(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 761 309**

(51) Int. CI.:

H04N 5/00 (2011.01)
H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.07.2011 PCT/EP2011/062689**

(87) Fecha y número de publicación internacional: **26.01.2012 WO12010706**

(96) Fecha de presentación y número de la solicitud europea: **22.07.2011 E 11734159 (4)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 2596623**

(54) Título: **Método para detectar el uso ilegal de un procesador de seguridad**

(30) Prioridad:

23.07.2010 FR 1056031

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.05.2020

(73) Titular/es:

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

(72) Inventor/es:

BOIVIN, MATHIEU y
DUBROEUCQ, GILLES

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método para detectar el uso ilegal de un procesador de seguridad

La invención se refiere a un método para detectar un uso ilegal de un procesador de seguridad utilizado para desencriptar diferentes contenidos multimedia transmitidos en varios canales respectivos. La invención también se refiere a este procesador de seguridad, así como a un soporte de registro de información para poner en práctica este método.

El solicitante conoce métodos para detectar un uso ilegal que comprende:

- la recepción por el procesador electrónico de seguridad de mensajes $ECM_{i,t}$ (Entitlement Control Message, Mensajes de Control de Derecho) para desencriptar una secuencia temporal de criptoperiodos de un canal encriptado i, conteniendo cada mensaje $ECM_{i,t}$ al menos un criptograma de una palabra de control $CW_{i,t}$ para desencriptar un criptoperiodo $CP_{i,t}$ del canal i, identificando el índice i el canal y siendo el índice t un número de orden,

- a cada recepción por el procesador de seguridad de un nuevo mensaje $ECM_{i,c}$, la verificación de que el mensaje $ECM_{i,c}$ se recibe dentro de una ventana temporal predeterminada inmediatamente consecutiva al mensaje anterior $ECM_{i,p}$ recibido por este procesador de seguridad para el canal i, donde los índices c y p son dos valores específicos del número de orden t.

Por "ventana temporal inmediatamente consecutiva al mensaje anterior $ECM_{i,p}$" se entiende una ventana temporal de duración predeterminada que comienza inmediatamente después de recibir el mensaje $ECM_{i,p}$.

Por contenido multimedia se entiende un contenido de audio y/o visual destinado a ser restablecido bajo una forma directamente perceptible y comprensible por un ser humano. Por regla general, un contenido multimedia corresponde a una sucesión de imágenes que forman una película, un programa de televisión o de publicidad. Un contenido multimedia también puede ser un contenido interactivo, tal como un juego.

Es conocido difundir varios contenidos multimedia al mismo tiempo. Para ello, cada contenido multimedia se transmite en su propio canal. El canal utilizado para transmitir contenido multimedia también se conoce bajo el término de "cadena". Un canal suele corresponder a una cadena de televisión. Esto permite al usuario simplemente elegir el contenido multimedia que desea ver cambiando de canal.

Para asegurar y enviar la visualización de contenido multimedia bajo ciertas condiciones, tal como la suscripción de un abonado de pago, por ejemplo, los contenidos multimedia se transmiten de forma encriptada y no de forma abierta. En esta descripción, se dice que el canal está "encriptado" cuando el contenido multimedia transmitido en este canal está encriptado. Más concretamente, cada contenido multimedia se divide en una sucesión de criptoperiodos. Durante toda la duración de un criptoperiodo, las condiciones de acceso al contenido multimedia encriptado permanecen sin cambios. En particular, durante toda la duración de un criptoperiodo, el contenido multimedia está encriptado con la misma palabra de control. En general, la palabra de control varía de un criptoperiodo a otro. Además, la palabra de control suele ser específica para un contenido multimedia, siendo este último obtenido de forma aleatoria o seudoaleatoria. Por lo tanto, si en un momento dado, N contenidos multimedia se transmiten simultáneamente en N canales, existen N palabras de control diferentes e independientes que se utilizan para encriptar uno de estos contenidos multimedia.

En este caso, los términos "encriptar"/"desencriptar" se consideran como sinónimos. Del mismo modo, los términos "cifrar"/"descifrar" se consideran como sinónimos.

El contenido multimedia en abierto corresponde al contenido multimedia antes de ser encriptado. Puede ser entendido directamente por un ser humano sin recurrir a operaciones de desencriptado y sin que su visualización sea sometida a ciertas condiciones.

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

Para asegurar la transmisión de las palabras de control, estas últimas se transmiten a los terminales en forma de criptogramas contenidos en mensajes ECM (Entitlement Control Message).

En este caso se entiende por criptograma una información insuficiente por sí sola para encontrar la palabra de control en abierto. Por lo tanto, si se intercepta la transmisión de la palabra de control, el único conocimiento del criptograma de la palabra de control no permite encontrar la palabra de control para desencriptar el contenido multimedia. Para encontrar la palabra de control en abierto, es decir, la palabra de control para desencriptar directamente contenido

multimedia, este último debe combinarse con una información secreta. A modo de ejemplo, el criptograma de la palabra de control se obtiene cifrando la palabra de control en abierto con una clave criptográfica. En este caso, la información secreta es la clave criptográfica que permite descifrar este criptograma. El criptograma de la palabra de control también puede ser una referencia a una palabra de control almacenada en una tabla que contiene una multitud de posibles palabras de control. En este caso, la información secreta es la tabla que asocia a cada referencia una palabra de control en abierto.

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

Los contenidos multimedia transmitidos en los diferentes canales se pueden coordinar temporalmente entre sí. A modo de ejemplo, los tiempos de transmisión de los contenidos multimedia se configuran para respetar los horarios de transmisión indicados en una programación preestablecida. Cada terminal en un canal dado recibe así sustancialmente el mismo contenido multimedia al mismo tiempo. Se dice que estos contenidos multimedia son transmisiones "en directo" o "linealizadas" porque el usuario no controla su momento de transmisión.

En este contexto, se han desarrollado acciones para permitir a los usuarios desencriptar contenido multimedia para los cuales no han adquirido legalmente derechos de acceso.

Una de estas acciones se conoce bajo el término de "tarjetas compartidas" (card sharing, en inglés). Esta acción consiste en adquirir legalmente un procesador de seguridad para tener los derechos de acceso necesarios para desencriptar varios canales. A continuación, este procesador de seguridad "legal" se introduce en un servidor ‘pirata’ que recibe mensajes ECM desde una multitud de terminales satélites piratas. Por lo tanto, cuando un terminal satélite pirata desea desencriptar ilegalmente un contenido multimedia transmitido, recibe este contenido multimedia y transmite los mensajes ECM correspondientes al servidor pirata. El servidor pirata transmite estos mensajes ECM al procesador de seguridad legal. En respuesta, el procesador de seguridad legal descifra las palabras de control contenidas en estos mensajes de ECM y reenvía las palabras de control abiertas al servidor pirata. El servidor pirata luego transmite entonces estas palabras de control en abierto al terminal satélite pirata que puede entonces desencriptar el contenido multimedia deseado.

En esta acción, el procesador de seguridad se usa normalmente, excepto que procesa los mensajes ECM de una multitud de terminales satélites, mientras que, en una utilización lícita, solamente trata los mensajes ECM de un terminal único. Para detectar esta acción, ya se ha propuesto:

- enumerar los cambios de canal que han ocurrido durante un período de tiempo predeterminado (véase la solicitud de patente EP 1 575 293),

- enumerar el número de canales diferentes desencriptados por el procesador de seguridad durante un período de tiempo predeterminado (véase la solicitud de patente EP 1 447 976), y

- enumerar el número de mensajes ECM recibidos por el procesador de seguridad durante un período predeterminado (véase la solicitud de patente WO 2008 049 882).

Estos métodos de detección aprovechan el hecho de que una acción mediante tarjeta compartida se traduce por:

- un número de cambios de canales anormalmente altos (también conocidos como "zapping"), y/o

- un número de mensajes ECM recibidos anormalmente altos.

La detección de esta acción permite establecer luego contramedidas.

También existen otra acción conocido con la expresión "compartir palabras de control" (“control word sharing” en inglés) que también utiliza un procesador de seguridad legal para desencriptar uno o más canales. En esta acción, el procesador de seguridad legal se introduce en un servidor de palabras de control. Este servidor recibe el contenido multimedia y extrae del mismo los mensajes ECM. Los mensajes ECM extraídos se transmiten al procesador de seguridad legal que luego descifra los criptogramas de las palabras de control y reenvía las palabras de control así descifradas al servidor. El servidor luego transmite estas palabras de control a una gran cantidad de terminales de satélite piratas, lo que les permite desencriptar ilegalmente los contenidos multimedia. A modo de ejemplo, en esta acción, los terminales satélites piratas simplemente se suscriben al flujo de palabras de control en abierto generado por el servidor y correspondiente al canal que desea desencriptar.

Esta última acción difiere de la acción de compartir tarjetas por el hecho de que los terminales satélites piratas no necesitan transmitir al servidor los mensajes ECM del canal que desea desencriptar. Como resultado, la cantidad de mensajes ECM procesados por el procesador de seguridad en esta acción es mucho menor que en una acción de uso compartido de tarjetas. Sin embargo, si para esta acción, se usa el mismo procesador de seguridad para procesar los

mensajes ECM de diferentes canales, esta acción aún puede detectarse utilizando los métodos de detección conocidos presentados con anterioridad.

Más recientemente, las acciones mediante el uso compartido de tarjetas o de palabras de control se han modificado para que sean más difíciles de detectar. La modificación consiste en utilizar no un único procesador de seguridad legal, sino, por ejemplo, tantos procesadores de seguridad legales como canales desencriptados. Cada procesador de seguridad legal se dedica entonces a un canal respectivo, es decir, solamente se usa para procesar los mensajes ECM de ese canal en particular o un número muy limitado de canales. El resto de la acción es idéntico al descrito con anterioridad. En estas condiciones, el procesador de seguridad ya no ve un cambio de canales, lo que hace que los métodos conocidos de detección no funcionen. De la técnica anterior se conoce, asimismo:

- EP1742474A1,

- EP1447976A1, y

- Francis et al: "Contramedidas para la acción sobre tarjetas de TV por satélite usando receptores abiertos", Australasian Information Security Workshop, Digital Rights Management, 6 de noviembre de 2004, páginas 1 a 6.

La invención tiene como objetivo superar esta desventaja al proponer un nuevo método para detectar un uso ilegal de un procesador de seguridad.

Por lo tanto, se refiere a un método de conformidad con la reivindicación 1.

El método anterior permite la detección de acciones mediante el uso compartido de tarjetas o palabras de control en el caso de que cada tarjeta esté dedicada a un número limitado de canales. De hecho, en este caso, el procesador de seguridad procesa, durante largos períodos de tiempo, los mensajes ECM del mismo canal. Esta prolongada falta de cambio de canal se utiliza aquí para detectar el uso ilícito del procesador de seguridad. Más concretamente, esta ausencia prolongada de cambio de canal resulta en el hecho de que el contador Kch_i alcanza el umbral predeterminado lo que inicia la detección de un uso ilícito.

Además, la solidez del método de detección frente a los cambios furtivos de los canales se puede ajustar regulando la duración de la ventana temporal.

Las formas de realización de este método pueden tener una o más de las características de las reivindicaciones dependientes.

Estas formas de realización también tienen las siguientes ventajas:

- la comparación de la diferencia entre etiquetas de tiempo o el intervalo $\Delta V_{c,p}$ en el intervalo ΔT permite evitar que el contador Kch_i se reinicie simplemente en un recorrido de ida y vuelta del canal i a otro canal, lo que permitiría burlar fácilmente el método de detección aquí descrito,

- la enumeración del número de mensajes ECM recibidos entre el mensaje $ECM_{i,p}$ y $ECM_{i,c}$, comparando luego este número con un umbral permite también evitar que el método de detección sea frustrado por un simple recorrido de ida y vuelta desde el canal i hacia otro canal;

- la selección del contador Kch_i que se incrementará de conformidad con un identificador del canal i hace posible poner en práctica el método de detección anterior incluso cuando el procesador de seguridad está destinado a recibir mensajes ECM para desencriptar simultáneamente X canales diferentes;

- la enumeración del número de contadores de Kch_i que han alcanzado o superado su umbral predeterminado y la comparación de este número con el límite P de canales de simultáneamente desencriptables permite detectar con certeza un uso ilegal;

- el bloqueo del desencriptado es la visualización en una pantalla de un mensaje que demanda al usuario que tome una acción específica, lo que hace que la puesta en práctica de acciones mediante usos compartidos de tarjeta o de palabras de control sea más difícil al tiempo que limita las consecuencias negativas para el usuario en caso de detección falsa de un uso ilegal;

- solicitar al usuario que cambie de canal para reestablecer el desencriptado de este último permite restablecer simplemente este desencriptado en caso de detección falsa de uso ilegal mientras hace que las acciones por uso compartido de tarjeta o de palabras de control sean más difíciles.

La invención también se refiere a un soporte de registro de información que comprende instrucciones para ejecutar el método anterior, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

Por último, la invención también se refiere a un procesador electrónico de seguridad según la reivindicación 11.

La invención se entenderá mejor con la lectura de la descripción dada a continuación, solamente a título de ejemplo no limitativo y con referencia a los dibujos en donde:

- la Figura 1 es una ilustración esquemática de un sistema para transmitir y recibir contenidos multimedia encriptados.

- la Figura 2 es una ilustración esquemática de una tabla utilizada en el sistema de la Figura 1, y

- la Figura 3 es un diagrama de flujo de un método para cifrar y descifrar contenido multimedia en donde se puede detectar el uso ilícito del procesador de seguridad utilizando el sistema de la Figura 1.

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

En la siguiente descripción, las características y funciones bien conocidas por los expertos en esta técnica no se describen en detalle. Además, la terminología utilizada es la de los sistemas de acceso condicionales con contenidos multimedia. Para obtener más información sobre esta terminología, el lector puede consultar el siguiente documento:

- "Modelo funcional del sistema de acceso condicional" (Funtional Model of Conditional Access System, en inglés"), EBU Review, Technical European Broadcasting Union, Bruselas, BE, Nº 266, 21 de diciembre de 1995.

La Figura 1 representa un sistema 2 para transmitir y recibir contenidos multimedia encriptados. Los contenidos multimedia transmitidos son contenidos multimedia linealizados. A modo de ejemplo, un contenido multimedia corresponde a una secuencia de un programa audiovisual tal como un programa de televisión o una película.

Los contenidos multimedia en abierto son generados por una o más fuentes 4 y transmitidos a un dispositivo de transmisión 6. El dispositivo 6 transmite los contenidos multimedia simultáneamente a una multitud de terminales de recepción a través de una red de transmisión de información 8. Los contenidos multimedia transmitidos están sincronizados temporalmente entre sí para, por ejemplo, respetar una programación preestablecida.

La red 8 suele ser una red de larga distancia para transmitir información tal como Internet o una red satélite o cualquier otra red de transmisión tal como la utilizada para la transmisión de televisión digital terrestre (TDT).

Para simplificar la Figura 1, solamente se muestran tres terminales de recepción 10 a 12.

El dispositivo 6 incluye un codificador 16 que comprime los contenidos multimedia que recibe. El codificador 16 procesa contenidos multimedia digitales. A modo de ejemplo, este codificador funciona de conformidad con la norma MPEG2 (Moving Picture Expert Group - 2) o ITU-T H264.

Los contenidos multimedia comprimidos se dirigen a una entrada 20 de un encriptador 22. El encriptador 22 encripta cada contenido multimedia comprimido para condicionar su visualización bajo ciertas condiciones, tales como la compra de un título de acceso por parte de los usuarios de los terminales de recepción. Los contenidos multimedia encriptados se reproducen en una salida 24 conectada a la entrada de un multiplexor 26.

El encriptador 22 encripta cada contenido multimedia comprimido utilizando una palabra de control $CW_{i,t}$ que se le suministra, y un sistema 28 de acceso condicional, por un generador 32 de claves. El sistema 28 es mejor conocido por el acrónimo CAS (Sistema de Acceso Condicional, Conditional Access System, en inglés). El índice i es un identificador del canal en donde se transmite el contenido multimedia encriptado y el índice t es un número de orden que identifica el criptoperiodo encriptado con esta palabra de control. En el resto de esta descripción, el criptoperiodo actualmente desencriptado por los terminales es el criptoperiodo t-1.

Por regla general, este encriptado cumple con una norma tal como la norma DVB-CSA (Digital Video Broadcasting - Common Scrambling Algorithm), ISMA Cryp (Internet Streaming Media Alliance Cryp), SRTP, Protocolo de Transporte Seguro en Tiempo Real (Secure Real-time Transport Protocol, en inglés), AES (Estándar de Encriptación Avanzado – Advanced Encryption Standard, en inglés), ... etc.

Para cada canal i, el sistema 28 genera mensajes $ECM_{i,t}$ (Entitlement Control Message) que contiene al menos el criptograma $CW^*_{i,t}$ de la palabra de control $CW_{i,t}$ generado por el generador 32 y utilizado por el encriptador 22 para encriptar el criptoperiodo t del canal i. Estos mensajes y los contenidos multimedia encriptados son multiplexados por el multiplexor 26, siendo estos últimos proporcionados respectivamente por el sistema de acceso condicional 28 y por el encriptador 22, antes de ser transmitidos en la red 8.

El sistema 28 inserta también 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 desencriptar los criptoperiodos inmediatamente consecutivos t y t_{+1} del canal i,

- las etiquetas de tiempo TS_t y TS_{t+1}, o "timestamp" en inglés, que identifican los tiempos en los que deben reproducirse los criptoperiodos t y t+1,

- las condiciones de acceso de CA destinadas a compararse con los títulos de acceso adquiridos por el usuario, y

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

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

- el índice i identifica el canal, y

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

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

Las etiquetas de tiempo se definen con respecto a un origen absoluto independiente del contenido multimedia transmitido y del canal en donde se transmite el contenido multimedia.

Se inserta el mismo identificador i en todos los mensajes $ECM_{i,t}$ que contiene un criptograma $CW^*_{i,t}$ para desencriptar los contenidos multimedia transmitidos en este canal i. A modo de ilustración, en este caso, el encriptado y la multiplexación de los contenidos multimedia está de conformidad con el protocolo DVB-Simulcrypt (ETSI TS 103 197). En este caso, el identificador i puede corresponder a un par de "ID de canal/ID de flujo" único en donde se envían todas las solicitudes de generación de mensajes ECM para este canal.

Cada mensaje $ECM_{i,t}$ comprende un par $CW^*_{i,t}/CW^*_{i,t+1}$ de criptogramas de palabras de control. Después del descifrado, este par $CW^*_{i,t}/CW^*_{i,t+1}$ de criptogramas hace posible obtener un par $CW_{i,t}/CW_{i,t+1}$ de palabras de control. El criptograma $CW^*_{i,t+1}$ contenido en el mensaje $ECM_{i,t}$ se usa en este caso como dato cronológico para identificar el mensaje $ECM_{i,t+1}$ inmediatamente consecutivo al mensaje $ECM_{i,t}$. De hecho, por ejemplo, después del descifrado de estos criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$, es posible comparar la palabra de control $CW_{i,t+1}$ con la primera palabra de control del par de palabras de control contenido en el mensaje $ECM_{i,t+1}$. En caso de correspondencia, ello significa que el mensaje $ECM_{i,t+1}$ es de hecho el mensaje que sigue inmediatamente al mensaje $ECM_{i,t}$. También es posible comparar la palabra de control $CW_{i,t}$ contenida en el mensaje $ECM_{i,t}$ con la segunda palabra de control del par contenido en el mensaje $ECM_{i,t-1}$. En caso de correspondencia, ello establece que el mensaje $ECM_{i,t-1}$ es en realidad el mensaje que precede inmediatamente al mensaje $ECM_{i,t}$.

A modo de ejemplo, los terminales 10 a 12 son idénticos y solamente el terminal 10 se describe con más detalle.

El terminal 10 se describe aquí en el caso particular en donde este último es capaz de desencriptar simultáneamente dos canales i, j diferentes. Para este propósito, el terminal 10 tiene dos líneas 60 y 62 de desencriptado para desencriptar de forma simultánea, respectivamente, los canales i, j. A modo de ejemplo, la línea 60 desencripta el canal i para mostrarlo en un visor 84 mientras que, en paralelo, la línea 62 desencripta el canal j para registrarlo con una ayuda de un registrador 64.

A modo de ejemplo, estas líneas 60 y 62 son idénticas y solamente la línea 60 se describirá ahora en detalle.

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

El desencriptador 74 desencripta el contenido multimedia encriptado a partir de la palabra de control transmitida por el procesador 76. El contenido multimedia desencriptado se transmite a un decodificador 80 que lo decodifica. El contenido multimedia descomprimido o decodificado se transmite a una tarjeta gráfica 82 que controla la visualización de este contenido multimedia en la pantalla 86 del visor 84.

El visor 84 muestra, sin codificar, el contenido multimedia en la pantalla 86.

El procesador 76 procesa información confidencial tal como claves criptográficas. Para preservar la confidencialidad de esta información, está diseñado para ser lo más sólido posible contra las acciones pirata. Por lo tanto, es más

sólido frente a estas acciones que los otros componentes del terminal 10. A modo de ejemplo, para este propósito, el procesador 76 es una tarjeta inteligente.

En esta forma de realización, el procesador 76 es común a las líneas 60 y 62.

A modo de ejemplo, el procesador 76 se pone en práctica usando un ordenador electrónico programable 77 capaz de ejecutar instrucciones grabadas en un soporte de registro de información. Para este propósito, el procesador 76 está conectado a una memoria 78 que contiene las instrucciones necesarias para la ejecución del método de la Figura3.

La memoria 78 también contiene:

- una tabla local 79 para el análisis de cambios de canal,
- un valor inicial Y para contadores de Kch_i,
- un número X cuyo valor indica el número máximo de canales supervisados de manera simultánea,
- un límite P de canales simultáneamente desencriptables utilizando el mismo procesador 76,
- un intervalo de tiempo ΔT, y
- un umbral ΔE correspondiente a varios mensajes ECM.

Por regla general, los valores de X, P, ΔT, ΔE e Y se configuran de una vez por todas en fábrica durante la fabricación del procesador 76 o se pueden configurar después de que el procesador 76 se ponga en servicio en el terminal 10 por intermedio de un mensaje EMM específico transmitido desde el dispositivo 6.

La Figura 2 representa esquemáticamente un ejemplo de estructura de la tabla 79. Esta tabla comprende cinco columnas y X líneas. Los tres pequeños puntos indicados en cada una de las columnas significan que los datos en esta tabla 79 no han sido representados.

Desde la primera columna hasta la quinta columna, estas columnas contienen, respectivamente:

- el identificador i del canal supervisado,
- el valor del contador Kch_i
- el valor de un contador $Kecm_i$,
- el valor de la palabra de control anterior recibida LCW_i en el canal i por el procesador 76, y
- el valor de la etiqueta de tiempo LTS_i contenida en el mensaje anterior $ECM_{i,p}$ recibido para el canal i.

En el resto de la descripción, los valores "p" y "c" del índice t corresponden a los números de orden, respectivamente, del mensaje ECM anterior y nuevo recibido para el mismo canal i.

El funcionamiento del sistema 2 se describirá a continuación con más detalle con respecto al método de la Figura 3.

Inicialmente, durante una etapa 120, el dispositivo 6 difunde varios contenidos multimedia diferentes de manera simultánea en diferentes canales. En cada canal, el criptoperiodo t y el criptoperiodo inmediatamente siguiente t+1 se encriptan con las palabras de control, respectivamente, $CW_{i,t}$ y $CW_{i,t+1}$. Los mensajes $ECM_{i,t}$ y $ECM_{i,t+1}$ que contienen los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ de las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$ se multiplexan con los contenidos multimedia transmitidos. Esta multiplexación permite sincronizar la difusión de las palabras de control con la difusión de los contenidos multimedia. En este caso, los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ se transmiten a los terminales durante el criptoperiodo t-1 que precede al criptoperiodo t.

Por regla general, cada mensaje $ECM_{i,t}$ se repite varias veces dentro de un mismo criptoperiodo. A modo de ejemplo, los mensajes $ECM_{i,t}$ se repiten cada 0,1 segundos a 0,5 segundos. La duración de un criptoperiodo es superior a cinco segundos y preferiblemente, comprendida entre 5 segundos y 10 minutos. En este caso, la duración de un criptoperiodo es de 10 segundos.

Los contenidos multimedia encriptados se reciben prácticamente al mismo tiempo por cada uno de los terminales 10 a 12. Por lo tanto, las siguientes etapas se realizan prácticamente en paralelo para cada uno de estos terminales. Se describen en el caso particular del terminal 10.

Del mismo modo, las operaciones realizadas en paralelo por las líneas 60 y 62 son similares. En este caso solamente se describen en el caso particular de la línea 60.

Durante una etapa 122, los contenidos multimedia encriptados y el mensaje $ECM_{i,t}$ se reciben por el receptor 70.

A continuación, durante una etapa 124, el demultiplexor 72 extrae el contenido multimedia encriptado correspondiente al canal i cuyo desencriptado es solicitado actualmente por el usuario. En la etapa 124, el demultiplexor 72 también extrae solamente los mensajes $ECM_{i,t}$ asociados con el canal i. El demultiplexor 72 transmite el contenido multimedia extraído hacia el desencriptador 74. El mensaje $ECM_{i,t}$ extraído se transmite a su vez al procesador 76. Este mensaje $ECM_{i,t}$ es el nuevo mensaje ECM recibido para el canal i y, por lo tanto, se indica $ECM_{i,c}$ de ahora en adelante.

Durante una etapa 126, el procesador 76 compara las condiciones de acceso CA contenidas en el mensaje $ECM_{i,c}$ con los títulos de acceso pregrabados en la memoria 78.

Si las credenciales de acceso del usuario no corresponden a las condiciones de acceso CA, entonces, durante una etapa 128, el procesador 76 inhibe el desencriptado del canal i por el terminal 10. A modo de ejemplo, a este efecto, el procesador 76 no transmite ninguna palabra de control al desencriptador 74.

En el caso en que los títulos de acceso corresponden a las condiciones de acceso CA, durante una etapa 132, el procesador 76 descifra los criptogramas $CW^*_{i,c}$ y $CW^*_{i,c+1}$ utilizando una clave operativa almacenada en la memoria 78. Por lo general, esta clave operativa se renueva una vez al mes.

A continuación, durante una etapa 134, el procesador 76 disminuye un contador Nb-ECM en un paso predeterminado. A modo de ejemplo, el paso predeterminado es igual a 1.

Durante una etapa 136, el procesador verifica si el contador Nb-ECM ha alcanzado un umbral predeterminado S_0. A modo de ejemplo, en este caso, el valor de este umbral S_0 es igual a 0.

En caso afirmativo, procede a una etapa 138 de salvaguardar la tabla 79 en una memoria no volátil del procesador 76. Además, durante esta etapa 138, el procesador reinicializa el contador Nb-ECM a un valor inicial V_{save}. A modo de ejemplo, el valor V_{save} es igual a 200.

En caso de fallo de suministro de energía o de reinicialización del procesador 76, la tabla 79 se precarga con los valores de esta tabla almacenados en la memoria no volátil. Por lo tanto, un fallo del suministro de energía o una reinicialización del procesador 76 no permite restablecer a sus valores iniciales los diversos datos contenidos en la tabla 79.

Después de la etapa 138, o directamente después de la etapa 136, si el valor del contador Nb-ECM no ha alcanzado el umbral S_0, el procesador 76 incrementa, durante una etapa 140, todos los contadores $Kecm_i$ cuyos valores se registran en la tabla 79 en un paso predeterminado. A modo de ejemplo, el paso predeterminado es igual a 1.

Durante una etapa 142, el procesador verifica si el canal, para el que se recibe el mensaje $ECM_{i,c}$, es un canal supervisado. Un canal supervisado es un canal cuyo identificador i está contenido en la primera columna de la tabla 79. Para este propósito, el procesador extrae el identificador i del canal contenido en el mensaje $ECM_{i,c}$ recibido y luego compara este identificador i con los contenidos en la primera columna de la tabla 79.

Si ninguno de los identificadores contenidos en la tabla 79 corresponde al identificador i, entonces, durante una etapa 143, el procesador 76 busca en esta tabla una línea para la que al menos se satisface una de las siguientes condiciones:

1) TS_i-LTS_i>ΔT, o

2) $Kecm_i$>Δ E.

Si una de las líneas de la tabla 79 cumple una de las condiciones 1) o 2), ello significa que el procesador 76 no ha recibido, desde hace mucho tiempo, un mensaje ECM para el canal correspondiente a esta línea. Por lo tanto, el procesador 76 ya no se utiliza para desencriptar el canal correspondiente a esta línea. Durante una etapa 144, esta línea se libera para ser utilizada para supervisar el canal i. Para ello, las celdas de esta línea se completan de la siguiente manera:

- el identificador i está registrado en la primera columna,
- el valor del contador Kch_i se restablece, es decir, se considera igual a Y,
- el valor del contador $Kecm_i$ se restablece, es decir, se considera igual a cero,

- la palabra de control $CW_{i,c+1}$ se registra como la palabra de control anterior recibida LCW_i,

- la etiqueta de tiempo TS_i se almacena como la etiqueta de tiempo recibida LTS_i anterior.

Al final de la etapa 144, el método retorna a la etapa 122 para procesar un nuevo ECM recibido.

En el caso de que el canal i ya esté supervisado, el procesador 76 selecciona la línea correspondiente en la tabla 79 y pasa a una etapa 150 en donde verifica que el mensaje $ECM_{i,c}$ se recibe dentro de una ventana temporal FT inmediatamente consecutiva al mensaje anterior $ECM_{i,p}$ recibido para este canal i. La duración de la ventana temporal FT es mayor o igual que la duración de un criptoperiodo. En este caso, la duración de la ventana FT es igual al máximo entre la duración D_{CP} de un criptoperiodo, la duración del intervalo ΔT y la duración $\Delta E*D_{CP}/P$.

En este caso, la etapa 150 comienza con una operación 152 en la que el procesador 76 verifica si el mensaje $ECM_{i,c}$ es inmediatamente consecutivo al mensaje anterior $ECM_{i,p}$. Para este propósito, compara la última palabra de control LCW_i, recibida cuyo valor se registra en la cuarta columna de la tabla 79, con la palabra de control $CW_{i,c}$ contenida en el mensaje $ECM_{i,c}$.

En el caso en que las palabras de control LCW_i y $CW_{i,c}$ sean iguales, el procesador 76 pasa directamente a una etapa 153. Durante la etapa 153, el contador Kch_i se reduce en un paso predeterminado, por ejemplo, igual a 1. Durante esta etapa, en la tabla 79, los valores de la palabra de control LCW_i y de la etiqueta LTS_i se modifican para que sean iguales, respectivamente, a la palabra de control $CW_{i,c+1}$ y a TS_c. Por último, solamente el valor del contador $Kecm_i$ se reinicializa a cero.

En el caso donde las palabras de control LCW_i y $CW_{i,c}$ son diferentes, durante una operación 154, la diferencia entre la etiqueta de tiempo TS_c contenida en el mensaje $ECM_{i,c}$ y la etiqueta de tiempo LTS_i contenía en la tabla 79 se compara con el intervalo ΔT. Si esta diferencia es menor que el intervalo ΔT, entonces el mensaje $ECM_{i,c}$ se recibe dentro de la ventana FT y el procesador 76 pasa directamente a la etapa 153.

De lo contrario, realiza una operación 156 en la que compara el valor del contador $Kecm_i$ asociado con el canal i en la tabla 79 en el umbral ΔE. En el caso en que el valor de este contador $Kecm_i$ sea menor que umbral ΔE, el nuevo mensaje $ECM_{i,c}$ se recibe dentro de la ventana FT. Por lo tanto, el método continúa con la etapa 153. El número de mensajes $ECM_{j,c}$ procesados por el procesador 76 para otros canales es representativo de un tiempo transcurrido desde la recepción del mensaje $ECM_{i,p}$.

En el caso contrario, se considera que el mensaje $ECM_{i,c}$ no se recibe dentro de la ventana FT. Esto significa que el procesador 76 no se usa exclusivamente para desencriptar el canal i. A continuación, se pasa a una etapa 158. Durante la etapa 158, los contadores Kch_i y $Kecm_i$ se reinicializan a sus valores iniciales. Más concretamente, los valores de los contadores Kch_i y $Kecm_i$ se reinicializan, respectivamente, al valor Y y cero. Además, durante la etapa 158, la palabra de control $CW_{i,c+1}$ se almacena en la tabla 79 como la última palabra de control recibida LCW_i. El valor LTS_i se considera igual a la etiqueta TS_c.

Las operaciones 154 y 156 hacen posible evitar un cambio furtivo de canal que conduce a una reinicialización del contador Kch_i. Un cambio de canal furtivo es un breve desplazamiento de ida y vuelta hacia otro canal. Este desplazamiento de ida y vuelta es lo suficientemente breve como para no provocar una interrupción del desencriptado del canal y responsable para su visualización. En ausencia de las operaciones 154 y 156, este cambio furtivo restablecería sistemáticamente el contador Kch_i lo que podría usarse para frustrar el método de detectar un uso incorrecto del procesador 76 aquí descrito.

Al final de la etapa 153 o 158, el procesador, durante una etapa 160, enumera el número de contador Kch_i igual a cero y registra el resultado en una variable Z.

Durante una etapa 162, el procesador verifica si la variable Z es estrictamente mayor que cero.

En caso afirmativo, ello significa que se ha detectado el uso ilegal del procesador 76. En este caso, el procesador 76 pasa a una etapa 164 en donde activa automáticamente una contramedida para combatir este uso ilegal. En este caso, la contramedida aplicada se elige en función del valor de la variable Z. Por lo general, cuanto mayor es el valor de la variable Z, más fuerte es la contramedida aplicada, es decir, más problemática para el usuario.

A continuación, se dan ejemplos de contramedidas en orden de fuerza creciente:

1) Suspensión del desencriptado del canal o de todos los canales por un tiempo predeterminado seguido de la reanudación automática del desencriptado de estos canales una vez que haya transcurrido este tiempo predeterminado.

2) Suspensión del desencriptado de este canal y visualización simultánea en la pantalla de un mensaje que solicita al usuario cambiar de canal antes de regresar al canal i para permitir, de nuevo, el desencriptado del canal i. En este

caso, el desencriptado se permite de nuevo solamente después de que el usuario haya cambiado del canal i a otro canal.

3) Suspensión del procesamiento de los mensajes de ECM que evita así el desencriptado de los canales hasta que el procesador 6 no se haya reiniciado, por ejemplo, cortando la alimentación del terminal.

4) Prevenir el desencriptado de los canales hasta que un valor almacenado en la memoria no volátil del procesador 76 se haya reiniciado usando un mensaje EMM. Dicha contramedida puede obligar al usuario a contactar con el operador para hacer que el envío del mensaje EMM desbloquee el procesador 76.

5) Bloqueo definitivo del procesador 76 que impida permanentemente el uso de este procesador.

Durante la etapa 164, el valor de la variable Z se compara de manera preferible con el límite P que indica el número de canales simultáneamente desencriptables utilizando el procesador 76. Si la variable Z es estrictamente mayor que el límite P, ello indica, de manera cierta, que este procesador 76 se está utilizando ilegalmente. En este caso, se aplica una contramedida fuerte como las contramedidas 5) o 6) indicadas con anterioridad.

Si el valor de la variable Z es nula o después de la etapa 164, el método vuelve a la etapa 122 para procesar un nuevo mensaje ECM.

En este caso, el valor inicial Y del contador de Kch_i, el paso de decremento y el umbral a alcanzar para activar la detección de un uso incorrecto del procesador 76, se eligen para que este umbral se alcance solamente después de al menos 3 horas y, preferiblemente, después de al menos 12 horas o tres días sin cambio de canal. A modo de ejemplo, aquí el valor Y es igual a 432000.

El intervalo ΔT es mayor que el doble de la diferencia entre las etiquetas de tiempo de dos mensajes ECM sucesivos. A modo de ejemplo, el intervalo ΔT es al menos igual a dos minutos.

El umbral ΔE es al menos mayor que dos y preferiblemente mayor que tres o seis.

Son posibles muchas otras formas de realización. A modo de ejemplo, los diferentes contadores aquí descritos pueden incrementarse en un paso predeterminado en lugar de reducirse.

El paso de incremento o de decremento puede ser negativo. Por lo tanto, en esta descripción, decrementar un contador se considera exactamente igual que incrementar un contador en un paso negativo.

Las líneas 60, 62 pueden ser independientes entre sí tal como se describe con referencia a la Figura 1 o compartir recursos comunes. Por regla general, el uso compartido de recursos comunes se realiza multiplexando temporalmente su uso. El recurso común puede ser el receptor, el demultiplexor o el desencriptador.

En una variante, el procesador de seguridad o el terminal está equipado con un reloj que mide el intervalo de tiempo transcurrido entre los tiempos de recepción de los mensajes $ECM_{i,c}$ y $ECM_{i,p}$. A continuación, es este intervalo el que se utiliza en lugar de la diferencia entre las etiquetas $TS_{i,c}$ y $TS_{i,p}$. En esta variante, ΔT es mayor que el doble del intervalo entre los instantes de recepción de dos mensajes ECM inmediatamente consecutivos.

Se pueden omitir una o dos de las operaciones 152, 154 y 156. En particular, se pueden omitir las diferentes etapas aquí descritas para evitar una reinicialización del contador de Kch_i en caso de cambio furtivo de canal.

El desencriptado de varios canales al mismo tiempo usando el mismo procesador de seguridad también se puede usar en otros contextos. A modo de ejemplo, este es el caso cuando es posible mostrar simultáneamente múltiples canales en la misma pantalla. Esta posibilidad se conoce, por ejemplo, bajo el término inglés de "picture in picture".

Las contramedidas se pueden aplicar solamente a los canales para los cuales el contador de Kch_i ha alcanzado el umbral de detección de un uso ilícito. Como variante, cada contramedida se aplica a todos los canales.

Por último, son posibles otros mecanismos para verificar que el mensaje $ECM_{i,c}$ se recibe dentro de una ventana que sigue inmediatamente al mensaje $ECM_{i,p}$. A modo de ejemplo, de manera alternativa, cada mensaje ECM incluye, además, un número de orden que identifica su posición con respecto a otros mensajes ECM transmitidos para el mismo canal. En este caso, la recepción del mensaje $ECM_{i,c}$ dentro de la ventana FT se verifica, por ejemplo, comparando la diferencia entre los números de orden de los mensajes $ECM_{i,c}$y $ECM_{i,p}$ con un umbral predeterminado. En particular, la continuidad entre el mensaje $ECM_{i,c}$ y el mensaje $ECM_{i,p}$ se controla verificando que su número de orden respectivo sea en realidad inmediatamente consecutivo. En esta variante, no es necesario que cada mensaje ECM incluya, a la vez, las dos palabras de control $CW_{i,t}$ y $CW_{i,t+1}$.

En esta variante, el número de orden se considera una etiqueta de tiempo, ya que constituye una medida, en número de criptoperiodos, del número de criptoperiodos transcurridos desde un origen común a todos los canales.

Preferiblemente, la duración de la ventana temporal es estrictamente mayor que la duración de un criptoperiodo.

REIVINDICACIONES

1. Un método para detectar un uso ilegal de un procesador de seguridad utilizado para el desencriptado de diferentes contenidos multimedia transmitidos por varios canales respectivos, comprendiendo dicho método:

- la recepción (122) por el procesador electrónico de seguridad de mensajes $ECM_{i,t}$ (Entitlement Control Message) para desencriptar una secuencia temporal de criptoperiodos de un canal encriptado i, conteniendo cada mensaje $ECM_{i,t}$:

  - al menos un criptograma de una palabra de control $CW_{i,t}$ para desencriptar un criptoperiodo $CP_{i,t}$ del canal i, identificando el índice i el canal y siendo el índice t un número de orden, y

  - el identificador del canal i,

caracterizado porque el método también comprende:

- en cada recepción por el procesador de seguridad de un nuevo mensaje $ECM_{i,c}$, la verificación (150) de que el mensaje $ECM_{i,c}$ se recibe dentro de una ventana temporal predeterminada inmediatamente consecutiva al mensaje anterior $ECM_{i,p}$ recibido por este procesador de seguridad para el canal i, donde los índices c y p son dos valores específicos del número de orden t,

- el incremento (153) de un contador de Kch_i en un paso predeterminado cada vez que, después de la verificación, el mensaje $ECM_{i,c}$ se recibe dentro de la ventana temporal inmediatamente consecutiva al mensaje $ECM_{i,p}$ y, en caso contrario, la reinicialización (158) del contador Kch_i a su valor inicial,

- la detección (162) de un uso ilegal tan pronto como el contador de Kch_i alcance un umbral predeterminado.

2. El método según la reivindicación 1, en donde cada mensaje $ECM_{i,t}$ recibido también incluye datos cronológicos para identificar el mensaje $ECM_{i,t\ -1}$ inmediatamente anterior o el mensaje $ECM_{i,t+1}$ inmediatamente siguiente, y el método incluye la verificación (150) de que el mensaje $ECM_{i,c}$ se recibe dentro de la ventana temporal comprobando (152) que el nuevo mensaje $ECM_{i,c}$ recibido es el mensaje que sigue inmediatamente al mensaje anterior $ECM_{i,p}$ a partir del datos cronológico contenido en el mensaje $ECM_{i,c}$ o $ECM_{i,p}$.

3. El método según la reivindicación 1 o 2, en donde el método incluye la verificación (150) de que el mensaje $ECM_{i,c}$ se recibe dentro de la ventana temporal comprobando (154) que la diferencia entre las etiquetas de tiempo TS_c y TS_p incluidas, respectivamente, en los mensajes $ECM_{i,c}$ y $ECM_{i,p}$ es menor que un intervalo de tiempo predeterminado ΔT mayor que dos veces el intervalo de tiempo entre las etiquetas de tiempo del mensaje $ECM_{i,t}$ y $ECM_{i,t+1}$ inmediatamente consecutivos.

4. Un método según una cualquiera de las reivindicaciones anteriores, en donde el método comprende:

- la medida de un intervalo $\Delta V_{c,p}$ de tiempo entre instantes de recepción de los mensajes $ECM_{i,c}$y $ECM_{i,p}$, y

- la verificación de que el mensaje $ECM_{i,c}$ se recibe dentro de la ventana temporal al verificar que el intervalo $\Delta V_{c,p}$ medido es menor o igual a un intervalo predeterminado ΔT mayor que dos veces un intervalo $\Delta V_{t,t+1}$ de tiempo medible entre instantes de recepción de mensajes $ECM_{i,t}$ y $ECM_{i,t+1}$ inmediatamente consecutivos.

5. Un método según una cualquiera de las reivindicaciones anteriores, en donde el método comprende:

- la enumeración (140, 153, 158) de los nuevos mensajes $ECM_{j,c}$ recibidos por este procesador de seguridad para canales distintos al canal i desde el último mensaje $ECM_{i,p}$, recibido, y

- la verificación (150) de que el mensaje $ECM_{i,c}$ se recibe dentro de la ventana temporal comprobando (156) que el número de mensajes nuevos $ECM_{j,c}$ recibidos para canales distintos al canal i alcanza o supera un umbral predeterminado mayor que dos.

6. Un método según una cualquiera de las reivindicaciones anteriores, en donde el método comprende la selección (150) del contador Kch_i para incrementar entre X posibles contadores Kch_j, donde X es un número entero mayor o igual a dos, en función de un identificador del canal i contenido en el mensaje $ECM_{i,c}$.

7. El método según la reivindicación 6 en donde el método comprende:

- la enumeración (162) de los canales asociados con un contador Kch_i que ha alcanzado o ha superado sus respectivos umbrales predeterminados,

- la comparación (164) del número Z del contador Kch_i que ha alcanzado o ha superado sus respectivos umbrales predeterminados con un límite predeterminado P igual al número máximo de canales simultáneamente desencriptables con la ayuda de este procesador de seguridad, y

- si el número Z alcanza o supera el límite P, entonces la activación automática de una contramedida fuerte y, en caso contrario, la activación de otra contramedida más débil.

8. Un método según cualquiera de las reivindicaciones anteriores, en donde, en respuesta a la detección de un uso ilegal, el método incluye la activación automática (164) de una contramedida que consiste en impedir el desencriptado del canal i y en mostrar en una pantalla un mensaje que demanda al usuario que inicie una acción específica para reestablecer el desencriptado del canal i.

9. El método según la reivindicación 8, en donde la acción específica es un cambio de canal.

10. Soporte (78) de registro de información, caracterizado porque comprende instrucciones para la ejecución de un método de conformidad con una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

11. Un procesador electrónico de seguridad (76) para un terminal utilizado para el desencriptado de diferentes contenidos multimedia transmitidos por varios canales respectivos, pudiendo este procesador:

- recibir mensajes $ECM_{i,t}$ (Entitlement Control Message) para desencriptar una sucesión temporal de criptoperiodos de un canal encriptado i, conteniendo cada mensaje $ECM_{i,t}$:

  - al menos un criptograma de una palabra de control $CW_{i,t}$ para desencriptar un criptoperiodo $CP_{i,t}$ del canal i, identificando el índice i el canal y siendo el índice t un número de orden, y

  - el identificador del canal i,

caracterizado porque el procesador también es capaz de:

- verificar, a cada recepción de un nuevo mensaje $ECM_{i,c}$, que este mensaje $ECM_{i,c}$ se recibe dentro de una ventana temporal predeterminada inmediatamente consecutiva al mensaje anterior $ECM_{i,p}$ recibido por este procesador de seguridad para el canal i, donde los índices c y p son dos valores específicos del número de orden t,

- incrementar un contador de Kch_i en un paso predeterminado cada vez que, después de la verificación, se recibe el mensaje $ECM_{i,c}$ dentro de la ventana temporal inmediatamente consecutiva al mensaje $ECM_{i,p}$ y, en caso contrario, reinicializar el contador de Kch_i a su valor inicial,

- detectar un uso ilegal tan pronto como el contador Kch_i alcance un umbral predeterminado.

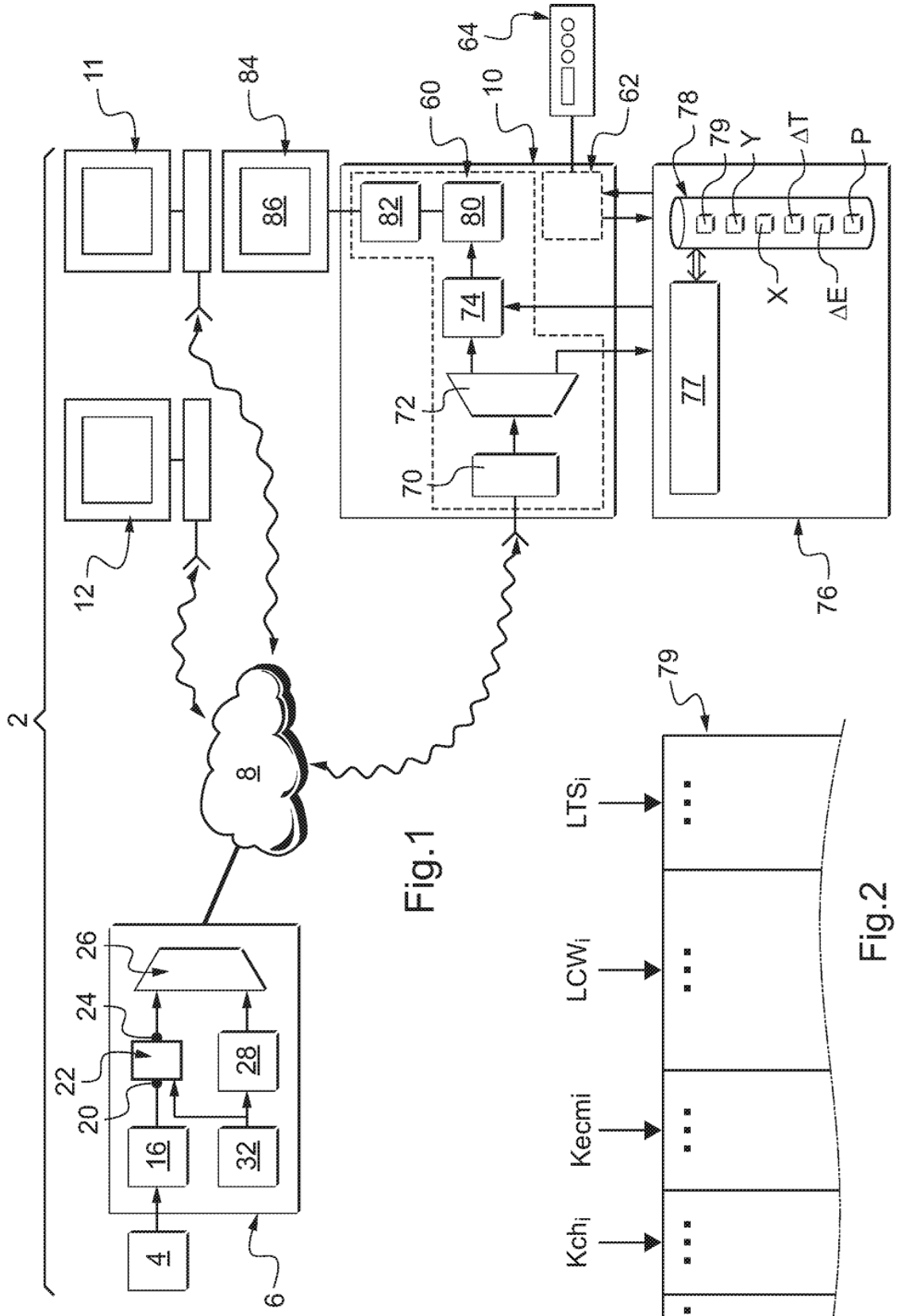
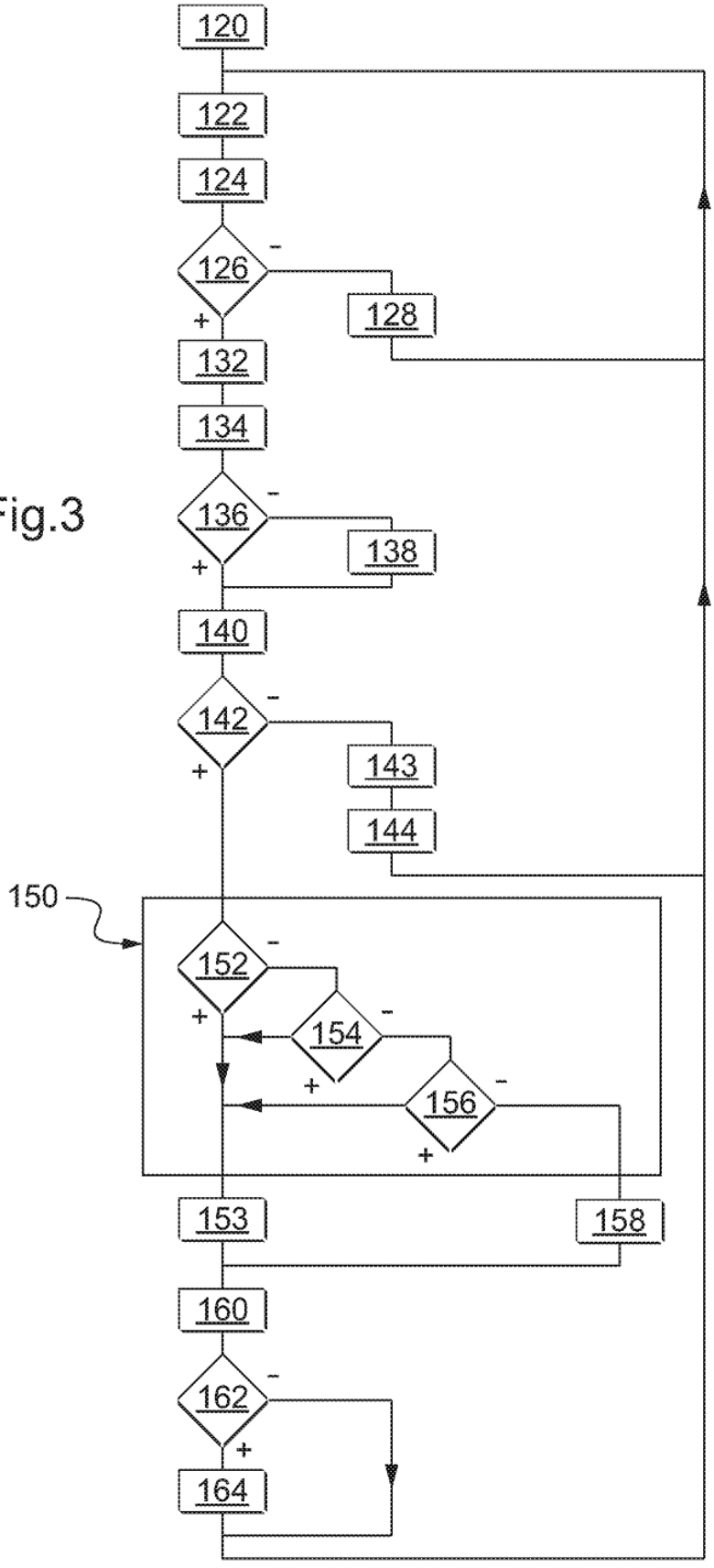

2
11
84
86
12
8
60
10
64
62
82
80
74
72
70
78
79
Y
ΔT
P
X
ΔE
77
76
26
24
22
20
16
28
32
4
6

Fig.1

79
LTSi
LCWi
Kecmi
Kchi
i

Fig.2

Fig.3


120
122
124
126
-
128
+
132
134
136
-
138
+
140
142
-
143
+
144
150
152
-
+
154
-
+
156
-
+
153
158
160
162
-
+
164