(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 959**

(51) Int. CI.:

H04N 21/266 (2011.01)
H04H 60/14 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.05.2009 E 09753766 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.11.2015 EP 2297950**

(54) Título: **Procedimientos y emisores por ráfagas de un contenido multimedia cifrado, soporte de almacenamiento para estos procedimientos**

(30) Prioridad:

30.05.2008 FR 0802970

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.02.2016

(73) Titular/es:

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

(72) Inventor/es:

CHEVALLIER, ANTHONY y
ROQUE, PIERRE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimientos y emisores por ráfagas de un contenido multimedia cifrado, soporte de almacenamiento para estos procedimientos

El invento se refiere a procedimientos y emisores por ráfagas de un contenido multimedia cifrado así como un soporte de almacenamiento de informaciones para la puesta en práctica de estos procedimientos.

La solicitante conoce procedimientos de emisión por ráfagas de un contenido multimedia cifrado que comprende:

a) la elección de una duración T cualquiera para criptoperíodos sucesivos,

b) la sustitución, por un sincronizador, de una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} a cada final de criptoperíodo,

c) el cifrado de segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo,

d) la construcción, por un generador, de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción de segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i.

Las ráfagas son más conocidas bajo el término inglés de « burst ».

El contenido multimedia es un contenido que contiene audio y/o video. Por ejemplo, un contenido multimedia puede ser una película, un programa audiovisual, una cadena de televisión, música u otros. Un contenido multimedia es igualmente denominado a veces « servicio ». El contenido multimedia está destinado a ser reproducido por un receptor a medida que es recibido.

La duración de reproducción de un segmento del contenido es la duración necesaria en la reproducción, a velocidad normal, del segmento considerado sobre un receptor.

Aquí los términos « cifrar » y « codificar » son considerados como intercambiables.

La emisión por ráfagas de contenidos multimedia cifrados está por ejemplo descrita en la norma DVB-H (Digital Video Broadcast-Handheld) o similares. El lector podrá referirse a esta norma para más detalles sobre la concepción y emisión de ráfagas.

La emisión por ráfagas de contenidos multimedia cifrados ha sido definida para permitir a un receptor móvil ahorrar energía después de la recepción de estos contenidos multimedia. El receptor móvil es por ejemplo un teléfono móvil, un asistente personal PDA (Asistente Personal Digital), un receptor portátil de televisión, un lector de medios portátil (o PMP, para Reproductor Portátil de Medios) o aún un ordenador portátil.

En estos procedimientos de emisión, el contenido multimedia está dividido en una sucesión de segmentos P_i inmediatamente consecutivos, donde el índice i indica el número de orden de un segmento particular en esta sucesión. Un segmento corresponde con la fracción del contenido multimedia incorporado y transmitido por una sola ráfaga. Así, una ráfaga contiene un solo y único segmento P_i. La ráfaga que contiene el segmento P_i es denominada S_i.

Cada segmento es comprimido y cifrado antes de ser transmitido en una ráfaga. Esta compresión del segmento permite obtener una ráfaga cuya duración de recepción es más corta que la duración de la reproducción del segmento P_i.

En la práctica, varios contenidos multimedia son emitidos de manera simultánea. A este efecto, las ráfagas correspondientes a estos diferentes contenidos multimedia son multiplexadas temporalmente. Por ejemplo, ventanas temporales a intervalos regulares son asignadas a las ráfagas de un contenido multimedia específico. Estas ventanas temporales asignadas a un contenido multimedia específico definen un canal.

El receptor de estas ráfagas no trata más que un solo canal a la vez. Así, entre dos ráfagas consecutivas de este canal, el receptor puede quedar inactivo, lo que permite ahorrar energía.

La gestión de las claves de cifrado para asegurar la transmisión de este contenido multimedia es realizada por un sistema de gestión de claves o « Key Management System », en inglés, que recoge del sistema de protección de contenidos empleado. Por ejemplo, la descripción es hecha aquí con referencia al sistema de gestión de claves del sistema de protección de contenido definido en la norma « OMA-BCAST Smartcard Profile » (Open Mobile Alliance-Broadcast Services Enabler Suite Smartcard Profile). Así, en esta descripción, la terminología utilizada es la definida en esta norma.

En un sistema conforme a la norma OMA-BCAST Smartcard Profile, una clave TEK_j (Traffic Encryption Key ("Clave de Cifrado de Tráfico")) actual es utilizada para cifrar segmentos actualmente emitidos del contenido multimedia. La clave TEK_j es cambiada a intervalos de tiempo regulares. Estos intervalos son conocidos bajo el término de « criptoperíodo ». Por ejemplo, un criptoperíodo dura menos de un minuto. Típicamente un criptoperíodo dura entre 5 y 20 segundos. Aquí, cada criptoperíodo es denominado T_j, donde j es un número de orden del criptoperíodo. Durante el criptoperíodo T_j solo la clave TEK_j es utilizada para cifrar el contenido multimedia. A continuación, durante el criptoperíodo T_{j+1} inmediatamente consecutivo, solo la clave TEK_{j+1} es utilizada para cifrar el contenido multimedia y así sucesivamente.

Al menos un mensaje $STKM_j$ (Short Time Key Message ("Mensaje de Clave a Corto Plazo")) es incluido en cada ráfaga para que sea posible descifrar el segmento P_i contenido en esta ráfaga. Cada mensaje $STKM_j$ contiene un criptograma de la clave TEK_j. EN la norma OMA-BCAST Smartcard Profile, un mensaje STKM sólo puede contener un criptograma de una clave TEK. Un mensaje STKM contiene igualmente a menudo condiciones de acceso al contenido multimedia destinadas a ser comparadas con títulos de acceso previamente almacenados en una memoria del receptor con el fin de autorizar y, alternativamente, prohibir el descifrado del contenido multimedia.

Cuando un receptor móvil recibe una ráfaga, debe descifrar el criptograma de la clave TEK_j contenida en el mensaje $STKM_j$ antes de poder descifrar el segmento Pi contenido en esta ráfaga. El descifrado del criptograma de la clave TEK_j lleva algún tiempo denominado T_{SKTM}. Así, cuando un usuario cambia de canal, es decir cuando "zapea" o cuando acaba de encender su receptor, el descifrado del segmento Pi encapsulado en la primera ráfaga S_i recibida puede comenzar lo antes posible T_{STKM} después del comienzo de la recepción de esta ráfaga.

Además, puede ocurrir otro problema después de un cambio de canal. Para explicar esto, se ha hecho referencia a las figs. 1 y 2. La fig. 1 representa una sucesión de segmentos P_i inmediatamente consecutivos de un contenido multimedia reproducido a velocidad normal. Cada segmento P_i comienza en un instante t_{di}. Este instante t_{di} está indicado sobre un eje de tiempo 2.

Un segundo eje de tiempo 4 representa los cripto-periodos sobre la misma escala. Aquí dos cripto-periodos T_j y T_{j+1} están representados. Durante el cripto-periodo T_j, los segmentos son cifrados con la ayuda de la clave TEK_j. Este cripto-periodo T_j se acaba en el momento en el que comienza el cripto-periodo siguiente T_{j+1}, es decir en un instante t_{ej+1}. Durante el cripto-periodo T_{j+1}, la clave utilizada para cifrar los segmentos del contenido multimedia es la clave TEK_{j+1}.

En el caso particular representado en la fig. 1, el cambio de criptoperíodo interviene entre los instantes t_{di} y $t_{di}+T_{STKM}$. En estas condiciones, el comienzo del segmento Pi es en primer lugar cifrado con la clave TEK_j hasta el instante t_{ej+1}. Luego, el final de este segmento es cifrado con la clave TEK_{j+1}. La ráfaga S_i que contiene el segmento P_i debe por tanto contener las dos claves TEK_j y TEK_{j+1} para permitir el descifrado del segmento P_i. A este efecto, para estar conforme con la norma OMA-BCAST Smartcard Profile, esta ráfaga S_i contiene dos mensajes $STKM_j$ y $STKM_{j+1}$ que contienen respectivamente los criptogramas de las claves TEK_j y TEK_{j+1}.

Supongamos ahora que un usuario acaba justo de cambiar de canal y de zapear sobre el canal correspondiente a la ráfaga S_i de manera que el receptor no tiene todavía ninguna información sobre este canal. En estas condiciones, el receptor espera la recepción de la primera ráfaga completa sobre este canal. Suponemos que esta primera ráfaga es la ráfaga S_i que contiene el segmento P_i. La ráfaga S_i es recibida en el instante t_{Si} representado sobre un eje de tiempo 6 de la fig. 2.

Una vez que la ráfaga S_i es recibida, el receptor descifra el criptograma de la clave TEK_j lo que requiere un tiempo T_{STKM}. Por lo tanto, antes del instante t_{Si} +T_{STKM}, el receptor no puede reproducir en claro el contenido multimedia recibido. Esto corresponde a un periodo de tiempo 8 en la fig. 2. Por ejemplo, durante este periodo 8, el receptor presenta únicamente una pantalla negra o no deja oír ningún sonido.

Por reproducción « en claro », se designa la reproducción del contenido multimedia después de que éste haya sido descifrado. Así, el contenido multimedia en claro corresponde con imágenes o sonidos directamente perceptibles y comprensibles por el usuario del receptor.

A partir del instante $t_{si}+T_{STKM}$, el receptor comienza a presentar en claro el comienzo del segmento P_i.

Del instante $t_{si}+T_{STKM}$, a un instante $t_{Si}+T_{STKM} + t_{ej+1} - t_{di}$, el comienzo del segmento P_i es presentado en claro. Este periodo lleva la referencia 10 en la fig. 2.

Además, en paralelo y a partir del instante $t_{si}+T_{STKM}$, el receptor descifra el criptograma de la clave TEK_{j+1}. Por consiguiente, la presentación en claro del final del segmento P_i no puede comenzar, lo más pronto posible, más que a partir del instante $t_{Si} + 2T_{STKM}$.

Ahora bien aquí, el instante $t_{Si} + T_{STKM} + t_{ej+1} - t_{di}$ es anterior al instante $t_{Si} + 2T_{STKM}$. Por lo tanto, la clave TEK_{j+1} no está todavía disponible al final de la presentación del comienzo del segmento P_i. En estas condiciones, el receptor presenta de nuevo una pantalla negra hasta el instante $t_{Si} + 2T_{STKM}$. Este segundo período de presentación de una

pantalla negra lleva la referencia 12 en la fig. 2.

A partir del instante $t_{Si} + 2T_{STKM}$, el receptor presenta en claro el final del segmento P_i (período 14).

La aparición de una pantalla negra durante el periodo 12 después de un período de presentación en claro del contenido multimedia es un fenómeno desagradable para el usuario.

Desde luego, una solución para evitar este fenómeno sería esperar el instante $t_{Si} + 2T_{STKM}$ antes de comenzar a presentar el segmento P_i en claro. Sin embargo, esta solución prolonga de manera inaceptable el tiempo necesario para la presentación del contenido multimedia en claro después de un cambio de canal.

El invento pretende remediar este inconveniente proponiendo un procedimiento de emisión por ráfagas de un contenido multimedia en el cual se elimina la aparición de una pantalla negra durante el periodo 12.

Tiene por tanto como objeto un procedimiento de emisión por ráfagas de un contenido multimedia cifrado en el que la sustitución de la clave actual TEK_j por la clave actual TEK_{j+1} para cifrar el segmento P_i es retardada hasta después de un instante $t_{di} + T_{STKM}$ o avanzada al instante t_{di} o antes del mismo en respuesta a una señal de sincronización intercambiada entre el generador y el sincronizador, siendo la duración T_{STKM} superior o igual al tiempo necesario para que un receptor descifre el criptograma de una clave actual contenida en la ráfaga S_i y estrictamente inferior a la duración T elegida.

En el procedimiento anterior, la sustitución de la clave TEK_j por la clave TEK_{j+1} es retardada o avanzada de manera que evite que el final del criptoperíodo caiga entre los instantes t_{di} y $t_{di} + T_{STKM}$. Dicho de otra manera, la duración T del criptoperíodo T_i es alargada o acortada dinámicamente en el curso del cifrado del contenido multimedia para que el instante t_{ej+1} no caiga en el intervalo $]t_{di} ; t_{di} + T_{STKM}[$ de un segmento P_i. A partir de entonces, la situación descrita con respecto a las figs. 1 y 2 no puede producirse, lo que evita la aparición de una pantalla negra durante el periodo 12. Además, este procedimiento permite resolver el problema sea cual sea la duración T elegida. En particular, no es necesario elegir la duración T como un múltiplo entero de la duración mínima de reproducción T_B de los segmentos P_i.

Los modos de realización de este procedimiento pueden presentar una o varias de las características siguientes:

- el procedimiento comprende:
  - antes del cifrado de un nuevo segmento P_i, la comparación de un instante actual t_C establecido a partir de la señal de sincronización, en un instante teórico tt_{ej+1} de final del criptoperíodo actual calculable a partir de un instante t_{ej} y de la duración T elegida, siendo el instante t_{ej} el instante de comienzo del criptoperíodo actual, y
  - si el instante t_C es anterior al instante tt_{ej+1}, el cifrado de la totalidad del segmento P_i con la clave actual TEK_j incluso si el final del criptoperíodo T_j cae durante este segmento P_i, y
  - si el instante t_C es posterior al instante tt_{ej+1}, el cifrado de la totalidad del segmento P_i con la nueva clave actual TEK_{j+1};
- el procedimiento comprende:
  - antes del cifrado de un nuevo segmento P_i en el curso del cual sobreviene un instante tt_{ej+1} de final del criptoperíodo actual calculable a partir de un instante t_{ej} de comienzo del criptoperíodo actual y de la duración T elegida, la comparación del instante tt_{ej+1} en un intervalo $]t_{di} ; t_{di} + T_{STKM}[$ establecido a partir de la señal de sincronización, y
  - únicamente si el instante tt_{ej+1} está comprendido en el intervalo $]t_{di} ; t_{di} + T_{STKM}[$, la sustitución (140, 142) de la clave actual TEK_j por la clave actual TEK_{j+1} para cifrar el segmento P_i es retardada hasta después de un instante $t_{di} + T_{STKM}$ o se adelantada al instante t_{di} o a antes del mismo.

Estos modos de realización presentan además las ventajas siguientes:

- comparar los instantes t_C y tt_{ej+1} facilita la implementación del procedimiento ya que no es entonces necesario estimar el instante t_{di+1} de comienzo del segmento P_{i+1};
- provocar la sustitución de la clave TEK_j por la clave TEK_{j+1} únicamente si el instante tt_{ej+1} está fuera del intervalo $]t_{di+1} ; t_{di+1} + T_{STKM}[$ permite resolver el problema permitiendo sustituciones de claves en el curso de un segmento.

El invento tiene igualmente por objeto otro procedimiento de emisión por ráfagas de un contenido multimedia cifrado que comprende:

a) la elección de una duración T para criptoperíodos sucesivos,

b) la sustitución inmediata de una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} en cada final de criptoperíodo,

c) el cifrado de segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo y que tiene una duración de reproducción mínima constante T_B,

d) la construcción de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i, en el que la duración de reproducción de cada segmento es superior o igual a una duración mínima T_B común a todos los segmentos.

Además, en este procedimiento, la duración T es elegida para verificar las condiciones siguientes:

- $T/T_B = r/q$, donde r y q son números enteros naturales no nulos y primos entre ellos, y

- $1/q \geq T_{STKM}/T_B$ donde la duración T_{STKM} es superior a igual al tiempo necesario para que un receptor descifre el criptograma de una clave actual contenida en la ráfaga S_i y estrictamente inferior a la duración T elegida.

En el procedimiento anterior, la duración T inicialmente elegida no es cualquiera. Al contrario, está duración T es elegida como un número racional r/q que verifica las dos condiciones enunciadas antes. Cuando T verifica estas dos condiciones, ello garantiza que el instante t_{ej+1} no caerá jamás en el intervalo $]t_{di} ; t_{di} + T_{STKM}[$. Por tanto, en el procedimiento anterior, la duración T es constante y no es necesaria prolongarla o reducirla dinámicamente para evitar que un instante t_{ej+1} caiga en el intervalo $]t_{di} ; t_{di} + T_{STKM}[$. Al contrario, la libertad en la elección de la duración T es restringida.

Los modos de realización de este procedimiento pueden presentar las características siguientes:

- la duración de reproducción de cada segmento P_i es igual a la duración T_B.

Estos modos de realización facilitan la implementación del procedimiento.

El invento tiene igualmente por objeto un soporte de almacenamiento de informaciones que contiene instrucciones para la ejecución de uno de los procedimientos anteriores cuando estas instrucciones son ejecutadas por un calculador electrónico.

El invento tiene igualmente por objeto un emisor por ráfagas de un contenido multimedia cifrado que comprende:

a) una memoria en la cual se almacena una duración T para criptoperíodos,

b) un sincronizador apto para sustituir una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} a cada final de criptoperíodo,

c) un codificador apto para cifrar los segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo,

d) un generador de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i.

Además, el generador y el sincronizador son aptos para intercambiar una señal de sincronización para retardar la sustitución de la clave actual TEK_j por la clave actual TEK_{j+1} justo después del instante $t_{di} + T_{STKM}$ o para adelantar esta sustitución al instante t_{di} o antes del mismo.

Finalmente, el invento tiene igualmente por objeto otro emisor por ráfagas de un contenido multimedia cifrado que comprende:

a) una memoria en la cual se almacena una duración T para criptoperíodos sucesivos,

b) un sincronizador rapto para sustituir inmediatamente una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} a cada final de criptoperíodo,

c) un codificador apto para cifrar los segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo y teniendo una duración de reproducción superior o igual a una duración mínima T_B común a todos los segmentos,

d) un generador de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción

del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i.

Además, en este emisor la duración T elegida contenida en la memoria verifica las condiciones siguientes:

- $T/T_B = r/q$, donde r y q son números enteros naturales no nulos y primos entre ellos, y

- $1/q \geq T_{STKM}/T_B$

Los modos de realización de este emisor pueden incluir la siguiente característica:

- el emisor es apto para limitar la elección de la duración T a una duración T que satisfaga las dos condiciones.

El invento será mejor comprendido con la lectura de la descripción que sigue, dada únicamente a título de ejemplo no limitativo y hecha con referencia a los dibujos en los cuales:

La fig. 1 es una ilustración esquemática, por cronogramas, de una sincronización particular entre segmentos P_i y un cambio de criptoperíodo,

La fig. 2 es un cronograma que ilustra esquemáticamente un problema del estado de la técnica,

La fig. 3 es una ilustración esquemática de la arquitectura de un sistema de transmisión de contenidos multimedia cifrados con la ayuda de un emisor por ráfagas,

La fig. 4 es un organigrama de un procedimiento de emisión por ráfagas de un contenido multimedia con la ayuda del emisor de la fig. 3,

La fig. 5 es un cronograma que ilustra la sincronización de los segmentos Pi con los cambios de criptoperíodos obtenida con la ayuda del procedimiento de la fig. 4,

Las figs. 6 y 7 son organigramas de otros modos de realización de procedimientos de emisión por ráfagas de un contenido multimedia cifrado.

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

En la siguiente descripción, las características y funciones bien conocidas por el experto en la técnica no son descritas en detalle.

La fig. 3 representa un sistema 20 de transmisión por ráfagas de contenidos multimedia. Este sistema 20 comprende un emisor 22 por ráfagas de un contenido multimedia hacia los receptores móviles. Para simplificar la ilustración, sólo han sido representados tres receptores móviles 24 a 26. Los receptores móviles 24 a 26 son conectados al emisor 22 por medio de una red 28 de transmisión de informaciones. Los receptores 24 a 26 son conectados a esta red 28 por medio de uniones inalámbricas respectivamente 30 a 32 de manera que permitan una movilidad.

Cada receptor 24 a 26 está equipado de una pantalla 34 y de al menos un altavoz 36 de manera que pueda presentar de forma perceptible y comprensible el contenido multimedia recibido. Por ejemplo, los receptores 24 a 26 son teléfonos móviles.

Por ejemplo, la red 28 es una red de telefonía móvil.

El emisor 22 comprende un puerto 40 por medio del cual se recibe el contenido multimedia en claro destinado a ser emitido en forma cifrada. Este puerto 40 está conectado a la entrada de un módulo 42 de compresión del contenido multimedia. Una salida del módulo 42 está conectada a una entrada de un codificador 44 apropiada para cifrar el contenido multimedia comprimido. A este efecto, el codificador 44 utiliza una clave actual TEK_j contenida en una memoria 46. Una salida del codificador 44 está conectada a una entrada de un generador 48 de ráfagas. Este generador 48 comprende igualmente una memoria tampón 49 en la cual es almacenado un segmento P_i del contenido multimedia cifrado así como otras informaciones diferentes a trasmitir en forma de una sola ráfaga. Las demás informaciones incorporadas en una ráfaga comprenden particularmente al menos un mensaje $STKM_j$ y eventualmente otras informaciones como identificadores de ráfagas, de canales y otros. Una salida del generador 48 está conectada a una entrada de un difusor 50 apropiado para difundir sobre la red 28 las ráfagas generadas por el generador 48.

El emisor 22 comprende igualmente un generador 52 de claves apropiado para generar una nueva clave TEK_j para cada nuevo criptoperíodo. Una salida de este generador 52 está conectada a una entrada de un sincronizador 54 y a una entrada de un constructor 56 de mensajes $SKTM_j$. El constructor 56 es apto para construir el mensaje $SKTM_j$ que contiene un criptograma de la clave TEK_j. Una salida del constructor 56 es conectada a una entrada del sincronizador 54.

El sincronizador 54 es apto para sustituir la clave TEK_j actualmente almacenada en la memoria 46 por una nueva clave TEK_{j+1} en el momento oportuno.

El sincronizador 54 es igualmente apto para comunicar, al generador 48, el mensaje $STKM_j$ correspondiente a la clave TEK_j actualmente utilizada por el codificador 44 para cifrar el segmento actual del contenido multimedia.

En este modo de realización, el generador 48 es igualmente apto para enviar una señal de sincronización al sincronizador 54. Por ejemplo, está señal de sincronización indica al sincronizador el final de la preparación de una ráfaga y el comienzo de la preparación de las ráfaga siguiente.

Por ejemplo, el emisor 22 está realizado a partir de uno o varios calculadores electrónicos programables apropiados para ejecutar instrucciones almacenadas en un soporte de almacenamiento de informaciones. Por ejemplo, el sincronizador 54 y el generador 48 están realizados a partir de calculadores electrónicos respectivos apropiados para ejecutar en paralelo. A este efecto, aquí, el emisor 22 está conectado a una memoria 60 que contiene instrucciones y las informaciones necesarias para la ejecución de al menos uno de los procedimientos de emisión descritos con referencia a las figs. 4, 7 y 8.

El funcionamiento del emisor 22 va a ser descrito a continuación más en detalle con la ayuda del procedimiento de la fig. 4 y del cronograma de la fig. 5.

Inicialmente, antes de cualquier emisión de un contenido multimedia, durante una operación 80, la duración T de los criptoperíodos es elegida y luego, por ejemplo, almacenada en la memoria 60. En este primer modo de realización la duración T elegida puede ser cualquiera. Dicho de otra manera, no existe restricción sobre la elección de esta duración T salvo la de que no debe ser superior a T_{STKM}.

A continuación, durante la emisión de un contenido multimedia cifrado, durante una operación 82, el generador 48 envía una señal de sincronización al sincronizador 54 para indicarle que va a comenzar pronto a preparar una nueva ráfaga. Por ejemplo, generador 48 envía esta señal cuando ha terminado de generar la ráfaga precedente y antes de generar la ráfaga siguiente.

Después, durante una operación 86, la próxima ráfaga a difundir es preparada. Por ejemplo, durante una operación 88, el módulo 42 comprime el segmento actual P_i del contenido multimedia después de que el codificador 44 cifra este segmento comprimido utilizando a este efecto la clave actualmente almacenada en su memoria 46. A medida que este segmento es cifrado, es almacenado en la memoria tampón 49.

A continuación, durante una operación 90, cuando la cantidad de informaciones almacenadas en la memoria 49 excede de un umbral predefinido, generador 48 comienza la construcción de la ráfaga S_i que contiene el segmento P_i. En particular, durante la operación 90, el generador 48 asocia en una sola y misma ráfaga:

- el segmento P_i comprimido y cifrado,

- un identificador de ráfaga,

- un mensaje $STKM_j$ si el segmento P_i ha sido únicamente cifrado con la ayuda de la clave TEK_j o dos mensajes $STKM_j$ y $STKM_{j+1}$ si el segmento P_i ha sido cifrado con la ayuda sucesivamente, de la clave TEK_j y de la clave TEK_{j+1}.

Una vez terminada la preparación de la ráfaga S_i, ésta es transmitida al difusor 50 que, durante una operación 92, la difunde hacia el conjunto de receptores conectados al emisor 22 por medio de la red 28.

A continuación, las operaciones 82 a 92 son reiteradas en bucle para cada segmento P_i del contenido multimedia a difundir.

En paralelo a las operaciones 82 a 92, el sincronizador 54 genera el cambio de criptoperíodo. Por ejemplo, a cada comienzo de criptoperíodo T_j, durante una operación 100, el sincronizador 54 almacena el instante t_{ej} de comienzo de este criptoperíodo.

A continuación, durante una operación 102, el generador 52 genera la clave TEK_{j+1} que debe ser utilizada durante el próximo criptoperíodo T_{j+1}. Durante la operación 102, una vez generada la clave TEK_{j+1}, el constructor 56 construye inmediatamente el mensaje $STKM_{j+1}$ que contiene un criptograma TEK_{j+1}* de la clave TEK_{j+1}. La clave TEK_{j+1} y el mensaje de $STKM_j$ son transmitidos al sincronizador 54.

A continuación, el generador 48 envía la señal de sincronización al sincronizador 54. En respuesta, el sincronizador 54 procede inmediatamente a una operación 104 de cálculo de una desviación Δt. La desviación Δt es calculada con la ayuda de la relación siguiente:

$$\Delta t = t_C - t_{ej},$$

donde el instante t_C es el instante actual del contenido, es decir la duración de reproducción acumulada de los segmentos o partes de segmentos del contenido ya cifrado, en el momento en que el sincronizador 54 recibe la señal de sincronización enviada por el generador 48.

A continuación, durante una operación 106, el sincronizador 54 compara la desviación Δt con la duración T elegida de los criptoperíodos. Esta operación es un modo particular de realización de una comparación entre el instante actual t_C y un instante teórico tt_{ej+1} de final del criptoperíodo actual T_j calculable a partir de un instante t_{ej} de comienzo del criptoperíodo T_j y de la duración T elegida.

Si la desviación Δt es estrictamente inferior a la duración T, ello significa que el final del criptoperíodo no ha sido aún alcanzado. En este caso, durante una operación 108, el sincronizador 54 inhibe cualquier sustitución de la clave TEK_j almacenada en la memoria 46 hasta la próxima indicación del generador 48 según la cual la preparación de una nueva ráfaga va a comenzar en breve. Procediendo así, el sincronizador 54 impide cualquier sustitución de la clave almacenada en la memoria 46 en el curso del cifrado de un segmento. Así, el sincronizador 54 garantiza que no puede producirse ningún cambio de clave TEK_j en el curso del cifrado de un segmento P_i. Ello puede por tanto conducir a prolongar la duración del criptoperíodo T_j si fuera necesario.

Después de la operación 108, el procedimiento vuelve a la espera de un nuevo mensaje de sincronización de la parte del generador 48.

En el caso contrario, es decir si la desviación Δt es superior o igual a la duración T, ello significa que el criptoperíodo T_j se acaba o que ya se ha acabado. En este caso, durante una operación 110, el sincronizador 54 sustituye en la memoria 46 la clave TEK_j por la clave TEK_{j+1} antes del comienzo del cifrado del segmento P_{i+1}. Durante la operación 110, el sincronizador 54 trasmite igualmente el mensaje $STKM_{j+1}$ al generador 48.

A continuación, durante una operación 112, el sincronizador 54 inhibe cualquier cambio nuevo de la clave almacenada en la memoria 46 hasta la siguiente señal de sincronización. Después de la operación 112, el procedimiento vuelve a la operación 100 de manera que memorice el instante t_{ej+1} en el que el sincronizador 54 ha procedido a la sustitución de la clave en la memoria 46 como un nuevo instante de comienzo del criptoperíodo T_{j+1} actual.

El cronograma de la fig. 5 permite comprender más en detalle el comportamiento y las consecuencias del procedimiento de la fig. 4. La fig. 5 representa un eje de tiempo 120 sobre el cual se han representado los instantes t_{di} de comienzo de cada uno de los segmentos P_i. En un contenido reproducido a velocidad normal sobre un receptor, los segmentos P_i son inmediatamente consecutivos de manera que el instante de final de la reproducción de un segmento corresponde al instante de comienzo de la reproducción del segmento siguiente. Se observará que esto no es necesariamente el caso del lado del emisor, de manera que los cifrados de segmentos consecutivos pueden ser separados por un intervalo de tiempo suficientemente largo, por ejemplo, para permitir la sustitución de la clave de cifrado en la memoria 46. El codificador 44 puede igualmente ser capaz, al menos durante un cierto tiempo, de cifrar en paralelo dos canales de contenido multimedia con, respectivamente, las claves TEK_j y TEK_{j+1}. En este caso, la sustitución de la clave actual es realizada enviando sobre estos dos canales el mismo contenido multimedia, y luego basculando de un canal al otro para pasar instantáneamente del criptoperíodo T_j al criptoperíodo T_{j+1} sin interrumpir el flujo de contenido multimedia. Otras soluciones son aún posibles.

Sobre otro eje de tiempo 122, de la misma escala, el instante t_{ej+1} y un instante teórico tt_{ej+1} de final del criptoperíodo T_j han sido representados.

El instante tt_{ej+1} se corresponde al instante teórico de final del criptoperíodo T_j calculado añadiendo al instante t_{ej} de comienzo del criptoperíodo T_j la duración T elegida durante la operación 80.

Finalmente, los instantes t_{C1} y t_{C2} representados sobre el eje 120 corresponden a dos instantes actuales sucesivos en los cuales el generador 48 envía al sincronizador 54 la señal de sincronización. Para la legibilidad de las figuras, los instantes t_{C1} y t_{C2} son representados como siendo anteriores, respectivamente, a los instantes t_{di} y t_{di+1}.

En la fig. 5, el instante t_{C1} es anterior al instante tt_{ej+1}. En este contexto, durante la operación 106, el sincronizador 54 determina que la desviación Δt es estrictamente inferior a la duración T. Impide por tanto cualquier nuevo cambio de clave en la memoria 46 hasta el siguiente instante t_{C2}. El instante t_{C2} es posterior al instante tt_{ej+1}. En estas condiciones, el sincronizador 54 determina que la desviación Δt es estrictamente superior a la duración T. Procede por tanto a la sustitución de la clave TEK_j por la clave TEK_{j+1} al final del cifrado del segmento P_i y antes del comienzo del cifrado del segmento P_{i+1}.

De ello, se comprende que el siguiente segmento, es decir el segmento P_{i+1} es completamente cifrado utilizando la clave TEK_{j+1}. Se constata igualmente que mientras que una sustitución de clave TEK_j habría debido producirse en el curso del segmento Pi, esta sustitución no se ha producido en realidad más que al final del segmento P_i. Esto corresponde a una prolongación de la duración del criptoperíodo T_j. Está prolongación de la duración del criptoperíodo T_j es provocada en respuesta a la señal de sincronización. Más precisamente, aquí, está prolongación de la duración del criptoperíodo T_j es provocada únicamente si el instante tt_{ej+1} cae en el curso de un segmento. En

el caso contrario, la duración del criptoperíodo es igual a la duración T elegida. Procediendo así, se garantiza que cualquiera que sea la duración T elegida, no se puede producir ninguna sustitución de clave TEK_j en el intervalo $]t_{di}$; $t_{di} + T_{STKM}[$.

En la fig. 5, se ha representado un eje de tiempo 124, de la misma escala, en el que son llevados los instantes t_{Si} de comienzo de recepción de las ráfagas S_i.

La fig. 6 representa otro modo de realización de un procedimiento de emisión por ráfagas de un contenido multimedia cifrado. Inicialmente, antes de la trasmisión del contenido multimedia, durante una operación 130, una duración T cualquiera es elegida para los criptoperíodos.

A continuación, las operaciones 82 a 92 son reiteradas en bucle para transmitir por ráfagas el contenido multimedia. En paralelo, el sincronizador 54 gestiona la sustitución de la clave almacenada en la memoria 46 por una nueva clave. Por ejemplo, durante una operación 132, el sincronizador 54 almacena el instante t_{ej} en el que ha comenzado el criptoperíodo T_j actual. Durante la operación 132, el sincronizador 54 calcula igualmente el instante tt_{ej+1} en el que debe producirse el final del criptoperíodo T_j actual. Para este cálculo, el sincronizador utiliza por ejemplo el instante t_{ej} así como la duración T elegida durante la operación 130.

A continuación, después de cada comienzo de criptoperíodo, durante una operación 134, el generador 52 y el constructor 56 proporcionan, respectivamente, la clave TEK_{j+1} y el mensaje $STKM_{j+1}$.

En paralelo con la operación 134, durante una operación 136, cada vez que el generador 48 envía al sincronizador 54 la señal de sincronización, el sincronizador 54 establece un instante t_{di} en el cual debe comenzar el siguiente segmento contenido en la ráfaga que va a ser preparada. Por ejemplo, la señal de sincronización es enviada en cada instante t_{di} de comienzo de un segmento P_i. Así, aquí, la señal de sincronización indica el comienzo de cada segmento.

A continuación, el sincronizador 54 procede a una operación 138 durante la cual verifica si se cumple la condición siguiente.

$$|t_{di} - tt_{ej+1}| > T_{STKM}$$

donde t_{di} es el instante de comienzo almacenado durante la operación 136.

La operación 138 consiste por tanto en comparar el instante tt_{ej+1} con un intervalo $]t_{di}$; $t_{di} + T_{STKM}[$ establecido a partir de la señal de sincronización.

En el caso en que esta condición se cumple, el sincronizador 54 procede inmediatamente a una operación 140 de sustitución de clave TEK_j por la nueva TEK_{j+1} sin esperar el cifrado del final del segmento P_i actual.

En el caso contrario, el sincronizador 54 retarda, durante una operación 142 la sustitución de la clave TEK_j. Por ejemplo, durante la operación 142, el sincronizador 54 introduce un retardo estrictamente superior a $t_{di} + T_{STKM} - tt_{ej+1}$. Después de haber introducido este retardo durante la operación 142, el sincronizador procede a la operación 140. Después de la operación 140, el procedimiento vuelve a la operación 132.

Así, en este procedimiento, contrariamente al procedimiento de la fig. 4, un cambio de criptoperíodo puede intervenir en el curso de un segmento. Sin embargo, el sincronizador 54 es apto para prolongar la duración del criptoperíodo T_j si el instante tt_{ej+1} cae en el intervalo $]t_{di}$; $t_{di} + T_{STKM}[$.

La fig. 7 ilustra aún otro modo de realización posible del procedimiento. Antes del comienzo de la emisión del contenido multimedia, durante una operación 150, la duración T de los criptoperíodos es elegida para verificar las relaciones siguientes:

$T/T_B = r/q$, y

$1/q \geq T_{STKM}/T_B$

donde:

- r y q son números enteros naturales no nulos y primos entre ellos, y

- T_B es una duración mínima que es inferior o igual a la duración más pequeña de reproducción de un segmento del contenido multimedia.

La duración T_B es por tanto un elemento de disminución, independiente del índice i, que disminuye la duración de todos los segmentos P_i del contenido multimedia. Aquí, se supone que la duración de reproducción de cada segmento P_i es igual a la duración T_B. La duración T_B es superior a T_{STKM}.

Tal elección de la duración T garantiza que no puede producirse ningún cambio de criptoperíodo en el intervalo $]t_{di}$; $t_{di} + T_{STKM}[$.

Por ejemplo, durante la operación 150, el emisor 22 limita la elección de la duración T únicamente a las duraciones que respetan las relaciones anteriores. A título de ilustración, durante la operación 150, una interfaz gráfica que permite únicamente a un operador elegir una duración T que verifica estas relaciones es presentada a un operador de este emisor 22. La interfaz gráfica es generada entonces por el sincronizador 54.

A continuación, durante la emisión del contenido multimedia, cada ráfaga es preparada durante una operación 152. La operación 152 es por ejemplo idéntica a la operación 86.

A continuación, una vez que la ráfaga ha sido preparada, ésta es difundida durante una operación 154 idéntica, por ejemplo, a la operación 92.

Las operaciones 152 y 154 son reiteradas en bucle para transmitir por ráfagas el contenido multimedia.

En paralelo, durante una operación 156, a cada comienzo de criptoperíodo, el generador 52 y el constructor 56 proporcionan, respectivamente, la nueva clave TEK_{j+1} y el nuevo mensaje $STKM_{j+1}$.

A continuación, una vez que sobreviene el instante tt_{ej+1}, durante una operación 158, el sincronizador 54 procede inmediatamente a la sustitución de la clave TEK_j por la clave TEK_{j+1} en la memoria 46. Durante la operación 158, sincronizador 54 trasmite igualmente al generador 48 el nuevo mensaje $STKM_{j+1}$ correspondiente a la clave TEK_{j+1}.

Las operaciones 156 y 158 son reiteradas en bucle. En este procedimiento, gracias a la elección particular de la duración T, no es ya necesario que el generador 48 informe al sincronizador 54 del comienzo de la preparación de una nueva ráfaga. Además, aquí, con la ayuda del procedimiento de la fig. 7, el sincronizador 54 no tiene ya por función prolongar o al contrario acortar la duración de un criptoperíodo. Al contrario, en este modo de realización, la duración T de los criptoperíodos es constante. En otros términos, en este modo de realización, el sincronizador 54 es únicamente utilizado para:

- limitar la elección de la duración T, y

- efectuar la sustitución de las claves en la memoria 46 y, en paralelo, transmitir los nuevos mensajes $STKM_j$ al generador 48.

Son posibles otros numerosos modos de realización. Por ejemplo, el criptograma de la clave TEK_j contenida en el mensaje $STKM_j$ puede ser una referencia a una clave cifrada y previamente almacenada en la memoria del receptor. De manera más general, se designa aquí por criptograma de la clave TEK_j todas las informaciones necesarias pero no suficientes en sí mismas para reconstruir la clave TEK_j.

El generador 48 y el sincronizador 54 pueden ser realizados con ayuda de circuitos electrónicos especialmente cableados para realizar las funciones requeridas. Así, estos circuitos no han recurrido necesariamente a instrucciones almacenadas sobre un soporte de almacenamiento de informaciones.

En otro modo de realización, para resolver el problema descrito con referencia a las figs. 1 y 2, es igualmente posible modificar los receptores para que cada receptor sea apto para tratar en paralelo dos mensajes $STKM_j$ y $STKM_{j+1}$. Así, después de una duración T_{STKM}, estos receptores tienen a su disposición a la vez la clave TEK_j y la clave TEK_{j+1}. Modificando así los receptores, se puede evitar la reaparición de una pantalla negra durante el periodo 12.

Cuando la duración de reproducción T_B es conocida y constante, es igualmente posible calcular de antemano si el instante tt_{ej+1} de comienzo del siguiente criptoperíodo T_{j+1} debe caer en el intervalo $]t_{di}$; $t_{di} + T_{STKM}[$. Si este cálculo es efectuado suficientemente por adelantado, es entonces posible igualmente acortar la duración del criptoperíodo actual T_j para provocar la sustitución de la clave en la memoria 46 no durante este intervalo sino antes del instante t_{di}. En este caso, la duración del criptoperíodo T_j es acortada.

Cuando la sustitución de la clave TEK_j por la clave TEK_{j+1} es adelantada o retardada, esta sustitución es adelantada o retardada para no caer en el intervalo $]t_{di}$; $t_{di} + T_{STKM}[$ de un segmento precedente o siguiente.

Durante la operación 150, no es necesario que el emisor 22 limite las elecciones posibles de esta duración T. La memorización en el emisor de una duración T satisfactoria es entonces únicamente realizada bajo el control del operador.

En una variante, la duración T es elegida como siendo un múltiplo entero de la duración T_B. En este caso, inicialmente, los instantes de comienzo del primer criptoperíodo y del primer segmento son sincronizados para que el final de un criptoperíodo no caiga nunca en el intervalo $]t_{di}$; $t_{di} + T_{STKM}[$ de un segmento. De esta manera, la duración de los criptoperíodos es constante.

REIVINDICACIONES

1. Procedimiento de emisión por ráfagas de un contenido multimedia cifrado, comprendiendo este procedimiento:

a) la elección (80) de una duración T cualquiera para criptoperíodos sucesivos,

b) la sustitución (110; 140), por un sincronizador, de una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} a cada final de criptoperíodo,

c) el cifrado (88) de los segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo,

d) la construcción (90), por un generador, de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i,

caracterizado por que la sustitución (110; 140) de la clave actual TEK_j por la clave actual TEK_{j+1} para cifrar el segmento P_i es retardada hasta después de un instante $t_{di} + T_{STKM}$ o adelantada al instante t_{di} o antes del mismo en respuesta a una señal de sincronización intercambiada (82) entre el generador y el sincronizador, siendo la duración T_{STKM} superior o igual al tiempo necesario para que un receptor descifre el criptograma de una clave actual contenida en la ráfaga S_i estrictamente inferior a la duración T elegida.

2. Procedimiento según la reivindicación 1, en que el procedimiento comprende:

- antes del cifrado de un nuevo segmento P_i, la comparación (106) de un instante actual t_C establecido a partir de la señal de sincronización, en un instante teórico tt_{ej+1} de final del criptoperíodo actual calculable a partir de un instante t_{ej} y de la duración T elegida, siendo el instante t_{ej} el instante de comienzo del criptoperíodo actual, y

-si el instante t_C es anterior al instante tt_{ej+1}, el cifrado (88, 108) de la totalidad del segmento P_i con la clave actual TEK_j incluso si el final del criptoperíodo T_j cae durante este segmento Pi, y

- si el instante t_C es posterior al instante tt_{ej+1}, el cifrado (88, 110) de la totalidad del segmento P_{i+1} con la nueva clave actual TEK_{j+1}.

3. Procedimiento según la reivindicación 1, en que el proced imiento comprende:

- antes del cifrado de un nuevo segmento P_i en el curso del cual sobreviene un instante teórico tt_{ej+1} de final del criptoperíodo actual calculable a partir de un instante t_{ej} de comienzo del criptoperíodo actual y de la duración T elegida, la comparación (138) del instante tt_{ej+1} en un intervalo $]t_{di} ; t_{di} + T_{STKM}[$ establecido a partir de la señal de sincronización, y

- únicamente si el instante tt_{ej+1} está comprendido en el intervalo $]t_{di} ; t_{di} + T_{STKM}[$, la sustitución (140, 142) de la clave actual TEK_j por la clave actual TEK_{j+1} para cifrar el segmento P_i es retardada hasta después de un instante $t_{di} + T_{STKM}$ o adelantada al instante t_{di} o antes del mismo.

4. Procedimiento de emisión por ráfagas de un contenido multimedia cifrado, comprendiendo este procedimiento:

a) la elección (150) de una duración T para criptoperíodos sucesivos,

b) la sustitución (158) inmediata de una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} en cada final de criptoperíodo,

c) el cifrado (88) de los segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo, y teniendo una duración de reproducción superior o igual a una duración mínima T_B común a todos los segmentos,

d) la construcción (90) de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i,

caracterizado por que la duración T elegida verifica las condiciones siguientes:

- $T/T_B = r/q$, donde r y q son números enteros naturales no nulos y primos entre ellos, y

- $1/q \geq T_{STKM}/T_B$ donde la duración T_{STKM} es superior o igual al tiempo necesario para que un receptor descifre el criptograma de una clave actual contenida en la ráfaga S_i y estrictamente inferior a la duración T elegida.

5. Procedimiento según la reivindicación 4, en el que la duración de reproducción de cada segmento P_i es igual a la duración T_B.

6. Soporte de almacenamiento de informaciones, caracterizado por que incluye instrucciones para la ejecución de un procedimiento conforme a una cualquiera de las reivindicaciones precedentes, cuando estas instrucciones son ejecutadas por un calculador electrónico.

7. Emisor por ráfagas de un contenido multimedia cifrado, comprendiendo este emisor:

a) una memoria (60) en la que es almacenada una duración T para criptoperíodos sucesivos,

b) un sincronizador (54) apto para sustituir una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} a cada final de criptoperíodo,

c) un codificador (44) apto para cifrar segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo,

d) un generador (48) de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i,

caracterizado por que el generador (48) y el sincronizador (54) son aptos para intercambiar una señal de sincronización para retardar la sustitución de la clave actual TEK_j por la clave actual TEK_{j+1} hasta después del instante $t_{di} + T_{STKM}$, o para adelantar esta sustitución al instante t_{di} o antes del mismo, siendo la duración T_{STKM} superior o igual al tiempo necesario para que un receptor descifre el criptograma contenido en la ráfaga S_i y estrictamente inferior a la duración T elegida.

8. Emisor por ráfagas de un contenido multimedia cifrado, comprendiendo este emisor:

a) una memoria (60) en la cual está almacenada una duración T para criptoperíodos sucesivos,

b) un sincronizador (54) apto para sustituir inmediatamente una clave actual TEK_j de cifrado por una nueva clave actual TEK_{j+1} a cada final de criptoperíodo,

c) un codificador (44) apto para cifrar los segmentos P_i inmediatamente consecutivos del contenido multimedia con la clave actual de cifrado, comenzando cada segmento P_i en un instante t_{di} respectivo y teniendo una duración de reproducción superior o igual a una duración mínima T_B común a todos los segmentos,

d) un generador (48) de una ráfaga S_i cuya duración de recepción es más corta que la duración de reproducción del segmento P_i, conteniendo la ráfaga S_i el segmento P_i cifrado y un criptograma de cada clave actual utilizada para cifrar el segmento P_i,

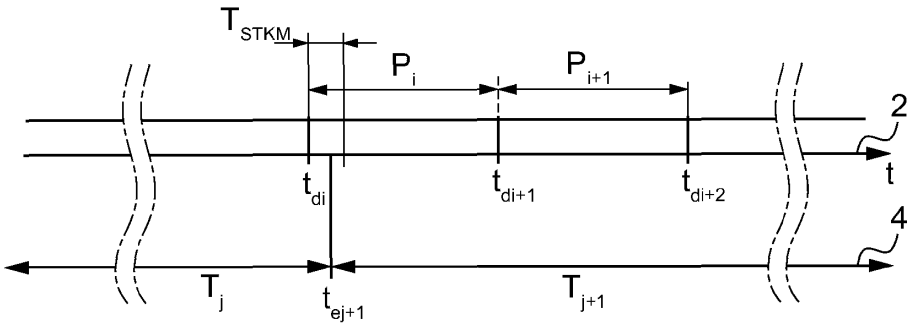
caracterizado por que la duración T contenida en la memoria verifica las condiciones siguientes:

- $T/T_B = r/q$, donde r y q números son enteros naturales no nulos y primos entre ellos, y

- $1/q \geq T_{STKM}/T_B$ donde la duración T_{STKM} es superior o igual al tiempo necesario para que un receptor descifre el criptograma de una clave actual contenida en la ráfaga S_i y estrictamente inferior a la duración T elegida.

9. Emisor según la reivindicación 8, en el que el emisor es apto para limitar la elección de la duración T a una duración T que satisfaga las dos condiciones.

Fig.1



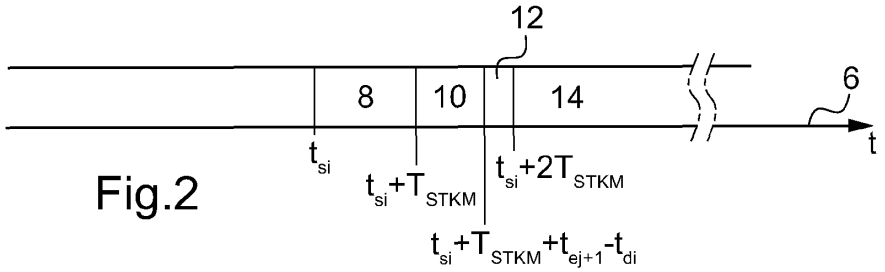


Fig.2

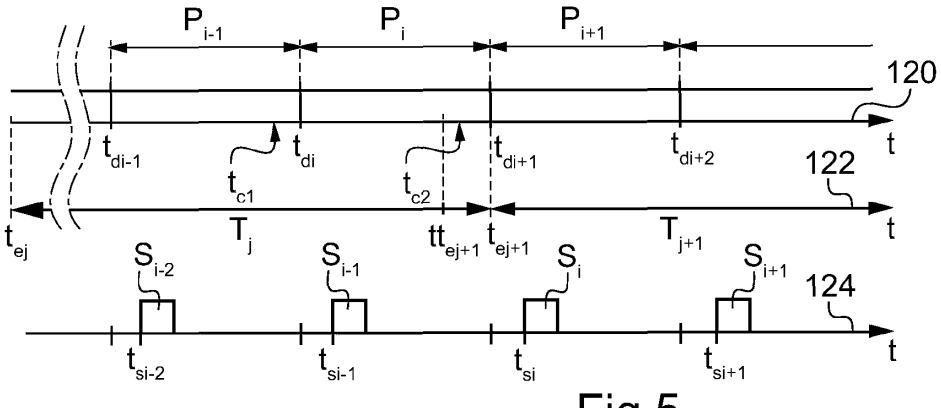


Fig.5

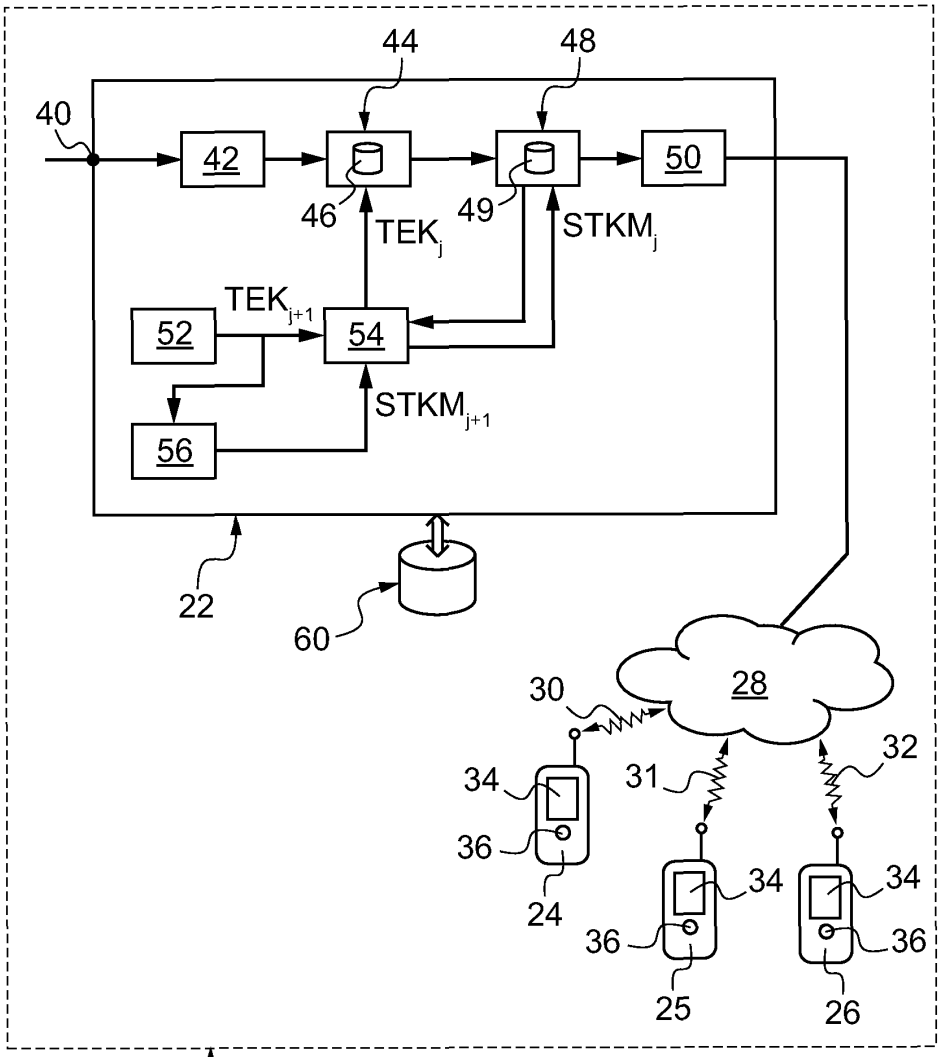

44
48
40
42
50
46
49
TEK$_j$
STKM$_j$
TEK$_{j+1}$
52
54
STKM$_{j+1}$
56
22
60
28
30
32
34
31
36
24
34
34
36
36
25
26
20

Fig.3

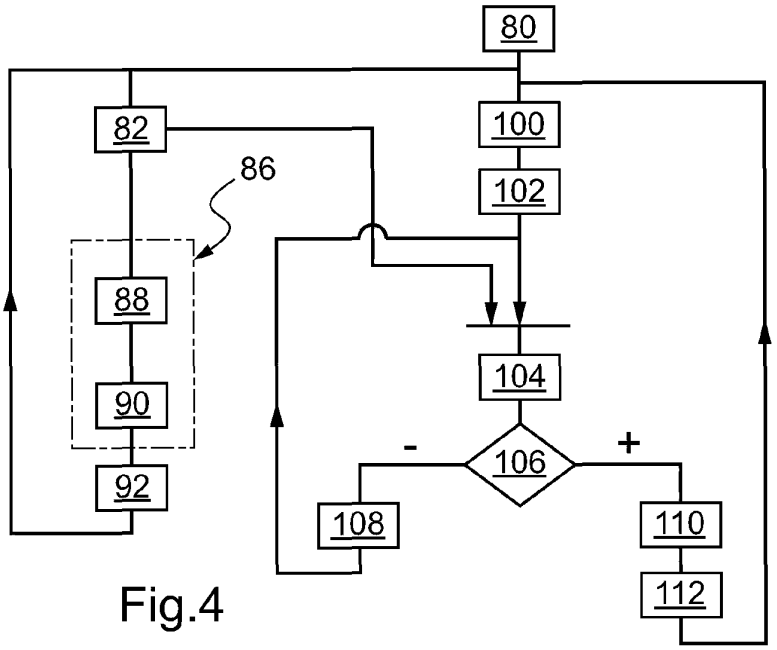


Fig.4

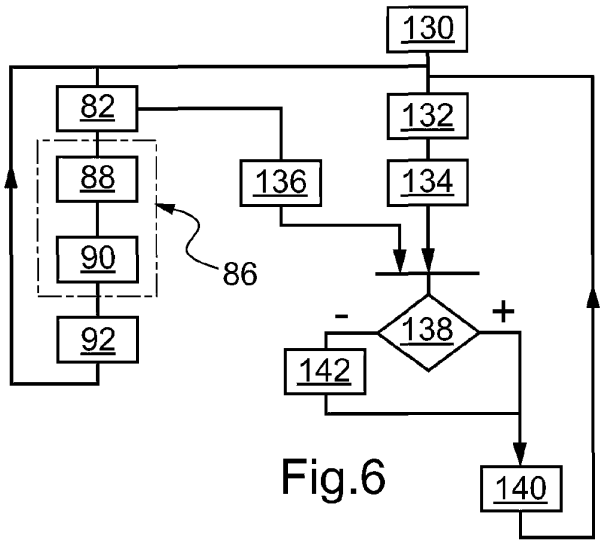


Fig.6

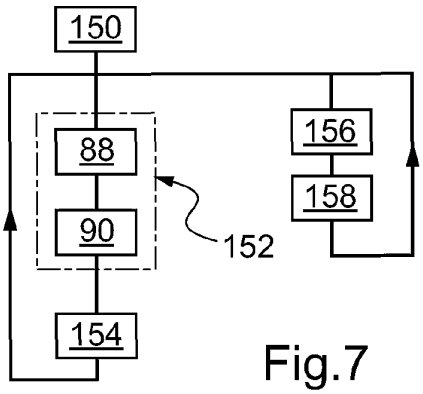


Fig.7