a la entrada de un demultiplexor 72 que transmite por un lado el contenido multimedia a un desencriptador 74 y por otro lado los mensajes $ECM_{i,t}$ y EMM (Entitlement Management Message) a un circuito integrado 76.

El circuito 76 es adecuado para descifrar un criptograma $CW^*_{i,t}$ de una palabra de control $CW_{i,t}$ contenida en el mensaje $ECM_{i,t}$ y para proporcionar esta palabra de control al desencriptador 74. El circuito 76 se detalla más adelante con referencia a la figura 3.

El desencriptador 74 desencripta el contenido multimedia encriptado a partir de una palabra de control transmitida por el circuito 76. El contenido multimedia desencriptado se transmite a un decodificador 80 que lo decodifica. El contenido multimedia descomprimido o decodificado se transmite a una tarjeta gráfica 82 que controla la presentación de este contenido multimedia en el presentador 84 equipado con una pantalla 86. El presentador 84 presenta en claro el contenido multimedia en la pantalla 86.

El sistema 28 se describirá ahora con referencia a la figura 2.

El sistema 28 comprende una memoria no volátil 36. La memoria 36 contiene unas bases de datos 38 y 42.

Las bases de datos 38 constituye una relación que asocia a cada canal i, un conjunto E_i de tarjetas virtuales madre $CM_{Ei,k}$, en las que el índice Ei identifica el conjunto al que pertenece cada tarjeta virtual $CM_{Ei,k}$ y k es un número entero. La tarjeta virtual madre $CM_{Ei,k}$ se identifica mediante un identificador $ICM_{Ei,k}$ propio únicamente de esta tarjeta virtual madre. Con el fin de simplificar la figura 1, la base de datos 38 se ilustra solamente para dos canales 1 y 2. Los conjuntos E_1 y E_2 comprenden en este caso tres tarjetas virtuales madre previamente registradas, respectivamente, $CM_{E1,1}$, $CM_{E1,2}$, $CM_{E1,3}$, y $CM_{E2,1}$, $CM_{E2,2}$, $CM_{E2,3}$.

Las tarjetas virtuales madre que pertenecen a un mismo conjunto son distintas. Preferentemente, una tarjeta virtual madre que pertenece a un conjunto E_i pertenece exclusivamente a este conjunto E_i. En estas condiciones, dos tarjetas virtuales madre que pertenecen a dos conjuntos E_i distintos son necesariamente distintas. Una definición del término “distinto” se da a continuación con referencia a la figura 4.

La estructura de las tarjetas virtuales madre es común a todas las tarjetas virtuales madre. Esta estructura se presenta más adelante con referencia a la figura 4.

La base de datos 42 contiene unos “parches de software” más conocidos bajo el término inglés de “software patches” o “patches”. Por “software patch” se designa un conjunto de porciones de código que incluyen al menos una instrucción, destinada a completar o sustituir una parte del código ejecutable de la tarjeta virtual madre o hija. Esta sustitución no necesita una recompilación del código modificado. Típicamente, un parche está constituido por uno o varios vectores de código (una serie de octetos) de longitud(es) variable(s) asociado cada uno a una dirección objetivo (o posición de inicio) en el código (zona de memoria contigua) a sustituir. En definitiva, se trata de una lista de modificaciones a aportar sobre el bloque de código.

En lo que sigue se designa por “parche madre” un parche destinado a aplicarse al código de una tarjeta virtual madre. Se designa por “parche hijo” un parche destinado a aplicarse al código de una tarjeta virtual hija.

Por ejemplo, un parche contiene una instrucción que define un número de iteraciones para un algoritmo de cifrado o de descifrado.

En el ejemplo, el tamaño de memoria de un parche de software es inferior a 10 kB y, preferentemente, inferior a 5 kB de manera que puedan transmitirse por medio de un mensaje ECM y/o de un mensaje EMM.

La base de datos 42 asocia a un parche madre PM_j, un parche hijo PF_j, en el que j es un número entero. Con el fin de simplificar la figura 1, la base de datos 42 incluye en el ejemplo tres pares de parches madre/hijo.

La memoria 36 es en este caso una memoria de tipo flash.

El sistema 28 incluye igualmente un procesador 46 adecuado para:

- seleccionar seudo-aleatoriamente una tarjeta virtual madre $CM_{Ei,k}$ entre un conjunto E_i de tarjetas en la base de datos 38,

- seleccionar seudo-aleatoriamente un parche madre PM_j en la base de datos 42 y
- generar un criptograma $CW^*_{i,t}$ de una palabra de control $CW_{i,t}$ generada por el generador 32 a partir de una tarjeta virtual madre $CM_{Ei,k}$ seleccionada, y de un parche madre PM_j seleccionado,

Por otro lado, el procesador 46 es adecuado para generar un mensaje $ECM_{i,t}$ que incorpora:

- un criptograma $CW^*_{i,t}$ generado,
- un identificador de una tarjeta virtual hija a utilizar para descifrar el criptograma $CW^*_{i,t}$,
- un parche hijo PF_j asociado a un parche madre PM_j seleccionado, y
- una firma o una redundancia criptográfica MAC (por “message authentication code”) que permita verificar la integridad del mensaje ECM.

Por ejemplo, el procesador 46 se realiza a partir de un calculador electrónico programable. Este calculador es adecuado para ejecutar instrucciones registradas en un soporte de registro de informaciones de manera que implemente el procedimiento de la figura 5. Por ejemplo, estas instrucciones se registran igualmente en la memoria 36.

El circuito 76 se describirá ahora con referencia a la figura 3.

El circuito 76 es más conocido bajo el acrónimo SoC (System On a Chip). En este caso, el circuito 76 es preferentemente además un circuito integrado de seguridad. La utilización de circuitos integrados de seguridad es conocida para el experto en la materia. Para una descripción detallada de un ejemplo de circuito integrado de seguridad es posible referirse a la Solicitud de Patente US20050169468. En este caso, el circuito 76 comprende:

- una memoria no volátil 90,
- una memoria volátil 92, y
- un procesador 96.

La memoria 90 contiene una base de datos 100 (más visible en la figura 3a). Esta base 100 asocia a un identificador $ICF_{Ei,k}$ de una tarjeta hija $CF_{Ei,k}$, un criptograma $CF^*_{Ei,k}$ de esta tarjeta virtual hija $CF_{Ei,k}$. Cada criptograma de código $CF^*_{Ei,k}$ de una tarjeta virtual hija se obtiene aquí cifrando el código ejecutable de una tarjeta virtual hija $CF_{Ei,k}$ con una clave $K\_CF_{Ei,k}$.

Ventajosamente, para cada tarjeta virtual madre de identificador $ICM_{Ei,k}$ previamente registrada en la memoria 36, existe como mucho un criptograma de código $CF^*_{Ei,k}$ previamente registrado en la base 100 asociado al identificador $ICF_{Ei,k}$. Por ello, se subraya la característica según la que, existen tarjetas madre previamente registradas en la memoria 36 para las que no se ha registrado previamente en la base 100 ningún criptograma de código de la tarjeta virtual hija asociada.

Con el fin de simplificar la figura 3a, la base de datos 100 contiene únicamente tres criptogramas del código de las tarjetas virtuales hija $CF^*_{E1,1}$, $CF^*_{E1,2}$ y $CF^*_{E1,3}$ asociadas, respectivamente, a los identificadores $ICF_{E1,1}$, $ICF_{E1,2}$ e $ICF_{E1,3}$.

En este caso, la base de datos 100 no comprende los criptogramas del código de las tarjetas virtuales hija $CF^*_{E2,1}$, $CF^*_{E2,2}$ y $CF^*_{E2,3}$.

La estructura de una tarjeta virtual hija es común a todas las tarjetas virtuales hija. Esta estructura se detalla más adelante con referencia a la figura 4.

La memoria 90 contiene igualmente una base de datos 102 (más visible en la figura 3b). Esta base de datos 102 se asocia a un canal $\underline{i}$ y a un identificador $ICF_{Ei,k}$:

- la clave $K\_CF_{Ei,k}$ para descifrar el criptograma $CF^*_{Ei,k}$ de la tarjeta virtual hija $CF_{Ei,k}$, y
- una clave $Kfirma\_CF_{Ei,k}$ para verificar la autenticidad de la tarjeta virtual hija $CF_{Ei,k}$.

En este ejemplo, la base de datos 102 comprende:

- las claves $K\_CF_{E1,1}$, $K\_CF_{E1,2}$, $K\_CF_{E1,3}$, y
- las claves $Kfirma\_CF_{E1,1}$, $Kfirma\_CF_{E1,2}$, y $Kfirma\_CF_{E1,3}$.

La memoria 92 contiene una tabla 104 (más visible en la figura 3c) que asocia a un identificador $ICF_{Ei,k}$ una dirección de una tarjeta virtual hija $CF_{Ei,k}$ memorizada en la memoria 90. Estas tarjetas virtuales hija $CF_{Ei,k}$ memorizadas en la memoria 90 son preferentemente de seguridad. Por “de seguridad” se indica en este caso que los códigos ejecutables de las tarjetas virtuales hija están oscurecidos de manera que no se puedan ejecutar como tales. Por ejemplo, una parte del código ejecutable está cifrado para ser inoperativa una tentativa de retro-ingeniería. En el

ejemplo, la tabla 104 es virgen. Por ello se designa la característica según el que la tabla no incluye ninguna dirección de tarjeta virtual hija $CF_{Ei,k}$ de seguridad.

El procesador 96 es en este caso un calculador electrónico programable. El procesador 96 es adecuado para ejecutar unas instrucciones registradas en un soporte de registro de informaciones para implementar el procedimiento de la figura 6. El procesador 96 comprende un coprocesador 97 de seguridad. Este coprocesador 97 se programa para:

- asegurar (oscurecer o como en este caso cifrar) los datos memorizados en la memoria 92, y
- restablecer (en este caso descifrar) los datos memorizados en la memoria 92 de manera que los convierta en aprovechables por el procesador 96.

En el ejemplo, el coprocesador 97 contiene una memoria no volátil de escritura única 94. La memoria 94 contiene una clave K_{chip} propia del terminal 10. Esta clave se graba por ejemplo, durante la fabricación del circuito integrado 76.

Se describirán ahora con referencia a la figura 4 una tarjeta virtual madre 120 y una tarjeta virtual hija 122 asociadas.

Las tarjetas virtuales madre 120 e hija 122 son unas librerías de software. Típicamente, las tarjetas virtuales madre 120 e hija 122 son librerías de tipo DLL (por “Dynamic Link Library”) que contienen su código ejecutable.

La tarjeta virtual madre 120 incluye:

- un identificador $ICM_{Ei,k}$,
- una clave de explotación $Kexp_{Ei,k}$,
- un algoritmo de cifrado 126 que utiliza la clave de explotación $Kexp_{Ei,k}$ para cifrar una palabra de control $CW_{i,t}$ y obtener el criptograma $CW^*_{i,t}$, y
- un constructor sintáctico 128, para formatear el ECM, y posicionar el criptograma de la palabra de control $CW_{i,t}$ así como los otros parámetros (tales como las condiciones de acceso) en el mensaje $ECM_{i,t}$, y esto de manera coherente con el analizador sintáctico de la tarjeta virtual hija asociada.

El algoritmo de cifrado y el constructor sintáctico forman un código destinado a ser ejecutado por el procesador 46.

En el ejemplo, el algoritmo de cifrado comprende una porción de código faltante 124. Esta porción 124 está destinada a recibir un parche de software madre. En el ejemplo, la porción 124 constituye únicamente una parte del algoritmo 126, y no el algoritmo 126 completo.

Por otro lado, en esta descripción, se designa por “tarjetas virtuales madre distintas”, las tarjetas virtuales diferentes entre sí por su clave de explotación $Kexp_{Ei,k}$ y/o por su algoritmo de cifrado 126 y/o por su constructor sintáctico 128.

La tarjeta virtual hija 122 incluye:

- un identificador $ICF_{Ei,k}$,
- una clave de explotación $Kexp_{Ei,k}$,
- un algoritmo de descifrado 130 que utiliza la clave de explotación $Kexp_{Ei,k}$ para descifrar el criptograma $CW^*_{i,t}$, cifrado a partir de la tarjeta madre 120 y obtener la palabra de control $CW_{i,t}$,
- un analizador sintáctico 134, para localizar el criptograma $CW^*_{i,t}$ en un mensaje $ECM_{i,t}$, y
- una firma 136 para verificar la integridad de la tarjeta virtual hija 122.

El algoritmo de cifrado y el analizador sintáctico forman un código destinado a ser ejecutado por el procesador 96.

Por “tarjetas virtuales hija distintas” se designan dos tarjetas virtuales hija diferentes entre sí por su clave de explotación y/o por su algoritmo de descifrado y/o por su analizador sintáctico.

Se describirá ahora con referencia a la figura 5 un procedimiento de transmisión de un contenido multimedia encriptado en el sistema de la figura 1. El procedimiento implementado es el mismo para cada canal. De ese modo, se describe en lo que sigue el procedimiento de transmisión en el caso particular del canal 1.

Durante una etapa 200 implementada en un instante t, el origen 4 transmite un criptoperiodo $CP_{1,t}$ en claro del canal 1 al codificador 16. En el ejemplo, un criptoperiodo posee una duración comprendida entre cinco segundos y un minuto. Típicamente, la duración de un criptoperiodo es de 10 segundos.

Durante una etapa 202, el codificador 16 codifica el criptoperiodo $CP_{1,t}$ y transmite el criptoperiodo codificado al encriptador 22.

Durante una etapa 204, el generador 32 selecciona una palabra de control $CW_{1,t}$ y transmite esta palabra de control al encriptador 22. Más particularmente, el generador 32 selecciona seudo-aleatoriamente una palabra de control $CW_{1,t}$ y transmite esta palabra de control $CW_{1,t}$ al encriptador 22 y al sistema 28.

Durante una etapa 206, el encriptador 22 encripta el criptoperiodo $CP_{1,t}$ codificado durante la etapa 202, a partir de la palabra de control $CW_{1,t}$ recibida durante la etapa 204. El encriptador 22 genera así un criptoperiodo encriptado $CP^*_{1,t}$. El encriptador 22 transmite el criptoperiodo encriptado $CP^*_{1,t}$ al multiplexor 26.

Durante una etapa 208, el sistema 28 genera las diferentes informaciones necesarias para construir el mensaje $ECM_{1,t}$ que permita el desencriptado del criptoperiodo $CP^*_{1,t}$.

Más particularmente, durante una operación 210, el procesador 46 selecciona el conjunto E_1 de las tarjetas madre asociadas al canal 1 gracias a la base de datos 38. A continuación, selecciona seudo-aleatoriamente en la base de datos 38 una tarjeta virtual madre $CM_{1,k}$ entre las tarjetas virtuales madre $CM_{1,1}$, $CM_{1,2}$, y $CM_{1,3}$ del conjunto E_1. Por ejemplo, el procesador 46 selecciona la tarjeta virtual madre $CM_{1,1}$.

Durante una operación 212, el procesador 46 selecciona seudo-aleatoriamente en la base de datos 42 un parche madre PM_i entre los parches madre PM_1, PM_2, y PM_3. Por ejemplo, el procesador 46 selecciona el parche madre PM_1.

Durante una operación 214, el procesador 46 completa la porción de código faltante 124 del algoritmo de cifrado 126 de la tarjeta virtual $CM_{1,1}$ seleccionada durante la operación 210 con el parche madre PM_1 seleccionado durante la operación 212. El algoritmo de cifrado formado durante la etapa 214 se denomina lo que sigue “algoritmo de cifrado operativo”.

Durante una operación 216, el procesador 46 genera el criptograma $CW^*_{1,t}$ de la palabra de control $CW_{1,t}$ a partir:

- del algoritmo de cifrado operativo formado durante la operación 214 y
- de la clave de explotación $Kexp_{E1,1}$ contenida en la tarjeta madre $CM_{E1,1}$ seleccionada.
- de la palabra de control $CW_{1,t}$ proporcionada por el generador 32.

Durante una operación 217, el procesador 46 ejecuta el constructor sintáctico de la tarjeta virtual madre $CM_{E1,1}$ para determinar en qué emplazamiento en la trama de mensaje $ECM_{1,t}$, debe insertarse el criptograma $CW^*_{1,t}$.

Durante una etapa 220, el sistema 28 genera un mensaje $ECM_{1,t}$ que contiene:

- el identificador $ICF_{E1,1}$ de la tarjeta virtual hija $CM_{E1,1}$ asociada a la tarjeta virtual madre $CM_{E1,1}$,
- el parche hijo PF_1,
- el criptograma $CW^*_{i,t}$ de la palabra de control $CW_{i,t}$ que permite desencriptar el criptoperiodo t del canal 1, y
- una redundancia criptográfica MAC.

Durante esta etapa 220, el sistema 28 coloca en la trama del mensaje $ECM_{1,t}$ el criptograma $CW^*_{1,t}$ en el emplazamiento determinado durante la operación 217.

Durante una etapa 222, el generador 28 transmite el mensaje $ECM_{1,t}$ al multiplexor 26.

Durante una etapa 224, el multiplexor 26 multiplexa el criptoperiodo encriptado $CP^*_{1,t}$ formado durante la etapa 206 y el mensaje $ECM_{1,t}$ transmitido durante la etapa 222.

Más precisamente, el mensaje $ECM_{1,t}$ se inserta en la señal por el multiplexor 26 antes del criptoperiodo $CP_{1,t}$.

Las etapas 200 a 224 se reiteran para cada criptoperiodo. En consecuencia, en este caso la tarjeta virtual madre se cambia todos los criptoperiodos.

Se describirá ahora con referencia a la figura 6 un procedimiento de recepción de un contenido multimedia encriptado por el terminal 10.

Durante una fase de 300 preliminar, un usuario del terminal 10 suscribe un abono ante un suministrador de contenidos multimedia. Por ejemplo, el suministrador ofrece la posibilidad de visionar los canales 1 y 2. Más particularmente, este usuario paga un canon para poder visionar únicamente el canal 1 en claro.

Como respuesta, el operador suministra al usuario solamente los datos necesarios para poder desencriptar el canal 1.

Durante una etapa 302, el dispositivo 6 cifra las tarjetas virtuales hija $CF_{E1,1}$, $CF_{E1,2}$, y $CF_{E1,3}$ asociadas a las tarjetas virtuales madre $CM_{E1,1}$, $CM_{E1,2}$, y $CM_{E1,3}$ del conjunto E1, respectivamente, con ayuda de las claves $K\_CF_{E1,1}$,

$K\_CF_{E1,2}$ y $K\_CF_{E1,3}$, de manera que obtenga unos criptogramas de código $CF^*_{E1,1}$, $CF^*_{E1,2}$, y $CF^*_{E1,3}$ de las tarjetas virtuales hija.

Durante una etapa 304, el dispositivo 6 transmite por medio de uno o de varios mensajes EMM:

- los criptogramas de código $CF^*_{E1,1}$, $CF^*_{E1,2}$, y $CF^*_{E1,3}$,
- los identificadores $ICF_{E1,1}$, $ICF_{E1,2}$, e $ICF_{E1,3}$ de las tarjetas virtuales hija $CF_{E1,1}$, $CF_{E1,2}$, y $CF_{E1,3,}$
- las claves $K\_CF_{E1,1}$, $K\_CF_{E1,2}$, y $K\_CF_{E1,3}$ para permitir al terminal 10 descifrar los criptogramas $CF^*_{E1,1}$, $CF^*_{E1,2}$ y $CF^*_{E1,3}$, y
- las claves $Kfirma\_CF_{E1,1}$, $Kfirma\_CF_{E1,2}$, y $Kfirma\_CF_{E1,3}$ para permitir al terminal 10 verificar la autenticidad de las tarjetas virtuales hija $CF_{E1,1}$, $CF_{E1,2}$, y $CF_{E1,3}$,

Las claves $K\_CF_{E1,1}$, $K\_CF_{E1,2}$, y $K\_CF_{E1,3}$ y las claves $Kfirma\_CF_{E1,1}$, $Kfirma\_CF_{E1,2}$, y $Kfirma\_CF_{E1,3}$ se cifran ventajosamente previamente con ayuda de la clave K_{chip}.

Durante una etapa 306, el terminal 10 recepciona el o los mensajes EMM transmitidos por el dispositivo 6 y registra previamente el contenido de este o de estos mensajes en las memorias 90 y 92 para formar las bases de datos 100, 102.

Cuando se acaba la fase preliminar 300, las bases de datos 100, 102, y la tabla 104 en la memoria 90 y 92 son tal como las representadas en las figuras 3a, 3b y 3c.

Durante una fase 307 de utilización, el usuario desea utilizar un contenido multimedia. Por ejemplo, el usuario desea ver una película en el canal 1 en el instante t.

Con este fin, durante una etapa 308 el terminal 10 se conecta a la red 8 y recibe un contenido multimedia multiplexado por medio del receptor 70. Este contenido multiplexado se demultiplexa mediante el demultiplexor 72. El demultiplexor 72 transmite el criptoperiodo encriptado $CP^*_{1,t}$ al desencriptador 74, y el mensaje $ECM_{1,t}$ al procesador 96.

Se recuerda que el mensaje $ECM_{1,t}$ contiene:

- el identificador $ICF_{E1,1}$ de la tarjeta virtual hija $CF_{E1,1}$,
- el parche hijo PF_1,
- el criptograma $CW^*_{1,t}$, y
- una redundancia criptográfica MAC.

Durante una etapa 309, el procesador 96 verifica la integridad del mensaje $ECM_{1,t}$ recibido recalculando la redundancia criptográfica MAC de este mensaje $ECM_{1,t}$ y comparando el resultado obtenido con la redundancia criptográfica MAC contenida en el mensaje $ECM_{1,t}$ recibido. Si el resultado del cálculo coincide con la redundancia criptográfica MAC contenida en el mensaje $ECM_{1,t}$ recibido entonces se procede a una etapa 310. Si no se interrumpe el procedimiento.

Durante una etapa 310, el procesador 96 recupera el identificador $ICF_{E1,1}$ en el mensaje $ECM_{1,t}$ recibido.

Durante una etapa 312, el procesador 96 verifica en la base de datos 104, con ayuda del identificador $ICF_{E1,1}$ recibido, si este incluye ya la tarjeta virtual hija $CF_{E1,1}$ para descifrar el criptograma $CW^*_{1,t}$ contenido en el mensaje $ECM_{1,t}$. Si la base 104 incluye la tarjeta virtual hija $CF_{E1,1}$ entonces se procede directamente a una etapa 314. En efecto, en este caso, no es necesario descifrar el criptograma $CF^*_{E1,1}$ para obtener la tarjeta $CF_{E1,1}$ en claro. En caso contrario, se procede a una etapa 315.

Durante la etapa 315, el procesador 96 verifica en la base de datos 100 si esta contiene el identificador $ICF_{E1,1}$. En caso afirmativo, esto significa que el terminal contiene el criptograma $CF^*_{E1,1}$ y que está por tanto autorizado a visualizar el canal 1.

Se procede entonces a una etapa 326.

Si la base 104 no contiene el criptograma $CF^*_{E1,1}$ entonces el procesador 96 no puede descifrar el criptograma $CW^*_{1,t}$. En estas condiciones, el usuario no está autorizado a visionar el canal 1 en claro y el procedimiento de recepción se termina.

Durante la etapa 326, el procesador 96 descifra las claves $K\_CF_{E1,1}$ y $Kfirma\_CF_{E1,1}$ asociadas al identificador $ICF_{E1,1}$ en la base 102 con ayuda de la clave K_{chip}. Posteriormente, el procesador 96 descifra el criptograma $CF^*_{E1,1}$ a partir de la clave $K\_CF_{E1,1}$ de manera que obtenga la tarjeta virtual hija descifrada $CF_{E1,1}$.

Durante una etapa 328, el procesador 96 verifica la firma de la tarjeta virtual hija descifrada $CF_{E1,1}$ con ayuda de la clave Kfirma_$CF_{E1,1}$. Por ejemplo, el procesador 96 aplica una función criptográfica de hash, más conocida bajo el término inglés de “Hash”, sobre la tarjeta virtual $CF_{E1,1}$ para obtener una primera huella de esta tarjeta. A continuación, descifra la firma 136 de la tarjeta $CF_{E1,1}$ con la clave pública Kfirma_$CF_{E1,1}$ para obtener una segunda huella. Si la primera y segunda huellas corresponden, entonces la tarjeta $CF_{E1,1}$ está correctamente autentificada.

En este caso, durante una etapa 330, el procesador 96 interroga a la memoria 92 para conocer su espacio de memoria disponible. Si la memoria 92 posee un espacio de memoria suficiente, la tarjeta virtual hija $CF_{E1,1}$ descifrada durante la etapa 326 está asegurada por el coprocesador 97, copiada en la memoria 90, catalogada en la base de datos 104 durante una etapa 332 y asociada al identificador $ICM_{E1,1}$. Por “catalogar” se designa una operación durante la que la dirección de memoria en la que se copia la tarjeta virtual hija $CF_{E1,1}$ se asocia con el identificador $ICF_{E1,1}$ en la base de datos 104. Si no, durante una etapa 334 la memoria 92 suprime una de las tarjetas virtuales $CF_{Ei,k}$ en la base 104 para poder recibir la tarjeta virtual hija $CF_{E1,1}$. A título de ejemplo, en este caso se aplica el algoritmo LRU (por “least recent used”). La tarjeta virtual hija en la memoria 90 más antiguamente utilizada se suprime primero. Posteriormente, la tarjeta virtual hija $CF_{E1,1}$ se asegura por el coprocesador 97, se copia en la memoria 90 y posteriormente se cataloga.

Una vez terminada la etapa 332 o 334, se procede a la etapa 314.

Si la firma calculada durante la etapa 328 no coincide con la firma 136 contenida en la tarjeta virtual descifrada durante la etapa 326 entonces la tarjeta virtual $CF_{E1,1}$ no está autenticada. En este caso, el procesador 96 no descifra el criptograma $CW^*_{1,t}$ y se interrumpe el procedimiento de recepción.

Durante la etapa 314, el procesador 96 ejecuta el analizador de sintaxis de la tarjeta virtual hija $CF_{E1,1}$ y extrae en el mensaje $ECM_{1,t}$ el criptograma $CW^*_{1,t}$ y el parche hijo PF_1.

Durante una etapa 316, el procesador 46 aplica el parche hijo PF_1 extraído durante la etapa 314 al algoritmo de descifrado de la tarjeta virtual hija $CF_{E1,1}$. El algoritmo de descifrado formado durante esta etapa 322 se denomina en lo que sigue “algoritmo de descifrado operativo”.

Durante una etapa 318, el procesador 96 descifra el criptograma $CW^*_{1,t}$ a partir del algoritmo de descifrado operativo formado durante la etapa 316 y de la clave de explotación $Kexp_{E1,1}$ contenida en la tarjeta virtual hija $CF_{E1,1}$. De ese modo, durante esta etapa 318, el procesador 96 obtiene la palabra de control $CW_{1,t}$ en claro.

Durante una etapa 320, el procesador 96 transmite la palabra de control $CW_{1,t}$ en claro al desencriptador 74.

Durante una etapa 322, el desencriptador 74 desencripta el criptoperiodo encriptado $CP^*_{1,t}$ a partir de la palabra de control $CW_{1,t}$ transmitida por el procesador 96 y obtiene un criptoperiodo $CP_{1,t}$ desencriptado. El criptoperiodo $CP_{1,t}$ desencriptado se transmite entonces al decodificador 80.

Durante una etapa 324, el decodificador 80 decodifica el criptoperiodo $CP_{1,t}$ y posteriormente transmite el resultado de la decodificación a la tarjeta gráfica 82. La tarjeta gráfica 82 controla finalmente la presentación de este resultado en la pantalla 86.

Las etapas 308 a 334 se reiteran para cada criptoperiodo.

Son posibles numerosos otros modos de realización.

Por ejemplo, las tarjetas madre no están necesariamente registradas previamente en la memoria 36. Las tarjetas virtuales madre pueden generarse dinámicamente por el procesador 46 durante la fase preliminar 300, antes de transmitir las tarjetas virtuales hija asociadas.

En una variante, la selección por el terminal 10 de una tarjeta virtual hija a utilizar para descifrar un criptograma CW^*_t consiste en la generación dinámica de la tarjeta virtual por el procesador 96, a partir de una función previamente registrada en la memoria 90 y del identificador $ICF_{Ei,k}$ recibido.

En otra variante, la sintaxis de los mensajes ECM es siempre la misma. En este caso, las tarjetas virtuales madre e hija incluyen, respectivamente, siempre el mismo constructor sintáctico y el mismo analizador sintáctico.

Siempre como variante, los parches de software madre e hijo se aplican respectivamente a los códigos del constructor sintáctico y del analizador sintáctico de tarjetas virtuales.

Como variante, a una tarjeta virtual madre o a un conjunto E_i de tarjetas virtuales madre se asocia un conjunto específico de parches madre propio únicamente de esta tarjeta o de este conjunto E_i.

Igualmente como variante, los parches madre y/o hijo se memorizan directamente en las tarjetas virtuales madre e hija, respectivamente.

Igualmente como variante, los parches de software madre e hijo pueden omitirse. En este caso, los algoritmos de cifrado y de descifrado de las tarjetas virtuales madre e hija no incluyen la parte de código faltante 124 y 132.

En otra variante, no existe un conjunto E_i de tarjetas virtuales madre específico para cada canal $\underline{i}$. Por ejemplo, existe un único conjunto E para todos los canales. En este caso, todas las tarjetas virtuales de este conjunto pueden utilizarse para cifrar una palabra de control que sirva para encriptar un criptoperiodo de uno de los canales $\underline{i}$.

Preferentemente, con el fin de restringir el acceso de ciertos canales a usuarios que posean unos títulos de acceso, se incorporan unas condiciones de acceso en los mensajes ECM transmitidos por el dispositivo 6. Estas condiciones de acceso y los títulos de acceso registrados en la tarjeta virtual hija se comparan durante la recepción del mensaje ECM con el fin de determinar si el procesador puede descifrar o no el criptograma incorporado en este mensaje ECM.

En otra variante, el procesador de seguridad que ejecuta el procedimiento de recepción de la figura 5 o 6 es el procesador de una tarjeta de chips.

Siempre como variante, los mensajes ECM no incluyen un identificador ICF de una tarjeta virtual hija en particular sino el identificador de un conjunto de tarjetas virtuales hija. En este caso, cuando el terminal de recepción recibe el mensaje ECM, el terminal prueba todas las tarjetas virtuales hija asociadas a este conjunto hasta encontrar la tarjeta virtual hija que permita descifrar el criptograma CW* contenido en el mensaje ECM.

En otra variante, no se transmite al terminal ningún identificador de la nueva tarjeta virtual hija a utilizar. Por ejemplo, en este caso, el terminal prueba cada vez que recibe un nuevo criptograma CW^*_t si la tarjeta virtual hija actualmente seleccionada permite descifrar correctamente este criptograma. En caso afirmativo, continúa utilizando la tarjeta virtual hija actual. En caso negativo, prueba sucesivamente todas las tarjetas virtuales hija que tiene en memoria hasta encontrar aquella que permita descifrar este criptograma. Esta última tarjeta virtual hija se selecciona entonces para ser utilizada en lugar de la antigua.

Como variante, durante la fase 300 las tarjetas virtuales hija no se transmiten por medio de mensajes EMM sino a través de un servicio dedicado de difusión (es decir una difusión a todos los terminales conectados a la red 8) o multi-emisión (es decir una difusión a un grupo particular de terminales conectados a la red 8) tales como DVB-SSU o CSM-CC, o incluso a través del mensaje ECM.

En el caso en el que la red 8 es una red híbrida (por ejemplo la red 8 está formada por una red TDT y una red de Internet), el dispositivo 6 puede transmitir a los terminales una URL (por Union Resource Locator) de un servidor de tarjetas virtuales hija. Cada terminal descarga las tarjetas virtuales hija en este servidor. Preferentemente, la descarga de las tarjetas virtuales es de seguridad. Por ejemplo, se recomienda la utilización de los protocolos SSL (por Secure Shell) o HTTPS (por Hyper Text Transfer Protocol Secured) y/o la utilización de una estructura de clave pública (más conocida bajo el nombre de PKI). Es posible implementar esta variante a partir de un sistema que utilice la IPTV o la WebTV.

Con el fin de limitar en el tiempo estas tarjetas virtuales hija, puede incorporarse una duración de validez en cada tarjeta.

En el procedimiento de la figura 5, como variante, durante varios criptoperiodos, se conserva la misma tarjeta virtual madre pero se cambia de parche de software madre en cada criptoperiodo.

En otra variante para este procedimiento, en cada nuevo criptoperiodo, se cambia de tarjeta virtual madre pero se conserva el mismo parche de software.

Preferentemente, la tarjeta virtual madre se cambia como mínimo cada treinta minutos, o como mínimo cada diez minutos, y de manera incluso más preferida como mínimo cada minuto.

REIVINDICACIONES

1. Procedimiento de transmisión y de recepción de un contenido multimedia en el que cada criptoperiodo CP_t se encripta con ayuda de una palabra de control CW_t respectiva, incluyendo el procedimiento:

- el cifrado, por un emisor, de la palabra de control CW_t con ayuda de una clave de explotación y de un código ejecutable de un algoritmo de cifrado contenidos en una tarjeta virtual madre para obtener un criptograma CW^*_t,
- la generación de un mensaje ECM (Entitlement Control Message) que incorpora el criptograma CW^*_t con ayuda de un código ejecutable de un constructor sintáctico contenido en la tarjeta virtual madre y la transmisión de este mensaje ECM a un terminal,
- la recepción por el terminal del mensaje ECM, la localización de la posición del criptograma CW^*_t en el mensaje ECM recibido con ayuda de un código ejecutable de un analizador sintáctico, posteriormente el descifrado del criptograma con ayuda de la clave de explotación y de un código ejecutable de un algoritmo de descifrado, estando contenidos en el código ejecutable del analizador sintáctico y el algoritmo de descifrado en una tarjeta virtual hija asociada a la tarjeta virtual madre, y
- el desencriptado del criptoperiodo CP_t del contenido multimedia encriptado con ayuda de la palabra de control descifrada CW_t,

caracterizado por que el procedimiento incluye igualmente:

- el cambio como mínimo cada dos horas, por el emisor, de la tarjeta virtual madre utilizada para obtener el criptograma CW^*_{t+n} de un criptoperiodo siguiente CP_{t+n} del mismo contenido multimedia, difiriendo la nueva tarjeta virtual madre utilizada de la precedente tarjeta virtual madre utilizada por su clave de explotación y al menos el código ejecutable de su algoritmo de cifrado o del constructor sintáctico,
- en respuesta, la selección por el terminal de una nueva tarjeta virtual hija a utilizar para descifrar el criptograma CW^*_{t+n} de manera que se obtenga la palabra de control CW_{t+n},
- la selección, en función del contenido multimedia a encriptar, de un conjunto de varias tarjetas virtuales madre diferentes entre varios conjuntos de tarjetas virtuales madre, con ayuda de una relación que asocia a cada contenido multimedia un único conjunto de tarjetas virtuales madre, perteneciendo cada tarjeta virtual madre exclusivamente a un único conjunto, y
- las palabras de control para encriptar un contenido multimedia se cifran únicamente con ayuda de tarjetas virtuales madre seleccionadas en el conjunto asociado a este contenido, de manera que se limite el acceso al contenido multimedia encriptado a los únicos terminales de recepción que disponen de un conjunto previamente registrado de tarjetas virtuales hija correspondientes a este conjunto de tarjetas virtuales madre.

2. Procedimiento según la reivindicación 1, en el que la nueva tarjeta virtual madre utilizada difiere de la precedente tarjeta virtual madre utilizada por el código ejecutable de su algoritmo de cifrado y del constructor sintáctico.

3. Procedimiento de generación de mensajes ECM para la implementación de un procedimiento de transmisión y de recepción de contenido multimedia de acuerdo con una cualquiera de las reivindicaciones anteriores, incluyendo cada mensaje ECM un criptograma CW^*_t de una palabra de control CW_t utilizada para encriptar un criptoperiodo CP_t respectivo de un mismo contenido multimedia, incluyendo el procedimiento:

a) el cifrado de la palabra de control CW_t con ayuda de una clave de explotación y de un código ejecutable de un algoritmo de cifrado contenidos en una tarjeta virtual madre para obtener el criptograma CW^*_t, y
b) la generación de un mensaje ECM que incorpora el criptograma CW^*_t con ayuda de un código ejecutable de un constructor sintáctico contenido en la tarjeta virtual madre,

caracterizado por que, el procedimiento incluye igualmente:

c) el cambio como mínimo cada dos horas de la tarjeta virtual madre utilizada para obtener el criptograma CW^*_{t+n} de un criptoperiodo siguiente CP_{t+n}, difiriendo la nueva tarjeta virtual madre utilizada de la precedente tarjeta virtual madre utilizada por la clave de explotación y al menos el código ejecutable de su algoritmo de cifrado o del constructor sintáctico,
- la selección, en función del contenido multimedia a encriptar, de un conjunto de varias tarjetas virtuales madre diferentes entre varios conjuntos de tarjetas virtuales madre, con ayuda de una relación que asocia a cada contenido multimedia un único conjunto de tarjetas virtuales madre, perteneciendo cada tarjeta virtual madre exclusivamente a un único conjunto, y
- las palabras de control para encriptar un contenido multimedia se cifran únicamente con ayuda de tarjetas virtuales madre seleccionadas en el conjunto asociado a este contenido, de manera que se limite el acceso al contenido multimedia encriptado a los únicos terminales de recepción que disponen del conjunto previamente registrado de tarjetas virtuales hija correspondientes a este conjunto de tarjetas virtuales madre.

4. Procedimiento según la reivindicación 3, en el que el procedimiento incluye la transmisión al terminal, en un mensaje ECM, de un identificador de la tarjeta virtual hija a utilizar para descifrar el criptograma CW^*_{t+n}.

5. Procedimiento según una cualquiera de las reivindicaciones 3 a 4, en el que durante la etapa c) la tarjeta virtual madre se selecciona entre un conjunto de tarjetas virtuales previamente registradas en el interior del emisor, siendo distintas entre sí las tarjetas virtuales que pertenecen a este conjunto.

6. Procedimiento según la reivindicación 5, en el que durante la etapa c) la tarjeta virtual madre se selecciona seudo-aleatoriamente entre el conjunto de tarjetas virtuales previamente registradas en el interior del emisor.

7. Procedimiento de recepción, por el terminal, para la implementación de un procedimiento de transmisión y de recepción de acuerdo con las reivindicaciones 1 a 2, incluyendo este procedimiento:

e) la recepción por medio de uno o varios mensajes ECM de un criptograma CW^*_t de la palabra de control CW_t,
f) la localización de la posición del criptograma CW^*_t en el mensaje ECM recibido con la ayuda de un código ejecutable de un analizador sintáctico y posteriormente el descifrado del criptograma con ayuda de una clave de explotación y de un código ejecutable de un algoritmo de descifrado, estando contenidos el código ejecutable del analizador sintáctico y del algoritmo de descifrado en una tarjeta virtual hija asociada a la tarjeta virtual madre, y el desencriptado del criptoperiodo CP_t del contenido multimedia encriptado con ayuda de la palabra de control descifrada CW_t,

caracterizado por que el procedimiento incluye:

g) en respuesta a un cambio de tarjeta virtual madre por el emisor,
- si el conjunto de tarjetas virtuales hija asociado a este contenido multimedia está previamente registrado en el terminal: la selección por el terminal de una tarjeta virtual hija a utilizar para el descifrado del criptograma CW^*_t entre este conjunto de tarjetas virtuales hija previamente registradas en el terminal de manera que se obtenga la palabra de control CW_t, difiriendo cada tarjeta virtual hija de otra tarjeta virtual hija del conjunto por su clave de explotación y al menos el código ejecutable de su algoritmo de cifrado o del analizador sintáctico, y
- si el conjunto de tarjetas virtuales hija asociado a este contenido multimedia no está previamente registrado en el terminal, la ausencia de selección por el terminal de una tarjeta virtual hija a utilizar para el descifrado del criptograma CW^*_t de manera que se inhiba la obtención de la palabra de control CW_t.

8. Procedimiento según la reivindicación 7, en el que el procedimiento incluye:

- la recepción de un identificador de una tarjeta virtual hija durante la etapa e), y
- la selección por el terminal de la tarjeta virtual hija entre el conjunto de tarjetas previamente registradas a partir del identificador recibido durante la etapa g).

9. Procedimiento según una cualquiera de las reivindicaciones 7 a 8, en el que el procedimiento incluye igualmente:

- la recepción, durante la etapa e), por el terminal, de una o varias instrucciones adicionales, y
- en respuesta, la modificación del código ejecutable de la tarjeta virtual hija seleccionada completando y/o sustituyendo una parte solamente de las instrucciones del código ejecutable de esta tarjeta virtual hija por la o las instrucciones recibidas.

10. Procedimiento según una cualquiera de las reivindicaciones 8 a 9, en el que el procedimiento incluye:

h) la recepción por el terminal de una tarjeta virtual hija cifrada,
i) la memorización de la tarjeta virtual hija cifrada recibida para añadir esta tarjeta al conjunto de tarjetas virtuales hija previamente registradas, y
j) el descifrado de la tarjeta virtual hija cifrada, en respuesta a la recepción del identificador,

siendo ejecutadas las etapas h), i) y j) antes de la implementación de las etapas e) y g).

11. Soporte de registro de informaciones, caracterizado por que incluye unas instrucciones para la ejecución de un procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 10, cuando estas instrucciones se ejecutan por un calculador electrónico.

12. Emisor para la implementación de un procedimiento de generación de mensajes ECM según una cualquiera de las reivindicaciones 3 a 6, incluyendo el emisor:

- un encriptador (22) para encriptar un criptoperiodo CP_t respectivo de un contenido multimedia con ayuda de una palabra de control CW_t,
- un sistema (28) para:

  • cifrar la palabra de control CW_t con ayuda de una clave de explotación y de un código ejecutable de un algoritmo de cifrado contenidos en una tarjeta virtual madre para obtener el criptograma CW^*_t, y para generar un mensaje ECM que incorpora el criptograma CW^*_t, y para

• generar un mensaje ECM (Entitlement Control Message) que incorpora el criptograma CW^*_t con ayuda de un código ejecutable de un constructor sintáctico contenido en la tarjeta virtual madre,

caracterizado por que el sistema (28) se programa para:

- cambiar la tarjeta virtual madre utilizada, como mínimo cada dos horas con el fin de obtener el criptograma CW^*_{t+n} de un criptoperiodo siguiente CP_{t+n}, difiriendo la nueva tarjeta virtual madre utilizada de la precedente tarjeta virtual madre utilizada por la clave de explotación y al menos el código ejecutable de su algoritmo de cifrado o del constructor sintáctico,
- seleccionar, en función del contenido multimedia a encriptar, un conjunto de varias tarjetas virtuales madre diferentes entre varios conjuntos de tarjetas virtuales madre, con ayuda de una relación que asocia a cada contenido multimedia un único conjunto de tarjetas virtuales madre, perteneciendo cada tarjeta virtual madre exclusivamente a un único conjunto, y
- cifrar las palabras de control para encriptar un contenido multimedia únicamente con ayuda de tarjetas virtuales madre seleccionadas en el conjunto asociado a este contenido, de manera que se limite el acceso al contenido multimedia encriptado a los únicos terminales de recepción que disponen de un conjunto previamente registrado de tarjetas virtuales hija correspondientes a este conjunto de tarjetas virtuales madre.

13. Terminal de recepción para la implementación de un procedimiento según una cualquiera de las reivindicaciones 7 a 10, incluyendo este terminal de recepción:

- un conjunto (100, 104) de tarjetas virtuales hija previamente registradas,
- un receptor (70) adecuado para recibir por medio de uno o varios mensajes ECM, un criptograma CW^*_t de la palabra de control CW_t,
- un circuito integrado (76) programado para:

• localizar la posición del criptograma CW^*_t en el mensaje ECM recibido con ayuda de un código ejecutable de un analizador sintáctico y posteriormente descifrar este criptograma con ayuda de una clave de explotación y de un código ejecutable de un algoritmo de descifrado, estando contenidos el código ejecutable del analizador sintáctico y del algoritmo de descifrado en una tarjeta virtual hija asociada a una tarjeta virtual madre, y
• desencriptar el criptoperiodo CP_t del contenido multimedia encriptado con ayuda de la palabra de control descifrada CW_t, y

caracterizado por que el circuito integrado (76) se programa para, en respuesta a un cambio de tarjeta virtual madre por el emisor:

- si el conjunto de tarjetas virtuales hija asociado a este contenido multimedia está previamente registrado en el terminal: seleccionar una nueva tarjeta virtual hija a utilizar para el descifrado del criptograma CW^*_t entre este conjunto de tarjetas virtuales hija previamente registradas de manera que se obtenga la palabra de control CW_{t+n}, difiriendo cada tarjeta virtual hija de otra tarjeta virtual hija del conjunto por su clave de explotación y al menos el código ejecutable de su algoritmo de cifrado o del analizador sintáctico, y
- si el conjunto de tarjetas virtuales hija asociado a este contenido multimedia no está previamente registrado en el terminal, la ausencia de selección por el terminal de una tarjeta virtual hija a utilizar para el descifrado del criptograma CW^*_t de manera que se inhiba la obtención de la palabra de control CW_t.

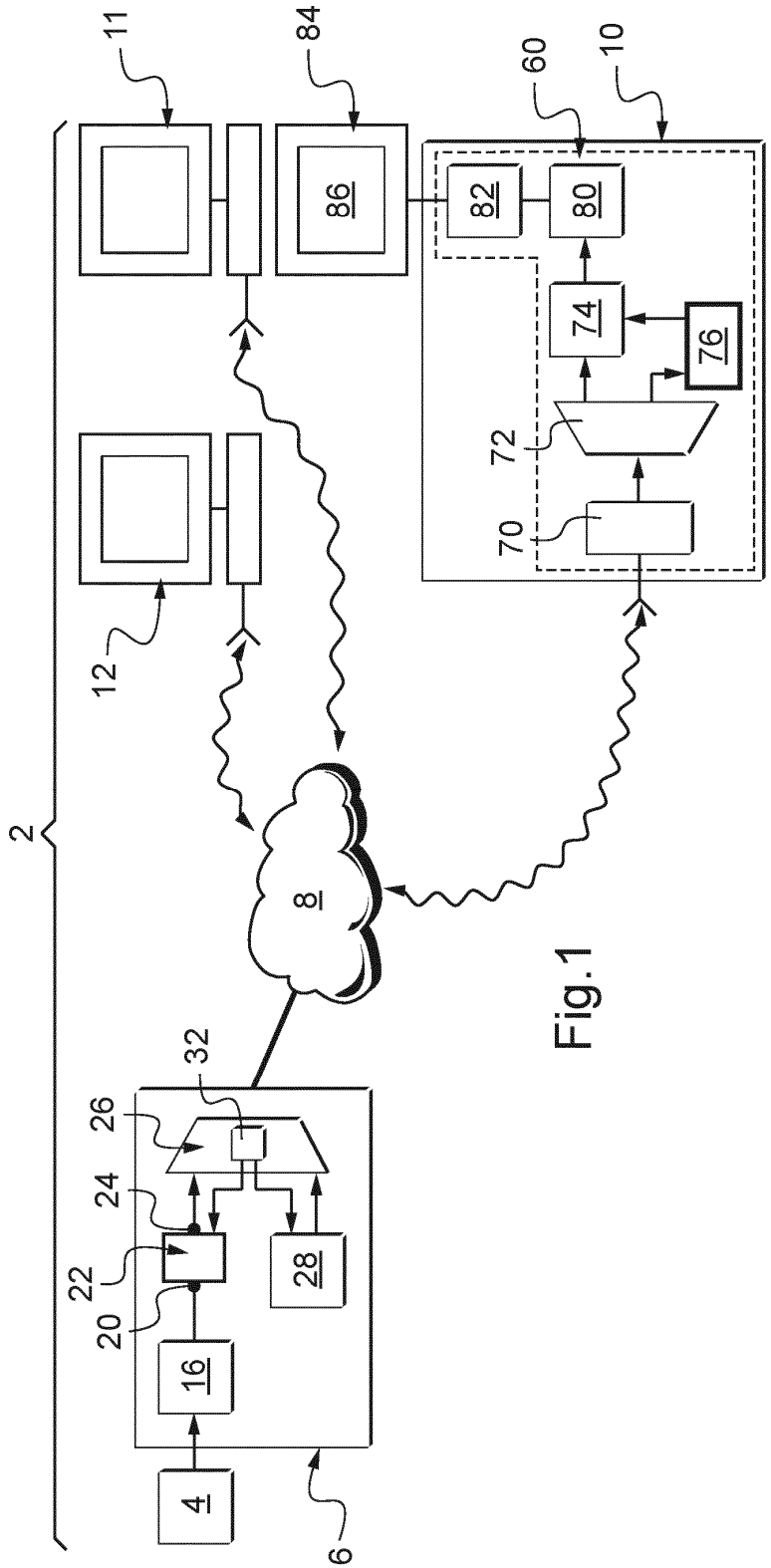
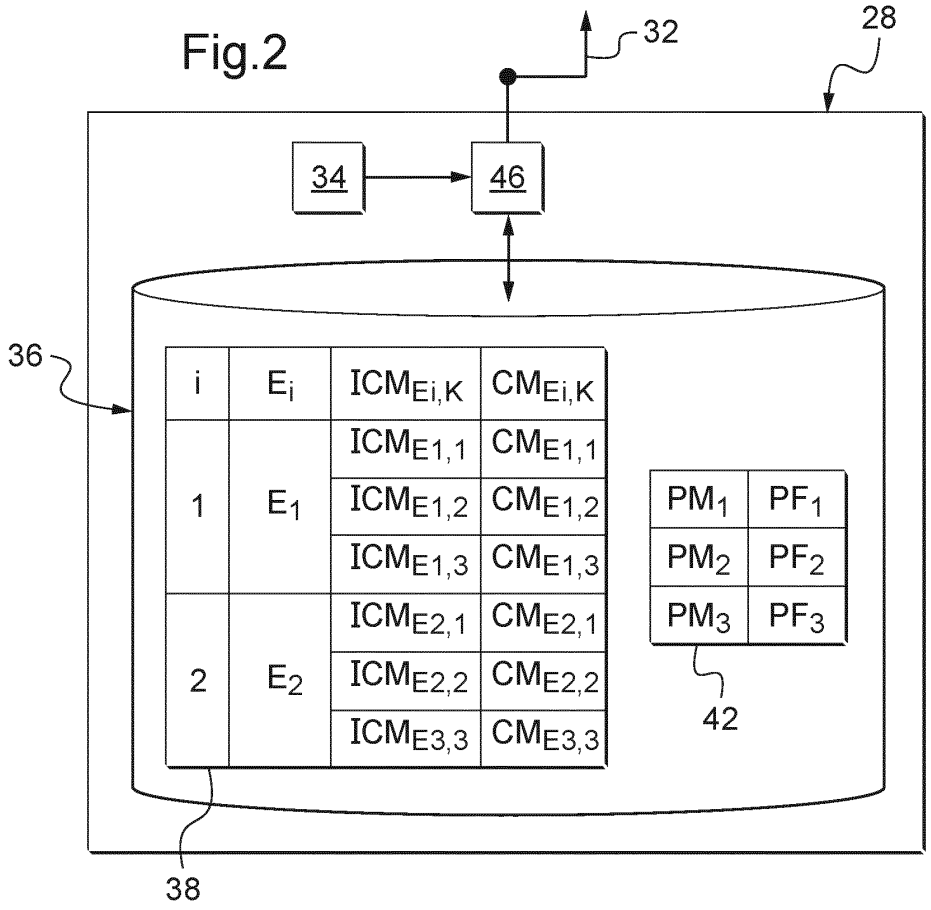


Fig.1

Fig.2



i	E_i	$ICM_{Ei,K}$	$CM_{Ei,K}$
1	E_1	$ICM_{E1,1}$	$CM_{E1,1}$
		$ICM_{E1,2}$	$CM_{E1,2}$
		$ICM_{E1,3}$	$CM_{E1,3}$
2	E_2	$ICM_{E2,1}$	$CM_{E2,1}$
		$ICM_{E2,2}$	$CM_{E2,2}$
		$ICM_{E3,3}$	$CM_{E3,3}$

PM_1	PF_1
PM_2	PF_2
PM_3	PF_3

Fig.3

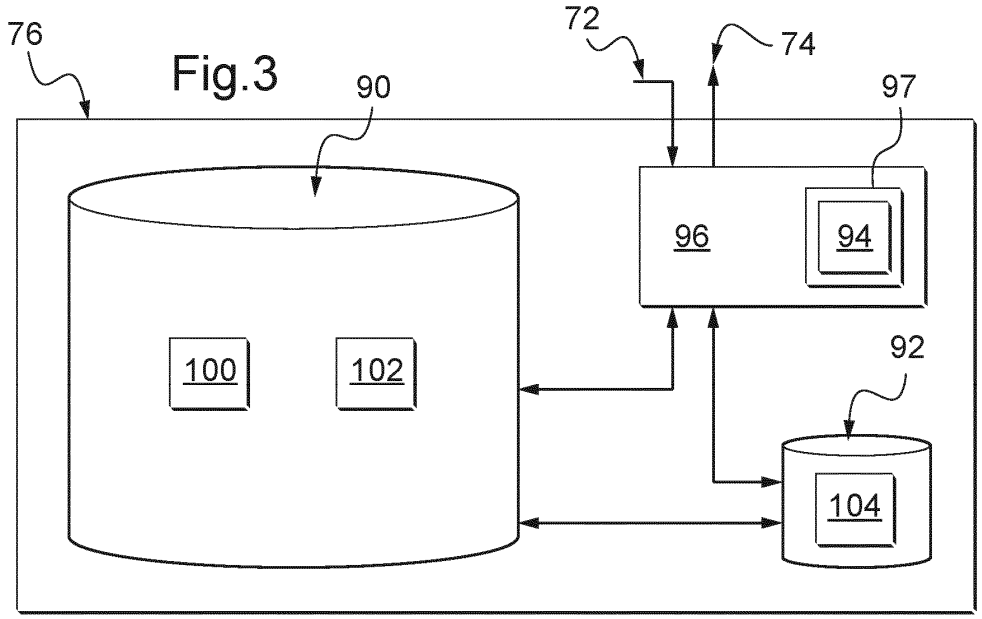


Fig.3a

100

i	$ICF_{Ei,K}$	$CF^*_{Ei,K}$
1	$ICF_{E1,1}$	$CF^*_{E1,1}$
	$ICF_{E1,2}$	$CF^*_{E1,2}$
	$ICF_{E1,3}$	$CF^*_{E1,3}$
2		

Fig.3b

102

i	$ICF_{Ei,K}$	$K\text{-}CF_{Ei,K}$	$Ksign\_CF_{Ei,K}$
1	$ICF_{E1,1}$	$K\text{-}CF_{E1,1}$	$K\text{-}CF_{E1,1}$
	$ICF_{E1,2}$	$K\text{-}CF_{E1,2}$	$K\text{-}CF_{E1,2}$
	$ICF_{E1,3}$	$K\text{-}CF_{E1,3}$	$K\text{-}CF_{E1,3}$
2			

Fig.3c

104

i:	$ICF_{Ei,K}$:	$CF_{Ei,K}$:
1	$ICF_{E1,1}$	
	$ICF_{E1,2}$	
	$ICF_{E1,3}$	
2	$ICF_{E2,1}$	
	$ICF_{E2,2}$	
	$ICF_{E3,3}$	

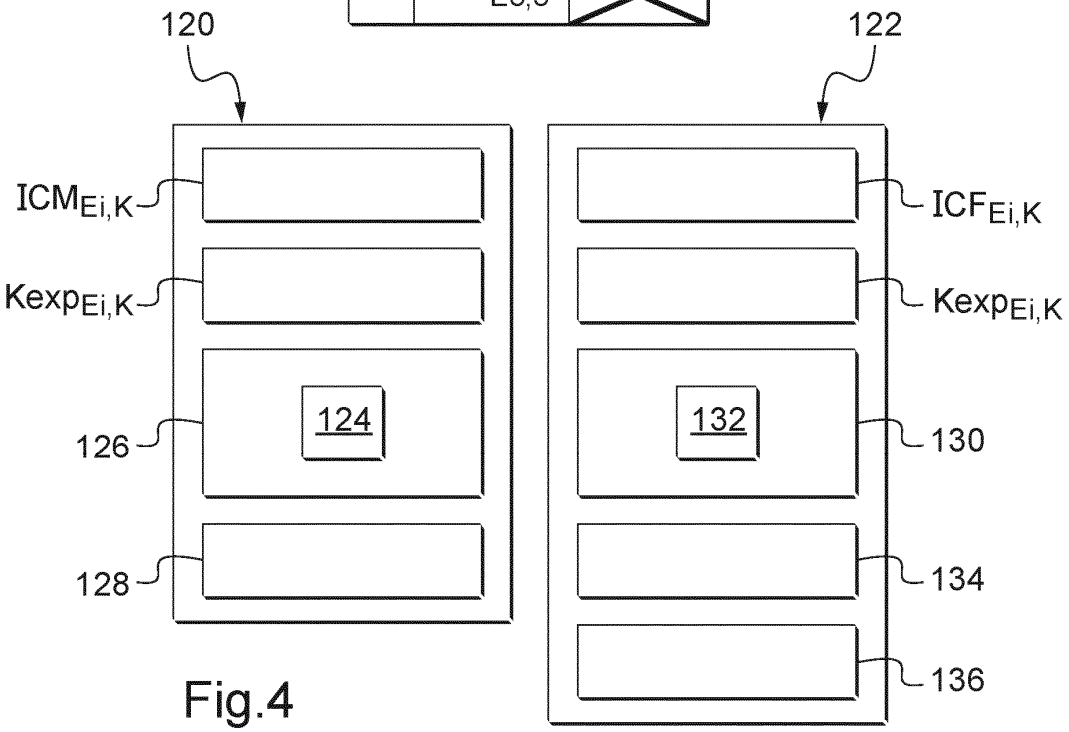
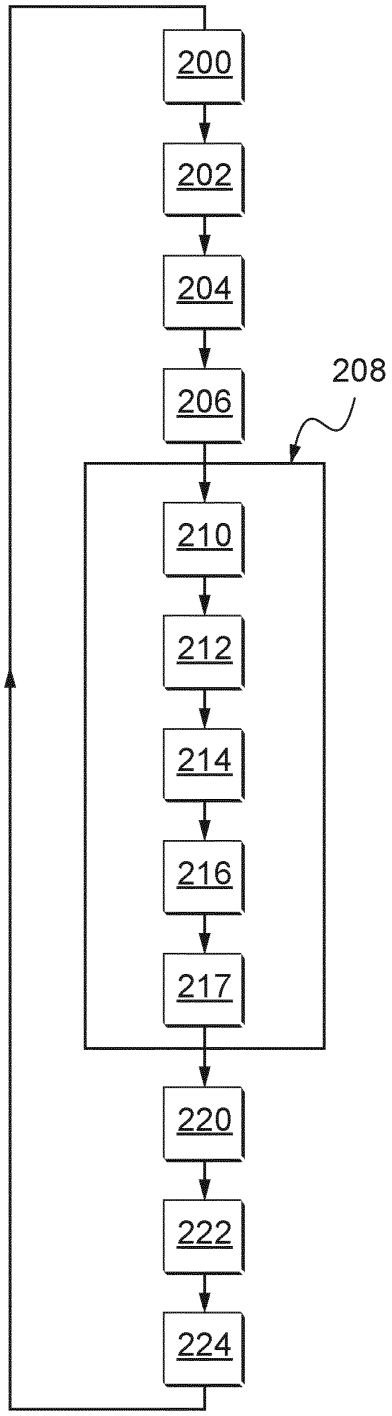


Fig.4

Fig.5



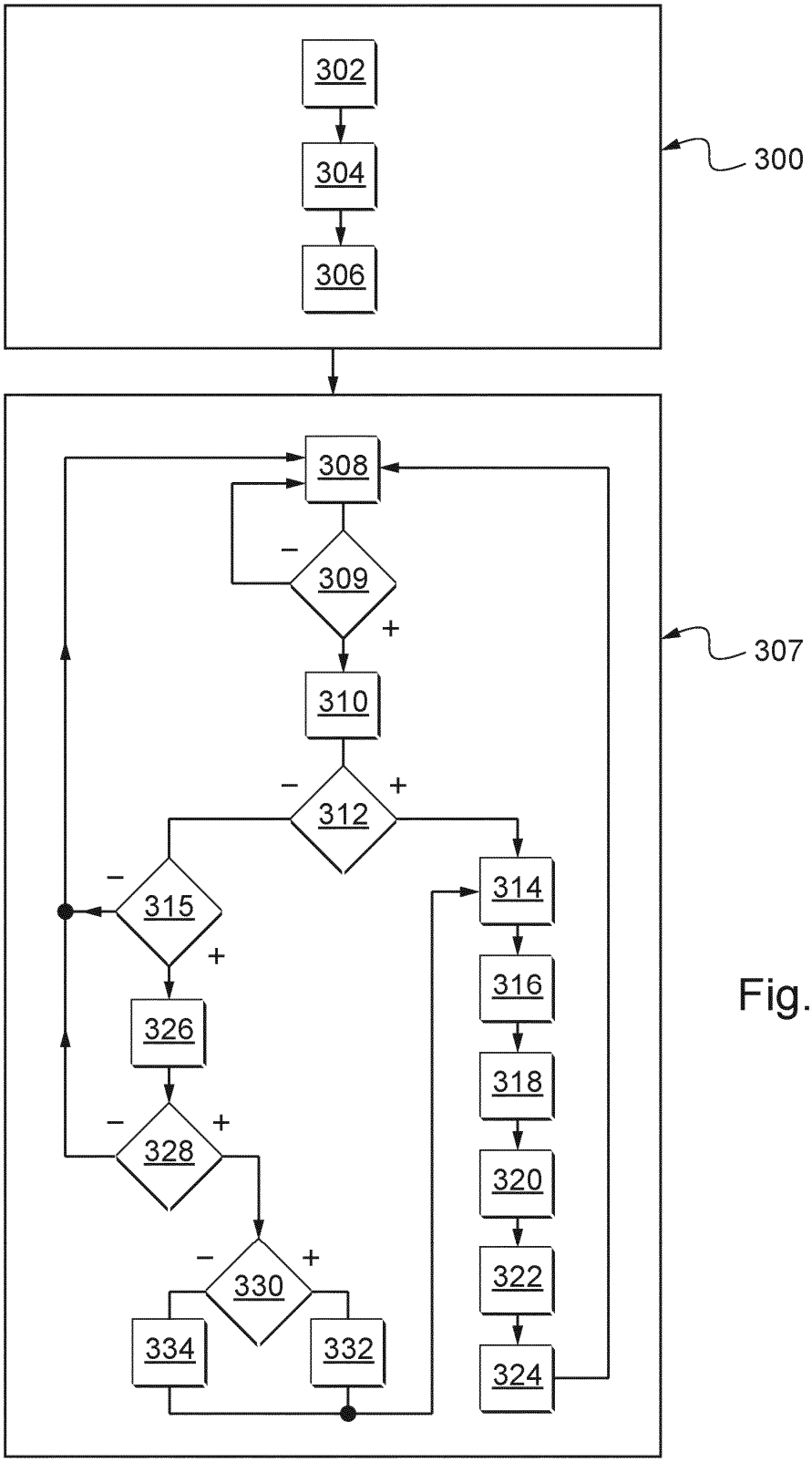

302
304
306
300
308
309
307
310
312
315
314
316
326
318
328
320
330
322
334
332
324

Fig.6