(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 602 137**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04N 21/4405 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/835 (2011.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.06.2011 PCT/EP2011/060258**

(87) Fecha y número de publicación internacional: **29.12.2011 WO11161066**

(96) Fecha de presentación y número de la solicitud europea: **20.06.2011 E 11725786 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.08.2016 EP 2586198**

(54) Título: **Procedimiento de protección, procedimiento de cifrado, soporte de registro y terminal para este procedimiento de protección**

(30) Prioridad:

22.06.2010 FR 1054943

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2017

(73) Titular/es:

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

(72) Inventor/es:

POCHON, NICOLAS;
CHIEZE, QUENTIN y
LAFRANCHI, STÉPHANE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de protección, procedimiento de cifrado, soporte de registro y terminal para este procedimiento de protección

La invención se refiere a un procedimiento de protección de la transmisión, de un contenido multimedia o de una palabra de control, entre un procesador de seguridad y un terminal. La invención tiene igualmente por objeto un procedimiento de descifrado de un contenido multimedia o de una palabra de control así como un soporte de registro y un terminal para la puesta en práctica de este procedimiento de protección.

Por contenido multimedia, se designa aquí un contenido destinado a ser presentado sobre una pantalla, y/o reproducir por altavoces. Típicamente, un contenido multimedia es una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

Para asegurar la transmisión de los contenidos multimedia hacia terminales por medio de una red pública, los contenidos multimedia son entrelazados con las palabras de control antes de su transmisión sobre esta red pública.

Más precisamente, una palabra de control es una palabra codificada sobre varios bits de informaciones utilizada para entrelazar un cripto-período del contenido multimedia. Un cripto-período es un período de contenido multimedia entrelazado con la misma palabra de control y durante el cual los derechos de acceso a este contenido multimedia no son modificados.

Aquí, los términos « entrelazar » y « cifrar » son considerados como sinónimos. Lo mismo sucede para los términos « deshacer el entrelazado » y « descifrar ».

Para proteger la transmisión de las palabras de control hacia los terminales por medio de la red pública, estas palabras de control son igualmente cifradas antes de su transmisión, por ejemplo, con una clave de suscripción Ka.

Un procesador de seguridad es un procesador que trata informaciones confidenciales tales como claves criptográficas o algoritmos criptográficos. Para preservar la confidencialidad de estas informaciones, está concebido para ser lo más robusto posible frente a tentativas de ataques llevados a cabo por piratas informáticos. Es por tanto más robusto frente a estos ataques que los otros componentes del terminal. En numerosas aplicaciones, este procesador de seguridad es amovible, es decir que puede ser introducido y, alternativamente, retirado del terminal fácilmente. En este caso, se presenta a menudo en forma de una tarjeta con chip.

En el contexto del entrelazado de los contenidos multimedia, el procesador de seguridad contiene informaciones secretas que permiten deshacer el entrelazado del contenido multimedia recibido por un terminal. Más precisamente, existen dos modos de funcionamiento posibles para este procesador de seguridad:

- o bien el procesador de seguridad deshace el entrelazado él mismo del contenido multimedia y transmite el contenido multimedia deshecho el entrelazado al terminal,

- o bien el procesador de seguridad descifra la palabra de control y transmite la palabra de control descifrada al terminal.

Si no se ha tomado ninguna precaución, el contenido multimedia deshecho el entrelazado o la palabra de control descifrada es transmitido sin codificar del procesador de seguridad hacia el terminal.

Por "sin codificar" se designa el estado de una información que corresponde a su estado antes de que sea entrelazada o cifrada por palabras de control secretas o claves secretas.

El contenido multimedia sin codificar o la palabra de control sin codificar transmitida sobre la interfaz entre el procesador de seguridad y el terminal es vulnerable. Se han puesto a punto ataques para explotar esta vulnerabilidad. Por ejemplo, se ha propuesto captar sobre esta interfaz la palabra de control sin codificar para a continuación difundirla ilícitamente hacia otros terminales.

Para remediar este inconveniente, se ha propuesto ya cifrar el contenido multimedia o la palabra de control transmitida del procesador de seguridad hacia el terminal.

Así existen procedimientos de protección de la transmisión, de un contenido multimedia o de una palabra de control, entre el procesador de seguridad y el terminal en los que:

- el procesador de seguridad construye una clave de sesión corriente SK_c por diversificación de una clave raíz SK_root en función de un parámetro P_c transmitido por el terminal,

- el procesador de seguridad descifra el contenido multimedia o la palabra de control y luego cifra el contenido multimedia descifrado o la palabra de control descifrada con la clave de sesión corriente SK_c y, finalmente, transmite al terminal el contenido multimedia o la palabra de control descifrada con la clave de sesión corriente SK_c y

- el terminal descifra el contenido multimedia o la palabra de control cifrada con la clave SK_c construida, con ayuda de un código secreto C_c^{-1} para obtener el contenido multimedia o la palabra de control sin codificar.

Por ejemplo, tal procedimiento es divulgado en la solicitud de patente EP 1 867 096. En este procedimiento conocido, el parámetro P_c es un identificador del terminal.

Sin embargo, puede suceder que la seguridad de la clave de sesión corriente SK_c esté comprometida. Por ejemplo, tentativas de ataque consisten en intentar descubrir esta clave de sesión corriente y/o la clave raíz SK_root a partir de la cual es construida.

Si la seguridad de la clave de sesión corriente está comprometida, ésta debe ser renovada. La renovación de una clave de sesión es un proceso largo y complicado. Por ejemplo, en el sistema descrito en la solicitud de patente EP 1 867 096, ello necesita la renovación de la clave raíz SK_root en cada procesador de seguridad y del criptograma SK_H* o SK_S* en cada terminal. Esta renovación no puede ser realizada más que dirigiéndose individualmente a cada terminal lo que es un proceso particularmente largo y que no puede ser realizado simultáneamente para todos los terminales. El cambio de clave de sesión necesita también el envío de varios mensajes al mismo terminal de los que en particular un mensaje es para reemplazar el criptograma SK_H* o SK_S* y un mensaje para reemplazar la clave SK_root. Además, los mensajes dirigidos individualmente a cada terminal pueden ser fácilmente filtrados para eliminarlos. Así, un usuario malintencionado puede fácilmente impedir la renovación de su clave de sesión.

El estado de la técnica es igualmente conocido por los documentos EP 0899956A2 y US 2009/238363 A1.

La invención pretende remediar al menos uno de estos inconvenientes. Tiene pues por objeto un procedimiento de protección de la transmisión, de un contenido multimedia o de una palabra de control, conforme a la reivindicación 1.

En el procedimiento anterior, el cambio de la clave de sesión es más rápido pues el o los parámetros que permiten renovar la clave de sesión tanto en el procesador de seguridad como en el terminal son transmitidos en el mismo mensaje. Así, un solo mensaje es suficiente para activar el cambio de la clave de sesión. Además estos parámetros están contenidos en el mismo mensaje que aquel que contiene el contenido multimedia entrelazado por la palabra de control cifrada. Así, si este mensaje es eliminado para impedir la renovación de la clave de sesión, la acción de deshacer el entrelazado del contenido multimedia es hecha imposible ya que el contenido multimedia entrelazado o la palabra de control cifrada necesario para ello no es transmitido al procesador de seguridad.

Finalmente, cada terminal contiene ya previamente varios códigos secretos que permiten cada uno descifrar el contenido multimedia o la palabra de control cifrada con una clave de sesión SK_i diferente de las otras claves de sesión. Así, el cambio de la clave de sesión puede ser realizado instantáneamente sin que haya un periodo transitorio durante el cual la antigua clave de sesión ya no es utilizable mientras que la nueva clave de sesión no está aún disponible.

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

Estos modos de realización del procedimiento de protección presentan además las ventajas siguientes:

- cuando el código secreto es un código ejecutable o interpretable, su implicación no da ninguna información sobre la clave raíz o el algoritmo criptográfico empleado para realizar los otros códigos secretos ejecutables o interpretables,

- la utilización de un mensaje ECM para transmitir el parámetro P_c permite realizar una renovación de esta clave de sesión a una frecuencia muy elevada,

- transmitir el contenido multimedia o la palabra de control cifrada dos veces aumenta la seguridad del sistema.

La invención tiene igualmente por objeto un procedimiento de descifrado de un contenido multimedia o de una palabra de control por un terminal conforme a la reivindicación 9.

La invención tiene igualmente por objeto un soporte de registro de informaciones que incluye instrucciones para la puesta en práctica de uno de los procedimientos precedentes, cuando éstas instrucciones son ejecutadas por un ordenador electrónico.

Finalmente, la invención tiene igualmente por objeto el terminal de descifrado conforme a la reivindicación 11.

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 transmisión y de recepción de contenidos multimedia entrelazados,

La fig. 2 es una ilustración esquemática y parcial de un mensaje ECM utilizado en el sistema de la fig. 1,

La fig. 3 es una ilustración esquemática y parcial de un mensaje EMM (Entitlement Management Message ("Mensaje de Gestión de Derecho")) utilizado en el sistema de la fig. 1.

La fig. 4 es una ilustración de una tabla igualmente utilizada en el sistema de la fig. 1,

La fig. 5 es un organigrama de un procedimiento de transmisión y de recepción de contenido multimedia entrelazado puesto en práctica con ayuda del sistema de la fig. 1, y

La fig. 6 es un organigrama de un procedimiento de registro de códigos secretos en un terminal del sistema de la fig. 1.

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 un experto en la técnica no están 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 informarse en el documento siguiente:

- "Functional Model of Conditional Access System", EBU Review, Technical European Broadcasting Union, Bruselas, BE, nº 266, 21 de Diciembre de 1995.

La fig. 1 representa un sistema 2 de emisión y de recepción de contenidos multimedia entrelazado. Por ejemplo, cada contenido multimedia corresponde a una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

Los contenidos multimedia sin codificar 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 la norma UIT-T H264.

Los contenidos multimedia comprimidos son dirigidos hacia una entrada de un entrelazador 22. El entrelazador 22 entrelaza cada contenido multimedia comprimido para condicionar su visualización a ciertas condiciones tales como la compra de un derecho de acceso para los usuarios de los terminales de recepción. Los contenidos multimedia entrelazados son restituidos sobre una salida conectada a la entrada de un multiplexor 26.

El entrelazador 22 entrelaza cada contenido multimedia comprimido con ayuda de una palabra de control $CW_{j,t}$ que le es proporcionada, así como a un sistema de acceso 28 condicional, por un generador 32 de claves.

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

El índice j es un identificador del canal sobre el que es difundido el contenido multimedia entrelazado y el índice t es un identificador del cripto-periodo entrelazado con esta palabra de control. En lo que sigue de esta descripción, el cripto-periodo que actualmente ha deshecho el entrelazado por los terminales es el cripto-periodo t-1.

Típicamente, este entrelazado 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 $CW^*_{j,t}$ de la palabra de control $CW_{j,t}$ generado por el generador 32 y utilizado por el entrelazador 22 para entrelazar el cripto-periodo t del canal j. Estos mensajes ECM y los contenidos multimedia entrelazados son multiplexados por el multiplexor 26, siendo estos últimos proporcionados respectivamente por el sistema 28 de acceso condicional y por el entrelazador 22, antes de ser transmitidos sobre la red 8.

El sistema 28 es igualmente capaz de insertar en el mensaje ECM dos parámetros P_i y Px_i.

El sistema 28 genera también mensajes EMM (Entitlement Management Message) tal como el ilustrado en la fig. 3.

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

El sistema 28 está igualmente conectado a una unidad 34 de gestión de la renovación de las claves de sesión. Esta unidad 34 proporciona al sistema 28 los parámetros P_i, Px_i así como códigos secretos asociados C_i^{-1}. Estos parámetros y estos códigos son descritos más adelante con más detalle.

Por ejemplo, los terminales 10 a 12 son idénticos y sólo él terminal el 10 esta 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 dispositivo para deshacer el entrelazado 74 y por otro lado los mensajes ECM y EMM (Entitlement Management Message) a un módulo 76 de seguridad.

El dispositivo para deshacer el entrelazado 74 deshace el entrelazado del contenido multimedia entrelazado a partir de la palabra de control transmitida por el módulo 76. El contenido multimedia cuyo entrelazado se ha deshecho es transmitido a un descodificador 80 que lo 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 sin codificar el contenido multimedia sobre la pantalla 86.

El módulo 76 gestiona los intercambios de informaciones con un procesador de seguridad amovible 80. En particular, coopera con el procesador 80 para proteger la interfaz entre este procesador 80 y el terminal 10. A este efecto, este módulo 76 es colocado en corte de flujo entre las informaciones transmitidas del terminal 10 hacia el procesador 80 y viceversa. El módulo 76 está por ejemplo realizado a partir de un ordenador electrónico programable. Está conectado a una memoria 82 que incluye el conjunto de las instrucciones y de los datos necesarios para la ejecución de los procedimientos de las figs. 5 y 6. Esta memoria 82 incluye por tanto en particular los elementos siguientes:

- un identificador D-ID del terminal 10 que permite identificar este terminal 10 entre el conjunto de los terminales del sistema 2,

- un criptograma TSK* de una clave de sesión TSK obtenida por diversificación de una clave raíz TSK_root con el identificador D_ID,

- una clave personal Ki que permite descifrar el criptograma TSK*,

- una tabla 84 que asocia a cada parámetro Px_i un código secreto C_i^{-1} que permite descifrar una información cifrada con una clave de sesión corriente SK_i y

- los códigos C_i^{-1}.

En este modo de realización, cada código C_i^{-1} es un código de una función de descifrado de las informaciones cifradas con una clave de sesión respectiva SK_i. Cada código C_i^{-1} es directamente ejecutable por el módulo 16. Cada código C_i^{-1} corresponde a una función de descifrado que admite como único parámetro la información a descifrar. Éste código es por tanto ya parametrizado con la clave de sesión SK_i. Esta clave de sesión SK_i es obtenida por diversificación de una clave raíz SK_root con ayuda de un parámetro P_i.

El procesador 80 está realizado igualmente a partir de un ordenador electrónico 86 que implementa un módulo de cifrado y de descifrado de informaciones. A este efecto, el procesador 80 incluye igualmente una memoria 88 conectada al ordenador 86. Esta memoria 88 es una memoria protegida que contiene en particular las informaciones secretas necesarias para la ejecución del procedimiento de la fig. 5. En particular, esta memoria contiene especialmente:

- derechos de acceso a uno o varios contenidos multimedia,

- una o varias claves de suscripción Ka,

- la clave raíz TSK_root,

- la clave raíz SK_root, e

- instrucciones para la ejecución del procedimiento de la fig. 5.

La fig. 2 representa una parte de una trama de un mensaje ECM 90 susceptible de ser generado por el sistema 28. Este mensaje ECM contiene en particular un campo 92 que contiene los parámetros P_i y Px_i. El parámetro Px_i puede ser la totalidad o parte del parámetro P_i y viceversa. La misión de estos parámetros P_i y Px_i esta descrita más en detalle con referencia a la fig. 5.

De manera clásica, este mensaje ECM 90 contiene igualmente:

- el identificador j del canal,

- los criptograma más $CW^*_{j,t}$ y $CW^*_{j,t+1}$ de las palabras de control $CW_{j,t}$ y $CW_{j,t+1}$ que permiten deshacer el entrelazado de los cripto-períodos t y t+1 del canal j,

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

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

La fig. 3 representa esquemática y parcialmente un mensaje EMM 100 susceptible de ser generado por el sistema 28. Este mensaje EMM 100 contiene en particular un identificador Message_Type ("Mensaje_Tipo") que permite indicar que este mensaje EMM es con destino al terminal y no al procesador de seguridad.

Este mensaje 100 contiene igualmente:

- varios códigos C_i^{-1} donde i está comprendido entre 1 y n, siendo n un número entero estrictamente superior o igual a dos,

- los parámetros Px_i, estando cada uno de estos parámetros asociado al código correspondiente C_i^{-1}, y

- un código CRC que permite verificar la integridad del mensaje 100.

La fig. 4 representa un ejemplo posible de estructura de la tabla 84. Esta tabla 84 comprende dos columnas 102 y 104. La columna 102 comprende el parámetro Px_i mientras que la columna 104 comprende el código C_i^{-1} asociado correspondiente o la dirección en la memoria 82 de este código C_i^{-1}.

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

Inicialmente, durante una fase 110 de inicialización, el procesador 80 es insertado en el interior del terminal 10. En respuesta, el terminal 10 transmite su identificador D-ID al procesador 80. Éste, genera entonces una clave de sesión TSK. Esta clave de sesión TSK es obtenida por diversificación de la clave raíz TSK_root registrada en la memoria 88.

Los detalles sobre el cifrado y el descifrado de las palabras de control con ayuda de esta clave de sesión TSK no están descritos aquí en detalle. En efecto, el procedimiento de cifrado de las palabras de control sobre la interfaz entre el procesador 80 y el terminal 10 es aquí el mismo que el descrito en la solicitud de patente EP 1 867 096. Así, el lector puede referirse a esta solicitud de patente para más informaciones.

Durante la fase de inicialización, el procesador 80 recibe igualmente, por ejemplo por medio de mensajes EMM, derechos de acceso y claves de suscripción Ka. Estos derechos de acceso y claves Ka le permiten descifrar los criptogramas de las palabras de control de los canales para los que ha suscrito un abono con un operador.

La transmisión de un contenido multimedia del dispositivo 6 hasta un terminal es descrita a continuación en el caso particular del terminal 10.

Durante una etapa 112, el generador 32 genera una palabra de control que es transmitida al entrelazador 22 y al sistema 28.

Durante una etapa 114, esta palabra de control es cifrada con una clave de suscripción Ka para obtener un criptograma CW^*_{Ka}. Por ejemplo, la clave Ka es renovada una vez al mes.

A continuación, durante una etapa 116, el sistema 28 genera un mensaje ECM que contiene el criptograma CW^*_{Ka} así como los derechos de acceso correspondientes. Eventualmente este mensaje ECM contiene igualmente parámetros P_c y Px_c si se requiere un refuerzo del nivel de seguridad de la protección de la interfaz entre el procesador 80 y el terminal 10. Los parámetros P_c y Px_c son elegidos entre los pares de parámetros P_i y Px_i utilizados para crear la tabla 84.

En paralelo, durante una etapa 118, la palabra de control generada es transmitida al entrelazador 22 que entrelaza un cripto-período del contenido multimedia con ayuda de esta palabra de control antes de transmitir el cripto-período entrelazado al multiplexor 26.

Durante una etapa 120, el multiplexor 26 multiplexa los mensajes ECM generados con el contenido multimedia entrelazado y luego los difunde al conjunto de terminales del sistema 2 por medio de la red 8.

Durante una etapa 122, el terminal 10 recibe, con ayuda de su receptor 70, las señales difundidas por el dispositivo 6.

Durante una etapa 124, estas señales son desmultiplexadas por el desmultiplexor 72.

Durante una etapa 126, el contenido multimedia entrelazado es entonces transmitido al dispositivo para deshacer el entrelazado 74.

Durante una etapa 128, los mensajes ECM y EMM son en cuanto a ellos mismos transmitidos hacia el módulo 76 de seguridad.

Durante una etapa 130, el módulo 76 verifica si hay presentes nuevos parámetros P_c, Px_c en el mensaje ECM recibido. Por nuevos parámetros P_c, Px_c se entienden parámetros P_c, Px_c que tienen valores diferentes de los precedentemente recibidos.

En caso afirmativo, procede a una etapa 132 durante la cual extrae el parámetro Px_c luego selecciona el código C_c^{-1} asociado a este parámetro con ayuda de la tabla 84.

A la salida de la etapa 132 o en el caso en que el mensaje ECM no incluye parámetro P_c, Px_c o nuevos parámetros P_c, Px_c durante una etapa 133, el módulo 76 transmite el mensaje ECM recibido al procesador 80.

Durante una etapa 134, el procesador 80 compara los derechos de acceso contenidos en la memoria 88 con los derechos de acceso contenidos en el mensaje ECM recibido.

Si los derechos de acceso no corresponden al derecho de acceso, entonces el procesador 80 procede a una etapa 138 de inhibición de la acción de deshacer el entrelazado del contenido multimedia recibido. Por ejemplo, a este efecto, no transmite la palabra de control necesaria para la acción de deshacer el entrelazado del contenido multimedia al terminal 10.

En caso contrario, durante una etapa 140, el procesador 80 descifra el criptograma CW^*_{Ka} con la clave Ka de manera que obtenga la palabra de control CW sin codificar.

A continuación, durante una etapa 142, el calculador 86 cifra la palabra de control CW con ayuda de la clave de sesión TSK registrada en la memoria 88 y generada durante la fase 110. El criptograma CW^*_{TSK} es entonces obtenido.

Durante una etapa 144, el procesador 80 verifica si un parámetro P_c está presente en el mensaje ECM recibido.

En caso afirmativo, el procesador 80 procede entonces a una etapa 146 durante la cual construye la nueva clave de sesión SKc, por diversificación de la clave raíz SK_root con ayuda del parámetro P_c recibido. La etapa 146 es realizada únicamente cuando se trata de un nuevo parámetro P_c. Si el parámetro P_c ha sido ya recibido, la clave SKc ha sido ya construida y se puede proceder directamente a la etapa siguiente.

A continuación, durante una etapa 148, cifra el criptograma CW^*_{TSK} con ayuda de la clave SK_c para obtener un criptograma $CW^{**}_{(TSK)(SKc)}$. Correspondiendo este criptograma $CW^{**}_{(TSK)(SKc)}$ a la palabra de control cifrada dos veces, una vez por la clave TSK y una vez por la clave SK_c. Se dice igualmente en este caso que la palabra de control CW está sobrecifrada con la clave SK_c.

A la salida de la etapa 148 o en el caso de que el mensaje ECM recibido no incluya parámetro P_c, durante una etapa 150, el procesador 80 procede a la transmisión del criptograma de la palabra de control hacia el terminal 10. Según que las etapas 146, 148 hayan sido ejecutadas o no, este criptograma es o bien el criptograma $CW^{**}_{(TSK)(SKc)}$ o bien el criptograma CW^*_{TSK}.

A continuación, si el parámetro Px_c estaba presente en el mensaje ECM recibido, durante una etapa 152, el módulo 76 descifra una primera vez el criptograma $CW^{**}_{(TSK)(SKc)}$ ejecutando el código C_c^{-1} seleccionado durante la etapa 132. Más precisamente, durante esta etapa, el código C_c^{-1} recibe únicamente como parámetro de entrada el criptograma $CW^{**}_{(TSK)(SKc)}$ a descifrar. En este estado, no es necesario que sea igualmente parametrizado con la clave de sesión SK_c ya que este parámetro está ya integrado en el código ejecutable. A la salida de la etapa 152, el criptograma CW^*_{TSK} es obtenido a partir del criptograma $CW^{**}_{(TSK)(SKc)}$.

Después de la etapa 152 o si la palabra de control transmitida por el procesador 80 no está cifrada más que una sola vez, durante una etapa 154, el módulo 76 descifra el criptograma CW^*_{TSK} con ayuda de la clave TSK. Durante esta etapa 154, la clave TSK es por ejemplo obtenida descifrando un criptograma de esta clave almacenado en la memoria 82 con ayuda de que su clave personal K_i. A la salida de la etapa 154, la palabra de control CW sin codificar es obtenida.

Durante una etapa 156, el módulo 76 transmite esta palabra de control CW sin codificar al dispositivo para deshacer el entrelazado 74 que deshace el entrelazado entonces del cripto-período correspondiente del contenido multimedia entrelazado con esta palabra de control.

Durante una etapa 158, el contenido multimedia cuyo entrelazado se ha deshecho es transmitido al descodificador 80 que le descodifica.

Durante una etapa 160, la tarjeta gráfica recibe el contenido multimedia descodificado y ordena su presentación sobre la pantalla 86. Así, durante una etapa 162 el contenido multimedia sin codificar es presentado sobre la pantalla 86.

En el procedimiento de la fig. 5, cuando se requiere un refuerzo de la protección de la interfaz entre el procesador 80 y el terminal 10, basta insertar parámetros P_c y Px_c en un mensaje ECM. A partir de este momento, la palabra de control transmitida del procesador 80 hacia el terminal 10 es cifrada dos veces en lugar de una sola vez. Además, para cambiar la clave de sesión SKc, basta cambiar los parámetros P_c y Px_c contenidos en el mensaje ECM. Sin embargo, este

cambio de clave de sesión SK_c supone que los códigos C_c^{-1} correspondientes hayan sido registrados previamente en la memoria 82. Esto es realizado con ayuda del procedimiento de la fig. 6 siguiente.

Cuando se requiere un refuerzo de la seguridad, durante una etapa 170, se eligen varios pares de parámetros P_i, Px_i.

A continuación, durante una etapa 172, la unidad 34 construye una clave de sesión SK_i para cada parámetro P_i elegido durante la etapa 170. Aquí, cada clave SK_i es obtenida por diversificación de la clave raíz SK_root en función del parámetro P_i. Un ejemplo de diversificación está descrito en la solicitud de patente EP 1 867 096.

A continuación, durante una etapa 174, los códigos C_i^{-1} que permiten descifrar los criptograma las obtenidos con las claves SK_i son generados. Por ejemplo, a este efecto, para cada código C_i^{-1} es utilizado el mismo algoritmo de descifrado que el utilizado por el procesador 80 es parametrizado con la clave SK_i y luego compilado con ayuda de un compilador. De preferencia, el código ejecutable es hecho robusto frente a tentativas de cripto-análisis que pretenden por ejemplo identificar la clave de sesión, la clave raíz o el algoritmo utilizado para descifrar los mensajes. Por ejemplo, a este efecto, la enseñanza del siguiente documento es empleada:

S. Chow, P. Eisen, H. Jhonson, P.C. Van Oorchot, « White Box Crytography And an AES Implementation », Proceedings of SAC 2002, 9th Annual Workshop on Selected Area in Criptography, 15-16 de Agosto de 2002, Saint John's, Canada.

Una vez generados los códigos C_i^{-1}, durante una etapa 176, estos son transmitidos con los parámetros Px_i correspondientes al sistema 28 del dispositivo 6. A este efecto, el sistema 28 genera un mensaje EMM tal como el mensaje EMM 100 que es a continuación multiplexado con el contenido multimedia entrelazado y difundido simultáneamente al conjunto de los terminales del sistema 2.

En respuesta a la recepción de este mensaje EMM 100, durante una etapa 178, este es transmitido al módulo 76 de seguridad.

Durante una etapa 180, el módulo 76 de seguridad actualiza la tabla 84 a partir de las informaciones contenidas en este mensaje EMM y registra los códigos C_i^{-1} en la memoria 82.

A partir de este momento, el sobre-cifrado de las palabras de control con una de las claves SK_i puede ser activado y el cambio de la clave de sobre-cifrado puede ser igualmente realizado rápida y frecuentemente.

Son posibles otros numerosos modos de realización. Por ejemplo, los códigos C_i^{-1} no son necesariamente códigos ejecutables y pueden ser reemplazados por códigos directamente interpretables por una máquina virtual implementada en el terminal 10. Típicamente, la máquina virtual es una máquina virtual Java®.

El código C_i^{-1} no es necesariamente un código ejecutable o interpretable. En una variante, el código C_i^{-1} es una clave SK_i o un criptograma de esta clave SK_i.

Los parámetros P_i y Px_i pueden ser la totalidad o parte de un mismo parámetro. En particular, el parámetro Px_i puede ser idéntico al parámetro P_i. En esta variante, sólo es transmitido entonces el parámetro P_i.

Los parámetros P_i o Px_i pueden ser el objeto de diferentes operaciones antes de ser utilizados por el terminal o el procesador 80. Por ejemplo estos parámetros pueden ser utilizados como un grano sirve para inicializar un generador de números seudo-aleatorios. Es entonces el número seudo-aleatorio generado el que es utilizado para diversificar la clave raíz SK_root o utilizado por el módulo 76.

En otra variante, sólo un parámetro Px_i y el código C_i^{-1} asociado son enviados a los terminales antes de la utilización de la clave SK_i. Así, la memoria 82 incluye únicamente el código C_c^{-1} y el código C_i^{-1} que será utilizado inmediatamente después del código C_c^{-1}. Ello evita exponer inútilmente los otros códigos C_i^{-1} susceptibles de ser utilizados.

El cambio de la clave SK_c puede intervenir inmediatamente como se ha descrito precedentemente o después de un número predeterminado de cripto-períodos recibidos después de la recepción del mensaje que contiene el nuevo parámetro P_c.

En otra variante, el primer cifrado de la palabra de control con ayuda de la clave TSK no es empleado. En este caso, la palabra de control es únicamente cifrada con ayuda de la clave de sesión SK_c.

El procesador de seguridad no es necesariamente amovible. Por ejemplo, está fijado sin ningún grado de libertad en el interior del terminal 10.

El procesador de seguridad no toma necesariamente la forma de una tarjeta con chip. Por ejemplo, puede igualmente presentarse en forma de una clave USB (Universal Serial Bus). En otra variante, no es amovible pero está integrado en la caja del terminal.

Los elementos del terminal 10 no están necesariamente contenidos en una misma caja. Por ejemplo, estos elementos pueden estar repartidos sobre una red local. En este caso, típicamente, una caja que recibe las señales transmitidas por

el dispositivo 6 utiliza el procesador 80 para descifrar las palabras de control y para cifrarlas con ayuda de la clave de sesión SK_c. Las palabras de control así cifradas son entonces transmitidas por medio de la red local a una o varias otras cajas situadas, por ejemplo, en la proximidad de pantallas de presentación. Estas otras cajas integran cada una un módulo de seguridad, por ejemplo, idéntico al módulo 76 precedentemente descrito de manera que puedan descifrar y obtener sin codificar la palabra de control necesaria para la acción de deshacer el entrelazado de los contenidos multimedia recibidos.

Finalmente, el sistema 2 ha sido descrito en el caso particular en que el procesador 80 es únicamente utilizado para descifrar las palabras de control recibidas. En otra variante, el procesador 80 deshace el entrelazado del contenido multimedia y es el contenido multimedia cuyo entrelazado se ha deshecho el que es transmitido desde el procesador 80 hacia el terminal 10. En esta variante, el cifrado con ayuda de la clave SK_c es aplicado al contenido multimedia transmitido del procesador 80 hacia el terminal 10 y no ya a la palabra de control ya que ésta no es ya transmitida sobre la interfaz entre el terminal 10 y el procesador 80.

REIVINDICACIONES

1. Procedimiento de protección de la transmisión, de un contenido multimedia o de una palabra de control, entre un procesador de seguridad introducido en un terminal de recepción y este terminal de recepción, en el que:

- el procesador de seguridad (146) construye una clave de sesión corriente SK_c por diversificación de una clave raíz SK_root en función de un parámetro P_c transmitido por el terminal,

- el procesador de seguridad descifra (140) el contenido multimedia o la palabra de control y luego cifra (148) el contenido multimedia descifrado o la palabra de control descifrada con la clave de sesión corriente SK_c y, finalmente, transmite (150) al terminal el contenido multimedia o la palabra de control cifrada con la clave de sesión corriente SK_c y

- el terminal (152) descifra el contenido multimedia o la palabra de control cifrada con la clave SK_c construida, con ayuda de un código secreto C_c^{-1} para obtener el contenido multimedia o la palabra de control sin codificar.

caracterizado por que el procedimiento comprende:

- el registro (180) por avance en el terminal de varios códigos secretos C_i^{-1}, permitiendo cada código secreto C_i^{-1} únicamente el descifrado del contenido multimedia o de la palabra de control cifrada por una clave de sesión SK_i respectiva obtenida por diversificación de la clave SK_root con un parámetro P_i, siendo uno de estos parámetros P_i el parámetro P_c,

- la recepción (122) del parámetro P_c por el terminal en un mensaje que contiene igualmente un contenido multimedia o una palabra de control a descifrar por el procesador de seguridad, y

- en respuesta a la recepción del parámetro P_c, la selección (132) por el terminal, entre el conjunto de los códigos secretos registrados, del código secreto C_c^{-1} a utilizar para descifrar el contenido multimedia o la palabra de control cifrada con la clave SK_c en función del parámetro P_c o de otro parámetro contenido en el mismo mensaje.

2. Procedimiento según la reivindicación 1, en el que cada código secreto C_i^{-1} es un código directamente ejecutable o interpretable por el terminal, siendo este código ya parametrizado por su clave de sesión SK_i, de manera que no tenga que ser parametrizado de nuevo por esta clave SK_i durante su ejecución o interpretación.

3. Procedimiento según la reivindicación 1, en el que cada código secreto C_i^{-1} es una clave SK_i o un criptograma de esta clave SK_i que hace posible el descifrado del contenido multimedia o de la palabra de control descifrada con la clave SK_i cuando ésta es utilizada para parametrizar un algoritmo de descifrado registrado previamente en el terminal.

4. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el que el mensaje que contiene el parámetro P_c es un mensaje ECM (Entitlement Control Message).

5. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el que el procesador de seguridad transmite (150) el contenido multimedia o la palabra de control cifrada dos veces, una vez por una clave específica determinada de manera independiente del parámetro P_c y otra vez por una clave de sesión SK_c.

6. Procedimiento según la reivindicación 5, en el que el procesador verifica (144) la presencia del parámetro P_c en el mensaje transmitido y, en caso de ausencia del parámetro P_c, el procesador no cifra (150) el contenido multimedia o la palabra de control con la clave de sesión corriente SK_c.

7. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el que el o los códigos secretos C_c^{-1} son transmitidos al terminal antes de la recepción del mensaje que contiene el parámetro P_c por medio de un mensaje EMM (Entitlement Conteol Message).

8. Procedimiento según una cualquiera de las reivindicaciones precedentes, en el que el procedimiento incluye el registro (180) por avance en el terminal de estrictamente más de dos códigos secretos C_i^{-1}.

9. Procedimiento de descifrado de un contenido multimedia o de una palabra de control por un terminal para la puesta en práctica de un procedimiento conforme a una cualquiera de las reivindicaciones precedentes, incluyendo el procedimiento:

- la transmisión (128) de un parámetro P_c a un procesador de seguridad, introducido en este terminal, apto para descifrar el contenido multimedia o la palabra de control,

- la recepción por el terminal del contenido multimedia o de la palabra de control cifrada, con una clave de sesión corriente SK_c construida por el procesador de seguridad por diversificación de una clave raíz SK_root en función del parámetro P_c transmitido por el terminal,

- el descifrado (152) por el terminal, del contenido multimedia o de la palabra de control cifrada con la clave SK_c con ayuda de un código secreto C_c^{-1} para obtener el contenido multimedia o la palabra de control sin codificar,

caracterizado por que el procedimiento comprende:

- el registro (180) por avance en el terminal de varios códigos secretos C_i^{-1}, permitiendo cada código secreto C_i^{-1} únicamente el descifrado del contenido multimedia o de la palabra de control cifrada por una clave de sesión SK_i respectiva obtenida por diversificación de la clave SK_root con un parámetro P_i, siendo uno de estos parámetros P_i el parámetro P_c,

- la recepción (122) del parámetro P_c por el terminal en un mensaje que contiene igualmente un contenido multimedia o una palabra de control a descifrar por el procesador de seguridad, y

- en respuesta a la recepción del parámetro P_c, la selección (132) por el terminal, entre el conjunto de los códigos secretos registrados, del código secreto C_c^{-1} a utilizar para descifrar el contenido multimedia con la palabra de control cifrada con la clave SK_c en función del parámetro P_c o de otro parámetro contenido en el mismo mensaje.

10. 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 ordenador electrónico.

11. Terminal de descifrado de un contenido multimedia o de una palabra de control cifrada, siendo apto el terminal (10):

- para transmitir un parámetro P_c a un procesador de seguridad, introducido en este terminal, apto para descifrar el contenido multimedia o la palabra de control,

- para recibir el contenido multimedia o la palabra de control cifrada con una clave de sesión corriente SK_c construida por el procesador de seguridad por diversificación de una clave raíz SK_root en función del parámetro P_c transmitido por el terminal,

- para descifrar el contenido multimedia con la palabra de control cifrada con la clave SK_c con ayuda de un código secreto C_c^{-1} para obtener el contenido multimedia o la palabra de control sin codificar,

caracterizado por que:

- el terminal comprende una memoria (82) en la que son registrados previamente varios códigos secretos C_i^{-1}, permitiendo cada código secreto C_i^{-1} únicamente el descifrado del contenido multimedia o de la palabra de control cifrada por una clave de sesión SK_i respectiva obtenida por diversificación de la clave SK_root con un parámetro P_i, siendo uno de estos parámetros P_i el parámetro P_c, y

- el terminal es apto:

  - para recibir el parámetro P_c en un mensaje que contiene igualmente un contenido multimedia o una palabra de control a descifrar por el procesador de seguridad, y

  - para seleccionar, entre el conjunto de los códigos secretos registrados, el código secreto C_c^{-1} a utilizar para descifrar el contenido multimedia o la palabra de control cifrada con la clave SK_c en función del parámetro P_c o de otro parámetro contenido en el mismo mensaje, en respuesta a la recepción del parámetro P_c.

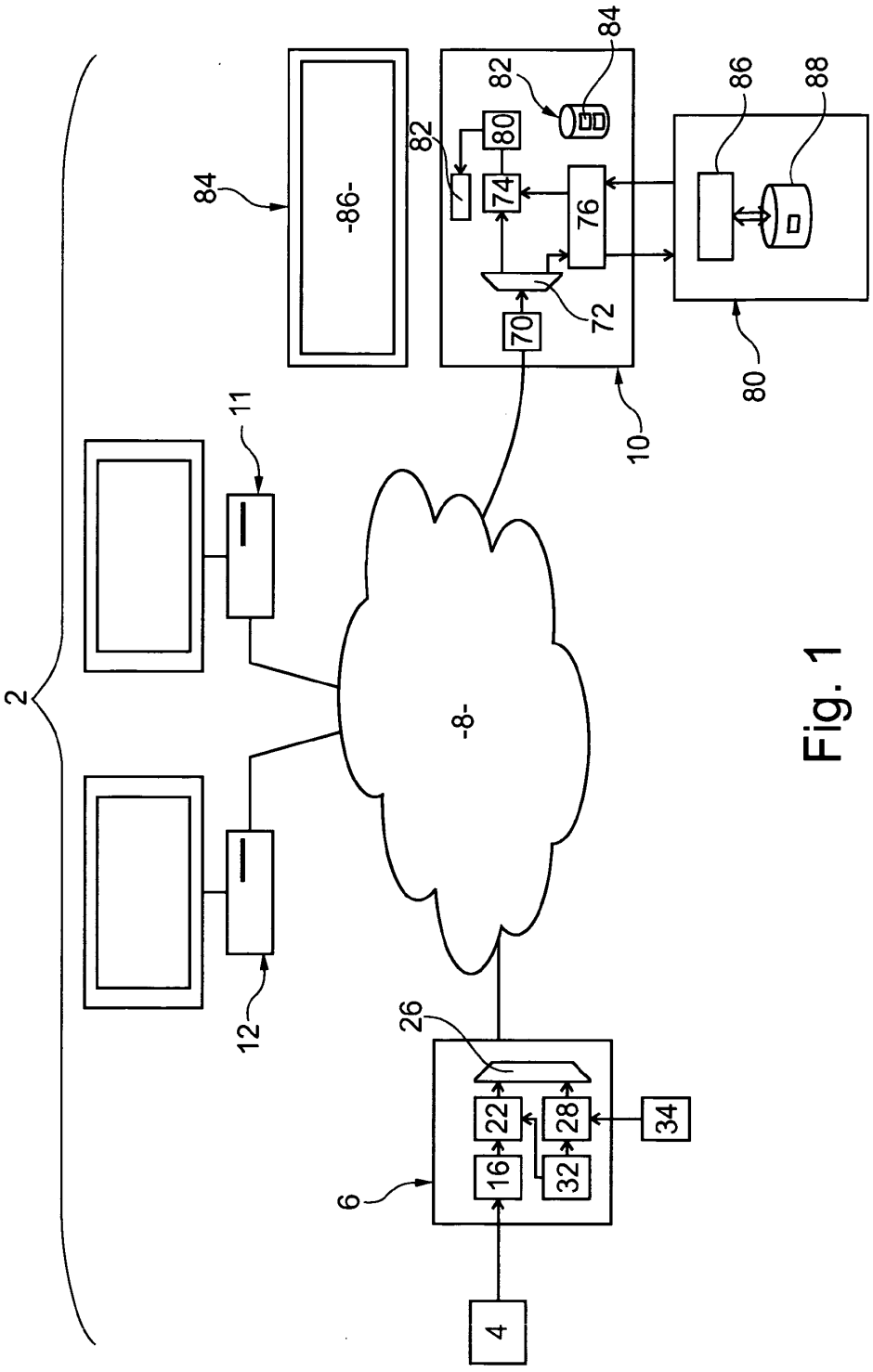

Fig. 1

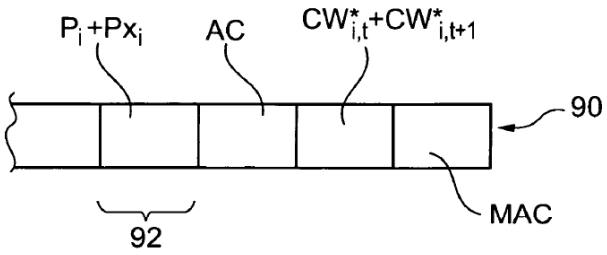

Fig. 2

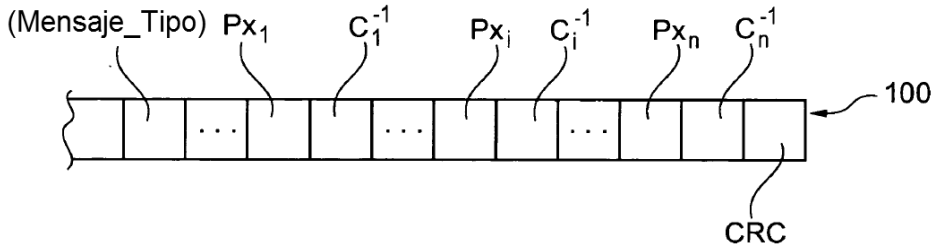

Fig. 3

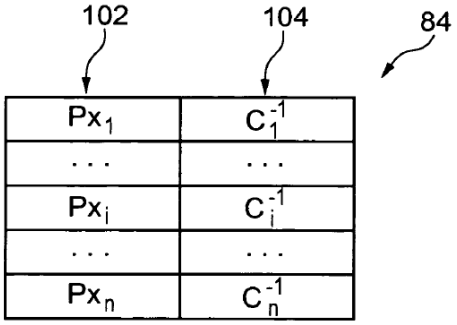

Fig. 4

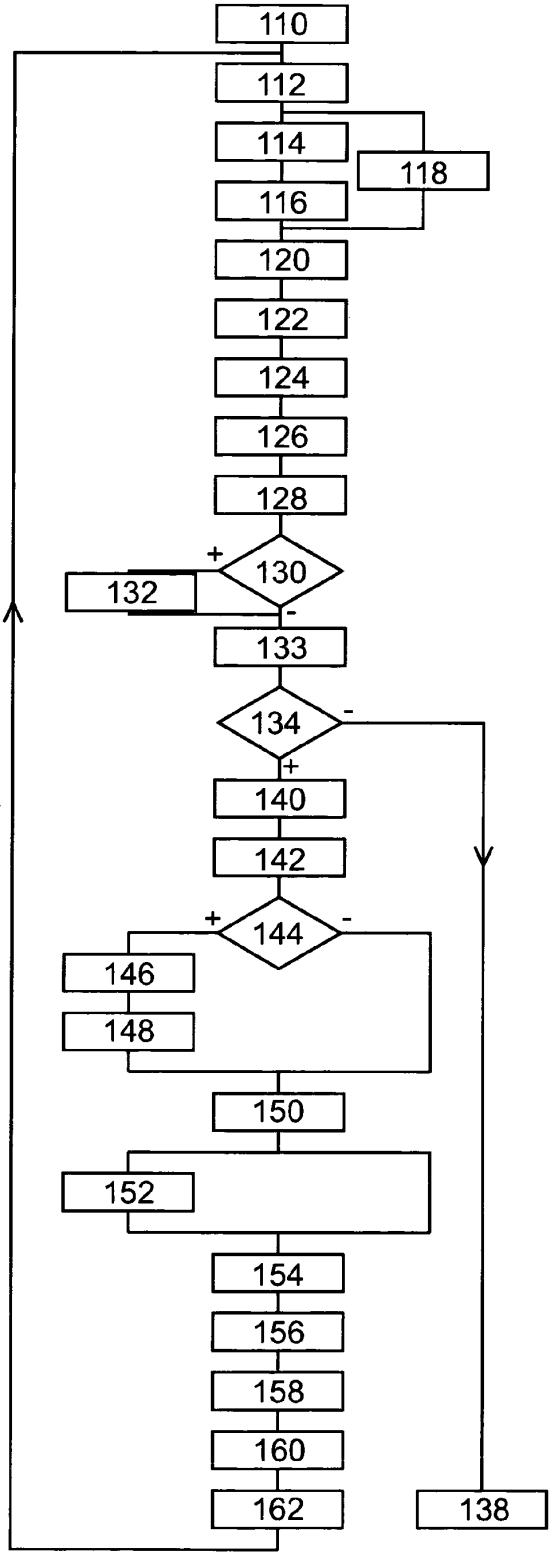
110
112
114
118
116
120
122
124
126
128
+
130
132
-
133
134
-
+
140
142
+
144
-
146
148
150
152
154
156
158
160
162
138

Fig. 5

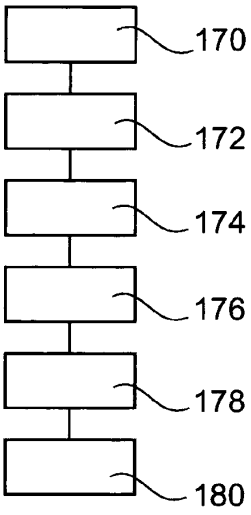
170
172
174
176
178
180

Fig. 6