(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 645 954**

(51) Int. CI.:

H04N 21/4623 (2011.01)
H04N 21/266 (2011.01)
H04N 21/418 (2011.01)
G06K 19/077 (2006.01)
G06K 19/073 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.06.2012 E 12173840 (5)**

(97) Fecha y número de publicación de la concesión europea: **30.08.2017 EP 2541964**

(54) Título: **Sistema y procedimiento de emisión y de recepción de contenidos multimedia codificados**

(30) Prioridad:

28.06.2011 FR 1155758

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2017

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
F-92057 Paris La Defense Cedex, FR

(72) Inventor/es:

DUBROEUCQ, GILLES

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema y procedimiento de emisión y de recepción de contenidos multimedia codificados

La invención se refiere a un sistema y a un procedimiento de emisión y de recepción de un contenido multimedia codificado así como a un procesador de seguridad para este sistema.

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

Es conocido el hecho de difundir varios contenidos multimedia al mismo tiempo. Para ello, cada contenido multimedia es difundido sobre su propio canal. El canal utilizado para transmitir un contenido multimedia es igualmente conocido con el término de « cadena ». Un canal corresponde típicamente a una cadena de televisión. Ello permite a un usuario elegir simplemente el contenido multimedia que desea visualizar cambiando de canal.

En esta descripción, se designa más específicamente por « contenido multimedia » 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 proteger y someter la visualización de los contenidos multimedia a ciertas condiciones, como la suscripción de un abono de paga por ejemplo, los contenidos multimedia son difundidos en forma codificada y no en abierto. En esta descripción, el canal es llamado « codificado » cuando el contenido multimedia difundido sobre este canal está codificado.

Más precisamente, cada contenido multimedia está dividido en una sucesión de criptoperíodos. Mientras dura un criptoperíodo, las condiciones de acceso al contenido multimedia codificado permanecen sin cambios. En particular, en toda la duración de un criptoperíodo, el contenido multimedia es codificado con la misma palabra de control. Generalmente, la palabra de control varía de un criptoperíodo al otro.

Además, la palabra de control es generalmente específica de un contenido multimedia, siendo este último extraído aleatoriamente o pseudo-aleatoriamente.

Aquí, los términos « codificar » y « cifrar » son considerados como sinónimos, lo mismo sucede para los términos « descodificar » y « descifrar ».

El contenido multimedia en abierto corresponde al contenido multimedia antes de que éste sea codificado. Este puede ser hecho directamente comprensible por un ser humano sin haber recurrido a operaciones de descodificado y sin que su visualización sea sometida a ciertas condiciones.

Las palabras de control necesarias para descodificar los contenidos multimedia son transmitidas de manera sincronizada con los contenidos multimedia. Para ello, por ejemplo, las palabras de control son multiplexadas con el contenido multimedia codificado.

Para proteger la transmisión de las palabras de control, estas son transmitidas a los terminales en forma de criptogramas contenidos en mensajes ECM (Entitlement Control Message). Se designa aquí por « criptograma » una información insuficiente por sí sola para encontrar la palabra de control en abierto. Así, si la transmisión de la palabra de control es interceptada, el único conocimiento del criptograma de la palabra de control no permite encontrar la palabra de control que permite descodificar el contenido multimedia.

Para encontrar la palabra de control en abierto, es decir la palabra de control que permite descodificar directamente el contenido multimedia, ésta debe ser combinada con una información secreta. Por ejemplo, el criptograma de la palabra de control es obtenido cifrando la palabra de control en abierto con una clave criptográfica. En este caso, la información secreta es la clave criptográfica que permite descifrar este criptograma. El criptograma de la palabra de control puede también ser una referencia a una palabra de control almacenada en una tabla que contiene una multitud de palabras de control posibles. En este caso, la información secreta es la tabla que asocia a cada referencia una palabra de control en abierto.

La información secreta debe ser preservada en lugar seguro. Para ello, se ha propuesto ya almacenar la información secreta en procesadores de seguridad tales como tarjetas de chip directamente conectadas a cada uno de los terminales.

Por otra parte, los contenidos multimedia difundidos sobre los diferentes canales pueden ser coordinados temporalmente entre ellos. Por ejemplo, los instantes de difusión de los contenidos multimedia son regulados para respetar los horarios de difusión indicados sobre una parrilla de programas preestablecida. Cada terminal sobre un canal dado recibe por tanto sensiblemente al mismo tiempo el mismo contenido multimedia. Se dice que estos contenidos multimedia son flujos « vivos » o « lineales » pues el usuario no controla su instante de transmisión.

En este contexto, se han desarrollado ataques para permitir a usuarios descodificar contenidos multimedia para los que no han adquirido lícitamente derechos de acceso.

Por ejemplo métodos de criptoanálisis de un procesador de seguridad están descritos en el siguiente artículo:

Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, Claire Whelan, « The sorcerer's apprentice Guide to Fault Attacks ».

Así a pesar de las precauciones tomadas para proteger los procesadores de seguridad, estos son a veces víctimas de un criptoanálisis con éxito. Los datos secretos que incluyen resultan entonces conocidos, se trata esencialmente de las claves y de los algoritmos criptográficos utilizados. Es entonces posible producir procesadores de seguridad llamados « piratas » que permiten descodificar los contenidos multimedia sin pagar suscripción.

Para luchar contra este problema, sistemas conocidos de emisión y de recepción de un contenido multimedia incluyen:

- un dispositivo de difusión de una sucesión temporal de un primer contenido multimedia cifrado. Con un segundo contenido multimedia cifrado, siendo apto el dispositivo para filtrar el contenido de un primer mensaje ECM (Entitlement Control Message) o EMM (Entitlement Management Message) necesario para descifrar el primer contenido multimedia según un primer procedimiento criptográfico y para cifrar el contenido de un segundo mensaje ECM o EMM necesario para descodificar el segundo contenido multimedia según un segundo procedimiento criptográfico diferente del primer procedimiento criptográfico,

- terminales aptos para recibir el primer y segundo contenidos multimedia codificados y el primer y segundo mensajes ECM o EMM,

- al menos un procesador de seguridad amovible equipado de un soporte de aprehensión y de un chip electrónico nominal apto para tratar los mensajes ECM y EMM recibidos por el terminal, estando alojado este chip electrónico nominal sin ningún grado de libertad en el interior del soporte de aprehensión, incluyendo cada chip electrónico un calculador electrónico y una memoria no volátil de solo lectura únicamente accesible por este calculador y siendo cada chip electrónico desplazado de manera reversible entre una posición insertada en la que el chip es apto para comunicar con el terminal para recibir los mensajes ECM y EMM a tratar y una posición retirada en la que la comunicación entre el chip y el terminal es imposible, conteniendo la memoria no volátil de solo lectura del chip nominal primeros datos secretos necesarios para descifrar el contenido del primer mensaje ECM o EMM cifrado según el primer procedimiento criptográfico y estando desprovista de segundos datos secretos necesarios para descifrar el contenido de los segundos mensajes ECM o EMM cifrados según el segundo procedimiento criptográfico, y

- al menos un chip electrónico de emergencia apto para reemplazar el chip nominal para tratar los mensajes ECM y EMM recibidos por el terminal, incluyendo la memoria de solo lectura del chip de emergencia los segundos datos secretos.

El chip de emergencia está alojado en un nuevo procesador de seguridad que tienen un soporte de aprehensión idéntico a aquel en el que está alojado el chip nominal pero mecánicamente independiente de este primero. A partir de entonces, en caso de criptoanálisis con éxito, el procesador de seguridad es pirateado, y el operario envía a cada abonado el nuevo procesador de seguridad, y luego el abonado reemplaza al antiguo procesador de seguridad por el nuevo procesador de seguridad.

Este sistema permite reemplazar los datos secretos contenidos en la memoria no volátil de solo lectura por otros datos secretos. Además, el nuevo procesador de seguridad dispone de mecanismos de protección distintos de los antiguos procesadores de seguridad. La seguridad del sistema es entonces restaurada pues los antiguos procesadores de seguridad no son ya utilizables para descodificar los contenidos multimedia. En efecto, en paralelo, el segundo procedimiento criptográfico es utilizado para cifrar las informaciones contenidas en los mensajes ECM y EMM de manera que estos contenidos no sean descifrables más que por los nuevos procesadores de seguridad.

Sin embargo este sistema es poco práctico pues supone el envío a cada abonado de un nuevo procesador de seguridad en caso de criptoanálisis con éxito del chip nominal.

El estado de la técnica es igualmente conocido por:

- el documento US 5 847 372A,

- el documento US 2002/023963 A1.

- el documento NL 9301540A

- el documento KR 101017425B1,

- el documento WO 2008/025900 A1.

El documento US 6922780 describe una tarjeta con chip que tienen dos procesadores: un procesador nominal y un

procesador de emergencia que puede ser activado si el procesador nominal cesa de funcionar normalmente. El basculamiento hacia el chip de emergencia es hecho cambiando la orientación de la tarjeta en el receptor.

La invención pretende remediar este problema proponiendo un sistema en que el reemplazamiento del chip nominal por el chip de emergencia es más simple. Tiene por tanto por objeto un sistema de emisión y de recepción conforme a la reivindicación 1.

En el sistema anterior, el procesador de seguridad está equipado con dos chips electrónicos desde el origen es decir el chip nominal y el chip de emergencia. Así, cuando un cambio de chip electrónico es deseable, no es necesario enviar a cada abonado el chip de emergencia. Por el contrario, en el sistema anterior, basta simplemente reemplazar el chip nominal por el chip de emergencia que está ya a disposición del abonado. Así, este sistema permite hacer economía del envío de un nuevo procesador de seguridad que incluye el chip de emergencia.

El hecho de que los dos chips electrónicos estén alojados en el mismo soporte permite igualmente hacer economía de un soporte de aprehensión con relación al sistema del estado de la técnica.

Además, el chip nominal y el chip de emergencia son solidarios del mismo soporte de aprehensión de manera que el riesgo de perder el chip de emergencia antes de que sea utilizado es nulo.

Finalmente, el cambio de procedimiento criptográfico hace el reemplazamiento del chip nominal por el chip de emergencia irreversible. En efecto, después de este reemplazamiento, el chip nominal no es ya utilizable para descodificar los contenidos multimedia.

La invención tiene igualmente por objeto un procesador de seguridad para la puesta en práctica del sistema anterior.

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

Estos modos de realización del procesador de seguridad presentan además las siguientes ventajas:

- la utilización de un conector eléctrico común para el chip nominal y para el chip de emergencia permite hacer el chip de emergencia inaccesible mientras el chip nominal es utilizado, lo que hace muy difícil cualquier tentativa de criptoanálisis de este chip de emergencia antes de que sea utilizado;

- el hecho de que sólo el chip nominal pueda hacer bascular el controlador hacia la posición de emergencia hace aún más difícil el acceso al chip de emergencia en tanto que el chip nominal es utilizado ya que es preciso antes de ello realizar el criptoanálisis del chip nominal si se desea realizar un basculamiento ilícito hacia la posición de emergencia;

- el hecho de que la instrucción de activación del chip de emergencia sea transmitida en un mensaje ECM o EMM aumenta la seguridad del sistema pues el basculamiento hacia el chip de emergencia puede entonces únicamente ser activado a partir del dispositivo de difusión;

- la utilización de un interruptor irreversible hace definitivo el basculamiento del chip nominal hacia el chip de emergencia de manera que el nominal no pueda ya ser utilizado;

- la utilización de un conector eléctrico nominal y de un conector eléctrico de emergencia permite reemplazar el chip nominal por el chip de emergencia por una simple rotación del procesador de seguridad alrededor de un eje de simetría de revolución;

- el hecho de que el chip de emergencia este en un estado desactivado antes de su utilización más difícil cualquier tentativa de criptoanálisis de este chip de emergencia.

La invención tiene igualmente por objeto un procedimiento de emisión y de recepción de un contenido multimedia cifrado conforme a la reivindicación independiente de este procedimiento.

La invención será mejor comprendida con la lectura de la descripción siguiente, dada únicamente a título de ejemplo no limitativo y hecha con referencia a los dibujos en los que:

La fig. 1 es una ilustración esquemática de un sistema de emisión y de recepción de contenidos multimedia;

La fig. 2 es una ilustración en vista desde arriba de un procesador de seguridad utilizado en el sistema de la fig. 1;

La fig. 3 es una ilustración parcial y en vista despiezada ordenadamente del procesador de seguridad de la fig. 2;

La fig. 4 es una ilustración esquemática de diferentes bloques funcionales integrados en el procesador de seguridad de las figs. 2 y 3;

La fig. 5 es un organigrama de un procedimiento de emisión y de recepción de contenidos multimedia con ayuda de un sistema de la fig. 1;

La fig. 6 es una ilustración esquemática de otro modo de realización de un procesador de seguridad utilizable en el sistema de la fig. 1;

La fig. 7 es un organigrama de un procedimiento de emisión y de recepción de contenidos multimedia utilizando el procesador de seguridad de la fig. 6.

En estas figuras las mismas referencias son utilizadas para designar los mismos elementos.

En la continuación de esta descripción, las características y funciones bien conocidas por el experto en la técnica no han sido descritas en detalle. Además, la terminología utilizada es la de los sistemas de acceso condicionales 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, Brussels, BE, nº 266, 21 de diciembre de 1995.

La fig. 1 representa un sistema 2 de emisión y de recepción de contenidos multimedia codificados. Los contenidos multimedia emitidos son contenidos multimedia lineales. 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 abierto son generados por una o varias fuentes 4 y transmitidos 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 son sincronizados temporalmente unos con otros para, por ejemplo, respetar una parrilla preestablecida de programas.

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

Para simplificar la fig. 1, sólo se han representado tres terminales 10 a 12 de recepción.

El dispositivo 6 comprende un codificador 16 que comprime los contenidos multimedia que recibe. El codificador 16 trata contenidos multimedia digitales. Por ejemplo, este codificador funciona conforme a la norma MPEG2 (Moving Picture Expert Group - 2) o a la norma UIT-T264.

Los contenidos multimedia comprimidos son dirigidos hacia una entrada 20 de un codificador 22. El codificador 22 codifica cada contenido multimedia comprimidos para acondicionar 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 codificados son restituidos sobre una salida 24 conectada a la entrada del multiplexador 26.

El codificador 22 codifica cada contenido multimedia comprimido con ayuda de una palabra de control $CW_{i,t}$ que le es proporcionada, así como a un sistema 28 de acceso condicional, por un generador 32 de claves. El índice i es un identificador del canal sobre el que es difundido el contenido multimedia cifrado y el índice t es un número de orden que identifica el criptoperíodo codificado con esta palabra de control.

Típicamente, este codificado es conforme a 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.

Para cada canal i, el sistema 28 genera mensajes $ECM_{i,t}$ (Entitlement Control Message), que contienen al menos el criptograma $CW^*_{i,t}$ de la palabra de control $CW_{i,t}$ generada por el generador 32 y utilizada por el codificador 22 para ilustrar el criptoperíodo t del canal i. Estos mensajes y los contenidos multimedia codificados son multiplexados por el multiplexor 26, siendo estos últimos respectivamente proporcionados por el sistema 28 de acceso condicional y por el codificador 22, antes de ser transmitidos sobre la red 8.

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

El sistema 28 insertar igualmente en cada ECM:

- los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ de las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$ que permiten descifrar los criptoperíodos t y t+1 inmediatamente consecutivos del canal i,

- condiciones de acceso CA destinadas a ser comparadas con títulos de acceso adquiridos por el usuario, y

- una firma o una redundancia criptográfica MAC que permite verificar la integridad del mensaje ECM.

El mensaje ECM que contiene el par de palabras de control $CW_{i,t}$ /$CW_{i,t+1}$ está referenciado $ECM_{i,t}$ en la continuación de la descripción donde:

- el índice i identifica el canal, y

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

A título de ilustración, aquí, el codificado y el multiplexado de los contenidos multimedia es conforme al protocolo DVB-Simulcrypt (ETSI TS 103 197).

El sistema 28 genera igualmente mensajes EMM (Entitlement Control Message). Generalmente, contrariamente a los mensajes ECM, los mensajes EMM están destinados a transportar informaciones dirigidas a un solo terminal o a un grupo limitado de terminales. Por ejemplo, los mensajes EMM son utilizados para transmitir títulos de acceso y una clave mensual de explotación Km a un terminal. La clave mensual es la clave utilizada para descifrar los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$. Los títulos de acceso y la clave mensual Km transmitidos al terminal son en primer lugar cifrados con una clave de gestión secreta Kt del terminal y sólo los criptogramas así obtenidos son incorporados al mensaje EMM. Para ello, el sistema 28 tiene necesidad de conocer los datos secretos asociados a este terminal tales como su clave Kt. A este efecto, el sistema 28 está conectado a un sistema 34 de autorización de acceso más conocido bajo el acrónimo SAS (Subscriber Authorization System). La clave secreta Kt es diferente de un terminal al otro. Típicamente la clave secreta está grabada en un procesador de seguridad insertado en este terminal.

Este sistema 34 incluye en particular una memoria 36 en la que está grabada una base de datos 38. La base de datos 38 asocia a cada identificador de un procesador de seguridad de un terminal, los datos secretos necesarios para generar criptogramas que pueda descifrar correctamente.

En este ejemplo, los terminales 10 a 12 son idénticos. También, en la continuación, sólo el terminal 10 se ha descrito con más detalle.

El terminal 10 descodifica el canal i para presentarlo en abierto sobre un presentador.

El terminal 10 comprende un receptor 70 de contenidos multimedia difundidos. Este receptor 70 está conectado a la entrada de un desmultiplexor 72 que transmite por un lado el contenido multimedia a un descodificador 74 y por otro lado los mensajes $ECM_{i,t}$ y EMM (Entitlement Management Message) a un procesador de seguridad 76.

El descodificador 74 descodifica el contenido multimedia codificado a partir de la palabra de control transmitida por el procesador 76. El contenido multimedia descodificado es transmitido a un descodificador 78 que le descodifica. El contenido multimedia descomprimido o descodificado es transmitido a una tarjeta gráfica 80 que pilota la presentación de este contenido multimedia sobre un presentador 82 equipado con una pantalla 84. El presentador 82 presenta en abierto el contenido multimedia sobre la pantalla 84. Por ejemplo, el presentador 82 es una televisión, un ordenador o aún un teléfono fijo o móvil. Aquí, el presentador es una televisión.

Típicamente, la interfaz entre el terminal 10 y el procesador 76 comprende un lector 86 gestionado por un módulo 88 de control de acceso. Aquí el lector 86 es un lector de tarjetas de chip. El módulo 88 gestiona en particular:

- la transmisión de los mensajes ECM y EMM desmultiplexados al procesador 76, y

- la recepción de las palabras de control descifrada por el procesador 76 y su transmisión al descodificador 74.

El procesador 76 trata informaciones confidenciales tales como claves criptográficas. Para preservar la confidencialidad de estas informaciones, está concebido para ser lo más robusto posible frente a tentativas de ataques llevadas a cabo por piratas informáticos. Es por tanto más robusto frente a estos ataques que los otros componentes del terminal 10. Aquí, el procesador 76 es una tarjeta con chip.

El procesador 76 está equipado con un chip electrónico nominal 90 y con un chip electrónico 92 de emergencia. Cada chip electrónico comprende un calculador electrónico y medios de almacenamiento de informaciones únicamente accesibles por el calculador. Típicamente, los medios de almacenamiento de informaciones de cada chip comprenden:

- una memoria no volátil de sólo lectura,

- una memoria no volátil regrabable, y

- una memoria volátil.

La memoria no volátil de sólo lectura contiene datos secretos necesarios para el descifrado de las palabras de control. La memoria no volátil regrabable contiene además datos configurables tales como títulos de acceso y claves mensuales Km. En la fig. 1, el calculador, los medios de almacenamiento de informaciones, la memoria no volátil de sólo lectura, la memoria no volátil regrabable y la memoria volátil del chip 90 llevan, respectivamente las referencias 94 a 98. Estos mismos elementos llevan, respectivamente, las referencias 100 a 104 para el chip 92. Cada calculador 94, 100 es un calculador electrónico programable apto para ejecutar instrucciones grabadas sobre un soporte de grabación de informaciones. A este efecto, las memorias 96 y 102 no volátil de lectura solamente contienen datos secretos tales como las instrucciones y las claves secretas necesarias para la ejecución del procedimiento de la fig. 5 o 7. Aquí, los datos secretos grabados en estas memorias 96 y 102 incluyen además:

- el código de un sistema de explotación;

- el código de las rutinas ejecutadas para tratar los mensajes ECM y EMM recibidos y algoritmos de descifrado/cifrado, y

- claves criptográficas.

Más precisamente y a título de ilustración, la memoria 96 contiene además una clave secreta Kt1 y el código ejecutable de un algoritmo ALGO1 de descifrado de los criptogramas de las palabras de control. La memoria 102 contiene de manera similar una clave secreta Kt2 y el código ejecutable de un algoritmo ALGO2 de descifrado de los criptogramas de las palabras de control.

En estas condiciones, la base de datos 38 asocia en particular a cada identificador de un procesador de seguridad, tal como el procesado 76 las claves secretas Kt1 y Kt2 contenidas, respectivamente, en las memorias 96 y 102.

Las figuras 2 y 3 representantes con más detalle el procesador 76.

El procesador 76 incluye un soporte de aprehensión 120. Aquí, el soporte 120 es una tarjeta plana y sensiblemente rectangular dispuesta en la horizontal. Típicamente, la anchura y la longitud del soporte 120 son al menos diez veces superiores a su grosor en la dirección vertical. Por ejemplo, la anchura de la tarjeta es inferior a 11 cm o a 9 cm. La longitud de la tarjeta es inferior a 6 o 7 cm. El grosor del soporte 120 es inferior a 5 o 2 mm. El soporte 120 presenta aquí dos planos de simetría verticales 122 y 124. En la fig. 2, estos planos 122 y 124 están representados por líneas que llevan las mismas referencias. Estos planos 122 y 124 son ortogonales entre sí. La intersección de estos planos define un eje vertical O.

Típicamente, el soporte 120 está realizado de plástico. Este soporte es por ejemplo conforme a la norma ISO 7816-1.

El soporte 120 presenta una cara plana superior 126, una cara plana inferior opuesta a la cara 126, un borde izquierdo 128 y un borde derecho 130. Los bordes 128 y 130 están conectados unos a otros por bordes laterales 132 y 134 paralelos entre sí.

Un chip electrónico 90, 92 es susceptible de ser conectado al lector 86 por medio de un conector eléctrico. Aquí, el procesador 76 incluye dos conectores eléctricos 140 y 142 para permitir la conexión al lector 86, respectivamente, de los chips 90 y 92. Aquí estos conectores 140 y 142 son conformes a la norma ISO 7816-2. Incluyen a partir de entonces ocho contactos eléctricos aptos para cooperar con contactos eléctricos correspondientes del lector 86. Estos conectores permiten alimentar los chips y comunicar con estos chips.

Los chips 90 y 92 están alojados en el interior del soporte 120 de tal manera que sólo los conectores eléctricos 140 y 142 son accesibles desde el exterior de este soporte. A este efecto, típicamente, los chips electrónicos están ocultos en el grosor del soporte 120. Aquí, los conectores 140 y 142 están enrasados sobre la cara superior 126 del soporte 120.

Cada contacto de los conectores 140 y 142 está eléctricamente conectado permanentemente por una unión mediante hilos a un borne correspondiente del chip electrónico.

Cada chip electrónico es desplazable entre:

- una posición insertada en la que el conector eléctrico al que está conectado está en contacto eléctrico con el conector del lector 86 para permitir la alimentación y la comunicación entre este chip y el terminal 10, y

- una posición retirada en la que el contacto eléctrico entre los conectores 140 y 142 y el lector es interrumpido de manera que cualquier comunicación entre el chip y el terminal es imposibilitada en esta posición.

Cada chip está alojado en un alojamiento ciego ahuecado a partir de una cara del soporte 120. Tal alojamiento ciego 144 está representado por ejemplo en la fig. 3. Aquí, los dos alojamientos ciegos que reciben respectivamente los chips 90 y 92 están ahuecados a partir de la cara superior 126 del soporte 120. En cada alojamiento ciego, el chip electrónico está fijado sin ningún grado de libertad al soporte con ayuda, por ejemplo, de pegamento 146. Aquí, el conector eléctrico 140 recubre el chip electrónico 90 de manera que le proteja del exterior.

En este modo de realización, los dos conectores eléctricos 140 y 142 están dispuestos sobre esta cara superior 126 de manera que permitan el reemplazamiento del chip 90 por el chip 92 por una simple inversión del soporte 120. Por ejemplo aquí, los conectores 140 y 142 están dispuestos de manera que cuando se hace girar 180° el soporte 120 alrededor del eje O, el conector 142 viene a ocupar el lugar del conector 140 y viceversa. Esta operación de rotación del soporte 120 para invertir las posiciones de los conectores eléctricos es denominada « inversión ».

La fig. 4 representa a título de ilustración diferentes bloques funcionales del chip electrónico 90. Aquí el chip 90 incluye los bloques funcionales siguientes:

- un gestor 150 del protocolo de comunicación entre el procesador 76 y el lector 86,

- dispositivos materiales 152 de protección del chip electrónico contra tentativas de criptoanálisis,

- un generador 154 de números pseudo-aleatorios,

- un acelerador criptográfico 156 formado en parte por una lógica cableada y que permite acelerar la ejecución de los algoritmos criptográficos,

- una unidad material 158 de tratamiento central, más conocida bajo el acrónimo inglés CPU (Central Processing Unit),

- un bus 160 que une entre sí los diferentes elementos materiales del chip 90,

- un módulo 162 de control de acceso a los medios 95 de almacenamiento de informaciones.

El dispositivo 152 es por ejemplo una película que recubre al menos una parte del chip electrónico y que libera un ácido cuando es perforada. Así, si esta película es perforada durante una tentativa de criptoanálisis, entonces el ácido viene a destruir los diferentes componentes sensibles del chip 90 para hacerle inutilizable. El dispositivo 152 puede igualmente incluir un sensor de intensidad luminosa o de tensión para detectar ataques por orden de fallos.

El chip 92 es idéntico al chip 90 salvo que:

- al menos una parte de los datos secretos grabados en la memoria 102 son diferentes de los datos secretos grabados en la memoria 96, y

- de preferencia, el chip 92 está realizado materialmente de manera diferente del chip 90.

Por ejemplo, aquí, las claves secretas Kt1 y Kt2 y los algoritmos ALGO1 y ALGO2 grabados, respectivamente, en las memorias 96 y 102 son diferentes. Además, aquí, los chips 90 y 92 son fabricados por fabricantes diferentes de manera que presentan diferencias materiales uno con relación al otro. Por ejemplo, el chip 92 incluye dispositivos materiales de protección diferentes de los del chip 90. Aquí, el código del sistema de explotación grabado en la memoria 96 es diferente del grabado en la memoria 102, lo mismo que los códigos de las rutinas utilizadas para tratar los mensajes ECM y EMM.

Finalmente, el chip 92 está programado para comenzar a tratar los mensajes ECM y EMM solamente después de haber recibido una instrucción de activación. Antes de la recepción de esta descripción de activación, el chip de emergencia están en estado desactivado. En este estado desactivado, el chip 92 realiza únicamente las operaciones siguientes:

- responde a la puesta bajo tensión, y

- compara los valores de los bits en posiciones predeterminadas en los mensajes ECM o EMM recibidos en un tique de activación grabado en la memoria 102. Si el valor de los bits recibidos corresponde a este tique de activación, entonces el chip 92 considera que acaba de recibir la instrucción de activación. En respuesta pasa a un estado activado.

En el estado activado, el chip 92 desempeña las mismas funciones que el chip 90 y, en particular, trata de los mensajes ECM y EMM para descifrar las palabras de control.

El funcionamiento del sistema 2 va a ser descrito a continuación con más detalle en referencia al procedimiento de la fig. 5 en el caso particular del terminal 10. El funcionamiento de los otros terminales se deduce del descrito para el terminal 10.

Inicialmente, durante una etapa 198, el procesado 76 es suministrado al titular del terminal 10. A partir de entonces, el chip 90 está en la posición insertada y el chip 92 está en el estado desactivado.

Durante una etapa 200, las palabras de control utilizadas para codificar el contenido multimedia difundido son cifradas con el algoritmo ALGO1 y con ayuda de una clave mensual Km1. La clave mensual Km1 es a su vez cifrada con ayuda de las claves Kt1 de cada terminal. El criptograma de la clave Km1 así obtenido es transmitido previamente a cada uno de estos terminales por medio de un mensaje EMM.

A continuación, durante una etapa de 202, el contenido multimedia cifrado es multiplexado con los mensajes ECM y EMM a transmitir a los terminales y luego difundido hacia cada uno de estos terminales por medio de la red 8.

Durante una etapa 204 cada terminal recibe el multiplex así difundido y lo demultiplexa. Los mensajes ECM y EMM extraídos de este multiplex son entonces transmitidos por el terminal 10 hacia el procesador 76.

Durante una etapa 206, el chip 90 compara derechos de acceso contenidos en el mensaje ECM recibido con títulos de acceso grabados en la memoria 97. Si los títulos de acceso corresponden a los derechos de acceso recibidos, entonces el chip 90 descifra los criptogramas $CW^*_{i,t}$ contenidos en el mensaje ECM recibido con ayuda del algoritmo ALGO1 y de la clave mensual Km1. A continuación, la palabra de control así descifrada es transmitida al terminal 10 por medio del lector 86.

En respuesta, durante una etapa 208, el terminal 10 descodifica el contenido multimedia con ayuda de la palabra de control descifrada por el chip 90 y luego presenta en abierto el contenido multimedia así descifrado sobre la pantalla 84.

Las etapas 200 a 208 son reiteradas mientras la seguridad del chip 90 no haya sido comprometida.

Cuando el chip 90 ha sido víctima de una tentativa con éxito de criptoanálisis, durante una etapa 210, el operador del sistema 2 solicita a sus abonados proceder a la inversión de sus procesadores de seguridad respectivos en una fecha determinada. A partir de entonces, el chip de emergencia se encuentra en la posición insertada en el lector 86.

En esta fecha determinada, durante una etapa 212, el dispositivo 6 difunde al conjunto de los terminales un mensaje ECM que contiene la instrucción de activación del chip de emergencia.

Durante una etapa 214, el chip 92 compara la instrucción de activación contenida en el mensaje ECM recibido con el tique de activación contenido en su memoria 102. Si la instrucción de activación no corresponde al tique de activación, entonces el chip 92 queda en el estado desactivado. En el caso contrario, bascula al estado activado durante una etapa 216.

En paralelo, durante la etapa 217, el dispositivo 6 envía, por medio de mensajes EMM, el conjunto de los títulos de acceso del abonado del terminal 10 para que sean almacenados en el chip 92.

A partir de la fecha determinada, se procede a etapas sucesivas 218, 220, 222, 224 y 226 idénticas, respectivamente, a las etapas 200, 202, 204, 206 y 208 salvo que:

- durante la etapa 218, es el algoritmo ALGO2 y las claves personales Kt2 almacenados en la memoria 102 los que son utilizados, y

- durante la etapa 224, es el chip 92 el que trata los mensajes ECM y EMM recibidos y no ya el chip 90.

Durante la etapa 224, el algoritmo ALGO2 es utilizado en lugar del algoritmo ALGO1 para descifrar la palabra de control.

La fig. 6 representa otro modo de realización de un procesador 228 de seguridad susceptible de ser utilizado en el sistema de la fig. 1. Este procesador 228 es idéntico al procesador 76 salvo en que:

- el conectador 142 es omitido,

- los chips 90, 92 son reemplazados por chips 230, 231, y

- un controlador 232 es interpuesto entre los chips 230, 231 y el conector eléctrico 140.

Así, en este modo de realización, el conector eléctrico 140 es común a los chips 230 y 231. El conector 140 incluye ocho contactos eléctricos 234 a 241 aptos para entrar en contacto eléctrico con contactos correspondientes del lector 86 para establecer la comunicación entre este procesador 230 y el lector 86. Estos ocho contactos 234 a 241 son conectados de manera permanente por medio de uniones con hilos a ocho entradas correspondientes del controlador 232 designadas. Estas ocho entradas están designadas colectivamente por la referencia 242.

El controlador 232 incluye igualmente:

- ocho salidas 244 conectadas de manera permanente, respectivamente, a ocho bornes 246 correspondientes del chip 230, y

- ocho salidas 248 conectadas de manera permanente, respectivamente, a ocho bornes 250 correspondientes del chip 231.

En la fig. 6, las salidas 244 y 248 así como los bornes 246 y 250 están representados por un solo punto para simplificar esta ilustración. Por las mismas razones, las uniones eléctricas entre las salidas 244 y 248 y los bornes 246 y 250 han sido representadas simplemente por una doble flecha.

El controlador 232 bascula entre:

- una posición nominal en la que conecta únicamente las ocho entradas 242 a las ocho salidas 244 para conectar el chip 230 a los contactos del conector 140, y

- una posición de emergencia en la que conecta eléctricamente únicamente las ocho entradas 242 a las ocho salidas 248 para conectar el chip 92 a los contactos del conector 140.

El controlador 232 incluye igualmente una entrada 252 de mando del basculamiento entre la posición nominal y la posición de emergencia. La entrada 252 está aquí conectada de manera permanente al contacto de masa 241 del conector 140 por medio de un interruptor irreversible 254. El interruptor 254 es únicamente desplazable una sola vez:

- desde una posición inicial, aquí la posición cerrada, en la que conecta eléctricamente la entrada 252 al contacto 241, hacia

- una posición final, aquí la posición abierta, en la que aísla eléctricamente la entrada 252 de este contacto 241.

Por ejemplo el interruptor 254 es un fusible susceptible de fundirse en respuesta a una orden del chip 230. A este efecto, una unión mediante hilos 256 conecta un borne de mando del interruptor 254 al chip 230.

El chip 230 es idéntico al chip 90 salvo en que está programado para mandar el basculamiento del controlador 232 desde su posición nominal hacia su posición de emergencia en respuesta a la recepción de una instrucción de activación transmitida en un mensaje ECM por el dispositivo 6. Para ello, el chip 230 manda la apertura del interruptor 254. En respuesta, el controlador 232 báscula desde su posición nominal hacia su posición de emergencia. Así, sólo el chip 230 es capaz de ordenar el basculamiento del controlador 232. De preferencia, la instrucción de activación está cifrada con una clave tal como la clave mensual Km1.

El chip 231 es idéntico al chip 92 salvo que no incluye código capaz de tratar la instrucción de activación como se ha descrito en el caso del chip 92.

El funcionamiento del sistema 2, cuando éste está equipado con el procesador 228, va a ser descrito a continuación con referencia al procedimiento de la fig. 7.

Este procedimiento comienza por las mismas etapas 198 a 208 que las precedentes. A la salida de la etapa 208, en caso de criptoanálisis con éxito del chip 230, el procedimiento procede directamente a la etapa 212 sin pasar por la etapa 210. En efecto, en este modo de realización, ya no es necesario invertir el procesador de seguridad para desplazar el chip 231 hacia su posición insertada.

A continuación, se procede a una etapa 280 e idéntica a la etapa 214 salvo en que la instrucción de activación del chip de emergencia es descifrada en primer lugar con la clave mensual Km1 antes de ser comparada con el tique de activación.

En el caso en que la instrucción de activación corresponde al tique de activación, durante una etapa 282, el chip 230 ordena la apertura del interruptor 254. Por ejemplo, el chip 230 hace fundir el fusible por medio de la unión mediante hilos 256.

En respuesta, durante una etapa 284, el controlador 232 báscula desde su posición nominal hacia su posición de emergencia. A partir de este instante, el chip 231 es activado y puede tratar los mensajes ECM y EMM recibidos por medio del conector 140. A la inversa, el chip 230 es desactivado definitivamente ya que el basculamiento inverso, es decir desde la posición de emergencia hacia la posición nominal, está prohibido por el interruptor 254.

En paralelo de las etapas 280 a 284, se procede a etapas 286, 288, 290, 292, 294 y 296 respectivamente idénticas a las etapas 217, 218, 220, 222, 224 y 226 del procedimiento de la fig. 5.

Son posibles otros numerosos modos de realización. Por ejemplo, el soporte de aprehensión puede tener otras formas. Por ejemplo, en una variante, el soporte de aprehensión puede tomar la forma de una clave USB (Universal Serial Bus). En este caso, los conectores eléctricos son colectores eléctricos conformes a la norma USB.

En el caso en que el procesador incluya un conector eléctrico para cada chip, éstos conectores eléctricos pueden estar dispuestos en otros emplazamientos distintos a los representados en la fig. 2. Por ejemplo, un conector eléctrico puede encontrarse sobre la cara superior mientras el otro se encuentra sobre la cara inferior. En este caso, la inversión del procesador de seguridad consiste en efectuar una rotación de 180° alrededor de un eje de rotación horizontal.

El número de conectores eléctricos y el número de chips alojados en el soporte 120 puede ser superior a dos. Por ejemplo, está comprendido entre dos y cuatro conectores eléctricos y por tanto dos y cuatro chips.

Igualmente, en el modo de realización de la fig. 6, el procesador 228 puede incluir más de dos chips electrónicos. En este caso, la desactivación del chip en el estado activado entraña la activación automática de un chip siguiente. Por ejemplo, el mismo mecanismo que el descrito para activar el chip 231 es empleado para activar el chip siguiente.

El chip de emergencia puede también ser activado en respuesta a una instrucción de activación contenida en un mensaje EMM. La activación del chip de emergencia, en otro modo de realización, es realizada tele-cargando una parte del código de este tipo a partir de un mensaje EMM recibido.

Lo que se ha descrito precedentemente en el caso de un sistema de emisión y de recepción de contenidos multimedia lineales se aplica igualmente a un sistema de emisión y recepción de contenidos multimedia no lineales tal como un sistema de video bajo demanda (« Video On Demand » en inglés).

REIVINDICACIONES

1. Sistema de emisión y de recepción de un contenido multimedia cifrado, incluyendo este sistema:

- un dispositivo (6) de difusión de un primer contenido multimedia codificado y luego de un segundo contenido multimedia codificado, siendo apto el dispositivo para filtrar y para difundir el contenido de un primer mensaje ECM (Entitlement Control Message) o EMM (Entitlement Management Message) necesario para descodificar el primer contenido multimedia según un primer procedimiento criptográfico, utilizando una primera clave criptográfica y un primer algoritmo criptográfico, y en cifrar y en difundir el contenido de un segundo mensaje ECM o EMM necesario para descodificar el segundo contenido multimedia según un segundo procedimiento criptográfico, utilizando una segunda clave criptográfica y un segundo algoritmo criptográfico, diferente del primer procedimiento criptográfico,

- terminales (10-12) aptos para recibir el primer y segundo contenidos multimedia codificados y el primer y segundo mensajes ECM o EMM,

- al menos un procesador (228) de seguridad amovible equipado:

  - de un soporte (120) de aprehensión,

  - de un chip electrónico nominal (230) apto para tratar el primer mensaje ECM o EMM recibido por el terminal, estando alojado este chip electrónico nominal sin ningún grado de libertad en el interior del soporte de aprehensión, y

  - de al menos un chip electrónico (231) de emergencia a todo para reemplazar el chip nominal para tratar el segundo mensaje ECM o EMM recibido por el terminal (10), estando el chip de emergencia (231) alojado, sin ningún grado de libertad, en el interior del mismo soporte de aprehensión que el chip nominal (230),

  - incluyendo cada chip electrónico un calculador electrónico (94, 100) y una memoria no volátil de solo lectura (96, 102) únicamente accesible por este calculador y siendo cada chip electrónico desplazable de manera reversible, por desplazamiento del procesador de seguridad, entre una posición insertada en la que el chip es apto para comunicar con el terminal para recibir los mensajes ECM y EMM a tratar y una posición retirada en la que la comunicación entre el chip y el terminal es imposible, conteniendo la memoria no volátil de solo lectura del chip nominal primeros datos secretos necesarios para descifrar el contenido del primer mensaje ECM o EMM cifrado según el primer procedimiento criptográfico, en el que la memoria no volátil de sólo lectura del chip nominal está desprovista de segundos datos secretos necesarios para descifrar el contenido del segundo mensaje ECM o EMM cifrado según el segundo procedimiento criptográfico y la memoria de sólo lectura (102) del chip de emergencia incluye los segundos datos secretos, y el procesador de seguridad incluye:

- un conector eléctrico (140) que incluye contactos eléctricos (234-241) aptos para entrar en contacto con contactos eléctricos correspondientes del terminal en posición insertada para establecer una conexión eléctrica entre uno de los chips electrónicos y el terminal, y

- un controlador (232) que se puede mandar apto para bascular de una posición nominal en la que conecta eléctricamente los contactos eléctricos del conector eléctrico (140) a bornes correspondientes (246) del chip nominal hacia una posición de emergencia en la que conecta estos mismos contactos eléctricos a bornes correspondientes (250) del chip de emergencia,

- al menos un interruptor irreversible (254) apto para bascular únicamente una sola vez desde una posición inicial, en la que mantiene de manera permanente el controlador (232) en su posición nominal, hacia una posición final en la que hace bascular el controlador hacia su posición de emergencia, estando programado el chip nominal para mandar el basculamiento del interruptor irreversible en respuesta a la recepción de una instrucción de activación.

2. Procesador de seguridad amovible tal como se ha descrito en la reivindicación 1.

3. Procesador según la reivindicación 2, en el que sólo el chip nominal (230) es apto para mandar el basculamiento del controlador (232) desde la posición nominal hacia la posición de emergencia.

4. Procesador según la reivindicación 3, en el que el chip nominal (230) está programado para mandar el basculamiento del controlador (232) desde la posición nominal hacia su posición de emergencia únicamente en respuesta a una instrucción de activación contenida en un mensaje ECM o EMM recibido.

5. Procesador según una cualquiera de las reivindicaciones 2 a 4, en el que el soporte (120) de aprehensión es una tarjeta cuya longitud y anchura son al menos diez veces superiores a su grosor.

6. Procedimiento de emisión y de recepción de un contenido multimedia codificado, incluyendo este procedimiento:

- la difusión (202, 290) de un primer contenido multimedia codificado y luego de un segundo contenido multimedia codificado,

- el cifrado (200, 288) del contenido de un primer mensaje ECM o EMM necesario para descodificar el primer contenido multimedia según un primer procedimiento criptográfico, utilizando una primera clave criptográfica y un primer algoritmo criptográfico, y el cifrado del contenido de un segundo mensaje ECM o EMM necesario para descodificar el segundo contenido multimedia según un segundo procedimiento criptográfico, utilizando una segunda clave criptográfica y un segundo algoritmo criptográfico, diferente del primer procedimiento criptográfico,

- la recepción (204, 292) por terminales del primer y segundo contenidos multimedia codificados y del primer y segundo mensajes ECM y EMM,

- el suministro (198) de al menos un procesador de seguridad amovible equipado:

  - de un soporte de aprehensión,

  - de un chip electrónico nominal apto para tratar el primer mensaje ECM o EMM recibido por el terminal, estando alojado este chip electrónico nominal sin ningún grado de libertad en el interior del soporte de aprehensión, y

  - de al menos un chip electrónico de emergencia apto para reemplazar el chip nominal para tratar el segundo mensaje ECM o EMM recibido por el terminal, estando alojado el chip de emergencia, sin ningún grado de libertad, en el mismo soporte de aprehensión que el chip nominal de manera que el suministro del procesador de seguridad y del chip de emergencia no formen más que una sola y misma etapa,

- incluyendo cada chip electrónico un calculador electrónico y una memoria no volátil de sólo lectura únicamente accesible por este calculador y siendo cada chip electrónico desplazable de manera reversible, por desplazamiento del procesador de seguridad, entre una posición insertada en la que el chip es apto para comunicar con el terminal para recibir los mensajes ECM y EMM a tratar y una posición retirada en la que la comunicación entre el chip y el terminal es imposible, conteniendo la memoria no volátil de sólo lectura del chip nominal primeros datos secretos necesarios para descifrar el contenido del primer mensaje ECM o EMM cifrado según el primer procedimiento criptográfico,

en el que el suministro (198) consiste en proporcionar un procesador de seguridad en el que la memoria no volátil de sólo lectura del tipo nominal está desprovista de segundos datos secretos necesarios para descifrar el contenido del segundo mensaje ECM o EMM cifrado según el segundo procedimiento y la memoria de sólo lectura del chip de emergencia incluye los segundos datos secretos, y en el que esté procesador de seguridad incluye:

- un conector eléctrico (140) que incluye contactos eléctricos (234-241) aptos para entrar en contacto con contactos eléctricos correspondientes del terminal en posición insertada para establecer una conexión eléctrica entre uno de los chips electrónicos y el terminal, y

- un controlador (232) que se puede mandar apto para bascular desde una posición nominal en la que conecta eléctricamente los contactos eléctricos del conector eléctrico (140) a bornes correspondientes (246) del chip nominal hacia una posición de emergencia en la que conecta estos mismos contactos eléctricos a bornes correspondientes (250) del chip de emergencia,

- al menos un interruptor irreversible (254) apto para bascular únicamente una sola vez desde una posición inicial, en la que mantiene de manera permanente el controlador (232) en su posición nominal, hacia una posición final en la que hace bascular el controlador hacia su posición de emergencia, estando programado el chip nominal para mandar el basculamiento del interruptor irreversible en respuesta a la recepción de una instrucción de activación.

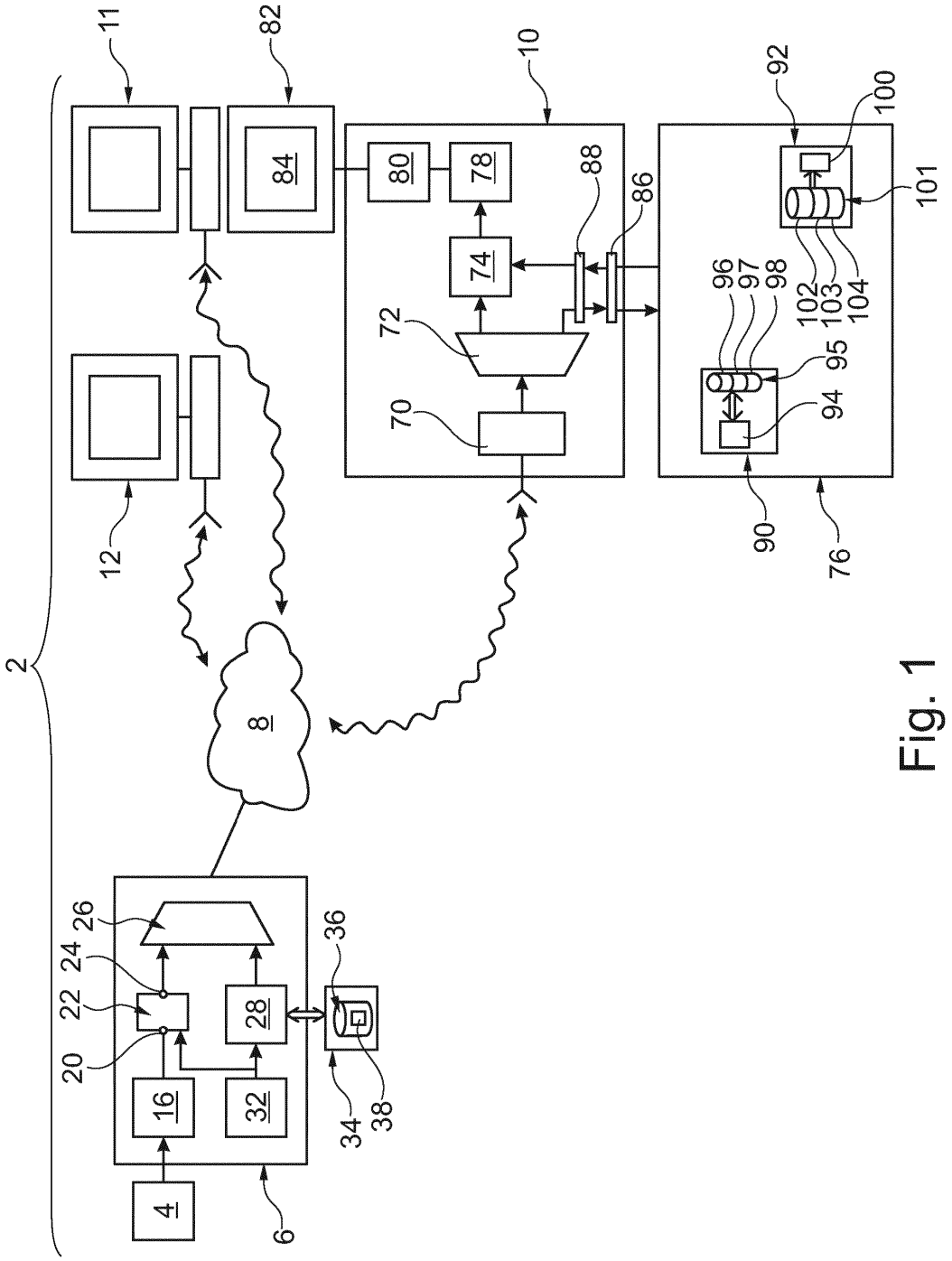
2
11
82
10
92
100
101
84
80
78
88
86
74
72
70
96
97
98
102
103
104
95
94
12
8
90
76
36
26
24
22
20
28
16
32
34
38
4
6

Fig. 1

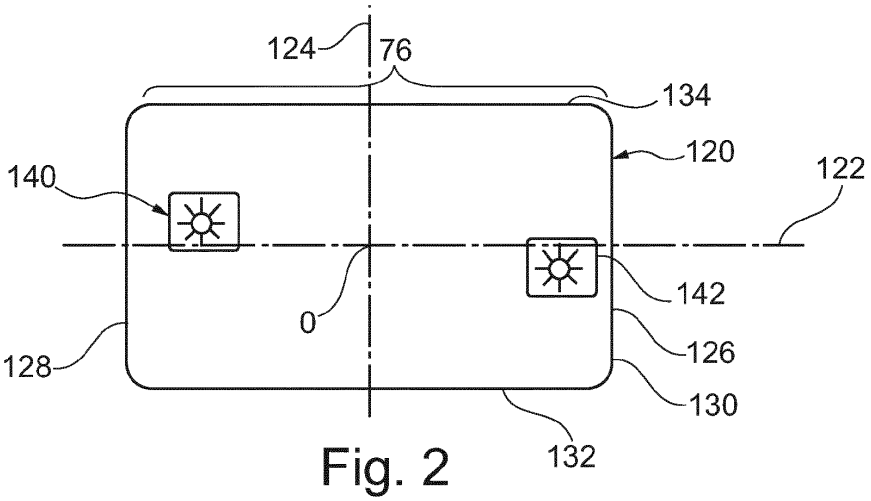

Fig. 2

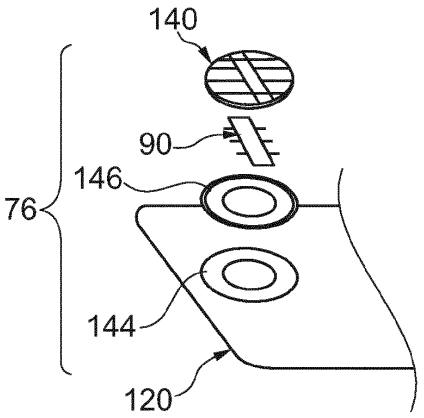

Fig. 3

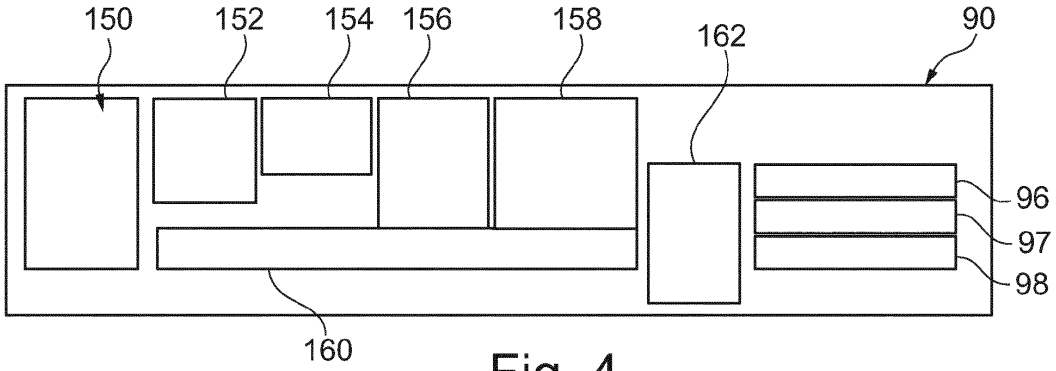

Fig. 4

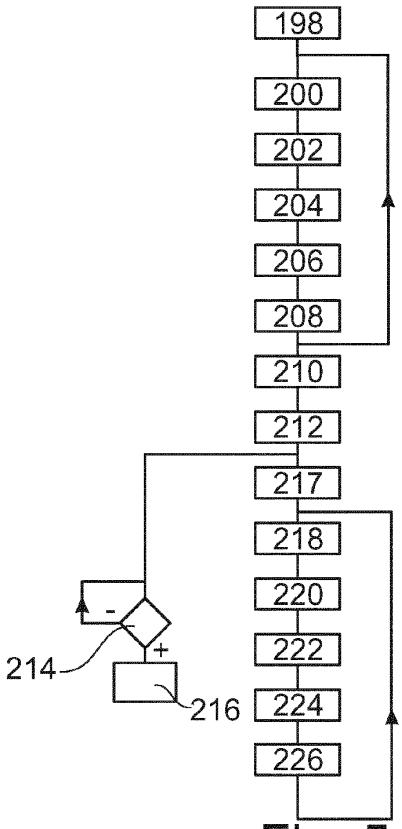

Fig. 5

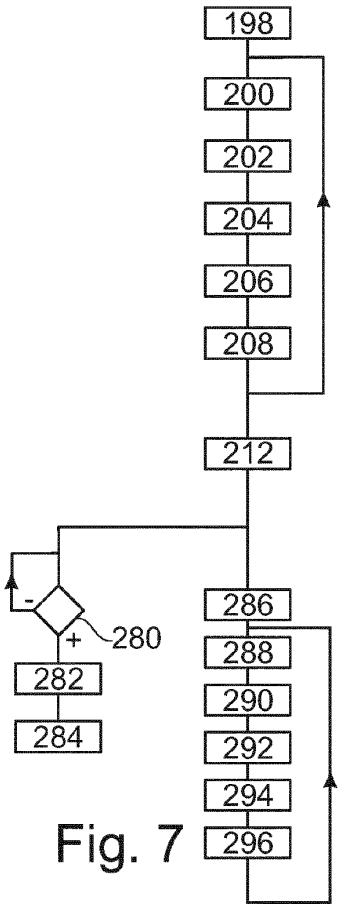

Fig. 7

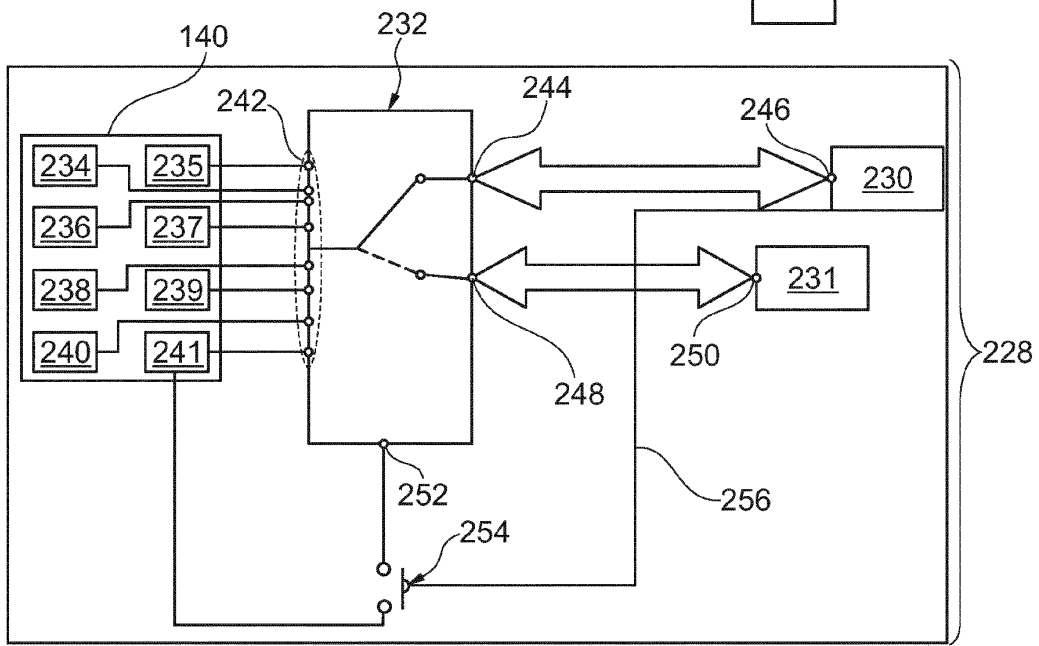

Fig. 6