(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 844**

(51) Int. CI.:

H04L 9/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.07.2003 E 03755619 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.10.2012 EP 1525707**

(54) Título: **Procedimiento de transmisión de datos cifrados, procedimiento de descifrado asociado, dispositivos para su puesta en práctica y terminal móvil que los incorpora**

(30) Prioridad:

30.07.2002 FR 0209668

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2013

(73) Titular/es:

EADS SECURE NETWORKS (100.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR

(72) Inventor/es:

MARQUE-PUCHEU, GERARD

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de transmisión de datos cifrados, procedimiento de descifrado asociado, dispositivos para su puesta en práctica y terminal móvil que los incorpora

La presente invención se refiere al ámbito de los sistemas de radiocomunicaciones digitales y, en particular, a los sistemas de tipo TDMA (del inglés "Time Division Multiple Access" que significa acceso múltiple por división de tiempo). Ésta encuentra aplicaciones particularmente ventajosas en los sistemas privados de radiocomunicaciones profesionales (o sistemas PMR, del inglés "Professional Mobile Radio").

Los sistemas PMR ofrecen en general un servicio de cifrado de principio a fin de los datos de tráfico transmitidos durante las comunicaciones. Se trata, especialmente, de datos que codifican fonía pero más generalmente de datos de cualquier naturaleza. El cifrado tiene por objetivo preservar la confidencialidad y la integridad de los datos transmitidos y evitar la usurpación de identidad de los terminales móviles que pertenecen al sistema.

La expresión "de principio a fin" (en inglés "end-to-end") se utiliza para designar el hecho de que el cifrado de los datos transmitidos es efectuado a nivel del terminal emisor y que el descifrado es efectuado a nivel del terminal receptor o de los terminales receptores. La totalidad del enlace queda entonces asegurada, y esto de manera ventajosamente independiente de la infraestructura del sistema. Esto se opone al caso del aseguramiento de solamente una porción del enlace entre el terminal emisor y el terminal receptor, por ejemplo la interfaz aire, en la cual el cifrado y/o el descifrado de los datos tiene lugar en ciertos puntos intermedios del enlace.

En el estado de la técnica, se conocen mecanismos de cifrado/descifrado de datos transmitidos entre un emisor y un receptor. El principio de un mecanismo de este tipo está ilustrado por el esquema de la figura 1.

El emisor comprende un generador de secuencia criptográfica 11, que genera un bloque de datos SC_i denominado secuencia criptográfica, independientemente del flujo de datos no encriptados, a partir de una clave de encriptado K secreta y de una información denominada vector de inicialización IV_i (del inglés "Initialization Vector"). La secuencia criptográfica SC_i es tal que:

$$SC_i = E_K(IV_i) \quad (1)$$

donde E_K designa el cifrado de la información IV_i con la clave K, según el algoritmo de cifrado determinado.

El algoritmo de cifrado es el mismo para todos los terminales móviles del sistema. El vector de inicialización IV_i y la clave de encriptado K secreta son conocidos a la vez por el terminal emisor y el terminal receptor. El vector de inicialización IV_i varía en el tiempo para evitar que la misma secuencia criptográfica sea utilizada dos veces con la misma clave K, lo que debilitaría gravemente la seguridad de los datos transmitidos. El índice i se refiere a un valor corriente del vector de inicialización.

El emisor comprende también un operador O-Exclusivo 21 que recibe la secuencia criptográfica SC_i en una primera entrada y una secuencia m_i de datos no encriptados en una segunda entrada, y que genera una secuencia de datos cifrados c_i a la salida, de modo que:

$$C_i = m_i \oplus SC_i \quad (2)$$

donde $\oplus$ designa la operación O-Exclusivo realizada bit a bit.

La secuencia c_i es transmitida a través del canal de transmisión 20.

El receptor comprende a su vez un generador de secuencia criptográfica 12 que genera, a partir del mismo vector de inicialización IV_i y de la misma clave de encriptado K secreta, una secuencia criptográfica SC_i idéntica a la generada por el generador 11 del emisor y que ha servido para el cifrado de la secuencia c_i. Asimismo, éste comprende también un operador O-Exclusivo 22 que recibe en una primera entrada la secuencia criptográfica SC_i generada por el generador 12, que recibe en una segunda entrada la secuencia de datos cifrados c_i, y que restituye a la salida la secuencia m_i de datos no encriptados, debido a que:

$$C_i \oplus SC_i = m_i \oplus SC_i \oplus SC_i = m_i \quad (3)$$

Para que la transmisión de datos cifrados de principio a fin sea correcta, el emisor y el receptor deben efectuar operaciones duales una de la otra. En particular, es por tanto necesario que el receptor conozca la relación temporal que hay que respetar en la entrada del operador 22, entre, por una parte, la secuencia criptográfica SC_i que éste

genera y, por otra, la secuencia de datos cifrados c_i que éste recibe, para que el cifrado se desarrolle correctamente. Esta limitación es conocida con el nombre de sincronización criptográfica.

El documento EP0446194 describe un sistema para la sincronización de los dispositivos de encriptado en un sistema celular digital de comunicación. Cada uno de los dispositivos de encriptado comprende un contador de varios bits y genera una secuencia seudoaleatoria que es combinada con los datos que deben ser cifrados. La secuencia seudoaleatoria es una función del valor de varios bits de contador que es incrementado periódicamente en respuesta a una serie de impulsos de reloj. Para permitir el desencriptado correcto de los datos cifrados, el sistema de la presente invención facilita actualizaciones en continuo o muy frecuentes del valor del contador emisor que pueden ser utilizadas para reinicializar el contador del receptor y sincronizar el sistema sin la necesidad de reinicialización y de la repetición de impulsos de reloj.

En el tipo de aplicaciones considerado, la sincronización criptográfica presenta en realidad dos aspectos. En primer lugar la sincronización inicial, es decir al principio de la comunicación. Y a continuación la sincronización periódica, que permite paliar una eventual pérdida de la sincronización criptográfica entre los terminales móviles que participan en la comunicación, y que permite además la entrada tardía (en inglés « late entry » de otros terminales móviles en la comunicación, en el marco de una comunicación en grupo.

Un ejemplo de la técnica de sincronización criptográfica para el cifrado de principio a fin de una comunicación radio ha sido propuesto ya para los sistemas de tipo FDMA (del inglés “Frequency Division Multiple Access” que significa acceso múltiple por división de frecuencia). Esta técnica está descrita, por ejemplo, en la patente americana US4757536. Ésta se basa en la inserción periódica, en el preámbulo de las tramas o paquetes de fonía, de una información de sincronización tanto radio como criptográfica, que en particular permite la función de entrada tardía en la comunicación. La información de sincronización está aquí constituida por el valor corriente del vector de inicialización.

Esta técnica ha sido aplicada sin modificación en sistemas de tipo TDMA como el sistema TETRA (del inglés « TErrestrial Trunked Radio », donde ningún recurso había sido reservado a priori para la transmisión de una información de sincronización criptográfica; ésta es transmitida de principio a fin por robo de trama de fonía (en inglés « Frame stealing »). De modo más particular, se reemplazan los datos de una trama de fonía conocida en ciertas tramas TDMA (o tramas radio) determinadas, por una información de sincronización criptográfica. Ésta permite al terminal receptor generar la secuencia criptográfica conveniente para el cifrado de los datos de fonía transmitidos en las tramas TDMA que siguen inmediatamente. Existe por tanto una relación temporal determinada y fija entre la transmisión de las informaciones de sincronización y la de los datos cifrados a los cuales se refieren estos. Se dice que la información de sincronización criptográfica es transmitida en la banda refiriéndose al hecho de que ésta ocupa recursos útiles de la comunicación. Podrá referirse por ejemplo a la patente americana US2002/0066013 para un ejemplo de esta técnica aplicada al sistema TETRA.

En esta aplicación, la técnica conocida presenta sin embargo numerosos inconvenientes.

En primer lugar, la sincronización inicial debe ser de buena calidad para evitar que errores de transmisión radioeléctrica priven a numerosos terminales de recepción en comunicaciones de grupo, de la posibilidad de recibir y de descifrar correctamente la fonía. Es por lo que la información de sincronización criptográfica es repetida en general 4 veces en el transcurso de la primera segunda de comunicación, o sea en el transcurso de las 34 primeras tramas, lo que provoca una tasa de robo de tramas del orden del 11%, que degrada severamente la calidad de la fonía.

A continuación, la elección de la periodicidad de la repetición de la información de sincronización criptográfica conduce a un compromiso entre la calidad de la fonía que, por una parte, demanda una periodicidad pequeña de los robos de tramas, y, por otra, la minimización del retardo durante las entradas tardías que por el contrario demanda una alta periodicidad. Este compromiso es en general poco satisfactorio.

Finalmente, en los sistemas que ofrecen servicios de cifrado de principio a fin, la sincronización criptográfica debe ser objeto de un cuidado particular cuando un terminal móvil en recepción efectúe un cambio de célula en curso de comunicación (en inglés: “handover”). En efecto, los tiempos de propagación diferentes de los paquetes de fonía en el subsistema red conducen generalmente a una pérdida de la sincronización durante el cambio de célula. Esta pérdida de sincronización es temporal en el caso en que las informaciones de sincronización se repitan periódicamente siendo transportadas por robo de tramas de fonía, como en el sistema TETRA. Sin embargo, la transmisión de estas informaciones de sincronización tiene lugar con una periodicidad mucho más baja que la duración de un cambio de célula correctamente concebido. Resulta así un retardo no despreciable del restablecimiento de la comunicación en la célula blanco, que conduce a una alta degradación de la calidad de servicio. La única solución para paliar este inconveniente sería aumentar la periodicidad de la repetición de la información de sincronización criptográfica. Sin embargo, siendo esta información transportada por robo de trama de fonía, la calidad de la fonía resultaría altamente degradada.

Un primer objeto de la invención es definir un mecanismo de sincronización criptográfica en un sistema TDMA que tenga un canal de señalización asociada que elimine los citados inconvenientes de la técnica anterior.

Un segundo objeto de la invención es proponer un mecanismo de mantenimiento de la sincronización criptográfica durante el cambio de célula en curso de comunicación por un terminal móvil en recepción.

De acuerdo con un primer aspecto de la invención, un procedimiento de transmisión de datos cifrados entre un terminal móvil emisor y al menos un terminal móvil receptor de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio que tiene una estructura de trama tal que una trama TDMA comprende intervalos de tiempo de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, comprende las etapas según las cuales:

- se transmite en el canal de tráfico una secuencia de paquetes de datos cifrados a partir de un intervalo de tiempo del primer tipo determinado, mientras que se transmite en el canal de señalización asociada una información de sincronización criptográfica asociada en interior de un intervalo de tiempo del segundo tipo determinado,

- y se transmite igualmente en el canal de señalización asociada una información de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el citado intervalo de tiempo del primer tipo determinado.

Así, la información de sincronización criptográfica es transmitida en el canal de señalización asociada cuando a tal efecto están disponibles recursos en éste, evitando así los inconvenientes de los robos de tramas de fonía de la técnica conocida por la técnica anterior.

Un segundo aspecto de la invención concierne a un procedimiento de descifrado de una secuencia de paquetes de datos cifrados transmitida entre un terminal móvil emisor y al menos un terminal móvil receptor de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio que tiene una estructura de trama tal que una trama TDMA comprende intervalos de tiempo de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, que comprende la etapas consistentes en:

a) recibir la citada secuencia de paquetes de datos cifrados a parir de un intervalo de tiempo del primer tipo determinado;

b) eventualmente, recibir una información de sincronización criptográfica asociada en el canal de señalización asociada, en el interior de un intervalo de tiempo del segundo tipo determinado y, en este caso,

c) recibir igualmente, en el canal de señalización asociada, una información de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el citado intervalo de tiempo del primer tipo determinado;

d) generar un valor de un vector de inicialización que haya servido para generar una secuencia criptográfica utilizada para el cifrado de la citada secuencia de paquetes de datos cifrados;

e) generar la misma secuencia criptográfica, a partir del valor del vector de inicialización generado en la etapa d);

f) desfasar la secuencia criptográfica generada en la etapa e) en función de la citada información de retardo de sincronización criptográfica; y

g) descifrar la citada secuencia de paquetes de datos cifrados a partir de la citada secuencia criptográfica desfasada.

Un tercer aspecto de la invención se refiere a un dispositivo de transmisión de datos cifrados entre un termal móvil emisor y al menos un terminal móvil receptor de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio que tiene una estructura de trama tal que una trama TDMA comprende intervalos de tiempo de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, que comprende:

- medios para transmitir una secuencia de paquetes de datos cifrados en el canal de tráfico a partir de un intervalo de tiempo del primer tipo determinado, y para transmitir una información de sincronización criptográfica en el canal de señalización asociada en el interior de un intervalo de tiempo del segundo tipo determinado, y

- medios para transmitir igualmente en el canal de señalización asociada, una información de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el citado intervalo de tiempo del primer tipo determinado.

Un cuarto aspecto de la invención se refiere a un dispositivo de descifrado de una secuencia de paquetes de datos cifrados transmitida entre un terminal móvil emisor y al menos un terminal móvil receptor de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio que tiene una estructura de trama tal que

una trama TDMA comprende intervalos de tiempo de un primer tipo que forma un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, que comprende:

a) primeros medios de recepción para recibir la citada secuencia de paquetes de datos cifrados a partir de un intervalo de tiempo del primer tipo determinado;

b) segundos medios de recepción para, eventualmente, recibir una información de sincronización criptográfica asociada en el canal de señalización asociada, en el interior de un intervalo de tiempo del segundo tipo determinado, y, en este caso,

c) medios de recepción para recibir igualmente, en el canal de señalización asociada, una información de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo de terminado y el citado intervalo de tiempo del primer tipo de terminado;

d) primeros medios de generación para generar un valor de un vector de inicialización que haya servido para generar una secuencia criptográfica utilizada para el cifrado de la citada secuencia de paquetes de datos cifrados;

e) segundos medios de generación, para generar la misma secuencia criptográfica, a partir del valor del vector de inicialización generado por los citados primeros medios de generación;

f) medios de desfase para desfasar la secuencia criptográfica generada por los citados segundos medios de generación, en función de la citada información de retardo de sincronización criptográfica; y

g) medios para descifrar la citada secuencia de paquetes de datos cifrados a partir de la citada secuencia criptográfica desfasada;

Finalmente, un quinto y último aspecto de la invención se refiere a un terminal móvil de un sistema de radiocomunicaciones digitales, que comprende un dispositivo de transmisión, y/o un dispositivo de descifrado tales como los definidos anteriormente.

Otras características y ventajas de la invención se pondrán de manifiesto todavía con la lectura de la descripción que sigue. Ésta es puramente ilustrativa y debe ser leída refiriéndose a los dibujos anejos, en los cuales:

- la figura 1, ya analizada, es un esquema sinóptico que ilustra el cifrado y el descifrado de datos transmitidos entre un emisor y un receptor;

- la figura 2 es un diagrama que muestra un ejemplo de estructura de trama en un sistema de radiocomunicaciones TDMA;

- la figura 3a y la figura 3b son, respectivamente, un diagrama y una tabla que ilustran un ejemplo de encapsulación de transmisión de fonía (o paquetes de fonía) en la estructura de trama de la figura 2;

- la figura 4 es un esquema sinóptico de un terminal móvil de acuerdo con la invención;

- la figura 5 es un diagrama que ilustra un ejemplo de secuencias de etapas de un procedimiento de transmisión de datos cifrados de acuerdo con la invención,

- la figura 6 es un diagrama que ilustra un ejemplo de vector de inicialización de acuerdo con la invención;

- la figura 7 es un diagrama que ilustra un ejemplo de información de sincronización de acuerdo con la invención, que corresponde al ejemplo de vector de inicialización según la figura 6;

- la figura 8 es un diagrama que ilustra un ejemplo de transmisión de cuatro primeras secuencias de datos cifrados en una supertrama del canal radio para una alternancia determinada;

- la figura 9 es un diagrama que ilustra un ejemplo de recepción de cuatro primeras secuencias de datos cifrados en una supertrama del canal radio para la alternancia considerada en la figura 8;

- la figura 10 es un diagrama que ilustra un ejemplo de secuencia de etapas de un procedimiento de descifrado de datos cifrados de acuerdo con la invención;

- la figura 11 es una tabla de conversión que da un valor de diferencia temporal expresado en número de tramas de fonía en función del valor de la citada diferencia temporal expresado en número de intervalos de tiempo, en el ejemplo de encapsulación de las figuras 3a y 3b;

- la figura 12 es un diagrama que muestra una configuración de handover en un sistema de radiocomunicaciones;

- la figura 13 es un diagrama que ilustra un ejemplo de secuencia de etapas de acuerdo con la invención, para mantener la sincronización criptográfica durante un handover.

La estación de base de una célula puede establecer canales lógicos de tráfico con uno o varios terminales móviles situados en su zona de cobertura radio, de acuerdo con un procedimiento de establecimiento de llamada efectuada por medio de un canal lógico de control específico. El canal de tráfico establecido con un terminal móvil es descendente y/o ascendente. Uno o varios canales lógicos de tráfico son multiplexados, en una frecuencia determinada, con un canal lógico de señalización asociada que sirve para intercambiar señalización en curso de comunicación.

La invención se ha descrito anteriormente en su aplicación a un ejemplo de sistema de radiocomunicaciones que es un sistema TDMA-2, es decir un sistema de tipo TDMA de orden 2.

La figura 2 es un diagrama que ilustra un ejemplo de estructura de una supertrama radio en canales físicos de tráfico en un ejemplo de este tipo. En esta figura, se han representado, yuxtaponiéndolas según la vertical, por una parte, la estructura de una supertrama radio en un canal físico de tráfico ascendente establecido en una frecuencia f_{TU} determinada y, por otra, la estructura de una supertrama radio en un canal físico de tráfico descendente establecido en una frecuencia f_{TD} determinada, diferente de la frecuencia f_{TU}.

Una supertrama del canal físico de tráfico está subdividida en cuatro tramas (denominadas también tramas radio, tramas TDMA o segmentos, en el argot del especialista en la materia), que están representadas una encima de otra en la figura. Dicho de otro modo, una trama TDMA corresponde a un cuarto de supertrama. Cada trama TDMA está compuesta por nueve intervalos de tiempo compuestos que tienen cada uno una duración d2 igual a 40 ms, y que comprenden cada uno dos intervalos de tiempo elementales consecutivos, cada uno de duración d1 igual a 20 ms.

Cada uno de los ocho primeros intervalos de tiempo compuestos de cada trama comprende un intervalo de tiempo elemental impar para el sentido descendente y un intervalo de tiempo elemental par para el sentido ascendente, que están representados por la letra T. La sucesión recurrente de estos intervalos de tiempo T forma un canal lógico de tráfico o canal TCH (del inglés “Trafic Channel”), respectivamente descendente y ascendente. En consecuencia, en el mismo canal físico de tráfico descendente establecido a la frecuencia f_{TD} determinada, la estación de base puede multiplexar, en los intervalos de tiempo elementales pares, otro canal lógico de tráfico establecido con otra estación móvil.

El noveno intervalo de tiempo compuesto de cada segmento está reservado a la transmisión de informaciones de señalización. La sucesión recurrente de estos intervalos de tiempo, que están representados por la letra S, forma un canal lógico de señalización asociada, respectivamente descendente y ascendente. En la práctica, varios canales lógicos pueden ser multiplexados en los intervalos de tiempo S de la supertrama. Sin embargo, por razones de comodidad, se hará referencia en lo que sigue a un solo canal de señalización. Se trata de un canal de tipo SACCH (del inglés “Slow Associated Control CHannel”) es decir, un canal de control lento que permite efectuar la supervisión del canal lógico de tráfico al cual está asociado.

En la figura 2, los números indicados encima de las tramas corresponden a los números de intervalos de tiempo compuestos en la supertrama, es decir, también a los números de intervalos de tiempo elementales en cada uno de los canales ascendente y descendente.

De acuerdo con la invención, este canal de señalización asociada es utilizado para la transmisión de las informaciones de sincronización criptográfica periódicas. Éstas por tanto son trasmitidas « fuera de banda ». Esta técnica permite evitar los robos de tramas durante toda la duración de la alternancia en curso. Robos de tramas intervienen solamente para la transmisión de la sincronización criptográfica inicial.

Por ejemplo, la información de sincronización criptográfica que es transmitida en un instante determinado es el valor corriente del vector de inicialización, es decir que haya servido para la generación de la secuencia criptográfica corriente, es decir también a la generación de la secuencia de datos cifrados corriente.

Ahora bien, una secuencia de datos cifrados es emitida en el canal TCH desde que ésta está disponible. En particular, la alternancia en curso puede empezar en cualquier intervalo de tiempo T entre dos intervalos de tiempo S consecutivos. Eligiendo una secuencia criptográfica cuya longitud en número de bits corresponda ventajosamente al número de bits útiles transmitidos entre dos intervalos de tiempo S consecutivos, se asegura que, para una alternancia determinada, cada secuencia de datos cifrados será transmitida a partir del mismo intervalo de tiempo en cada trama TDMA.

Es necesario sin embargo paliar la ausencia de relación temporal fija (de una alternancia a otra) entre, por una parte, las secuencias criptográficas tales como éstas son generadas en el terminal emisor para el cifrado y, por otra, los intervalos de tiempo S que pueden ser utilizados para la transmisión de las informaciones de sincronización criptográficas periódicas correspondientes. Además, es necesario también paliar la ausencia de relación temporal fija entre, por una parte, las secuencias de sincronización que deben ser generadas por el terminal receptor para el descifrado y, por otra, los intervalos de tiempo utilizados para la transmisión de las informaciones de sincronización

criptográfica, en una célula que puede ser diferente de aquélla en la que se encuentra el terminal emisor y no estar sincronizada (desde un punto de vista temporal) con respecto a ésta.

La unidad de datos en la salida de un codificador de palabra del terminal emisor es una trama de fonía, y corresponde a un paquete de datos de tamaño determinado. Se indica por M el tamaño (en número de bits) de una trama o paquete de fonía, es decir, el número de bits de un paquete de fonía. En el ejemplo considerado en lo que sigue, M = 88. Cuando el caudal binario a la salida del codificador de palabra es igual a 4,4 Kbits/s (kilobits por segundo), la duración de una trama o paquete de fonía es así igual a 20 ms.

Se indica por N la longitud (en número de bits) de la secuencia criptográfica SC_i. Preferentemente, N es un múltiplo entero de M. Dicho de otro modo, existe un número entero P tal que:

N = PxM

Se obtiene así que, para el cifrado, cada secuencia criptográfica SC_i es combinada bit a bit en el operador O-Exclusivo (se denomina a veces “XORée”) con P tramas de fonía facilitadas sucesivamente por el codificador de palabra. Se genera por tanto una nueva secuencia criptográfica SC_i una vez cada P tramas de fonía.

En el ejemplo considerado en lo que sigue, N = 1584 y P = 18.

Cuando N corresponde al número de bits útiles transmitidos entre dos intervalos de tiempo S, los PxM bits de P tramas de fonía consecutivas pueden ser encapsulados exactamente en ocho intervalos de tiempo radio. En el ejemplo considerado, el caudal binario en el canal radio es igual a 16 Kbits/s, lo que permite ampliamente transmitir en cada intervalo de tiempo T (del que se recuerda que la duración d1 es igual a 20 ms) un número de bits útiles igual a N/8. Estos 198 bits útiles pueden descomponerse de cuatro maneras diferentes.

De acuerdo con una primera manera, un intervalo de tiempo comprende, en este orden:

- 88 bits de un primer paquete de fonía transmitido en entero;

- 88 bits de un segundo paquete de fonía transmitido en entero; y

- 22 bits de un tercer paquete de fonía del que solo un cuarto es transmitido en este intervalo de tiempo.

De acuerdo con una segunda manera, un intervalo de tiempo comprende, sucesivamente:

- 66 bits de un primer paquete de fonía transmitido del que solamente tres cuartos de los bits son transmitidos en este intervalo de tiempo;

- 88 bits de un segundo paquete de fonía transmitido en entero; y

- 44 bits de un tercer paquete de fonía del que solamente la mitad de los bits son transmitidos en este intervalo de tiempo.

De acuerdo con una tercera manera, un intervalo de tiempo comprende, en este orden:

- 44 bits de un primer paquete de fonía del que solamente la mitad de los bits son transmitidos en este intervalo de tiempo;

- 88 bits de un segundo paquete de fonía transmitido en entero; y

- 66 bits de un tercer paquete transmitido del que solamente tres cuartos de los bits son transmitidos en este intervalo de tiempo.

De acuerdo con una cuarta y última manera, se colocan en un intervalo de tiempo y en este orden:

- 22 bits de un primer paquete de fonía del que solo un cuarto es transmitido en este intervalo de tiempo;

- 88 bits de un segundo paquete de fonía (datos contenidos en una trama de fonía) transmitido en entero; y

- 88 bits de un tercer paquete de fonía transmitido en entero.

Combinado estas cuatro maneras de repartir un grupo de 196 bits en un intervalo de tiempo radio, una tras otra, y renovando esta combinación una segunda vez, es posible transmitir 18 paquetes de fonía, indicados respectivamente por P1 a P18 en 8 intervalos de tiempo o sea una trama TDMA, como se presenta en el cronograma de la figura 3a y en la tabla de la figura 3b. Por razones de claridad, el cronograma de la figura 3a muestra solamente los intervalos de tiempo, indicados por T1 a T9, de una de las vías ascendente o descendente del canal de tráfico.

En la figura 4 está representado un esquema sinóptico de un terminal móvil de acuerdo con la invención. La antena 40 del terminal está unida a su etapa radio 41 correspondiente a la parte analógica del terminal.

En la parte de recepción, la señal en banda baja facilitada por la etapa radio 41 es facilitada a una unidad de sincronización 42 y a un desmodulador 43. La unidad 42 busca motivos de sincronización en la señal recibida. Ésta asegura la función de sincronización temporal del terminal. El desmodulador 43, que es sincronizado por la unidad 42, estima los símbolos transmitidos a partir de la señal en banda baja, y facilita estos símbolos estimados a un circuito 44 de tratamiento de la señal recibida.

En la parte de emisión, un circuito 45 de tratamiento de la señal que hay que emitir facilita símbolos que hay que emitir que son modulaos por un modulador 46. Éste facilita los símbolos modulados a la etapa radio 41.

Un generador de trama 47, que es sincronizado por la unidad 42, controla la etapa radio 41, el desmodulador 43 y el modulador 46 para colocar el terminal en modo recepción o en modo emisión en los intervalos de tiempo apropiados según la estructura de trama del sistema de radiocomunicaciones. En el caso del ejemplo de estructura de trama descrito en la figura 2, el terminal está alternativamente en modo emisión y en modo recepción, cambiando cada 20 ms. El generador de tramas 47 asegura igualmente la secuenciación del circuito 44 de tratamiento de la señal recibida, y la del circuito 45 de tratamiento de la señal que hay que emitir.

La figura 4 ilustra en cada uno de los bloques 44 y 45, circuitos respectivamente 51 y 52, y 53 y 54 de tratamiento de los canales lógicos respectivamente de tráfico y de señalización, que han sido citados anteriormente refiriéndose a la figura 2.

Cuando el terminal es emisor en una comunicación en curso, una primera vía A de un conmutador de dos vías 61 recibe secuencias de datos no encriptados m_i sucesivas, que son facilitadas por un codificador de palabra 62 a partir de la señal analógica producida por un micro 63 cuando un botón PTT (« Push-To-Talk ») del terminal es activado por el usuario.

La salida del conmutador 61 está unida a una primera entrada de un operador O-Exclusivo 56 para el cifrado de la secuencia mi. Una segunda entrada del operador 56 recibe una secuencia criptográfica SC_i generada por un generador de secuencia criptográfica 58, a través de un registro de desfase 57. La secuencia SC_i es generada por el generador 58 a partir de, por una parte, una clave de encriptado K secreta determinada y, por otra, del valor corriente IV_i de un vector de inicialización. Una unidad 55 de mando de sincronización criptográfica facilita al generador 58 el valor corriente IV_i del vector de inicialización.

El vector de inicialización IV_i varía en el tiempo y cambia de valor (paralelamente en el lado emisor y en el lado receptor) en cada renovación de la secuencia SC_i, es decir cada P paquetes de fonía. En un ejemplo simple, el valor del vector IV_i depende del valor del contador de intervalos de tiempo en la célula del terminal emisor. Naturalmente, cualquier otra evolución del valor del vector IV_i es posible, desde el momento en que esta ley es determinista a fin de poder ser seguida en paralelo por el terminal emisor y el o los terminales receptores.

La clave de encriptado K, por su parte, es constante para una comunicación determinada. Ésta es generada durante el establecimiento de la comunicación por un algoritmo de elección de clave de encriptado apropiada. Si es necesario, un índice que define esta clave puede ser transmitido en la señalización de establecimiento de llamada o ser transmitido en la secuencia de señalización inicial de la alternancia, y después en el canal de señalización asociada para la función de entrada tardía.

La salida del operador 56 facilita una secuencia de datos cifrados c_i que es facilitada al circuito 53 del circuito de tratamiento 45 a través de una primera vía A de un segundo conmutador 64 de dos vías.

La unidad 55 facilita una información de sincronización criptográfica CSI_i al circuito de tratamiento 45 de los datos que hay que emitir. Esta información de sincronización criptográfica es separada del valor del vector de inicialización IV_i utilizado para la generación de la secuencia SC_i que ha servido para el cifrado de la secuencia c_i. Ésta es emitida, bajo el control del generador de trama 47, al menos en un intervalo de tiempo de tráfico T al inicio de una alternancia, que en la estructura de trama viene inmediatamente antes del intervalo de tiempo en el cual la primera secuencia de datos cifrados c_i con i=0 es transmitida (sincronización criptográfica inicial). Para esta emisión “en la banda”, el circuito 53 es el que está activo. La información CSI_i es repetida también, con una periodicidad determinada (que puede ser variable en el transcurso de la duración de la comunicación), en intervalos de tiempo S determinados del canal de señalización asociada, para las secuencias de datos cifrados siguientes, es decir, las secuencias c_i con i diferente de 0 (sincronización periódica). Para estas emisiones “fuera de banda”, el circuito 54 es el que está activo.

Por otra parte, una información$\Delta 1_i$ de retardo de sincronización criptográfica es facilitada igualmente por la unidad 55 al circuito de tratamiento 45. Ésta es relativa, por una parte, a la diferencia temporal entre el inicio de la transmisión de los paquetes de datos cifrados de la secuencia c_i distinta de la primera y, por otra la transmisión de la información de sincronización criptográfica periódica CSI_i (para i diferente de 0). La información $\Delta 1_i$ es expresada preferentemente en número de intervalos de tiempo, porque ésta está codificada entonces solamente por tres bits (tomando valores de 0 a 7). Sin embargo, esto no es obligatorio. Ésta puede ser expresada también en número de paquetes de fonía. Ésta es emitida en el intervalo de tiempo S del canal de señalización asociada (preferentemente el mismo que aquél en el cual es transmitida la información de sincronización periódica CSI_i, porque es más simple, pero también puede tratarse de un intervalo de tiempo S diferente).

Cuando el terminal es receptor en una comunicación en curso, el circuito 51 del circuito de tratamiento de la señal recibida 44 facilita secuencias de datos cifrados c_i que son transmitidos en una segunda vía B del conmutador 61. Además, al inicio de la alternancia, el circuito 51 facilita a la unidad 55 la información de sincronización criptográfica CSI_i recibida en el canal de tráfico TCH. Después del inicio de la alternancia, el circuito 52 del circuito 44 es el que, al menos para ciertas secuencias c_i, facilita a la unidad 55 la información CSI_i así como la información $\Delta 1_i$, siendo recibidas éstas en el canal de señalización asociada SACCH.

El operador O-Exclusivo 56 recibe la secuencia c_i a través de la citada vía B del conmutador 61 y asegura su descifrado de una manera dual de aquélla en la que asegura el cifrado cuando el terminal es emisor. La salida del operador 56 facilita entonces una secuencia de datos no encriptados m_i que es facilitada a un descodificador de canal 65 a través de una segunda vía B del conmutador 64. El descodificador 65 facilita, a partir de la secuencia m_i, una señal analógica que es restituida en forma audible a través del altavoz 66.

Un valor IV_i del vector de inicialización es facilitado por la unidad 55 al generador 58 para cada secuencia c_i que hay que descifrar. Se observará que, en el lado del terminal receptor, el valor del vector de inicialización IV_i puede ser separado del valor de información de sincronización criptográfica CSI_i recibido. Sin embargo, el valor CSI_i adecuado solamente es recibido en al menos ciertos intervalos de tiempo S del canal SACCH, es decir para solamente algunas de las secuencias de datos cifrados que hay que descifrar. Son recibidas otras secuencias de datos cifrados c_i, para las cuales la información de sincronización criptográfica CSI_i correspondiente no es recibida.

Cuando la información de sincronización criptográfica CSI_i (para i diferente de 0) es recibida en un intervalo de tiempo S del canal SACCH, ésta es facilitada a la unidad 55 por el circuito 52. La información IV_i es separada de ésta por la unidad 55 y entonces es facilitada por la unidad 55 al generador 58. Además, el circuito 52 facilita entonces a la unidad 55 igualmente la información $\Delta 1_i$ antes citada. Un módulo 68 de mando de desfase de la unidad 55, genera entonces una información$\Delta 2_i$ a partir de la información$\Delta 1_i$. Esta información sirve para desfasar la secuencia criptográfica SC_i a fin de tener en cuenta, por una parte, la diferencia temporal entre el inicio de la transmisión de los paquetes de datos cifrados de la secuencia c_i distinta a la primera y, por otra, la transmisión de la información de sincronización criptográfica periódica CSI_i que se refiere a la secuencia c_i. La información $\Delta 2_i$ es expresada en número de bits que hay que desfasar. El desfase se efectúa controlando el registro de desfase 57 de modo apropiado, de una manera que está al alcance del especialista en la materia.

Cuando, a la inversa, una secuencia de datos cifrados c_i es recibida pero no la información de sincronización criptográfica CSI_i (siempre para i diferente de 0), que ha sido utilizada para el cifrado de la secuencia c_i, la información IV_i es generada, por una parte, por un módulo 67 de la unidad 55, denominado módulo de “rueda libre”, a partir del conocimiento del último valor IV_i separado de un valor SCI_i recibido y, por otra, de la ley de evolución del valor IV_i. Un módulo de este tipo pone en práctica un algoritmo reversible, denominado algoritmo de “rueda libre”, que en sí es conocido. Por reversible, se entiende el hecho de que éste puede cambiar en un sentido o en el otro, dando cada vez un valor de salida obtenido de modo determinista a partir del valor de entrada. Por consiguiente, si se le aplica una primera vez en un sentido determinado a un valor de entrada determinado, y después una segunda vez en sentido inverso al valor de salida obtenido anteriormente, se debe encontrar el citado valor de entrada determinado. Podrá referirse, por ejemplo, al retenido en el estándar del sistema PMR denominado Proyecto 25 – Fase I, de la APCO (del inglés “Association of Public-Safety Communications Officials-International, Inc”). Un algoritmo de este tipo explota el carácter determinista de la ley de evolución del valor del vector de inicialización.

Para resumir, los conmutadores 61 y 64 son gobernados de manera que su vía A respectiva sea activada cuando el terminal es emisor (caso representado en la figura), y que su vía B respectiva sea activada cuando el terminal es receptor.

En la figura 5, se ha representado un ejemplo de secuencia de etapas para la transmisión de una secuencia de datos cifrados determinada de acuerdo con el procedimiento de transmisión de la invención. Este procedimiento es puesto en práctica en un terminal móvil cuando éste es un emisor en una comunicación (es decir, el terminal que dispone de la alternancia en curso).

En una etapa 71, la unidad 55 genera el valor corriente del vector de inicialización IV_i, según una ley de evolución determinista. En un ejemplo de realización ventajoso, el valor IV_i corriente es función del valor del contador de intervalos de tiempo en la célula en que se encuentra el terminal emisor. El valor del contador de intervalos de tiempo es mantenido al día por la infraestructura de red para cada célula. Ésta es conocida por cada terminal móvil que esté en comunicación en esta célula. Este contador tiene la función de permitir la sincronización radio de los terminales con la estación de base de la célula.

En este ejemplo de realización, de supone que las diferentes células están sincronizadas entre sí, desde un punto de vista radio, de manera poco precisa, por ejemplo con la precisión facilitada por NTP (del inglés “Network Time Protocol”). Así pues, los valores de los contadores de intervalos de tiempo en las diferentes células, pueden ser diferentes, pero la diferencia entre estos valores es pequeña y puede estar limitada a priori.

Al inicio de una alternancia, la unidad 55 del terminal emisor genera un valor aleatorio codificado en Q1 bits, donde Q1 es un número entero determinado. Este valor es conservado en memoria durante toda la duración de la alternancia.

Como está ilustrado por el diagrama de la figura 6, cada valor del vector de inicialización IV_i resulta de la concatenación binaria de los Q1 bits de este valor aleatorio y de un número determinado Q2+Q3 de bits del valor corriente del contador de intervalos de tiempo, donde Q2 y Q3 son números enteros determinados. En el ejemplo representado, los Q1 bits del valor aleatorio forman los Q1 bits más significativos o MSB (del inglés “Most Significant Bits”) de IV_i, los Q3 bits menos significativos o LSB (del inglés “Least Significant Bits”) del valor del contador de intervalos de tiempo forman los Q3 LSB de IV_i, y los Q2 MSB del valor del contador de intervalos de tiempo forman los Q2 bits intermedios de IV_i. El vector de inicialización IV_i comprende por tanto un número Q determinado de bits, tal que Q=Q1+Q2+Q3.

La unidad 55 genera, también, la información de sincronización criptográfica CSI_i, al menos cuando esta información puede o debe ser transmitida. Se recuerda que el valor CSI_i es separado del valor IV_i. En el ejemplo representado en la figura 7, los Q1 bits del valor aleatorio forman los Q1 MSB de CSI_i, y los Q3 LSB del valor del contador de intervalos de tiempo forman los Q3 LSB de CSI_i, de modo que CSI_i es codificado en un número Q’ determinado de bits tal que Q’=Q1+Q3.

La sincronización al menos aproximada de los contadores de intervalos de tiempo de cada una de las células del terminal emisor y del terminal receptor, permite en efecto transmitir al terminal receptor solamente los Q3 LSB del valor del contador de la célula del terminal emisor (naturalmente, además del valor aleatorio codificado en Q1 bits). En efecto, el terminal receptor que se encuentra en una célula cualquiera del sistema puede entonces reconstituir la totalidad del valor del contador de intervalos de tiempo de la célula del terminal emisor a partir, por una parte, del valor del contador de intervalos de tiempo en su propia célula (de los cuales se tomarán los Q2 MSB, salvo en su caso una unidad) y, por otra, de los Q3 LSB recibidos.

La ventaja presentada por este método es que la variabilidad introducida por el contador de intervalos de tiempo se añade a la variabilidad del valor aleatorio generado por el terminal emisor. En efecto, esto aumenta el grado de seguridad sin aumento del tamaño del valor aleatorio que hay que generar. Además, este método garantiza una total protección contra lo que está en juego.

En variante, se puede transmitir en la información SCI_i la diferencia entre los valores de los contadores de intervalos de tiempo en las células respectivas del terminal emisor y del terminal receptor, en lugar de transmitir los LSB del valor del contador de intervalos de tiempo en la célula del terminal emisor.

Se observará que la ley de evolución del vector de inicialización IV_i es determinista en el sentido de que, conociendo un valor del vector en un instante dado, se puede deducir su valor IV_j en un instante posterior (con j>i), en función de la evolución del valor del contador de intervalos de tiempo en la célula del terminal emisor. Se observará igualmente que el valor aleatorio inicial debe ser transmitido cada vez en el valor CSI_i a fin de permitir la entrada tardía de otros terminales.

Volviendo a la figura 5, el generador 58 produce la secuencia criptográfica SC_i corriente en una etapa 72, según la relación ya dada anteriormente:

$$SC_i = E_K(IV_i) \quad (1)$$

donde E_K designa el cifrado de la información IV_i con la clave K, según el algoritmo de cifrado determinado que es el mismo par todos los terminales móviles del sistema, y que, naturalmente, es el mismo que el terminal sea emisor o sea receptor. La secuencia SC_i es almacenada en el registro 57 a medida que se produce su generación.

Cuando la secuencia SC_i es totalmente disponible, entonces, en una etapa 73, el operador 56 efectúa la operación O-Exclusivo bit a bit entre los N bits de la secuencia SC_i y un número idéntico PxM de bits que provienen de P paquetes de fonía consecutivos que forman una secuencia de datos no encriptados m_i de PxM bits (siendo almacenados estos PxM bits en un registro de desfase apropiado, no representado).

Se distingue después el caso de la primera secuencia de datos cifrados, es decir cuando i es igual a 0, que corresponde a la sincronización criptográfica inicial (al inicio de la alternancia), del caso de las secuencias de datos cifrados siguientes, es decir cuando i es diferente de 0, que corresponde a la sincronización criptográfica periódica.

Considérese en primer lugar el caso en que i es igual a cero (i=0). En este ejemplo, el intervalo de tiempo 2 (véase la figura 2) de una trama TDMA dada lleva la petición de la alternancia (inicio de transmisión por el terminal emisor). La información de sincronización criptográfica inicial CSI_0 es transmitida entonces, en una etapa 74, en uno o varios de los intervalos de tiempo T siguientes, por ejemplo los dos intervalos de tiempo 3 y 4, siendo repetida ésta varias veces (por ejemplo tantas veces como su longitud lo permita, habida cuenta de los bits de señalización que hay que transmitir además de los bits útiles, sabiendo que un intervalo de tiempo de 20 ms puede contener como máximo 320 bits con un caudal de 16 Kbits/s).

La secuencia de datos cifrados c_0 es transmitida entonces, en una etapa 75, a partir del intervalo de tiempo T siguiente, en este caso el intervalo de tiempo 5. Este intervalo de tiempo contiene las dos primeras tramas de fonía, así como un cuarto de trama de fonía siguiente (véase la tabla de la figura 3b). Se observará que en el caso en que la primera información de fonía transmitida en un intervalo de tiempo determinado corresponda a una trama de fonía incompleta (por ejemplo intervalos de tiempo 2, 3, 4, 6, 7, 8, 11, 12, etc.), la primera trama de fonía es preferentemente insertada en este intervalo de tiempo determinado a partir de la primera posición temporal tal que la primera trama de fonía será transmitida completamente en este intervalo de tiempo (se hace referencia al diagrama y a la tabla de las figuras 3a y 3b, respectivamente). De esta manera, se asegura que las informaciones de fonía transmitidas hasta el intervalo de tiempo de señalización S siguiente corresponden siempre a un número entero de tramas de fonía. Esto simplifica la determinación de la información $\Delta 2_i$ para la sincronización periódica (véase más adelante).

Dicho de otro modo, la transmisión de fonía va por tanto precedida por una transmisión en la banda de la información de sincronización criptográfica inicial. Esta transmisión no genera en general ninguna degradación de calidad de la fonía, porque ésta se produce durante un período de tiempo que sirve para el cálculo por el codificador de palabra de las primeras tramas de fonía que hay que transmitir.

Considérese ahora el caso en que i sea diferente de cero. Se observa en primer lugar que las secuencia criptográficas CS_i y por tanto las secuencias de datos cifrados c_i tienen preferentemente una longitud en bits igual a la duración que separa dos intervalos de tiempo S consagrados a la señalización (habida cuenta del caudal útil en el canal). Así, la posición de las secuencias c_i es fija con respecto a los intervalos de tiempo S en el transcurso de una alternancia determinada. Pero esta posición varía de una alternancia a la otra. En el ejemplo considerado anteriormente, las secuencias c_i van del intervalo de tiempo 5 al intervalo de tiempo 13, del intervalo de tiempo 14 al intervalo de tiempo 22, etc

En una etapa 76, la secuencia de datos cifrados corriente c_i es transmitida a partir de un intervalo de tiempo del canal de tráfico TCH, aquí el intervalo 14 para la segunda secuencia c_1 (i=1), el intervalo 23 para la tercera secuencia c_2 (i=2), etc, habida cuenta de la hipótesis hecha anteriormente.

Cuando existen las condiciones para que la información de sincronización criptográfica sea transmitida, el valor CSI_i es transmitido también, en una etapa 77, en el interior del intervalo de tiempo S determinado del canal de señalización asociada SACCH. En un ejemplo, el citado intervalo de tiempo S determinado es el intervalo de tiempo S que viene en la estructura de trama inmediatamente antes, o el primer intervalo de tiempo del segundo tipo que viene en la estructura de ramas después del intervalo de tiempo T a partir del cual la secuencia c_i es transmitida. Se trata así del intervalo 9 (para i=1), del intervalo 18 (para i=2), etc. Gracias a esta característica, la información CSI_i y la secuencia c_j son transmitidas en intervalos de tiempo lo más próximos posibles, lo que simplifica su tratamiento por el terminal receptor.

En la etapa 77, la información $\Delta 2_i$ es también transmitida en un intervalo de tiempo S del canal SACCH, preferentemente el mismo que aquél en el cual la información CSI_i es transmitida. De esta manera, la información

$\Delta 1_i$ es recibida por el receptor sensiblemente al mismo tiempo que la información CS_i. Esto simplifica el tratamiento por el terminal receptor, y garantiza un retardo mínimo durante la entrada tardía de un nuevo terminal receptor en la comunicación, puesto que todas las informaciones que se necesitan para descifrar la secuencia c_i le llegan en un período de tiempo lo más reducido posible.

En un ejemplo ventajoso, la información $\Delta 1_i$ es el número de intervalos de tiempo T del canal de tráfico TCH que separan el intervalo de tiempo T a partir del cual la secuencia c_i es transmitida en una trama determinada, y el intervalo de tiempo S del canal SACCH en el cual la información CSI_i igual que la información $\Delta 1_i$ son transmitidas. En el ejemplo considerado anteriormente, este número es igual a cuatro (9-5=4; 18-14=4, etc.). Esto es ventajoso porque el valor de $\Delta 1_i$ está así comprendido entre 0 (cuando la información CSI_i y la información $\Delta 1_i$ son transmitidas en el intervalo de tiempo S que viene en la estructura de trama inmediatamente antes del intervalo de tiempo T a partir del cual la secuencia c_i es transmitida) y 7. Así pues, el valor $\Delta 1_i$ puede ser codificado con 3 bits solamente. Se observará que si el valor $\Delta 1_i$ fuera contado en número de paquetes de fonía (lo que constituye una variante posible), ésta podría tomar un valor entre 0 y 16, y por tanto debería ser codificada con 4 bits.

Las etapas anteriores son repetidas para cada secuencia de datos no encriptados m_i durante la alternancia en curso.

La figura 8 es un diagrama que ilustra la transmisión, en una supertrama determinada, de las cuatro primeras secuencias de datos cifrados c_0 a c_3, de una alternancia determinada, por un terminal emisor determinado, de acuerdo con el ejemplo considerado en lo que precede. La extensión de los datos cifrados de cada secuencia en la supertrama está simbolizada por flechas horizontales respectivas, que están en trazo continuo en relación con los intervalos de tiempo del canal de tráfico en los cuales son emitidos datos, y en trazo discontinuo si no.

De acuerdo con este ejemplo, se transmiten por la vía ascendente: la petición de alternancia en el intervalo de tiempo 2; la información de sincronización inicial CSI_0 en los intervalos de tiempo 3 y 4; las secuencias c_0, c_1, c_2 y c_3 a partir, respectivamente, de los intervalos de tiempo 5, 14, 23 y 32; la información de sincronización periódica CSI_1 y la información relativa al desfase temporal $\Delta 1_1$ correspondiente en el intervalo de tiempo de señalización 18; así como la información de sincronización periódica CSI_3 y la información relativa al desfase temporal $\Delta 1_3$ correspondiente en el intervalo de tiempo se señalización 36. Se recuerda que en este ejemplo las informaciones $\Delta 1_1$ y $\Delta 1_3$ son iguales a 4. Se observará que la transmisión de la secuencia c_3 continúa en la supertrama siguiente (no representada).

En la figura 9, se ilustra la recepción de las mismas secuencias de datos cifrados c_0, c_1, c_2 y c_3 por el terminal receptor en una supertrama determinada.

La encapsulación de los datos en la supertrama considerada es gestionada por la estación de base. Habida cuenta de la diferencia de sincronización radio entre la célula del terminal emisor y la del terminal receptor, puede ocurrir, como es el caso en el ejemplo representado, que exista un desfase de números de intervalos de tiempo entre los datos recibidos por la estación de base de la célula del terminal emisor y los transmitidos por la estación de base de la célula del terminal receptor.

En este ejemplo, en efecto, la petición de alternancia (acordada) del emisor es recibida en la célula del receptor en el intervalo de tiempo 3. Asimismo, las informaciones CSI_0 son recibidas en los intervalos de tiempo 4 y 5. Las secuencias c_0, c_1, c_2 y c_3 son recibidas a partir, respectivamente, de los intervalos de tiempo 6, 15, 24 y 33. Sin embargo, la información de sincronización criptográfica periódica CSI_1 y la información relativa al desfase temporal $\Delta 1_1$ correspondiente son siempre recibidas en el intervalo de tiempo de señalización 18. Asimismo, la información de sincronización periódica CSI_3 y la información relativa al desfase temporal $\Delta 1_3$ correspondiente son recibidas siempre en el intervalo de tiempo de señalización 36. Por esta razón, el valor de las informaciones $\Delta 1_1$ y $\Delta 1_3$ es modificado por la infraestructura fija de modo que se tenga en cuenta la disposición de las secuencias de datos cifrados en la supertrama en la célula del terminal receptor. En este ejemplo, su valor es cambiado de 4 a 3.

Se va a describir ahora el descifrado de una secuencia de datos cifrados por el terminal receptor, de acuerdo con otro aspecto de la invención, refiriéndose al diagrama de etapas de la figura 10.

En una etapa 81, el terminal receptor recibe una secuencia de datos cifrados c_i en el canal de tráfico, a partir de un intervalo de tiempo T determinado, en una supertrama determinada. Esta secuencia es facilitada por el circuito 51 del circuito 44 de tratamiento de los datos recibidos. Si la secuencia c_i es recibida a partir de uno de los intervalos de tiempo 1, 10, 19 y 29, es decir el primer intervalo de tiempo de una de las cuatro tramas de la citada supertrama determinada, se solicita entonces, en una etapa 82, si se ha recibido la información de sincronización CSI_i (y por

tanto también la información $\Delta 1_1$) en el intervalo de tiempo de señalización S precedente, a saber, respectivamente el intervalo de tiempo 36 de la trama precedente, el intervalo 9, el intervalo 18 o el intervalo 27. Si, por el contrario, la secuencia c_i es recibida a partir de otro de los intervalos de tiempo de tráfico T de la supertrama, entonces, en la etapa 82, se pregunta si se ha recibido la información de sincronización CSI_i (y por tanto también la información $\Delta 1_1$) en el intervalo de tiempo de señalización S siguiente, a saber uno de los intervalos 9, 18, 27, y 36.

Si la respuesta a la pregunta de la prueba 82 es sí, entonces, en una etapa 83, la unidad 55 genera el valor corriente IV_i del vector de inicialización a partir del valor de la información CSI_i recibida. Para esto, se consideran los Q3 LSB y los Q1 MSB del valor CSI_i recibido, que forman respectivamente, por una parte, los Q3 LSB y los Q1 MSB del valor IV_i y, por otra, los Q2 MSB del valor del contador de intervalos de tiempo en la célula considerada (la del terminal receptor), que forman los Q2 bits intermedios del valor IV_i. El lector puede referirse a la descripción anterior de las figuras 6 y 7.

Si, por el contrario, la respuesta a esta pregunta es no, entonces, en una etapa 84, el valor corriente IV_i es generado por el módulo de "rueda libre" 67 de la unidad 55. Se observará que en realidad el valor $\Delta 1_1$ es constante para toda la duración de la alternancia en curso, de modo que el terminal que es parte de la comunicación puede conservar en memoria el valor recibido inicialmente, es decir al inicio de la alternancia, y no tener en cuenta los valores recibidos a continuación durante la misma alternancia.

Se observará que la puesta en práctica de la etapa 84 anterior solamente es posible para un terminal receptor que es ya parte de la comunicación, y no para un terminal receptor en fase de entrada tardía. Tal terminal deberá esperar a la recepción efectiva de la información CSI_i (y por tanto también la información $\Delta 1_1$) para poder comenzar a descifrar las secuencias de datos cifrados recibidos. Por esta razón, en la figura, el camino que pasa por el bloque que simboliza la etapa 84 está representado en trazos discontinuos. Se observará sin embargo que, de acuerdo con la invención, no siendo recibida la información CSI_i por robo de trama, sino en intervalos de tiempo de señalización, la periodicidad de la emisión de esta información puede ser, sin inconveniente alguno, más elevada que en la técnica anterior. La única limitación es la disponibilidad de recursos en el canal de señalización asociada SACCH.

En una etapa 85, el generador 58 genera a continuación a secuencia criptográfica SC_i a partir del valor corriente del vector de inicialización IV_i producido en la etapa 83 o en la etapa 84, según la relación (1) dada en la introducción. Paralelamente a las etapas 82 a 85, la unidad 55 genera la información $\Delta 2_i$ a partir de la información $\Delta 1_i$ corriente. Se observará que, lo mismo que para la información $\Delta 1_i$ (véase el párrafo anterior), el valor de la información $\Delta 2_i$ es constante para toda la duración de la alternancia en curso. Así pues, la etapa 85 solamente puede ser ejecutada una sola vez al inicio de la alternancia por un terminal receptor, o durante la entrada tardía en la comunicación, según el caso. A continuación, el valor $\Delta 2_i$ puede ser conservado en memoria hasta el inicio de la alternancia siguiente.

La generación de la información $\Delta 2_i$ a partir de la información $\Delta 1_i$ vuelve a convertir la información $\Delta 1_i$ expresada en número de intervalos de tiempo en una información $\Delta 2_i$ correspondiente expresada en número de paquetes de fonía. Esta conversión puede ser efectuada con la ayuda de una tabla de valores almacenada en memoria, que está ilustrada por la tabla de la figura 11. Esta tabla se comprende considerando el diagrama y la tabla de la figuras respectivamente 3a y 3b.

En una etapa 87, el operador O-Exclusivo 56 restituye la secuencia de datos no encriptados m_i a partir de la secuencia de datos cifrados c_i y de la secuencia criptográfica SC_i, según la relación (3) dada en la introducción, y en función además de la información $\Delta 2_i$. De modo más exacto, la secuencia SC_i es combinada con la secuencia c_i después del desfase de sus bits hacia la derecha un número de bits igual a $\Delta 2_i \times \frac{N}{P}$, donde se recuerda que N designa la longitud en número de bits de la secuencia SC_i, y P designa el número de tramas de fonía en una trama TDMA. Esto es realizado simplemente por medio de un puntero en el registro de desfase 57, que está desfasado $\Delta 2_i \times \frac{N}{P}$, filas en el registro. De este desfase resulta que, para un terminal entrante de manera tardía en la comunicación, mientras que una alternancia está en curso, los paquetes de fonía de la secuencia c_i que han sido recibidos antes del intervalo de tiempo S en el cual la información CSI_i y la información $\Delta 1_i$ son recibidas por primera vez, no son descifradas. Se observará que todas las secuencias de datos cifrados recibidas posteriormente son sin embargo descifradas en su integridad.

La figura 12 ilustra una configuración de cambio de célula ("handover") concerniente a un terminal móvil receptor MTR que está en comunicación con un terminal móvil emisor MTE. Se supone que el terminal MTR se encuentra en

una célula A (célula de origen) y se dirige hacia otra célula B (célula blanco), y que el terminal MTE se encuentra en una tercera célula C. Cada una de las células A, B y C está cubierta, desde el punto de vista radio, por una estación de base respectivamente BTSA, BTSB y BTSC. Estas estaciones de base están unidas a la red de infraestructura fija del sistema de radiocomunicaciones celular.

Refiriéndose a la configuración de la figura 12, se va presentar ahora una solución para mantener la sincronización criptográfica durante el "handover" de un terminal receptor en el transcurso de una comunicación cifrada de principio a fin.

Durante el "handover" del terminal MTR, de la célula A hacia la célula B, un técnica de acuerdo con la técnica anterior clásica consistiría en facilitar al terminal MTR, en el mando de cambio de célula transmitido en el canal de señalización asociada, únicamente las informaciones puramente radio que le permiten sincronizarse desde un punto de vista radio con el canal deseado en la célula B. Una vez en la célula B, el terminal debería esperar a la recepción de las informaciones de sincronización criptográfica transmitidas por la técnica descrita anteriormente para realizar la sincronización criptográfica. Hasta la recepción de esta información, el terminal MTR no podría descifrar los datos recibidos, de modo que la comunicación quedaría cortada y esto aunque el "handover" se haya realizado de modo satisfactorio. Esta técnica se traduce por tanto en una sincronización criptográfica tardía, en razón de esta espera de la información de sincronización criptográfica en el canal de tráfico en la célula blanco, y por tanto en un corte de la comunicación mucho más largo que el debido al "handover" propiamente dicho.

En un modo de realización de la invención, se utilizan de nuevo los contadores de intervalos de tiempo en la célula fuente y en la célula blanco para resolver este problema. Conviene observar en este caso que el contador de intervalos de tiempo tiene en cuenta los intervalos de tiempo elementales, y no los intervalos de tiempo compuestos de la estructura de la trama. Por consiguiente, el número de intervalos de tiempo que en este caso hay que considerar, salvo mención en contrario, se refiere al número de intervalos de tiempo elementales, es decir teniendo en cuenta los intervalos de tiempo a la vez en la vía ascendente y en la vía descendente. Por ejemplo, la longitud de una trama TDMA corresponde así a 72 unidades (36x2) del contador de intervalos de tiempo de la célula considerada.

Sustancialmente, la estación de base BTSA facilita al terminal MTR en el mando de cambio de célula transmitido por el canal de señalización asociada de la célula A, además de las informaciones de naturaleza radioeléctrica que le permite sincronizarse con el canal deseado de la célula B, una información relativa al desfase de sincronización criptográfica entre la célula fuente y la célula blanco, que es obtenido de la manera que va a exponerse. Esta información se expresa como la diferencia Δ_{CPT} entre los respectivos contadores de intervalos de tiempo de la célula fuente y de la célula blanco.

La estación de base BTBS de la célula B comienza a recibir de la red, durante una fase transitoria del procedimiento de cambio de célula, paquetes de fonía cifrados que están destinados a ser emitidos por la vía descendente del canal que va a llevar la comunicación a la célula B entre ella misma y el terminal MTR (en lo sucesivo canal blanco). Estos paquetes de fonía llevan una estampilla temporal insertada por la red para permitir verificar su correcta secuenciación y la ausencia de pérdida. Ésta es necesaria en razón del hecho de que el tiempo de transferencia de los paquetes de fonía a través de la red puede ser variable de un paquete a otro, y de que además ciertos paquetes pueden perderse durante la transmisión a través de la red. Esta estampilla temporal es naturalmente sincronizada con el valor del contador de intervalos de tiempo de la célula A.

La estación BTSB retransmite entonces hacia la estación de base BTSA de la célula A una información compuesta, por una parte, por el valor del contador de intervalos de tiempo en la célula B correspondiente a la transmisión por el canal blanco de un paquete de fonía determinado, que haya sido recibido de la red y, por otra, por la estampilla temporal correspondiente llevada por el citado primer paquete de fonía recibido.

Sobre la base de esta información, la estación de base BTSA de la célula fuente puede calcular fácilmente el desfase de sincronización criptográfica entre las dos estaciones de base comparando el valor recibido con el valor CA_i de su propio contador de intervalos de tiempo correspondiente al intervalo de tiempo del paquete de fonía considerado (es decir, correspondiente a una estampilla temporal dada). Ésta transmite entones una información de desfase de sincronización criptográfica al terminal MTR en el mando de cambio de célula. Un convenio posible es transmitir la diferencia Δ_{CPT} entre los valores CB_i y CA_i respectivamente del contador de número de intervalos de tiempo en la célula blanco B y del contador de número de intervalos de tiempo en el célula fuente A, correspondiente por ejemplo al inicio de la misma secuencia criptográfica es decir al intervalo de tiempo S en el interior del cual un información de sincronización criptográfica CSI_i ha sido o abría podido ser transmitida.

Esta diferencia Δ_{CPT} es fácil de obtener en función de las informaciones transmitidas por la estación de base BTSB de la célula blanco a la estación de base BTSA de la célula fuente como se indicó anteriormente. Dicho de otro modo, si el mando de cambio de célula es transmitido en el transcurso del intervalo de tiempo de señalización para el cual el contador de intervalos de tiempo en la célula fuente A vale CA_i, correspondiente al intervalo de tiempo en el interior del cual habría sido transmitida la información de sincronización criptográfica CSI_i para una secuencia

criptográfica SC_i determinada, el valor de la información de desfase de sincronización criptográfica Δ_{CPT} transmitida con el mando de cambio de célula es entones igual a CB_i-CA_i, donde CB_i es el valor del contador de intervalos de tiempo en la célula blanco B al inicio de la misma secuencia criptográfica SC_i.

El terminal MTR conoce, por escrutinio de las células próximas y en particular de la célula blanco B, el valor del contador de intervalos de tiempo en cada una de estas células, éste es capaz entonces de determinar, gracias a la utilización del algoritmo de "rueda libre", el valor de la información de sincronización criptográfica CS_i que hay que utilizar para el descifrado de una secuencia de datos cifrados c_i recibida a través del canal blanco (es decir, el canal asignado a la comunicación en la célula B), y la posición temporal del inicio de la secuencia criptográfica a la cual corresponde este valor (y que normalmente es determinada por la información que es indicada por $\Delta 1_i$ en lo que precede). Éste puede sincronizarse entonces inmediatamente no solamente desde el punto de vista radio, sino igualmente desde el punto de vista de la criptografía de principio a fin, y esto sin esperar a la recepción efectiva de una información de sincronización criptográfica CSI_i. Se evita así cualquier corte de comunicación suplementario perjudicial para la calidad de servicio.

El diagrama de la figura 13 ilustra una secuencia de etapas de un algoritmo que permite mantener la sincronización criptográfica para el terminal MTR entre las células A y B.

Antes de abandonar la célula A, el terminal MTR recibe, en una etapa 91, una información de desfase de sincronización criptográfica Δ_{CPT}, relativa al desfase de sincronización criptográfica entre la célula fuente A y la célula blanco B. Esta información Δ_{CPT} es transmitida por la estación de base BTSA de la célula A como se ha dicho anteriormente. En un ejemplo, la información Δ_{CPT} es transmitida por la estación de base BTSA al terminal MTR con el mando de cambio de célula en un intervalo de tiempo S determinado en el canal de transmisión asignado a la comunicación en la célula A.

En una etapa 92, el terminal MTR memoriza el valor de una primera información de sincronización criptográfica CSI_i determinada, que puede ser simplemente el valor corriente de la información de sincronización criptográfica en el momento en que el mando de cambio de célula es recibido. Éste memoriza igualmente el valor CB_i del contador de intervalos de tiempo de la célula fuente B correspondiente al intervalo de tiempo S en el cual la información CSI_i ha sido recibida (en el caso en que éste sea un valor que ha sido generado por medio del algoritmo de "rueda libre"). Este valor CB_i es obtenido añadiendo el valor Δ_{CPT} al valor CA_i, es decir haciendo $CB_i = CA_i + \Delta_{CPT}$.

En una etapa 93, el terminal MTR efectúa el cambio de célula. Por consiguiente, éste pasa del canal de transmisión asignado a la comunicación en la célula A al canal de transmisión asignado a la comunicación en la célula B.

En una etapa 94, éste recibe una secuencia de paquetes de datos cifrados c_j determinada, en el interior de un intervalo de tiempo T determinado en el canal de transmisión asignado a la comunicación en la célula B. Se trata de la primera secuencia de paquetes de datos cifrados que recibe después de su transferencia a la célula B.

Si el terminal MTR recibe igualmente el valor de la información de sincronización criptográfica CSI_j que hay que utilizar para el cifrado de la secuencia c_j (y por consiguiente, igualmente el valor de la información de retardo de sincronización criptográfica $\Delta 1_j$ asociada correspondiente), entonces, en una etapa 95, éste efectúa el descifrado de la secuencia cj a partir de los valores CSI_j y $\Delta 1_j$ recibidos. Este descifrado tiene lugar de la manera anteriormente indicada (refiriéndose al diagrama de la figura 10). Éste es el caso, por ejemplo, de la secuencia c_1 o de la secuencia c_3 en la figura 9.

En ausencia de recepción de los valores CS_j y $\Delta 1_j$, el terminal MTR determina, en una etapa 96, el valor CSI_j así como el valor $\Delta 1_j$, a partir del valor CB_i del contador de intervalos de tiempo en la célula fuente y del valor de la información de sincronización criptográfica CSI_j, que éste ha memorizado en la etapa 92, y a partir además del valor CB_j del contador de intervalos de tiempo correspondiente al intervalo de tiempo S en el cual la información de sincronización criptográfica CSI_j habría podido ser recibida en el canal de transmisión asignado a la comunicación en la célula B. Éste es el caso, por ejemplo, de la secuencia c_2 en la figura 9, siendo el intervalo de tiempo S en el cual la información de sincronización criptográfica CSI_2 habría podido ser recibida, el intervalo 27 en esta figura. Después, el terminal salta a la etapa 95, en la cual efectúa el cifrado de la secuencia cj a partir de los valores CSI_j y $\Delta 1_j$ que así han sido determinados.

A continuación se da un ejemplo de las operaciones detalladas que son efectuadas durante la etapa de determinación 96.

Al llegar a la célula B, el terminal MTR determina el valor CB_j del contador de intervalos de tiempo en la célula B, que corresponde al intervalo de tiempo en el que habría sido emitida la información de sincronización criptográfica CSI_j antes de su llegada a la célula B.

El terminal MTR calcula a continuación la diferencia $\Delta_{CPT'} = CB_j - CB_i$ que puede ser positiva (lo que significa que la secuencia criptográfica SCj ha comenzado en el pasado) o negativa (lo que significa que la secuencia criptográfica SC_j comenzará en el futuro).

El terminal efectúa entonces la división euclidiana de $\Delta_{CPT'}$ por el número 2xP de intervalos de tiempo (elementales) que separan dos intervalos de tiempo de señalización S en la estructura de trama, y que corresponde igualmente a la longitud de una secuencia criptográfica. Se recuerda que, en el ejemplo aquí considerado, 2xP es igual a 72. El divisor es denominado Δ_S y el resto es denominado Δ_{IT} en lo que sigue. Dicho de otro modo, se tiene la relación:

$$\Delta_{CPT'} = \Delta_S x(2xP) + \Delta_{IT}$$

El terminal MTR hace entonces cambiar el algoritmo de "rueda libre" del módulo 67 de la unidad 55 un número de veces igual a Δ_S (aplicando el algoritmo Δ_S veces si Δ_S es positivo o el algoritmo inverso un número de veces igual a abs(Δ_S) si Δ_S es negativo). El resultado da un nuevo valor del vector de inicialización IV_j que permite al generador 58 generar una nueva información de sincronización criptográfica SC_j.

El resto Δ_{IT} (contado en intervalos de tiempo elementales) es dividido por dos para obtener el desfase en intervalos de tiempo compuestos correspondientes al número de intervalos de tiempo (elementales) en la única vía descendente del canal de transmisión (en el caso de un sistema TDMA de orden 2 correspondiente al ejemplo considerado en este caso). Este valor $\Delta_{IT} / 2$ es el valor de la información de retardo de sincronización criptográfica $\Delta 1_j$ correspondiente a la secuencia criptográfica SC_j).

Dicho de otro modo, el terminal se sincroniza desde el punto de vista de la criptografía a partir de la información de sincronización criptográfica CSIj y de la información de retardo de sincronización criptográfica $\Delta 1_j = \Delta_{IT} / 2$, así obtenidas, que habían sido recibidas de una manera asociada a la secuencia de paquetes de datos cifrados cj. No hay por tanto ningún retardo de reestablecimiento de la comunicación en la célula B debido a la sincronización criptográfica.

REIVINDICACIONES

1. Procedimiento de transmisión de datos cifrados entre un terminal móvil emisor (MTE) y al menos un terminal móvil receptor (MTR) de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio con una estructura de trama en la cual una trama TDMA comprende intervalos de tiempo (T) de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo (S) de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización

según el cual secuencia (c_i) de paquetes de datos cifrados es transmitida en el canal de tráfico a partir de un intervalo de tiempo del primer tipo (14, 32) determinado, mientras que una información de sincronización criptográfica (CSI_i) asociada es transmitida en el canal de señalización asociada en el interior de un intervalo de tiempo del segundo tipo (18, 36) determinado,

y según el cual una información ($\Delta 1_i$) de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el citado intervalo de tiempo del primer tipo determinado, es igualmente transmitida en el canal de señalización asociada.

2. Procedimiento de transmisión de acuerdo con la reivindicación 1, según el cual el valor de la información de sincronización criptográfica es separado del valor de un vector de inicialización (IV_i) que haya servido para generar una secuencia criptográfica (SC_i) utilizada para el cifrado de la citada secuencia de paquetes de datos cifrados.

3. Procedimiento de transmisión de acuerdo con la reivindicación 2, según el cual la longitud de la secuencia criptográfica es igual a un número entero N determinado de bits, que corresponde al número de bits útiles transmitidos entre dos intervalos de tiempo del segundo tipo consecutivos en los cuales puede ser transmitida una información de sincronización criptográfica.

4. Procedimiento de transmisión de acuerdo con la reivindicación 3, según el cual el número N es un múltiplo entero de un número entero M determinado que corresponde al número de bits de un paquete de datos cifrado.

5. Procedimiento de transmisión de acuerdo con una cualquiera de las reivindicaciones precedentes, según el cual la citada información de retardo de sincronización criptográfica es el número de intervalos de tiempo del primer tipo que separa el citado intervalo de tiempo del primer tipo determinado y el citado intervalo de tiempo del segundo tipo determinado.

6. Procedimiento de transmisión de acuerdo con una cualquiera de las reivindicaciones precedentes, según el cual la citada información de retardo de sincronización criptográfica es transmitida en el interior del citado intervalo de tiempo del segundo tipo determinado con la citada información de sincronización criptográfica.

7. Procedimiento de transmisión de acuerdo con una cualquiera de las reivindicaciones precedentes, según el cual el citado intervalo de tiempo del segundo tipo (18, 36) determinado es el intervalo de tiempo del segundo tipo que viene en la estructura de trama inmediatamente anterior, o el primer intervalo de tiempo del segundo tipo que viene en la estructura de trama después del citado intervalo de tiempo del primer tipo determinado (14, 32).

8. Procedimiento de transmisión de acuerdo con una cualquiera de las reivindicaciones precedentes, según el cual el valor de la información de sincronización criptográfica es inicializado, al inicio de una alternancia, en un valor determinado codificado en un número entero Q determinado de bits, y obtenido como la concatenación binaria de, por una parte, un número entero Q1 determinado de primeros bits que codifican un valor aleatorio y, por otra, un número Q2 determinado de segundos bits que son los bits de peso más pequeño del valor de un contador de intervalos de tiempo, dónde Q, Q1 y Q2 son números enteros determinados.

9. Procedimiento de descifrado de una secuencia de paquetes de datos cifrados (c_i) transmitida entre un terminal móvil emisor (MTE) y al menos un terminal móvil receptor (MTR) de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio con una estructura de trama en la cual una trama TDMA comprende intervalos de tiempo (T) de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo (S) de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, que comprende las etapas consistentes en:

a) recibir la citada secuencia de paquetes de datos cifrados a partir de un intervalo de tiempo del primer tipo (6, 15, 24, 33) determinado;

b) recibir una información de sincronización criptográfica (CSI_i) asociada en el canal de señalización asociada, en el interior de un intervalo de tiempo del segundo tipo (18, 36) determinado, y

c) recibir igualmente, en el canal de señalización asociada, una información ($\Delta 1_i$) de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el intervalo de tiempo del primer tipo determinado;

d) generar un valor (IV_i) de un vector de inicialización que haya servido para generar una secuencia criptográfica (SC_i) utilizada para el cifrado de la citada secuencia de paquetes de datos cifrados;

e) generar la misma secuencia criptográfica (SC_i), a partir del valor del vector de señalización generado en la etapa d);

f) desfasar la secuencia criptográfica generada en la etapa e), en función de la citada información ($\Delta 1_i$) de retardo de sincronización criptográfica; y

g) descifrar la citada secuencia de paquetes de datos cifrados (c_i) a partir de la citada secuencia criptográfica desfasada

10. Procedimiento de descifrado de acuerdo con la reivindicación 9, según el cual, en la etapa d), el valor (IV_i) del vector de inicialización es separado del valor de la información de sincronización criptográfica (CS_i) recibido en la etapa b).

11. Procedimiento de descifrado de acuerdo con la reivindicación 9, según el cual, en ausencia de recepción del valor de la información de sincronización criptográfica (CS_i) de conformidad con la etapa b), el valor (IV_i) del vector de inicialización es generado, en la etapa d), con la ayuda de un algoritmo de “rueda libre” a partir de un valor de la información de sincronización criptográfica.

12. Procedimiento de descifrado de acuerdo con una cualquiera de las reivindicaciones 9 a 11, según el cual, siendo expresada la información ($\Delta 1_i$) de retardo de sincronización criptográfica en número de intervalos de tiempo, la etapa f) comprende la generación de una información ($\Delta 2_i$) correspondiente expresada en número de paquetes de datos.

13. Procedimiento de descifrado de acuerdo con una cualquiera de las reivindicaciones 9 a 12, según el cual, durante un cambio de célula del terminal móvil receptor, de una célula fuente (A) determinada hacia una célula blanco (B) determinada, el terminal móvil receptor:

h) recibe una información de desfase de sincronización criptográfica (Δ_{CPT}), relativa al desfase de sincronización criptográfica entre la célula fuente y la célula blanco, que es transmitida con el mando de cambio de célula en un intervalo de tiempo del segundo tipo determinado en el canal de transmisión asignado a la comunicación en la célula fuente;

i) memoriza el valor de una primera información de sincronización criptográfica (CSI_i) determinada y un primer valor (CB_i) del contador de intervalos de tiempo de la célula blanco correspondiente al intervalo de tiempo del segundo tipo en el cual habría podido ser recibida la citada información de sincronización criptográfica;

j) efectúa el cambio de célula;

k) recibe una secuencia de paquetes de datos cifrados (c_i) determinada, a partir de un intervalo de tiempo del primer tipo (24) determinado en el canal de transmisión asignado a la comunicación en la célula blanco, y

l) en ausencia de recepción de acuerdo con la etapa b) del valor de una segunda información de sincronización criptográfica (CS_i), que hay que utilizar para el descifrado de la citada secuencia de paquetes de datos cifrados (c_i), determina el valor de la citada segunda información de sincronización criptográfica (CS_i), así como el valor de la información de retardo de sincronización criptográfica ($\Delta 1_i$) asociada correspondiente, a partir del citado primer valor (CB_i) del contador de intervalos de tiempo en la célula blanco, del valor de la citada primera información de sincronización criptográfica (CS_i), y además de un segundo valor (CB_i) del contador de intervalos de tiempo en la célula blanco correspondiente al intervalo de tiempo del segundo tipo en el cual habría podido ser recibida la citada segunda información de sincronización criptográfica (CS_i) en el canal de transmisión asignado a la comunicación en la célula blanco.

14. Dispositivo de transmisión de datos cifrados entre un terminal móvil emisor (MTE) y al menos un terminal móvil receptor (MTR) de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio con una estructura de trama en la cual una trama TDMA comprende intervalos de tiempo (T) de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo (S) de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, que comprende:

- medios para transmitir una secuencia (c_i) de paquetes de datos cifrados en el canal de tráfico a partir de un intervalo de tiempo del primer tipo (14, 32) determinado, y para transmitir una información de sincronización

criptográfica (CSI_i) asociada en el canal de señalización asociada en el interior de un intervalo de tiempo del segundo tipo (18, 36) determinado, y

- medios para transmitir igualmente en el canal de señalización asociada, una información ($\Delta 1_i$) de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el citado intervalo de tiempo del primer tipo determinado.

15. Dispositivo de transmisión de acuerdo con la reivindicación 14, que comprende además medios para separar el valor de la información de sincronización criptográfica del valor de un vector de inicialización (IV_i) que haya servido para generar una secuencia criptográfica (SC_i) utilizada para el cifrado de la citada secuencia de paquetes de datos cifrados.

16. Procedimiento de transmisión de acuerdo con la reivindicación 15, en el cual la longitud de la secuencia criptográfica es igual a un número entero N determinado de bits, que corresponde al número de bits útiles transmitidos entre dos intervalos de tiempo del segundo tipo consecutivos en los cuales puede ser transmitida una información de sincronización criptográfica.

17. Dispositivo de transmisión de acuerdo con la reivindicación 16, según el cual el número N es un múltiplo entero de un número entero M determinado que corresponde al número de bits de un paquete de datos cifrado.

18. Dispositivo de transmisión de acuerdo con una cualquiera de las reivindicaciones 14 a 17, en el cual la citada información de retardo de sincronización criptográfica es el número de intervalos de tiempo del primer tipo que separa el citado intervalo de tiempo del primer tipo determinado y el citado intervalo de tiempo del segundo tipo determinado.

19. Dispositivo de transmisión de acuerdo con una cualquiera de las reivindicaciones 14 a 18, según el cual la citada información de retardo de sincronización criptográfica es transmitida en el interior de citado intervalo de tiempo del segundo tipo determinado con la citada información de sincronización criptográfica.

20. Dispositivo de transmisión de acuerdo con una cualquiera de las reivindicaciones 14 a 19, en el cual el citado intervalo de tiempo del segundo tipo (18, 36) determinado es el intervalo de tiempo del segundo tipo que viene en la estructura de trama inmediatamente antes, o el primer intervalo de tiempo del segundo tipo que viene en la estructura de trama después del citado intervalo de tiempo del primer tipo determinado (14, 32).

21. Dispositivo de transmisión de acuerdo con una cualquiera de las reivindicaciones 14 a 20, que comprende medios para, al inicio de una alternancia, inicializar el valor de la información de sincronización criptográfica en un valor determinado codificado en un número entero Q determinado de bits, y obtenido como la concatenación binaria de, por una parte, un número entero Q1 determinado de primeros bits que codifican un valor aleatorio y, por otra, de un número entero Q2 determinado de segundos bits que son los bits de peso más pequeño del valor de un contador de intervalos de tiempo, donde Q, Q1 y Q2 son números enteros determinados.

22. Dispositivo de descifrado de una secuencia de paquetes de datos cifrados (c_i) transmitida entre un terminal móvil emisor (MTE) y al menos un terminal móvil receptor (MTR) de un sistema de radiocomunicaciones digitales, a través de un canal de transmisión radio con una estructura de trama en la cual una trama TDMA comprende intervalos de tiempo (T) de un primer tipo que forman un canal de tráfico para la transmisión de informaciones de tráfico y al menos un intervalo de tiempo (S) de un segundo tipo que forma un canal de señalización asociada para la transmisión de informaciones de señalización, que comprende:

a) primeros medios de recepción para recibir la citada secuencia de paquetes de datos cifrados a partir de un intervalo de tiempo del primer tipo (6, 15, 24, 33) determinado;

b) segundos medios de recepción para recibir una información de sincronización criptográfica (CSI_i) asociada en el canal de señalización asociada, en el interior de un intervalo de tiempo del segundo tipo (18, 36) determinado, y

c) medios de recepción para recibir igualmente, en el canal de señalización asociada, una información ($\Delta 1_i$) de retardo de sincronización criptográfica relativa a la diferencia temporal entre el citado intervalo de tiempo del segundo tipo determinado y el citado intervalo de tiempo del primer tipo determinado;

d) primeros medios de generación para generar un valor (IV_i) de un vector de inicialización que haya servido para generar una secuencia criptográfica (SC_i) utilizada para el cifrado de la citada secuencia de paquetes de datos cifrados;

e) segundos medios de generación, para generar la misma secuencia criptográfica (SC_i), a partir del valor del vector de inicialización generado por los citados primeros medios de generación;

f) medios de desfase para desfasar la secuencia criptográfica generada por los citados segundos medios de generación, en función de la citada información ($\Delta 1_i$) de retardo de sincronización criptográfica; y

g) medios para descifrar la citada secuencia de paquetes de datos cifrados (c_i) a partir de la citada secuencia criptográfica desfasada.

23. Dispositivo de descifrado de acuerdo con la reivindicación 22, en el cual los citados primeros medios de generación comprenden medios para separar el valor (IV_i) del vector de inicialización del valor de la información de sincronización criptográfica (CS_i) recibida por los citados medios de recepción.

24. Dispositivo de descifrado de acuerdo con la reivindicación 22, en el cual, en ausencia de recepción del valor de la información de sincronización criptográfica (CSI_i) por los citados primeros medios de recepción, los citados primeros medios de generación comprenden medios (67) para generar el valor (IV_i) del vector de inicialización con la ayuda de un algoritmo de “rueda libre” a partir de un valor anterior de la información de sincronización criptográfica.

25. Dispositivo de descifrado de acuerdo con una cualquiera de las reivindicaciones 22 a 24, en el cual, siendo expresada la información ($\Delta 1_i$) de retardo de sincronización criptográfica en número de intervalos de tiempo, los citados medios de desfase comprenden medios para generar una información ($\Delta 2_i$) correspondiente expresada en número de paquetes de datos.

26. Dispositivo de descifrado de acuerdo con una cualquiera de las reivindicaciones 22 a 24, que comprende, además, medios para, durante un cambio de célula del terminal móvil receptor, de una célula fuente (A) determinada hacia una célula blanco (B) determinada:

h) recibir una información de desfase de sincronización criptográfica (Δ_{CPT}), relativa al desfase de sincronización criptográfica entre la célula fuente y la célula blanco, que es transmitida con el mando de cambio de célula en un intervalo de tiempo del segundo tipo determinado en el canal de transmisión asignado a la comunicación en la célula fuente;

i) memorizar el valor de una primera información de sincronización criptográfica (CSI_i) determinada y un primer valor (CB_i) del contador de intervalos de tiempo de la célula blanco correspondiente al intervalo de tiempo del segundo tipo en el cual habría podido ser recibida la citada información de sincronización criptográfica;

j) efectuar el cambio de célula;

k) recibir una secuencia de paquetes de datos cifrados (c_j) determinada, a partir de un intervalo de tiempo del primer tipo (24) determinado en el canal de transmisión asignado a la comunicación en la célula blanco; y

l) en ausencia de recepción por los citados primeros medios de recepción del valor de una segunda información de sincronización criptográfica (CSI_j), que hay que utilizar para el descifrado de la citada secuencia de paquetes de datos cifrados (c_j), determinar el valor de la citada segunda información de sincronización criptográfica (CSI_j), así como el valor de la información de retardo de sincronización criptográfica ($\Delta 1_j$) asociada correspondiente, a partir del citado primer valor (CB_i) del contador de intervalos de tiempo en la célula blanco, del valor de la citada primera información de sincronización criptográfica (CSI_i), y además de un segundo valor (CB_j) del contador de intervalos de tiempo en la célula blanco correspondiente al intervalo de tiempo del segundo tipo en el cual habría podido ser recibida la citada segunda información de sincronización criptográfica (CSI_j) en el canal de transmisión asignado para la comunicación en la célula blanco.

27. Terminal móvil de un sistema de radiocomunicaciones digitales, que comprende un dispositivo de transmisión de acuerdo con una cualquiera de las reivindicaciones 14 a 21, y/o un dispositivo de descifrado de acuerdo con una cualquiera de las reivindicaciones 22 a 26.

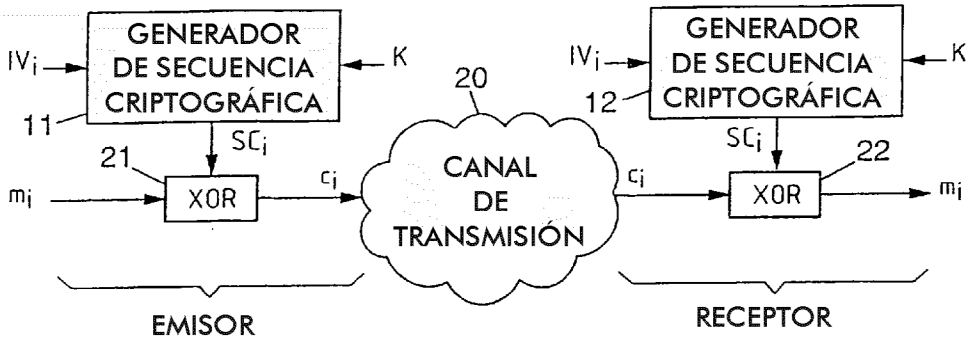

FIG. 1

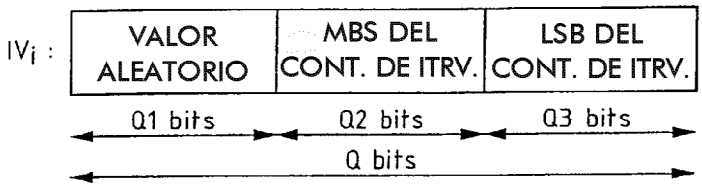

FIG. 6

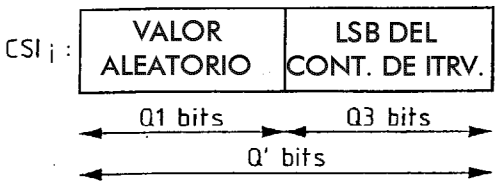

FIG. 7

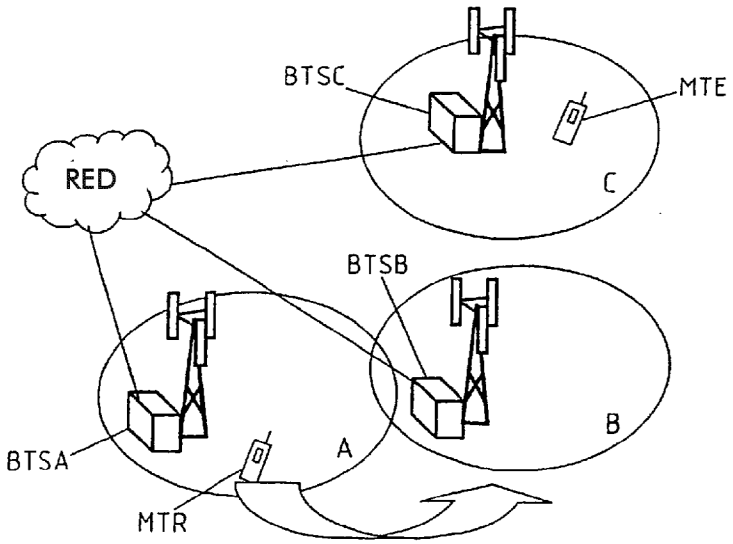

FIG. 12

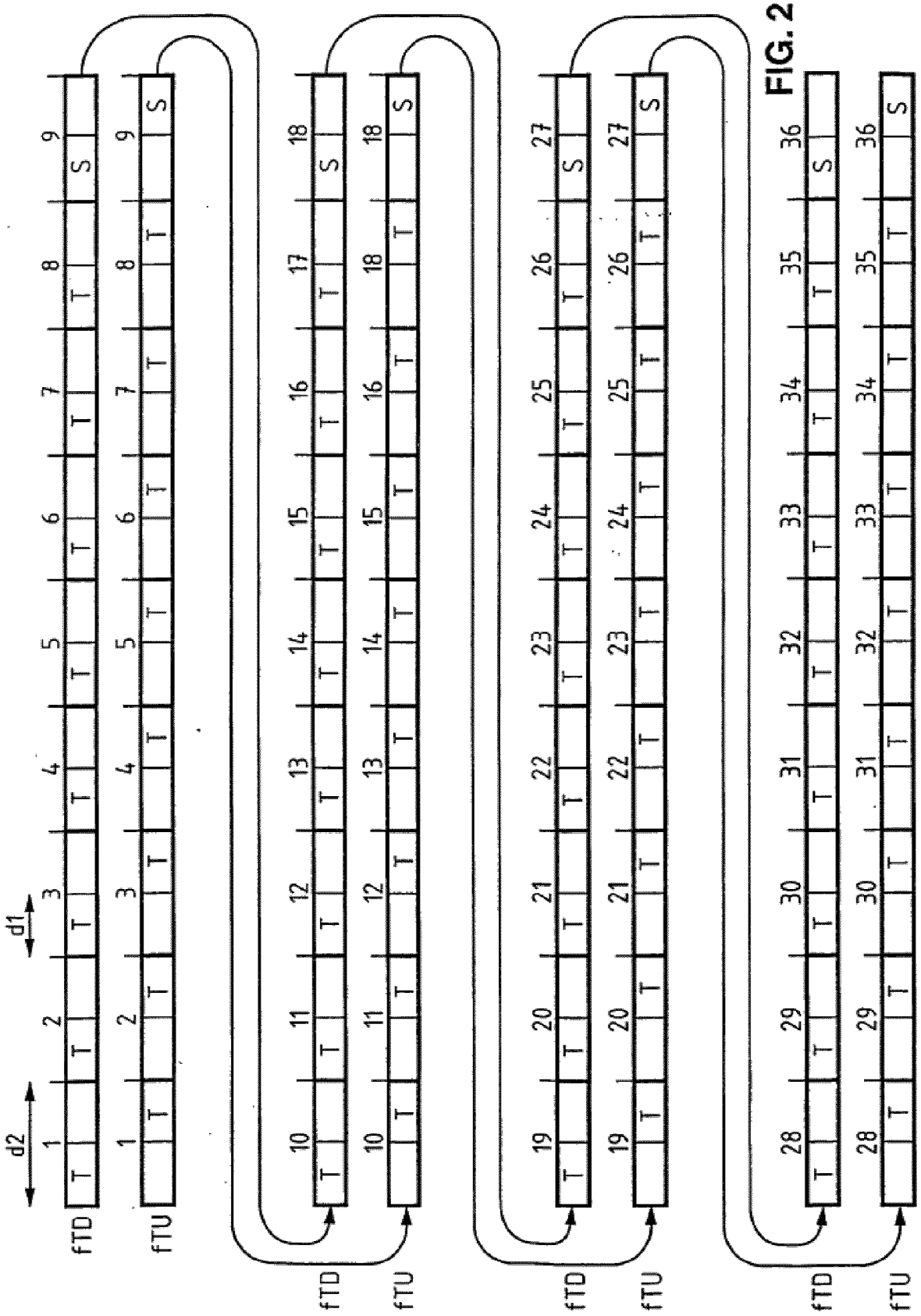
d2
d1
fTD
fTU
T
S
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36

FIG. 2

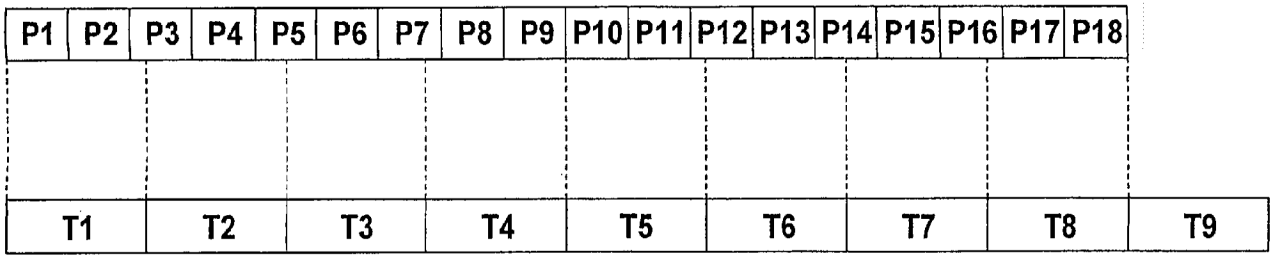

FIG. 3a

Intervalos de Tiempo	1ª trama de Fonía	2ª trama de Fonía	3ª trama de Fonía
1, 10, 19, 28	P1	P2	¼ de P3
2, 11, 20,29	¾ de P3	P4	½ de P5
3, 12, 21, 30	½ de P5	P6	¾ de P7
4, 13, 22, 31	¼ de P7	P8	P9
5, 14, 23, 32	P10	P11	¼ de P12
6, 15, 24, 33	¾ de P12	P13	½ de P14
7, 16, 25, 34	½ de P14	P15	¾ de P16
8, 17, 26, 35	¼ de P16	P17	P18

FIG. 3b

$\Delta 1_i$:	7	6	5	4	3	2	1	0
$\Delta 2_i$:	15	13	11	9	6	4	2	0

FIG. 11

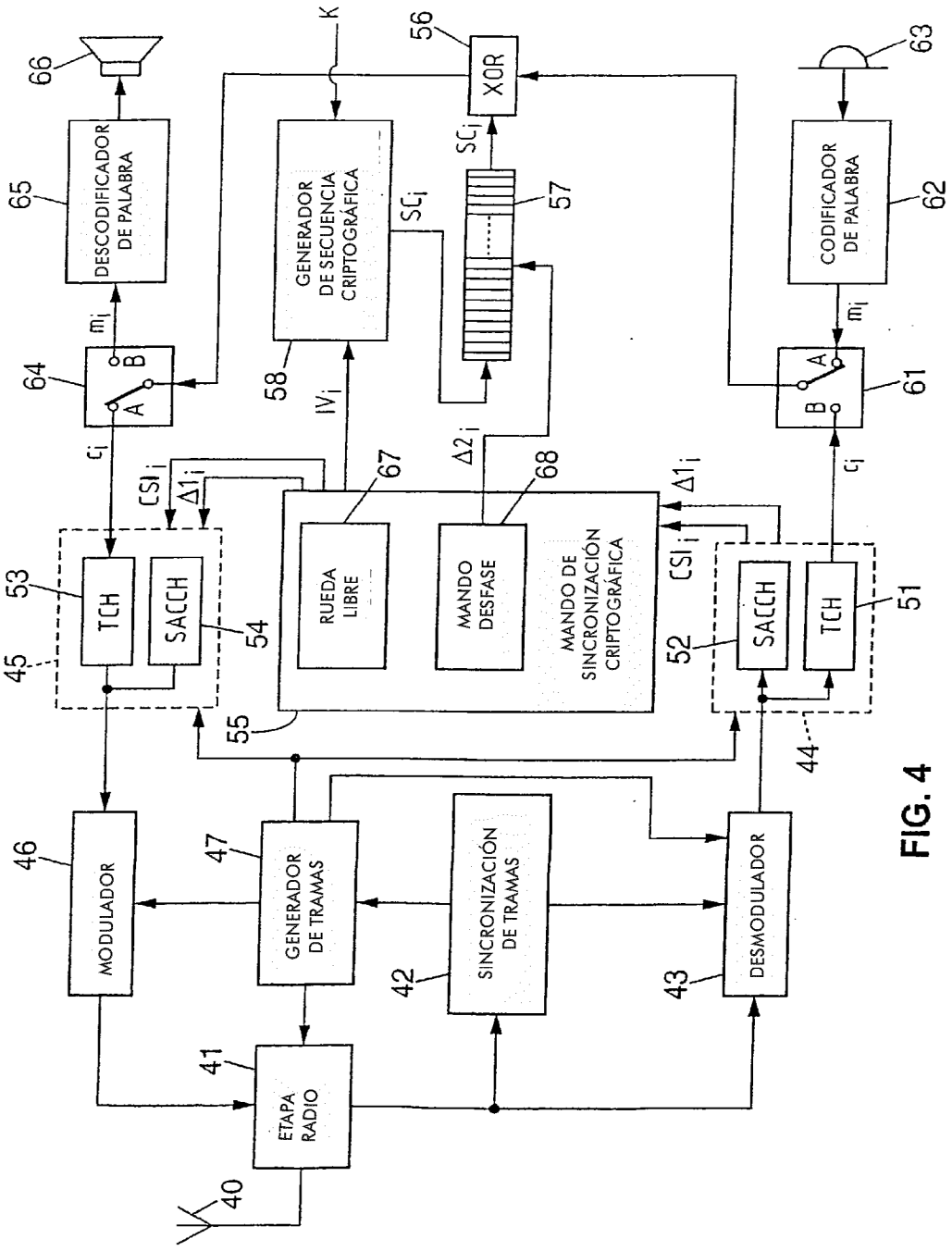
66
DESCODIFICADOR DE PALABRA
65
m_i
64
B
A
c_i
CSI_i
$\Delta 1_i$
53
TCH
SACCH
54
45
K
56
XOR
SC_i
57
GENERADOR DE SECUENCIA CRIPTOGRÁFICA
SC_i
58
IV_i
$\Delta 2_i$
67
68
RUEDA LIBRE
MANDO DESFASE
MANDO DE SINCRONIZACIÓN CRIPTOGRÁFICA
55
$\Delta 1_i$
CSI_i
52
SACCH
TCH
51
44
63
CODIFICADOR DE PALABRA
62
m_i
61
A
B
c_i
46
MODULADOR
47
GENERADOR DE TRAMAS
42
SINCRONIZACIÓN DE TRAMAS
43
DESMODULADOR
41
ETAPA RADIO
40

FIG. 4

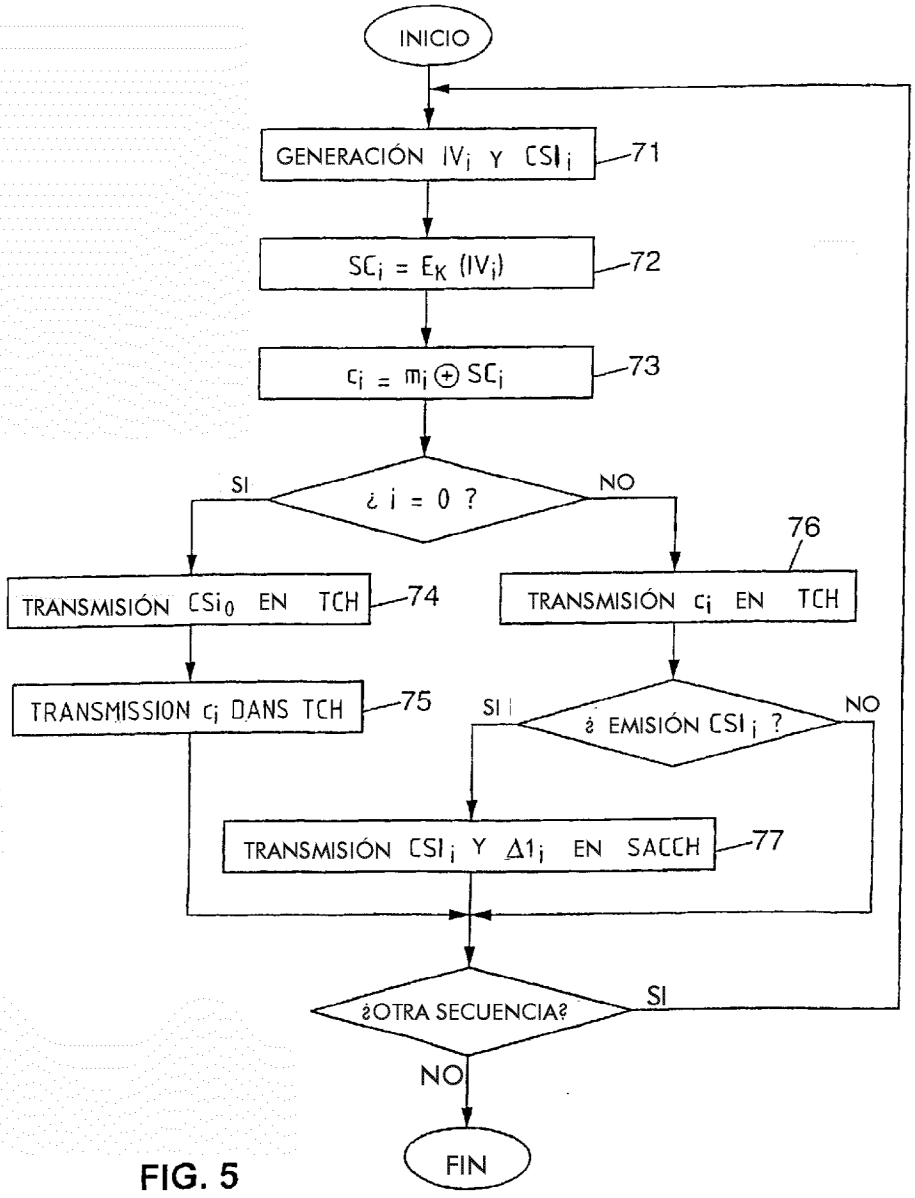
INICIO
GENERACIÓN IVi Y CSIi
71
SCi = EK (IVi)
72
ci = mi ⊕ SCi
73
SI
¿ i = 0 ?
NO
76
TRANSMISIÓN CSi0 EN TCH
74
TRANSMISIÓN ci EN TCH
TRANSMISSION ci DANS TCH
75
SI
¿ EMISIÓN CSIi ?
NO
TRANSMISIÓN CSIi Y Δ1i EN SACCH
77
¿OTRA SECUENCIA?
SI
NO
FIN

FIG. 5

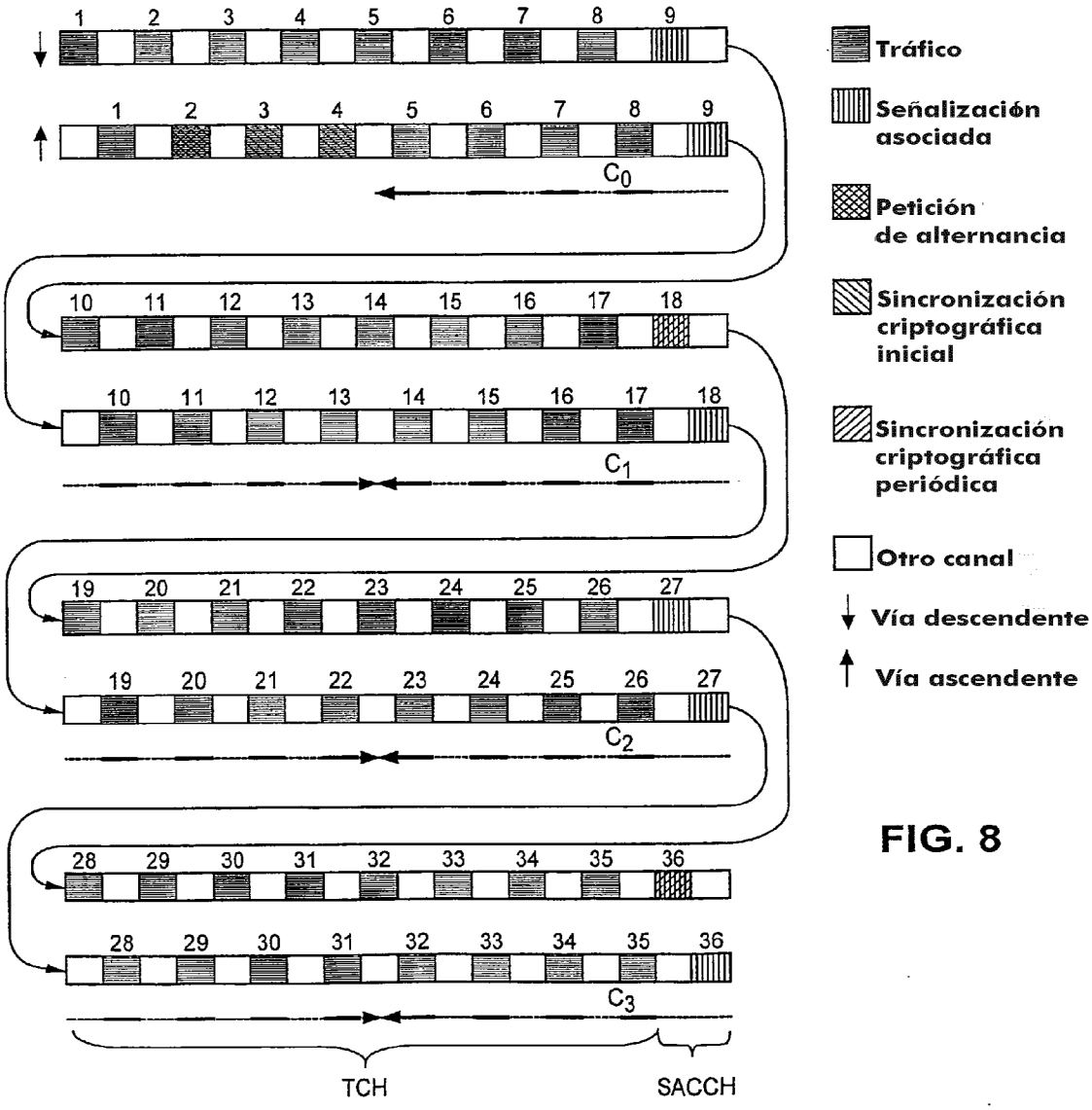
1 2 3 4 5 6 7 8 9
1 2 3 4 5 6 7 8 9
C0
10 11 12 13 14 15 16 17 18
10 11 12 13 14 15 16 17 18
C1
19 20 21 22 23 24 25 26 27
19 20 21 22 23 24 25 26 27
C2
28 29 30 31 32 33 34 35 36
28 29 30 31 32 33 34 35 36
C3
TCH
SACCH
Tráfico
Señalización asociada
Petición de alternancia
Sincronización criptográfica inicial
Sincronización criptográfica periódica
Otro canal
Vía descendente
Vía ascendente

FIG. 8

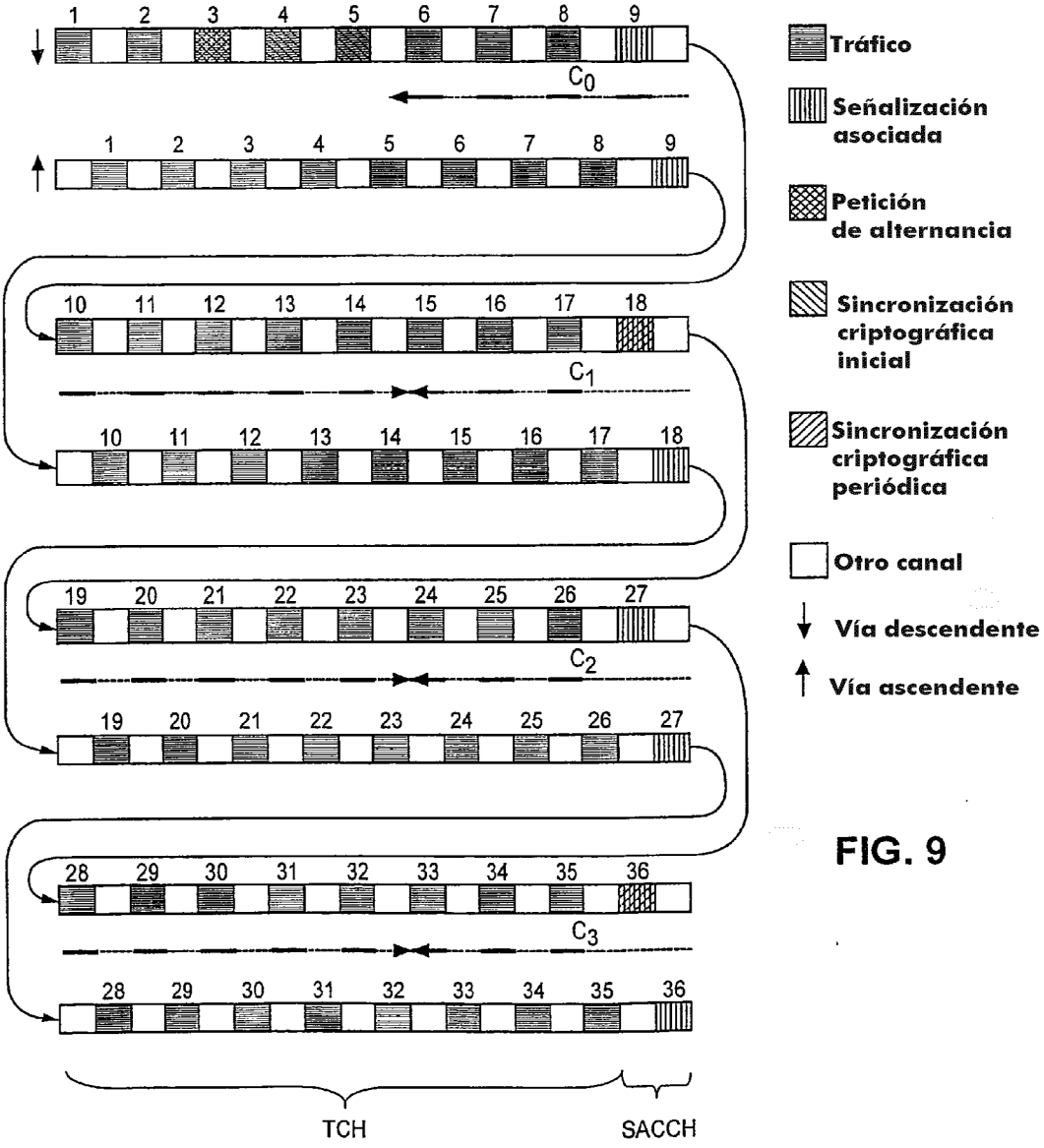
1 2 3 4 5 6 7 8 9
C0
1 2 3 4 5 6 7 8 9
10 11 12 13 14 15 16 17 18
C1
10 11 12 13 14 15 16 17 18
19 20 21 22 23 24 25 26 27
C2
19 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35 36
C3
28 29 30 31 32 33 34 35 36
TCH
SACCH
Tráfico
Señalización asociada
Petición de alternancia
Sincronización criptográfica inicial
Sincronización criptográfica periódica
Otro canal
Vía descendente
Vía ascendente

FIG. 9

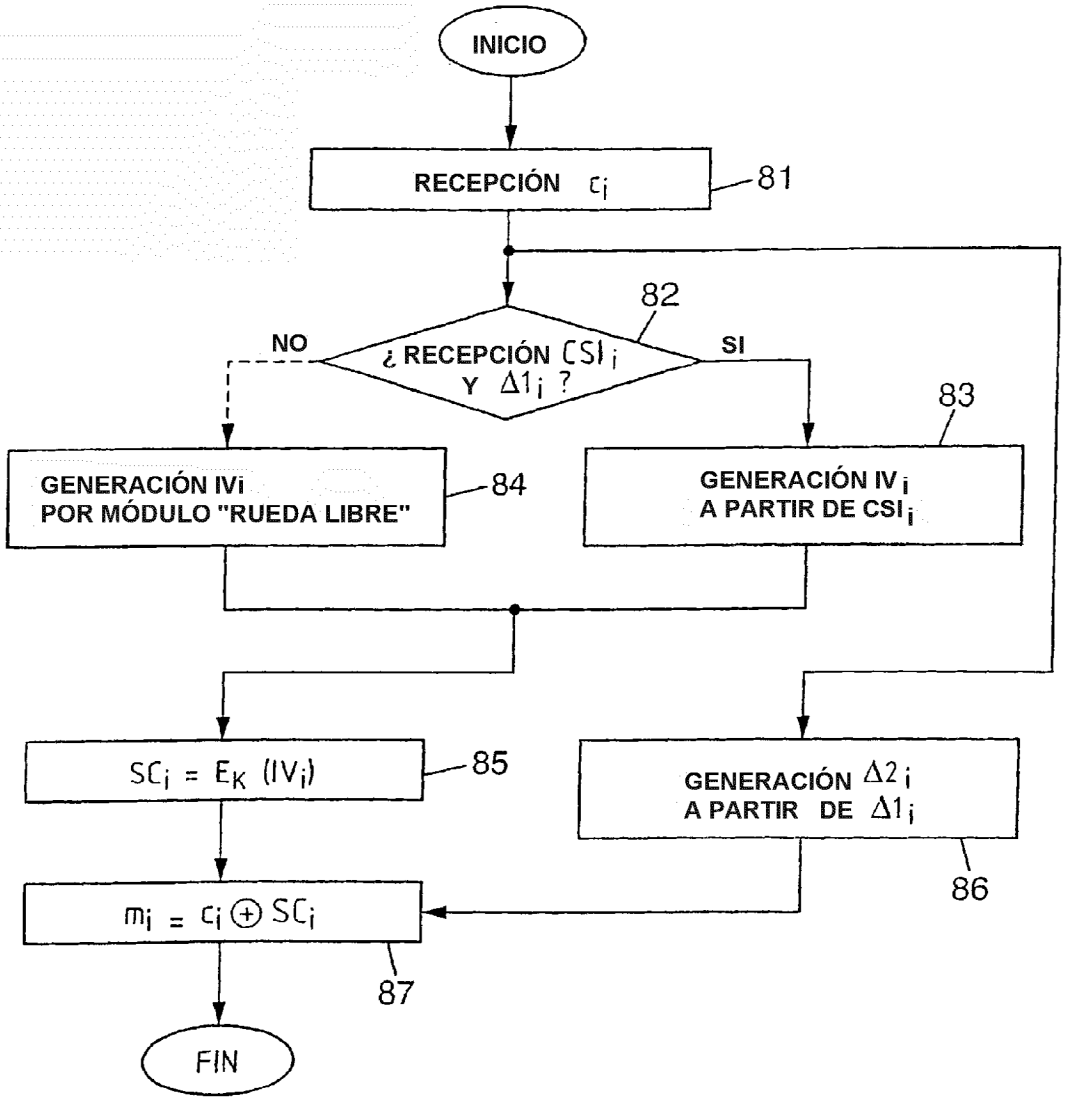
INICIO
RECEPCIÓN c_i
81
82
NO
¿ RECEPCIÓN CSI_i Y $\Delta 1_i$?
SI
83
GENERACIÓN IVi POR MÓDULO "RUEDA LIBRE"
84
GENERACIÓN IV_i A PARTIR DE CSI_i
$SC_i = E_K (IV_i)$
85
GENERACIÓN $\Delta 2_i$ A PARTIR DE $\Delta 1_i$
86
$m_i = c_i \oplus SC_i$
87
FIN

FIG. 10

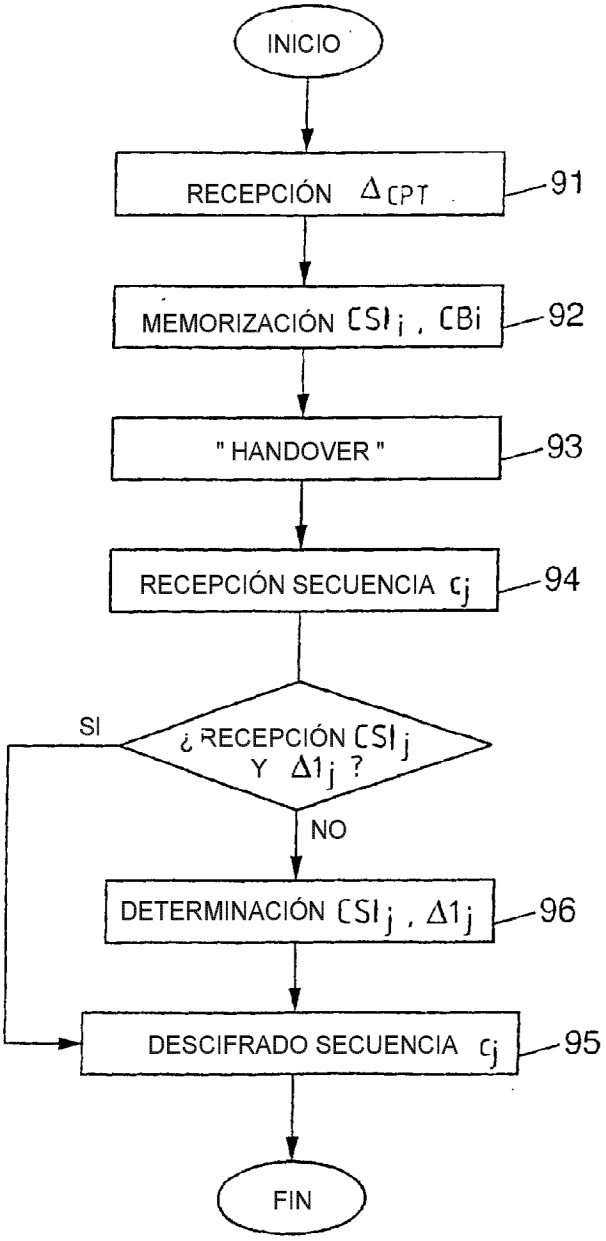
INICIO
RECEPCIÓN Δ CPT
91
MEMORIZACIÓN CSIj , CBi
92
" HANDOVER "
93
RECEPCIÓN SECUENCIA cj
94
SI
¿ RECEPCIÓN CSIj Y Δ1j ?
NO
DETERMINACIÓN CSIj , Δ1j
96
DESCIFRADO SECUENCIA cj
95
FIN

FIG. 13