(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 627 916**

(51) Int. CI.:

***H04L 9/08*** (2006.01)
***H04N 7/16*** (2011.01)
***H04N 7/167*** (2011.01)
***H04N 7/173*** (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.05.2011 PCT/EP2011/057066**

(87) Fecha y número de publicación internacional: **10.11.2011 WO11138333**

(96) Fecha de presentación y número de la solicitud europea: **03.05.2011 E 11716949 (0)**

(97) Fecha y número de publicación de la concesión europea: **19.04.2017 EP 2567500**

(54) Título: **Procedimientos de descifrado, de transmisión y de recepción de palabras de control, soporte de registro y servidor de palabras de control para la puesta en práctica de estos procedimientos**

(30) Prioridad:

**04.05.2010 FR 1053467**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**01.08.2017**

(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 y**
**MAGIS, ERWANN**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Procedimientos de descifrado, de transmisión y de recepción de palabras de control, soporte de registro y servidor de palabras de control para la puesta en práctica de estos procedimientos

La invención se refiere a un procedimiento de descifrado de palabras de control para terminales mecánica y electrónicamente independientes entre sí. La invención se refiere igualmente a un procedimiento de transmisión y a un procedimiento de recepción de palabras de control para la puesta en práctica del procedimiento de descifrado. La invención se refiere también a un soporte de registro o grabación de informaciones y a un servidor de palabras de control para la puesta en práctica de este procedimiento.

Existen procedimientos de cifrado de palabras de control en los que:

- en respuesta a la ausencia, en uno cualquiera de los terminales, de una o varias palabras de control $CW_c$ para descodificar uno o varios períodos de cifrado de un contenido multimedia, este terminal transmite a un servidor de palabras de control una solicitud que contiene el o los criptogramas de una o varias de las palabras de control ausentes, y en respuesta

- el servidor de palabras de control transmite a este terminal la o las palabras de control ausentes.

Por contenido multimedia se designa 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 igualmente ser un contenido interactivo tal como un juego.

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 bajo 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.

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 son difundidos en forma codificada y no en abierto. Más precisamente, cada contenido multimedia es dividido en una sucesión de criptoperíodos. Durante toda la duración de un criptoperíodo, las condiciones de acceso al contenido multimedia codificado permanecen sin cambios. En particular, durante 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 extraído este último aleatoriamente o pseudo-aleatoriamente. Así, si en un instante dado N contenidos multimedia son difundidos simultáneamente sobre N canales, existen N palabras de control diferentes e independientes empleadas cada una para codificar uno de estos contenidos multimedia.

Aquí los términos « codificar »/« descodificar » y «cifrar »/« descifrar » son considerados como sinónimos.

El contenido multimedia en abierto corresponde al contenido multimedia antes de que sea codificado. Éste puede ser hecho directamente comprensible para un ser humano sin haber recurrido a operaciones de descodificación 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. Por ejemplo, las palabras de control necesarias para descodificar el criptoperíodo t-ésimo son recibidas por cada terminal durante el criptoperíodo (t-1)-ésimo. Para ello, por ejemplo, las palabras de control son multiplexadas con el contenido multimedia codificado.

Para asegurar la transmisión de las palabras de control, éstas son transmitidas a los terminales en forma de criptogramas. Se designa aquí por criptograma una información suficiente por sí sola para encontrar la palabra de control en abierto. Así, si la transmisión de la palabra de control es interceptada, tan solo el 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 y la clave criptográfica permiten 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 libre.

La información secreta debe ser preservada en lugar seguro. Para ello, se ha propuesto ya almacenar la información secreta:

- bien en procesadores de seguridad tales como tarjetas con chip directamente conectadas a cada uno de los terminales,

- bien, más recientemente, en un servidor de palabras de control común a varios terminales.

En este último caso, los terminales están desprovistos de tarjeta con chip. Se habla entonces de terminales sin tarjeta o « cardless terminal » en inglés.

El servidor de palabras de control está conectado a cada uno de los terminales por una red con gran distancia de transmisión de informaciones tal como la red Internet. Cuando un servidor de palabras de control es utilizado, los criptogramas de las palabras de control son en primer lugar transmitidos a los diferentes terminales antes de ser reenviados por estos terminales hacia el servidor de palabras de control. Esta manera de proceder presenta varias ventajas. En particular, la red de transmisión de informaciones utilizada para difundir los contenidos multimedia y los criptogramas de las palabras de control puede ser diferente de la utilizada para unir los terminales al servidor de palabras de control. Por ejemplo, la red para la difusión de los contenidos multimedia y de los criptogramas de las palabras de control es una red unidireccional de banda ancha pasante tal como una red de satélites. A la inversa, la red que une los terminales al servidor de palabras de control es una red bidireccional cuya banda pasante puede ser más reducida.

A continuación, ello simplifica la sincronización temporal entre la difusión de los contenidos multimedia y la difusión de los criptogramas de las palabras de control correspondientes.

El servidor de palabras de control tiene normalmente por función descifrar los criptogramas de las palabras de control transmitidas por los terminales para a continuación devolver hacia cada uno de estos terminales las palabras de control descifradas. Así, de alguna manera, el servidor de palabras de control desempeña la misión de una tarjeta con chip común a varios terminales mecánica y electrónicamente independientes entre sí. Terminales electrónicamente independientes entre sí son terminales capaces de funcionar de manera autónoma y que no presentan ninguna parte electrónica o de software compartida.

Cuando un terminal tiene necesidad de una palabra de control para descodificar un contenido multimedia, envía al servidor de palabras de control una solicitud que contiene el criptograma de la palabra de control. En respuesta, el servidor de palabras de control descifra este criptograma y luego reenvía la palabra de control descifrada al terminal que puede entonces descodificar el contenido multimedia deseado.

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 « en vivo » o « linealizados » pues el usuario no controla su instante de transmisión.

A la inversa, ciertos contenidos multimedia son transmitidos bajo demanda. Es por ejemplo el caso de servicios tales como el video a petición o « Video On Demand » en inglés. Es igualmente el caso cuando los contenidos multimedia son grabados localmente desde el terminal o a distancia desde la red y el lanzamiento y el desarrollo de la visualización son controlados por el usuario. Tal servicio es conocido por ejemplo con el acrónimo NPVR (« Network Private Video Recorder »). Puede también tratarse de un servicio que permite retroceder en el tiempo o diferir la visualización tal como el servicio conocido bajo el acrónimo NTS (Network Time Shifting). En estos últimos casos, el contenido multimedia es llamado contenido « deslinealizado » pues es el usuario el que decide el momento en que el terminal reproduce este contenido.

Generalmente, el número de palabras de control cifradas contenidas en una solicitud está limitado a una o dos para aumentar la seguridad del sistema criptográfico. En efecto, si el número de palabras de control cifradas contenidas en una solicitud aumenta, entonces aumenta el número de palabras de control en abierto almacenadas en cada terminal para descodificar un mismo contenido multimedia. O cuanto más aumenta el número de palabras de control en abierto almacenadas en los terminales, más riesgo corre la seguridad del sistema de ser comprometida. Por ejemplo, un número importante de palabras de control almacenadas en cada terminal facilita ataques tales como el hecho de compartir palabras de control. Este ataque consiste en difundir ilícitamente hacia otros terminales que no han suscrito abono correspondiente las palabras de control en abierto obtenidas por un terminal que ha suscrito un abono para descifrar estas palabras de control.

A partir de entonces, cada terminal envía al servidor de palabras de control una solicitud a cada criptoperíodo o a cada dos criptoperíodos.

El tratamiento de una solicitud por el servidor de palabras de control requiere un cierto tiempo y cuanto más aumenta el número de solicitudes a tratar más aumenta la carga de trabajo de este servidor. Cuanto más aumenta la carga de trabajo, más importante debe ser la potencia de cálculo del servidor de palabras de control.

Del estado de la técnica es conocido:

- el documento US2008/0301437A1, y

- el documento WO2009/112966A2.

Es deseable por consiguiente poder disminuir la carga de trabajo del servidor de palabras de control para utilizar servidores que tengan una potencia de cálculo más limitada.

La invención pretende satisfacer este deseo proponiendo un procedimiento de descifrado conforme a la reivindicación 1.

El hecho de enviar palabras de control suplementarias además de las palabras de control ausentes permite aumentar el número de palabras de control presentes en el terminal y por tanto reducir la frecuencia de las solicitudes transmitidas por este terminal al servidor de palabras de control. Esta reducción de la frecuencia se traduce por una reducción de la carga de trabajo del servidor de palabras de control.

Además, aquí, este aumento del número de palabras de control almacenadas en el terminal no es hecho en detrimento de la seguridad del sistema criptográfico ya que este aumento es únicamente empleado para ciertos terminales elegidos selectivamente donde el riesgo de compromiso de las palabras de control almacenadas es pequeño.

La invención tiene igualmente por objeto un procedimiento de transmisión de palabras de control a terminales mecánica y electrónicamente independientes entre sí conforme a la reivindicación 2.

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

Estos modos de realización del procedimiento de transmisión de palabras de control presentan además las siguientes ventajas:

- determinar el número de palabras de control suplementarias a transmitir en función de estimaciones del número de solicitudes a tratar por el servidor de palabras de control por criptoperíodos permite suavizar la carga de trabajo del servidor de palabras de control sobre varios criptoperíodos,

- determinar el número de palabras de control suplementarias en función de un número aleatorio permite suavizar la carga de trabajo del servidor de palabras de control sobre varios criptoperíodos sin recurrir a una estimación de la carga de trabajo de este servidor sobre cada uno de estos criptoperíodos;

- ajustar el número de palabras de control suplementarias en función del número probable de criptoperíodos sucesivos de este contenido multimedia que serán a descodificar permite limitar aún más la carga de trabajo del servidor de palabras de control evitando un envío excesivo de palabras de control suplementarias.

La invención tiene igualmente por objeto un procedimiento de recepción de palabras de control por un terminal para la puesta en práctica del procedimiento anterior, en el que:

- en respuesta a la ausencia de este terminal de una o varias palabras de control $CW_c$ para descodificar uno o varios criptoperíodos de un contenido multimedia, este terminal transmite al servidor de palabras de control una solicitud que contiene el o los criptogramas de una o varias palabras de control ausentes, y

- el terminal recibe, además de las palabras de control ausentes requeridas, un número determinado de palabras de control suplementarias para permitir a este terminal descodificar criptoperíodos suplementarios del mismo contenido multimedia además de los criptoperíodos que se pueden descodificar con ayuda de las palabras de control ausentes $CW_c$ requeridas.

La invención tiene igualmente por objeto un soporte de registro de informaciones que incluye instrucciones para la puesta en práctica de los procedimientos anteriores cuando estas instrucciones son ejecutadas por un calculador electrónico.

Finalmente, la invención tiene igualmente por objeto un servidor de palabras de control hacia terminales mecánica y electrónicamente independientes entre sí conforme a la reivindicación 10.

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 codificados,

Las figs.2 a 4 son ilustraciones esquemáticas de tablas utilizadas en el sistema de la fig. 1,

La fig. 5 es un organigrama de un procedimiento de descifrado de palabras de control con ayuda del sistema de la fig. 1, y

La fig. 6 es un organigrama del procedimiento de actualización de una tabla de palabras de control.

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 expertos en la técnica no se

han descrito 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 linealizados o deslinealizados. Por ejemplo, un contenido multimedia corresponde a una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

En la continuación de esta descripción, el sistema 2 es descrito en el caso particular entre los contenidos multimedia son linealizados.

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 los otros para, por ejemplo, respetar una parrilla preestablecida de programas.

La red 8 es típicamente una red a 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 (TNT).

Para simplificar la fig. 1, solamente están representados 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 la norma UIT-T H264.

Los contenidos multimedia comprimidos son dirigidos hacia una entrada 20 de un codificador 22. El codificador 22 codifica 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 codificados son restituidos sobre una salida 24 conectada a la entrada de un multiplexor 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 un sistema 28 de acceso condicional, por un generador 32 de claves. El sistema 28 es más conocido bajo el acrónimo CAS (Conditional Access System). El índice i es un identificador del canal sobre el que es difundido el contenido multimedia codificado y el índice t es un identificador del criptoperíodo codificado con esta palabra de control. En la continuación de esta descripción, el criptoperíodo actualmente descodificado por los terminales es el criptoperíodo t-1.

Típicamente, esta codificación 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.

El sistema 28 genera mensajes ECM (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 codificar 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 inserta igualmente en cada ECM:

- el identificador i del canal,

- 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 descodificar los criptoperíodos t y t+1 del canal i,

- los números t y t+1 que identifican los criptoperíodos que se pueden descodificar con las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$,

- etiquetas de tiempos $TS_t$ y $TS_{t+1}$ o «timestamp » en inglés, que referencian los instantes en los que deben ser reproducidos los criptoperíodos t y t+1,

- derechos de acceso DA destinados a ser comparados a título de acceso adquiridos por el usuario, y

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

Las etiquetas de tiempo son o bien definidas con relación a un origen absoluto independiente del contenido multimedia difundido o bien con relación a un origen relativo al contenido multimedia difundido. Por ejemplo, un origen relativo puede

ser el comienzo de la película cuando el contenido multimedia es una película.

El mismo identificador i es insertado en todos los mensajes ECM que contienen un criptograma $CW^*_{i,t}$ para la descodificación de los contenidos multimedia difundidos por un mismo canal.

A título de ilustración, aquí, la codificación y el multiplexado de los contenidos multimedia es conforme al protocolo DVB-Simulcrypt (ETSI TS 103 197). En este caso, el identificador i puede corresponder a un par « ID de canal /ID de flujo » único sobre el que son enviadas todas las solicitudes de generación de mensaje ECM para este canal.

Por ejemplo los terminales 10 a 12 son idénticos y sólo el terminal 10 se ha descrito más en detalle.

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 y EMM (Entitlement Management Message) a un procesador 76. 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. Esta robustez es por ejemplo obtenida implementando un módulo de software dedicado a la protección de las informaciones secretas.

El procesador 76 es realizado por ejemplo con ayuda de calculadores electrónicos programables aptos para ejecutar instrucciones registradas sobre un soporte de registro de informaciones. A este efecto, el procesador 76 está conectado a una memoria 78 que contiene las acciones necesarias para la ejecución del procedimiento de la fig. 5.

La memoria 78 contiene igualmente:

- un certificado criptográfico para identificar y autentificar el terminal 10, y

- una tabla local 79 de palabras de control.

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 80 que le descodifica. El contenido multimedia descomprimido o descodificado es transmitido a una tarjeta gráfica 82 que pilota la presentación de este contenido multimedia sobre un dispositivo de presentación 84 equipado con una pantalla 86.

El dispositivo de presentación 84 presenta en abierto el contenido multimedia sobre la pantalla 86.

El terminal 10 comprende igualmente un emisor 88 que permite establecer una conexión segura con una cabeza de red 90 por medio de una red 92 de transmisión de informaciones. Por ejemplo la red 92 es una red a gran distancia de transmisión de informaciones y más precisamente una red de conmutación de paquetes tal como la red Internet. La conexión segura es por ejemplo un túnel asegurado con ayuda del certificado criptográfico.

La cabeza de red 90 comprende un módulo 100 de gestión de los títulos de acceso de los diferentes usuarios del sistema 2. Este módulo 100 es más conocido bajo el término inglés de « suscriber authorisation system ». Este módulo 100 genera y mantiene actualizada una base de datos 102. La base de datos 102 asocia a cada identificador de usuario los títulos de acceso adquiridos por este usuario. Esta base de datos 102 es almacenada en una memoria 104.

La cabeza de red 90 comprende igualmente un servidor 106 de palabras de control conectado a un módulo 108 de verificación de derecho de acceso y a una memoria 110. La memoria 110 contiene:

- una tabla 112 de palabras de control,

- una tabla 114 de índices de confianza en los terminales,

- una tabla 116 de índices de criticidad de los contenidos multimedia, y

- contadores de error de funcionamiento $C_1$, $C_2$, $C_3$ y $C_4$ asociados a cada terminal.

El funcionamiento de los contadores de error $C_1$ a $C_4$ esta descrito más en detalle con respecto a la fig. 5.

Típicamente, el servidor 106 está realizado a partir de calculadores electrónicos programables aptos para ejecutar instrucciones registradas sobre un soporte de registro de informaciones. A este efecto, la memoria 110 comprende igualmente instrucciones para la ejecución de los procedimientos de las figs. 5 y 6.

Un ejemplo de estructura de la tabla 112 está representado más en detalle en la fig. 2. Cada línea de la tabla 112 corresponde a un registro. La tabla 112 contiene varios registros. Cada registro corresponde a un criptoperíodo. En particular, la tabla 112 contiene registros para más de tres criptoperíodos sucesivos que provienen de cada contenido multimedia. Cada uno de estos registros contiene los campos siguientes:

- un campo i que contiene el identificador i del canal difundido,

- un campo t que contiene el número del criptoperíodo,

- un campo $TS_t$ que contiene la etiqueta de tiempo asociada al criptoperíodo t,

- un campo CA que contiene las condiciones de acceso a este criptoperíodo t.

La estructura de la tabla 79 que es por ejemplo idéntica a la estructura de la tabla 112.

La fig. 3 representa más en detalle un ejemplo de estructura para la tabla 114. La tabla 114 asocia a cada identificador $Id_T$ de un terminal un índice de confianza $IC_T$ para este terminal. El índice de confianza $IC_T$ es representativo de la probabilidad de que la seguridad de las palabras de control registradas en este terminal sea comprometida. Se considera que la seguridad de un terminal es comprometida cuando las palabras de control que están registradas o almacenadas en este terminal son utilizadas con fines ilícitos para, por ejemplo, permitir la descodificación de contenidos multimedia por otros terminales que no disponen de título de acceso que autorice tal descodificación. En la continuación de esta descripción, cuanto menor es el valor del índice, más importante es la probabilidad de que la seguridad de las palabras de control almacenadas en el terminal sea comprometida.

Aquí, el índice $IC_T$ representa la probabilidad de que los medios materiales empleados en este terminal resistan a una tentativa de pirateo. Es por tanto representativo del nivel de dificultad a obtener y a utilizar ilícitamente palabras de control almacenadas en este terminal.

Por ejemplo, la tabla 114 es proporcionada por el operador del sistema 2.

A título de ilustración, el valor del índice $IC_T$ para cada terminal es la suma de las notas obtenidas por este terminal sobre varios criterios de seguridad diferentes.

La tabla siguiente da un ejemplo de baremo de notación:

| Criterio de seguridad | Nota si este criterio es satisfecho | Nota si este criterio no es satisfecho |
|---|---|---|
| Los tratamientos criptográficos son ejecutados por un procesador de seguridad | 50 | 0 |
| El código de ejecución de los tratamiento criptográficos es cifrado en una memoria no volátil | 15 | 0 |
| El código de ejecución de los tratamiento criptográficos es cifrado en memoria volátil durante la ejecución de este código | 30 | 0 |
| Un procedimiento de oscurecimiento del código de ejecución de los tratamientos criptográficos es empleado para hacer la observación de su desarrollo difícil | 5 | 0 |

El valor del índice $IC_T$ para un terminal dado es la suma de las notas obtenidas para cada uno de los criterios de seguridad indicados en la tabla anterior. Por ejemplo si un terminal utiliza un procesador de seguridad y posee un código de ejecución de tratamiento criptográfico cifrado en memoria no volátil, el índice $IC_T$ de este terminal es entonces igual a 65. El índice $IC_T$ está asociado a cada identificador del terminal almacenado en base de datos y accesible al servidor de palabras de control.

La fig. 4 representa un ejemplo de estructura posible para la tabla 116. Esta tabla 116 asocia a cada identificador i de canal un índice de confianza $IC_c$ representativo de la probabilidad de que el contenido multimedia sea víctima de una tentativa de ataque. Este índice $IC_c$ representa también la importancia de las consecuencias perjudiciales si la seguridad de las palabras de control para descifrar este canal i estaba comprometida. Este índice $IC_c$ es por tanto igualmente representativo de la probabilidad de que la seguridad de las palabras de control almacenadas en un terminal esté comprometida. En efecto, cuanto menor interés hay en descodificar ilegalmente un contenido multimedia, menor es la probabilidad de que la seguridad de las palabras de control que permiten descodificar este contenido multimedia esté comprometida. Por ejemplo, no hay ningún interés en comprometer la seguridad de palabras de control que permiten descodificar un canal difundido gratuitamente, es decir que puede ser visualizado en abierto sin que se suscriba para ello un abono de pago. Por el contrario, el interés para descodificar ilícitamente un contenido multimedia aumenta con el valor de este contenido multimedia. Por ejemplo, un canal sobre el que son difundidas películas recientes está asociado a un índice $IC_c$ débil ya que el riesgo de que la seguridad de las palabras de control que permiten descifrarle esté comprometido es más importante.

Aquí la tabla 116 incluye dos columnas, cada línea de esta tabla 116 comprende un campo que contiene el identificador i y un campo que asocia a este identificador i un valor del índice $IC_c$. La tabla 116 es suministrada por ejemplo por un

operador del sistema 2.

El funcionamiento del sistema 2 va a ser descrito a continuación con más detalle con referencia al procedimiento de la fig. 5.

Inicialmente, durante una etapa 120, el dispositivo 6 difunde varios contenidos multimedia diferentes simultáneamente sobre diferentes canales. En cada canal, el criptoperíodo t y el criptoperíodos siguiente t+1 son codificados con las palabras de control, respectivamente, $CW_{i,t}$ y $CW_{i,t+1}$. Los mensajes ECM que contienen los programas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ de las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$ son multiplexados con los contenidos multimedia difundidos. Este multiplexado permite sincronizar la difusión de las palabras de control con la difusión de los contenidos multimedia. Aquí, los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ son transmitidos a los terminales durante el criptoperíodo t-1 que precede al criptoperíodo t.

Típicamente, los mensajes ECM son repetidos varias veces en el seno de un mismo criptoperíodo. Por ejemplo, los mensajes ECM son repetidos cada 0,1 segundo en 0,5 segundos. La duración de un criptoperíodo es superior a cinco segundos y, de preferencia, está comprendida entre 5 segundos y 10 minutos.

Los contenidos multimedia codificados son recibidos sensiblemente al mismo tiempo por cada uno de los terminales 10 a 12. Las etapas siguientes son por tanto ejecutadas sensiblemente en paralelo para cada uno de estos terminales. Las etapas siguientes están descritas en el caso particular del terminal 10.

Durante una etapa 122, los contenidos multimedia codificados con mensajes ECM son recibidos por el terminal 70.

A continuación, durante una etapa 124, el desmultiplexor 72 extrae el contenido multimedia codificado correspondiente al canal i cuya descodificación es actualmente solicitada por el usuario. Durante la etapa 124, el desmultiplexor 72 extrae de igual manera únicamente los mensajes ECM que contienen los criptogramas de las palabras de control que permiten descodificar este mismo canal. El multiplexor 72 transmite el contenido multimedia extraído hacia el descodificador 74. Los mensajes ECM extraídos son en cuanto a ellos transmitidos al procesador 76.

Durante una etapa 126, el procesador 76 busca en la tabla 79 si ésta contiene ya la palabra de control $CW_{i,t}$ del próximo criptoperíodo a descodificar del canal i.

En caso afirmativo, el procesador 76 procede a una fase 127 de descodificación del criptoperíodo t difundido sobre el canal i.

Más precisamente, durante una etapa 128, el procesador 76 envía al descodificador 74 la palabra de control $CW_{i,t}$ encontrada en la tabla 79. Ninguna solicitud para descifrar los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ es entonces transmitida al servidor 106.

A continuación, durante una etapa 130, el descodificador 74 descodifica el criptoperíodo t del contenido multimedia recibido con ayuda de esta palabra de control $CW_{i,t}$.

A continuación durante una etapa 132, el contenido multimedia descodificado es descodificado por el descodificador 80 y luego transmitido a la tarjeta de video 82.

Finalmente, durante una etapa 134, la tarjeta de video 82 trasmite la señal de video al dispositivo de presentación 84 para que el contenido multimedia sea presentado en la pantalla 86 de manera directamente perceptible y comprensible para un ser humano.

Si la palabra de control $CW_{i,t}$ no está contenida en la tabla 79, durante una etapa 140, el terminal 10 transmite en el curso del criptoperíodo t-1 una solicitud hacia el servidor 106 para descifrar los criptograma $CW^*_{i,t}$ y $CW^*_{i,t+1}$ contenidos en el mensaje ECM recibido. Por ejemplo, esta solicitud contiene:

- el mensaje ECM recibido y por tanto el par de criptogramas $CW^*_{i,t}$/ CW*i,t+1, y

- un identificador $Id_u$ del usuario del terminal que ha enviado la solicitud.

Esta solicitud es transmitida al servidor 106 por medio del emisor 88 y de la red 92. Todos los intercambios de informaciones entre el terminal 10 y el servidor 106 se hacen por medio de un túnel asegurado establecido a través de la red 92. El establecimiento del túnel ha requerido la autentificación y la identificación del terminal por el servidor 106, por ejemplo, con la ayuda del certificado criptográfico contenido en la memoria 78. Así, el servidor 106 dispone del identificador $Id_T$ del terminal que le envía una solicitud.

Durante una etapa 142, en respuesta a la recepción de esta solicitud, el módulo 108 extrae de la base 102 los títulos de acceso asociados al identificador $Id_u$ contenido en esta solicitud. Luego el módulo 108 compara los títulos de acceso extraídos a las condiciones de acceso CA contenidas en la solicitud.

Si los títulos de acceso del usuario no corresponden a las condiciones de acceso CA entonces el servidor 106 procede a una etapa 144 de inhibición del descodificado del canal i por el terminal 10. Por ejemplo, a este efecto, el servidor 106 no

transmiten ninguna palabra de control al terminal 10.

En el caso contrario, el servidor 106 procede a una etapa 146 de actualización de un perfil del usuario. El perfil del usuario contiene informaciones que permiten determinar la duración probable durante la cual el usuario del terminal 10 va a continuar descodificando el mismo canal i. Este perfil del usuario permite por tanto determinar el número probable de criptoperíodos sucesivos del canal i que serán descodificados.

Esta probabilidad depende en particular de las costumbres del usuario del terminal 10. A este efecto, durante la etapa 146, el servidor 106 detecta si la solicitud recibida demanda la descodificación de las palabras de control para un nuevo canal. En caso afirmativo, ello significa que el usuario ha cambiado de canal. En este caso, registra en una base de datos el instante en el que el usuario ha dejado el canal antiguo y el instante en el que el usuario ha basculado sobre el nuevo canal. El servidor 106 registra igualmente el identificador i del nuevo canal sobre el que ha basculado el usuario. Las informaciones registradas en esta base de datos permiten por tanto estimar el número de criptoperíodos sucesivos que el usuario del terminal 10 va a visualizar.

De preferencia, los datos registrados en esta base de datos son conservados durante un período de tiempo muy grande de manera que afinen la probabilidad calculada a partir de los datos registrados en esta base de datos.

Además, durante la etapa 146, el servidor 106 construye un índice de fiabilidad de este perfil del usuario. Este índice de fiabilidad indica el grado de confianza que se puede tener en el perfil del usuario actualmente registrado. Por ejemplo, para ello, el servidor 106 calcula las desviaciones entre las mismas probabilidades calculadas con ayuda del perfil del usuario actual y con ayuda de las informaciones contenidas en esta misma base de datos algún tiempo antes. Cuanto más importante es esta desviación, menor es el índice de fiabilidad. En efecto, ello significa que el perfil del usuario no es estable y que no es por tanto posible concederle un grado de confianza elevado.

A continuación, durante una etapa 148, el servidor 106 construye el índice $IC_T$ del terminal 10. A este efecto, extrae el valor de este índice $IC_T$ de la tabla 114 a partir del identificador $Id_T$ del terminal 10 recibido, por ejemplo, durante la autentificación del terminal durante la fase de establecimiento del túnel asegurado.

Durante una etapa 150, el servidor 106 construye un índice de confianza $IC_u$ sobre la utilización del terminal. Este índice $IC_u$ representa la probabilidad de que el terminal sea sometido actualmente a un ataque que pretenda comprometer la seguridad de las palabras de control almacenadas en éste. Este índice $IC_u$ es por tanto igualmente representativo de la probabilidad de que la seguridad de las palabras de control almacenadas en este terminal sea comprometida.

El valor de este índice $IC_u$ para un terminal dado es construido a partir de los valores de los contadores de error $C_1$ a $C_4$.

Más precisamente, durante una operación 152, cada vez que una solicitud es transmitida por el terminal 10, los contadores de errores $C_1$ a $C_4$ son actualizados.

Aquí, el contador $C_1$ representa el número de cambios de canal por hora.

El contador $C_2$ representa el número de solicitudes idénticas enviadas por el terminal 10 al servidor 106 por minuto. En efecto, durante un funcionamiento normal, cada solicitud transmitida por el terminal 10 al servidor 106 debe ser diferente de la precedente. Así, la recepción de varias solicitudes idénticas permite sospechar de que una utilización anormal del terminal 10 y por tanto una eventual tentativa de comprometer la seguridad de las palabras de control almacenadas en este terminal.

El contador $C_3$ cuenta el número de veces en que la integridad del mensaje ECM recibido en la solicitud no ha podido ser verificada durante 24 horas. La integridad del mensaje ECM de una solicitud es verificada cuando la firma aplicada a los diferentes campos del mensaje ECM permite encontrar la firma MAC contenida en este mensaje. En caso contrario, ello significa que el mensaje ECM ha sido corrompido.

Finalmente, el contador $C_4$ cuenta el número de mensajes ECM que tienen una sintaxis incorrecta transmitidos por el terminal 10 al servidor 106 durante 24 horas.

A continuación, durante una operación 154, el valor de cada uno de estos contadores $C_1$ a $C_4$ es convertido en una nota tanto menor cuanto más anormal es el funcionamiento actual del terminal. Por ejemplo, se utilizan tablas de conversión de los valores de los contadores en nota. A título de ilustración se han utilizado las tablas siguientes.

| Número de cambios de canal por hora | Nota_NBZ |
|---|---|
| Inferior a 100 | 100 |
| Comprendido entre 100 y 360 | 50 |
| Comprendido entre 360 y 450 | 20 |
| Superior a 450 | 0 |

| Número de solicitudes idénticas por minuto | Nota_NBR |
|---|---|
| Igual a 0 | 100 |
| Comprendido entre 1 y 2 | 50 |
| Estrictamente superior a 2 | 0 |

| Número de mensajes ECM corrompidos por 24 horas | Nota_NBA |
|---|---|
| Igual a 0 | 100 |
| Superior o igual a 1 y estrictamente inferior a 4 | 50 |
| Superior o igual a 4 | 0 |

| Número de errores de sintaxis por 24 horas | Nota_NBA |
|---|---|
| Igual a 0 | 100 |
| Superior o igual a 2 y estrictamente inferior a 6 | 50 |
| Superior o igual a 6 | 0 |

Durante una operación 156, el valor del índice $IC_u$ es calculado en función del valor de los contadores $C_1$ a $C_4$ convertido en una nota. Por ejemplo, el valor del índice $IC_u$ es determinado con ayuda de la relación siguiente:

$$IC_u = \min \{note\_NBZ, note\_NBR, note\_NBA, note\_NBE\}$$

donde « min » es la función que devuelve el mínimo de los diferentes valores contenidos entre los abarcados.

El valor del indicador $IC_u$ puede igualmente ser calculado con ayuda de otras relaciones. Por ejemplo, la relación siguiente puede ser utilizada igualmente

$$IC_u = (note\_NBZ, note\_NBR, note\_NBA, note\_NBE)/4$$

Durante una etapa 160, el servidor 106 construye el índice $IC_c$ asociado al canal i actualmente descodificado por el terminal 10. A este efecto, extrae el índice $IC_c$ asociado a este identificador i en la tabla 116.

Durante la etapa 164, el servidor 106 determina un número NbCP de palabras de control a transmitir al terminal 10 en respuesta a su solicitud. Este número NbCP puede ser superior a dos lo que significa que además de las palabras de control ausentes $CW_{i,t}$ y $CW_{i,t+1}$ requeridas por el terminal 10, el servidor 106 puede igualmente transmitirle palabras de control suplementarias $CW_s$, que permiten descodificar los criptoperíodos suplementarios del canal i sin que incluso el terminal 10 haya transmitido al servidor 106 los criptogramas correspondientes a estas palabras de control suplementarias $CW_s$.

El número NbCP es elegido tanto mayor cuanto menor es la probabilidad de que la seguridad de las palabras de control suplementarias transmitidas a este terminal 10 sea comprometida. A este efecto, el número NbCP es determinado en función de los índices de confianza $IC_T$, $IC_u$ e $IC_c$ precedentemente construidos.

Por ejemplo, durante una operación 166, un número máximo NbMaxCP de palabras de control a transmitir al terminal 10 es calculado en primer lugar en función de los índices $IC_T$, $IC_u$, e $IC_c$. Aquí el valor de este número máximo NbMaxCP es calculado con ayuda de la tabla siguiente:

| Umbral para el índice $IC_T$ | Umbral para el índice $IC_u$ | Umbral para el índice $IC_c$ | Valor de NbMaxCP |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 65 | 60 | 0 | 1 |
| 20 | 50 | 50 | 1 |
| 65 | 50 | 50 | 5 |
| 20 | 50 | 100 | 5 |
| 65 | 50 | 100 | 10 |

El valor del número NbMaxCP retenido es el valor máximo en la columna de la derecha de la tabla anterior para la que los índices $IC_T$, $IC_u$ e $IC_c$ sobrepasan cada uno el valor de un umbral respectivo indicado en la misma línea. Por ejemplo, si los valores construidos de los índices $IC_T$, $IC_u$ e $IC_c$ son respectivamente 70, 54 y 100, el valor del número NbMaxCP es igual a diez.

A continuación, durante una operación 168, el número NbMaxCP es ajustado en función del perfil del usuario determinado durante la etapa 146. Típicamente, el valor del número NbMaxCP es disminuido si la probabilidad de que el usuario permanezca sobre el canal i durante NbMaxCP criptoperíodos sucesivos es inferior a un umbral predeterminado.

A continuación, durante una operación 170, el valor del número NbMaxCP es comparado a cero. Si el valor de este

número es nulo, entonces el servidor 106 inhibe la descodificación de los criptoperíodos siguientes del canal i. Para ello, procede a la etapa 144.

En el caso contrario, el número NbCP es temporalmente tomado igual al número NbMaxCP.

Luego, durante una operación 172, el número NbCP es ajustado de manera que reparta lo más uniformemente posible la carga de trabajo del servidor 106 sobre cada uno de los próximos criptoperíodos. Para ello, aquí, el servidor 106 ajusta el valor del número NbCP en función de:

- estimaciones de la carga de trabajo del servidor 106 sobre cada uno de los criptoperíodos que ha de venir, y

- una ley que entrega el valor final del número NbCP de palabras de control a transmitir permitiendo repartir más uniformemente la carga de trabajo del servidor 106 sobre cada uno de los criptoperíodos que han de venir.

Aquí, la carga de trabajo del servidor 106 es medida por el número probable de solicitudes a tratar por este servidor 106 durante un mismo criptoperíodo.

A título de ilustración, las estimaciones de la carga de trabajo para las diez próximos criptoperíodos que están por venir son almacenadas en una tabla de carga de trabajo. Un ejemplo de tal tabla está dado a continuación.

| Nº del criptoperíodo / identificador del canal | t | t+1 | t+2 | t+3 | t+4 | t+5 | t+6 | t+7 | t+8 | t+9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 11000 | 8464 | 8891 | 6712 | 5998 | 11865 | 8011 | 7776 | 8612 | 12567 |
| 2 | 12007 | 6801 | 11128 | 10218 | 9996 | 9857 | 6850 | 6880 | 7589 | 8359 |
| 3 | … | … | … | … | … | … | … | … | … | … |
| I | 22963 | 21117 | 22546 | 22989 | 23151 | 17896 | 15069 | 15033 | 15077 | 14211 |
| N | 880 | 891 | 765 | 610 | 877 | 880 | 910 | 898 | 961 | 499 |

Aquí, la ley que entrega el valor final del número NbCP está construida para optimizar los dos criterios siguientes:

1) NbCP debe ser igual o lo más próximo posible a su valor máximo NbMaxCP, y

2) el valor del número NbCP debe permitir repartir más uniformemente la carga de trabajo del servidor 106 sobre cada uno de los diez próximos criptoperíodos que han de venir.

Por ejemplo, la ley utilizada es la siguiente:

$$NbCP = Min\{Carga(j)*K^{(NbMaxCP-j)}\}$$

donde:

- Carga(j) es la carga de trabajo del servidor 106 durante el criptoperíodo j para la descodificación del canal i;

- K es una constante estrictamente superior a 1;

- j es un número entero que varía de t a NbMaxCP.

Por ejemplo, con ayuda de esta ley y con ayuda de los valores contenidos en la tabla precedente, en el caso en que el canal i es el segundo, el valor de NbCP es igual a 8 si la constante K es igual a 1,1 y NbMaxCP es igual a 10.

Finalmente, cuanto más próxima es la constante K a 1 más se autoriza al número NbCP ajustado a que esté alejado del valor del número NbMaxCP.

Una vez que el número NbCP ha sido determinado, la estimación de la carga de trabajo del servidor 106 es actualizada durante una etapa 174. Para ello, se hacen las dos hipótesis siguientes:

1) el usuario no cambia de canal, y

2) la próxima solicitud es transmitida por el terminal durante el criptoperíodo que precede al criptoperíodo para el que ninguna palabra de control le ha sido transmitida.

Por consiguiente, con estas hipótesis, la próxima solicitud transmitida por el terminal 10 se sitúa durante el criptoperíodo t+NbCP-2. Se incrementa por tanto el valor de estimación de la carga de trabajo del servidor 106 para el canal i durante el criptoperíodo t+NbCP-2 en un paso predeterminado. Por ejemplo el paso es típicamente igual a uno. Este valor es memorizado en la tabla de carga de trabajo descrita precedentemente.

Durante la etapa 174, al final del criptoperíodo corriente t-1, la columna correspondiente al criptoperíodo t es borrada de la tabla de carga de trabajo y las columnas correspondientes a los criptoperíodos t+1 a t+9 son desplazadas en una columna hacia la izquierda. Esto libera una columna virgen para el nuevo criptoperíodo t+9.

A continuación, durante una etapa 176, las palabras de control necesarias para descodificar los criptoperíodos sucesivos t a t+NbCP-1 son extraídas de la tabla 112.

Durante una etapa 178, las NbCP palabras de control extraídas son transmitidas al terminal 10 para que éste pueda descodificar los NbCP próximos criptoperíodos del canal i sin tener que enviar una solicitud hacia el servidor 106. Ello permite por tanto disminuir la carga de trabajo del servidor 106 ya que la frecuencia de las solicitudes disminuye al menos para ciertos terminales. Sin embargo, la seguridad del sistema 2 no es comprometida ya que sólo los terminales en los que la probabilidad es débil de que la seguridad de las palabras de control transmitidas sea comprometida se benefician de la recepción de palabras de control suplementarias.

Durante la etapa 178, eventualmente, el servidor 106 transmite igualmente palabras de control para otros canales distintos del canal i. Ello permite en particular acelerar la descodificación del nuevo canal después del basculamiento del canal precedente hacia este nuevo canal. Ello permite igualmente disminuir la carga de trabajo del servidor 106 ya que en respuesta a un cambio de canal, el terminal no envía necesariamente una nueva solicitud hacia el servidor de palabras de control. El número de palabras de control para los otros canales distintos del canal i transmitidas durante la etapa 178 es por ejemplo determinado de la misma manera que se ha descrito para el canal i o por otro procedimiento.

Finalmente, durante una etapa 180, el terminal 10 recibe las nuevas palabras de control y las registra en la tabla 79 para poderlas utilizar para descodificar los criptoperíodos siguientes del canal i.

Para poner en práctica el procedimiento de la fig. 5, la tabla 112 debe ser actualizada permanentemente para que ésta contenga previamente las palabras de control necesarias para la descodificación de los criptoperíodos que han de venir de cada uno de los canales. Para ello, se emplea el procedimiento de la fig. 6. Durante una etapa 190, el generador 32 de palabras de control genera previamente las palabras de control que serán utilizadas para codificar los criptoperíodos que han de venir de los contenidos multimedia difundidos. Por ejemplo, el generador 32 genera previamente entre dos y 100 palabras de control y, de preferencia, entre 10 y 30 palabras de control.

Durante una etapa 192, estas palabras de control son transmitidas al servidor 106 que las registra en la tabla 112 de manera que ésta contenga siempre las palabras de control necesarias para la descodificación de los criptoperíodos t, t+1, t+2,… etc. Por ejemplo, estas palabras de control son transmitidas al servidor 106 por medio de una unión segura que une directamente el dispositivo 6 a la cabeza de red 90.

Durante una etapa 194, el servidor 106 actualiza la tabla 112 con ayuda de las palabras de control suplementarias recibidas. De manera que permita la visualización de contenidos multimedia deslinealizados, el servidor 106 conserva igualmente en la tabla 112 los registros correspondientes a los criptoperíodos pasados.

Son posibles otros numerosos modos de realización. Por ejemplo pueden utilizarse otros índices de confianza distintos de los descritos para estimar la probabilidad de que la seguridad de las palabras de control almacenadas en el terminal dado sea comprometida. Igualmente, pueden emplearse otros modos de cálculo de los índices de confianza $IC_T$, $IC_u$ e $IC_c$. Por ejemplo el valor del índice $IC_c$ puede ser calculado en función de una medida de la audiencia actual del canal i descodificado por el terminal y no, como se ha descrito precedentemente, a partir de valores predeterminados registrados en la tabla 116.

El número NbCP puede ser determinado a partir de uno solo o de solamente dos de los índices $IC_T$, $IC_u$ e $IC_c$.

De manera similar, son posibles otros modos de cálculo del número NbCP. Por ejemplo, el número NbMaxCP puede ser obtenido a partir de otras fórmulas tales como por ejemplo con ayuda de la relación siguiente:

$$NbMaxCP = E(10 \times (IC_T + IC_u + IC_c)/300)$$

donde E es la función de la parte entera.

En otro modo de realización, el perfil del usuario no es utilizado para determinar el número NbCP.

Existen igualmente otros métodos de ajuste del número NbCP para repartir la carga de trabajo del servidor 106. Por ejemplo, para repartir la carga de trabajo sobre diferentes criptoperíodos. No es necesario estimar la carga de trabajo sobre cada uno de estos criptoperíodos. Por ejemplo, el ajuste del número NbCP consiste en extraer de manera aleatoria o pseudo-aleatoria un número comprendido entre 1 y NbMaxCP.

La estimación de la carga de trabajo tenida en cuenta para el ajuste del número NbCP puede ser la estimación de una carga de trabajo global para el conjunto de los canales y no como se ha descrito precedentemente una estimación carnal por canal. Por ejemplo, la carga global durante un criptoperíodo es obtenida sumando las cargas de trabajo del servidor 106 para cada uno de los canales i durante el mismo criptoperíodo.

El criptograma de la o de las palabras de control contenidas en la solicitud transmitida al servidor 106 por el terminal puede ser el identificador del canal a descodificar así como el número con la etiqueta de tiempo del próximo criptoperíodo sobre este canal a descodificar. En tal modo de realización, no es entonces necesario que la solicitud transmitida contenga además un criptograma de la palabra de control $CW_{i,t}$ obtenida cifrando esta palabra de control con ayuda de una clave secreta. En efecto, el identificador del canal y el número del próximo criptoperíodo son suficientes por sí solos para que el servidor 106 encuentre en la tabla 112 la palabra de control a enviar al terminal en respuesta a esta solicitud.

La actualización del perfil del usuario puede ser realizada de manera diferente. En particular, en otro modo de realización, es el terminal el que detecta los cambios de canales y el que envía, a cada cambio de canal, una información correspondiente al servidor 106 para que éste pueda actualizar el perfil del usuario de este terminal. En este caso, es posible tener en cuenta cambios de canales incluso si estos no están asociados a la transmisión inmediata de una nueva solicitud hacia el servidor 106. En efecto, la palabra de control que permite descodificar el nuevo canal puede ya haber sido recibida previamente y estar ya almacenada en la tabla 79.

Así, las tablas 112, 114 y 116 así como los contadores $C_1$ a $C_4$, han sido representados como que están contenidos en la memoria 110. Sin embargo, estas tablas pueden estar contenidas por otra parte en el sistema 2 y, por ejemplo, en una memoria que se puede interrogar a distancia, por el servidor 106.

En otro modo de realización, las palabras de control transmitidas desde el servidor hacia el terminal son transmitidas en forma cifrada de manera que sólo el terminal destinatario de esta palabra de control pueda descifrar estas palabras de control. En tal caso, el empleo de un túnel asegurado puede ser omitido.

En una variante del sistema 2, la palabra de control $CW_{i,t}$ es transmitida durante el criptoperíodo t y no durante el criptoperíodo t-1.

Lo que se ha descrito se aplica tanto a los contenidos multimedia linealizados como a los contenidos multimedia deslinealizados.

**REIVINDICACIONES**

1. Procedimiento de descifrado de palabras de control para terminales mecánica y electrónicamente independientes entre sí, en el que:

- en respuesta a la ausencia, en uno cualquiera de los terminales, de una o varias palabras de control $CW_c$ para descodificar uno o varios períodos de cifrado de un contenido multimedia, este terminal transmite (140) a un servidor de palabras de control una solicitud que contiene el o los criptogramas de una o varias de las palabras de control ausentes, y en respuesta

- el servidor de palabras de control transmite (178) a este terminal la o las palabras de control ausentes.

caracterizado por que el servidor de palabras de control:

- determina (164) selectivamente para cada terminal, un número de palabras de control suplementarias $CW_s$ a transmitir al terminal en función de la probabilidad de que la seguridad de estas palabras de control suplementarias sea comprometida, sobre la base de un índice de confianza para dicho terminal, y

- transmite (178) hacia este terminal, además de las palabras de control ausentes $CW_c$, el número determinado de palabras de control suplementarias $CW_s$ para permitir al terminal descodificar criptoperíodos suplementarios del contenido multimedia además de los criptoperíodos que se pueden descodificar con ayuda de las palabras de control ausentes $CW_c$ requeridas.

2. Procedimiento de transmisión de palabras de controlar terminales mecánica y electrónicamente independientes entre sí para la puesta en práctica de un procedimiento conforme a la reivindicación 1, incluyendo este procedimiento:

- la transmisión (178) a uno cualquiera de estos terminales de una o varias palabras de control ausentes $CW_c$ en respuesta a una solicitud de este terminal que contiene el o los criptogramas de las palabras de control ausentes,

caracterizado por que el procedimiento comprende igualmente:

- la determinación (164), selectivamente para cada terminal, de un número de palabras de control suplementarias $CW_s$ a transmitir al terminal en función de la probabilidad de que la seguridad de estas palabras de control suplementarias sea comprometida, sobre la base de un índice de confianza para dicho terminal, y

- la transmisión (178) hacia este terminal, además de las palabras de control ausentes $CW_c$, del número determinado de palabras de control suplementarias $CW_s$ para permitir al terminal descodificar criptoperíodos suplementarios del contenido multimedia además de los criptoperíodos que se pueden descodificar con ayuda de las palabras de control ausentes $CW_c$ requeridas.

3. Procedimiento según la reivindicación 2, en el que el número de palabras de control suplementarias es ajustado (172) en función de:

- estimaciones del número de solicitudes a tratar por el servidor de palabras de control durante varios criptoperíodos que han de venir, y

- una ley que entrega el número de palabras de control suplementarias a transmitir permitiendo repartir más uniformemente sobre los criptoperíodos que han de venir el número de solicitudes a tratar por el servidor de palabras de control durante cada uno de estos criptoperíodos que han de venir en función de dichas estimaciones.

4. Procedimiento según la reivindicación 3, en el que el servidor de palabras de control estima (174) el número de solicitudes a tratar en el curso de un criptoperíodo que ha de venir a partir del número de palabras de control suplementarias transmitidas a los terminales por este servidor en el curso de los criptoperíodos pasados y del criptoperíodo presente.

5. Procedimiento según la reivindicación 2, en el que el número de palabras de control suplementarias es determinado en función de un numero aleatorio extraído, de manera aleatoria o pseudo-aleatoria, en una región de números cuya extensión en función de la probabilidad de que la seguridad de las palabras de control almacenadas en el terminal sea comprometida.

6. Procedimiento según una cualquiera de las reivindicaciones 2 a 5, en el que el número de palabras de control suplementarias $CW_s$ es igualmente ajustado (168) en función del número probable de criptoperíodos sucesivos de este contenido multimedia que serán descodificados por este terminal.

7. Procedimiento según una cualquiera de las reivindicaciones 2 a 6, en el que la probabilidad de que la seguridad de las palabras de control suplementarias $CW_s$ sea comprometida es función de un identificador del terminal y/o de un contador de error de funcionamiento de este terminal y/o de un identificador del contenido multimedia.

8. Procedimiento de recepción de palabras de control por un terminal para la puesta en práctica del procedimiento conforme a la reivindicación 1, en el que en respuesta a la ausencia en este terminal de una o varias palabras de control $CW_c$ para descodificar uno o varios criptoperíodos de un contenido multimedia, este terminal transmite (140) al servidor de palabras de control una solicitud que contiene el o los criptogramas de una o varias palabras de control ausentes,

caracterizado por que el terminal recibe (180), además de las palabras de control ausentes requeridas, un número determinado de palabras de control suplementarias para permitir a este terminal descodificar criptoperíodos suplementarios del mismo contenido multimedia además de los criptoperíodos que se pueden descodificar con ayuda de las palabras de control ausentes $CW_c$ requeridas.

9. Soporte de registro de informaciones, caracterizado por que incluye instrucciones para la ejecución de un procedimiento conforme a una cualquiera de las reivindicaciones precedentes, cuando éstas instrucciones son ejecutadas por un calculador electrónica.

10. Servidor de palabras de control hacia terminales mecánica y electrónicamente independientes entre sí, para la puesta en práctica de un procedimiento conforme a la reivindicación 1, siendo apto este servidor (106) para trasmitir a uno cualquiera de los terminales una o varias palabras de control ausentes $CW_c$, en respuesta a una solicitud de este terminal que contiene el o los criptogramas de la o de las palabras de control ausentes,

caracterizado por que el servidor (106) de palabras de control es igualmente apto:

- para determinar, selectivamente para cada terminal, un número de palabras de control suplementarias $CW_s$ a transmitir al terminal en función de la probabilidad de que la seguridad de estas palabras de control suplementarias sea comprometida, sobre la base de un índice de confianza para dicho terminal, y

- para trasmitir hacia este terminal, además de las palabras de control ausentes $CW_c$, el número determinado de palabras de control suplementarias $CW_s$ para permitir al terminal descodificar criptoperíodos suplementarios del contenido multimedia además de los criptoperíodos descodificados con ayuda de las palabras de control ausentes $CW_c$ requeridas.

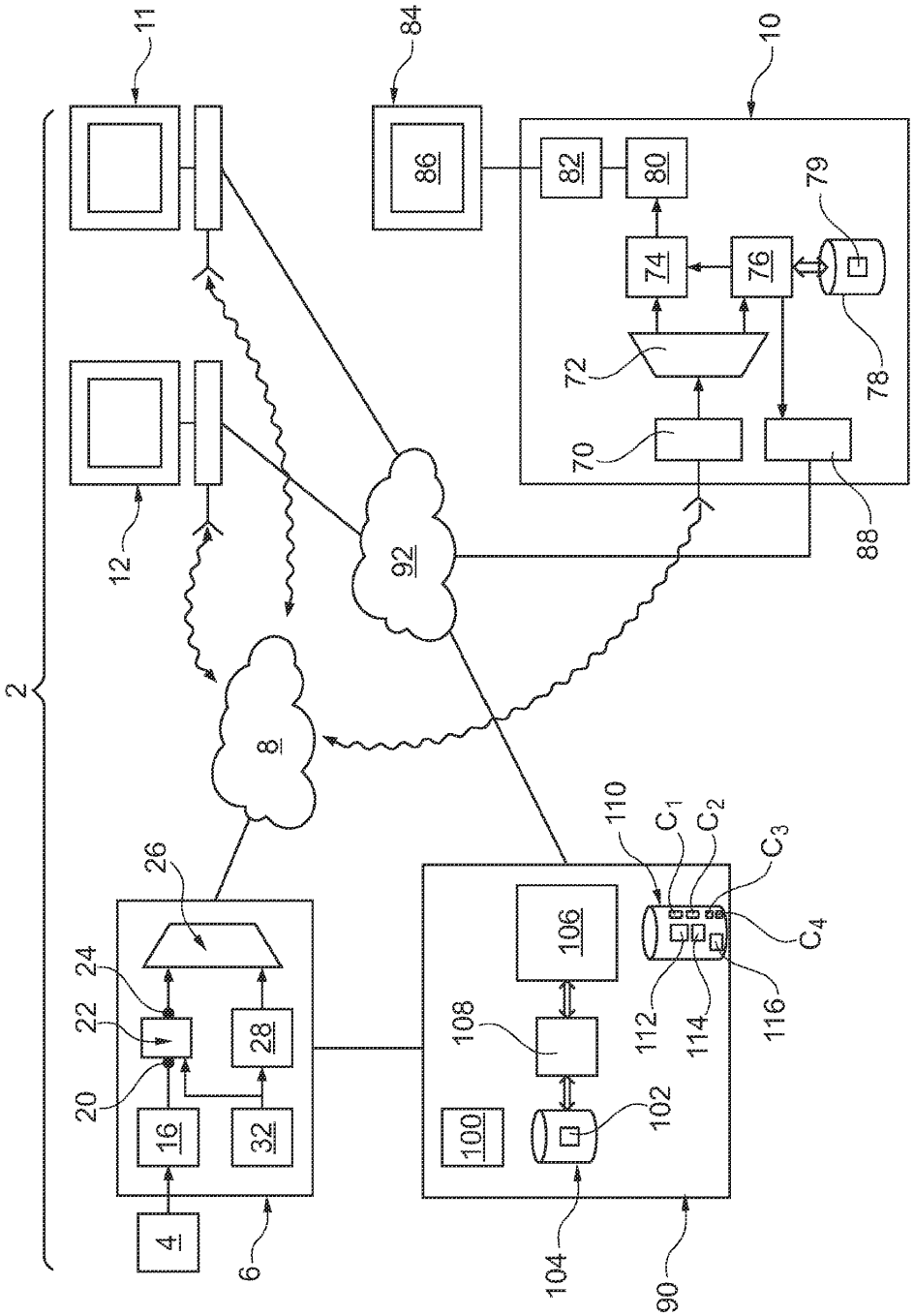
11
84
10
86
82
80
79
74
76
72
78
70
88
12
92
8
2
110
$C_1$
$C_2$
$C_3$
$C_4$
26
24
22
20
28
16
32
4
6
106
108
100
102
112
114
116
104
90

Fig. 1

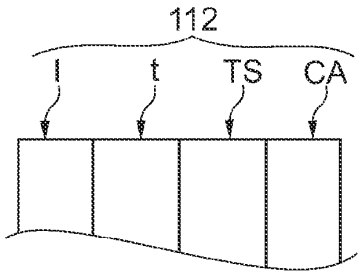


Fig. 2

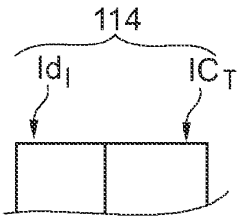


Fig. 3

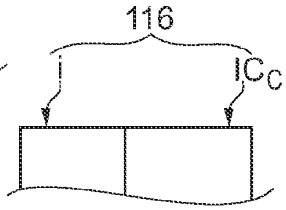


Fig. 4

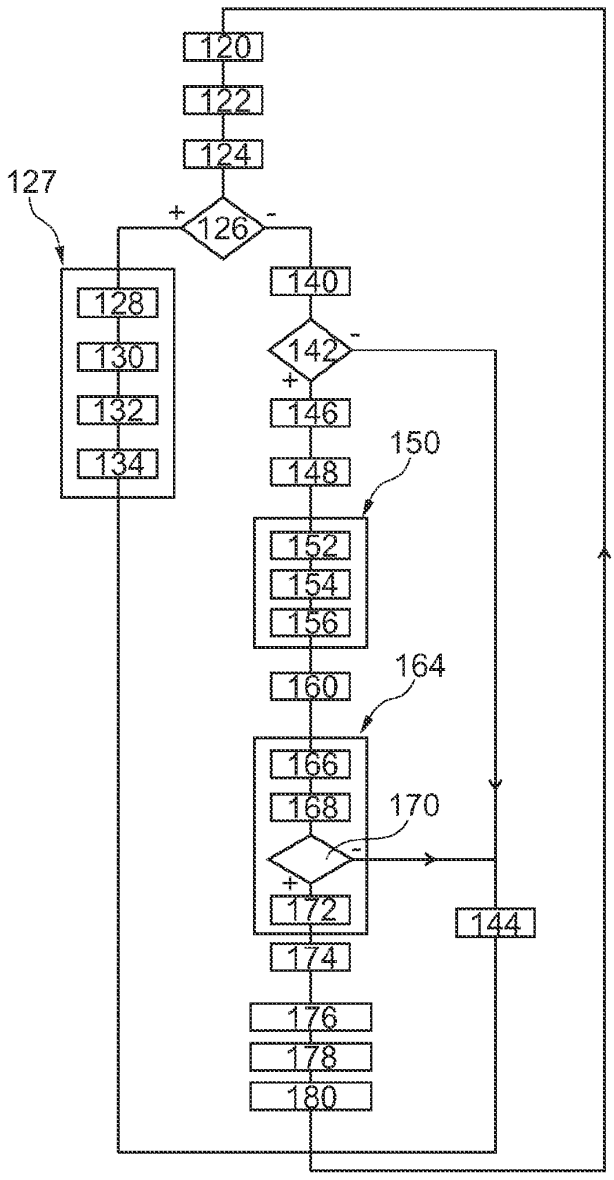


Fig. 5

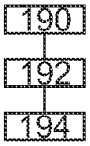


Fig. 6