



19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 355 002**

51 Int. Cl.:  
**H04L 9/12** (2006.01)  
**H04J 3/06** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **07731671 .9**  
96 Fecha de presentación : **27.02.2007**  
97 Número de publicación de la solicitud: **1992102**  
97 Fecha de publicación de la solicitud: **19.11.2008**

54 Título: **Sincronización criptográfica entrelazada.**

30 Prioridad: **06.03.2006 FR 06 01951**

45 Fecha de publicación de la mención BOPI:  
**22.03.2011**

45 Fecha de la publicación del folleto de la patente:  
**22.03.2011**

73 Titular/es: **EADS SECURE NETWORKS**  
**La Clef Saint Pierre**  
**1 boulevard Jean Moulin**  
**78990 Elancourt, FR**

72 Inventor/es: **Rousseau, Frédéric**

74 Agente: **Elzaburu Márquez, Alberto**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

La presente invención se refiere a una sincronización aplicada a un flujo de datos estructurado en supertramas formadas cada una por bloques de tramas, particularmente en un contexto de criptografía de datos con el fin de sincronizar emisores y receptores en equipos que transmiten entre ellos un flujo de datos cifrados en tiempo real.

5 Ésta encuentra aplicaciones especialmente en el ámbito de las telecomunicaciones seguras.

Previamente, se definen los términos siguientes:

trama: una secuencia binaria, por ejemplo resultante de una iteración de un módulo criptográfico, de longitud  $S_{trama}$  ( $S_{trama} \geq 1$  bit);

bloque: un grupo de  $n$  tramas consecutivas, con  $n \geq 1$ ;

10 supertrama: un grupo formado por  $p$  bloques consecutivos, con  $p \geq 1$ ;

flujo de datos cifrados: una sucesión de supertramas.

15 Los términos trama, bloque y supertrama definidos anteriormente a título de un flujo aplicativo entre equipos terminales distantes no prejuzgan estructuración subyacente de los flujos por el servicio soporte de transmisión ("bear service" en inglés): una supertrama, o un bloque o una trama, emitidos por una aplicación puede corresponder, por ejemplo, a un paquete no segmentado transmitido en capa de transporte.

20 A este respecto, es bien conocido que un bloque que comprende un encabezamiento con una palabra de sincronización, y varias tramas consecutivas es designado por trama o multitrama en ciertas aplicaciones. Por ejemplo, la solicitud de patente US 2003/0037297 divulga, para un multiplexado por división del tiempo conocido, un bloque que comprende un encabezamiento que incluye una palabra de sincronización indivisible "a", tramas consecutivas que comprenden, cada una, una palabra de sincronización "b", y finalmente un campo de control de error. En un receptor, la palabra de sincronización "b" se repite en las tramas de un bloque y se utiliza, conjuntamente con al menos una detección de la palabra de sincronización "a", para adquirir una sincronización de bloque más rápidamente que una sincronización que únicamente estuviera basada en una detección de la palabra de sincronización "a" en bloques consecutivos.

25 La puesta en práctica de comunicaciones seguras genera la dificultad de que los receptores en los equipos deben ser sincronizados o resincronizados de modo suficientemente rápido con un flujo de datos cifrados. Las especificaciones de las sucesiones criptográficas conocidas consideran únicamente una sola hipótesis sobre la frecuencia de las sincronizaciones criptográficas, dimensionadas sobre constantes de tiempo asociadas a una red subyacente dada. Esto es problemático para un flujo de datos cifrados de principio a fin en el que los equipos terminales operan en redes heterogéneas. Por ejemplo, para una comunicación punto a punto o para una teleconferencia, los equipos terminales de comunicación pueden ser diversos: un equipo terminal puede estar vinculado a una red de cable, un segundo equipo terminal puede estar situado en una célula de una red de radiocomunicación celular para móviles, un tercer equipo terminal es un terminal de comunicación por satélite, y un cuarto equipo terminal es un aparato de radio HF que funciona con saltos de frecuencia.

35 Una transmisión de un flujo de datos cifrados entre equipos terminales fijos de una red de cable en la que el servicio de comunicación es fiable, solamente necesita esencialmente una sincronización criptográfica lenta.

40 Una transmisión de un flujo de datos cifrados a través de una red en la que ciertos segmentos aseguran transmisiones no fiables, por ejemplo transmisiones radio, puede dar lugar a que ciertos receptores no reciban el conjunto íntegro de las informaciones de sincronización criptográfica necesarias para el tratamiento del flujo de datos cifrados o puede dar lugar a que ciertos receptores pierdan el sincronismo necesario entre el descifrado y la recepción de tramas del flujo de datos cifrados. Se necesita entonces un procedimiento de sincronización rápida.

45 Una sincronización rápida es igualmente necesaria cuando un equipo terminal de la comunicación requiere una transferencia intercelular ("handover" en inglés) o una reelección de célula anunciada ("announced cell reselection" en inglés), es decir cuando el flujo de datos cifrados cambia de canal de transmisión, lo que interrumpe temporalmente la recepción y hace perder el sincronismo criptográfico al equipo terminal.

Una sincronización rápida es también necesaria cuando un equipo terminal que desea participar en una comunicación cifrada ya comenzada entre otros equipos terminales requiere una entrada tardía ("late entry" en inglés) en la comunicación.

Además, una sincronización rápida es útil cuando el flujo de datos cifrados, recibido continuamente por un receptor para una comunicación dada ha sido sometido aguas arriba a un derecho preferente ("pre-emption" en inglés) de un emisor por un emisor más prioritario.

Se presentan a continuación la medición de la rapidez de sincronización criptográfica y las limitaciones de la técnica anterior.

Existen diferentes modos de sincronización criptográfica, de los cuales algunos requieren la transmisión explícita de parámetros de una palabra de estado criptográfica con el fin de inicializar el proceso de descifrado. Algunos de estos modos, tales como los modos OFB (Output FeedBack mode) y CTR (CounteR mode), están descritos por ejemplo en la publicación americana del National Institute of Standards and Technology "NIST" Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes Operation – Methods and Techniques". Los parámetros transmitidos de la palabra de estado criptográfico definen una palabra de gestión de sincronización SY (que corresponde a "Synchronization Management SM" en inglés).

En la técnica anterior, la palabra de gestión de sincronización es transmitida típicamente en asociación con cada supertrama de un flujo de datos cifrados.

A continuación, se recuerdan dos métodos de asociación conocidos.

En el primer método de asociación, la banda pasante  $B_{SY}$  necesaria para la transmisión de la trama que contiene la palabra de gestión de sincronización es obtenida por robo de tramas ("frame stealing" en inglés) en la banda pasante  $B_T$  del flujo de tramas de tráfico cifradas. La banda pasante total necesaria, expresada en bits/s, es entonces  $B = B_T$ . El primer método de asociación por robo de tramas está descrito en la norma ETSI EN 302 109 V.1.1, "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption" junio 2003, páginas 1-17.

En el segundo método de asociación, la banda pasante  $B_{SY}$  necesaria para la transmisión de la palabra de gestión de sincronización puede ser complementaria de la banda pasante  $B_T$  necesaria para la transmisión del flujo de datos de tráfico cifrados. Se definen entonces dos canales lógicos: un canal de tráfico para las tramas cifradas y un canal de señalización asociado al canal de tráfico para las tramas que contienen la palabra de gestión de sincronización. La banda pasante total necesaria es entonces  $B = B_{SY} + B_T$ . El segundo método está descrito en la solicitud de patente internacional WO 2004/014019.

Sea  $S_{SY}$  el tamaño de la palabra de sincronización SY expresado en bits, determinado en coherencia con la elección del algoritmo de cifrado, del modo de sincronización y de un criptoperíodo. Este tamaño no depende directamente de la estructuración en tramas, bloques y supertramas del flujo.

De acuerdo con una primera hipótesis, la palabra de gestión de sincronización tiene un tamaño  $S_{SY}$  inferior o igual al tamaño de una trama de tráfico.

El flujo efectivamente transmitido de acuerdo con el primer método de asociación consiste en una sucesión de supertramas de dimensión 1. Cada una de estas supertramas está formada por un único bloque ( $p = 1$ ) que comprende una trama de sincronización que contiene la palabra de gestión de sincronización de la supertrama y  $n - 1$  tramas de datos de tráfico cifrados. La primera trama de tráfico es robada y reemplazada por la trama de sincronización y por tanto no es transmitida.

El flujo efectivamente transmitido de acuerdo con el segundo método de asociación consiste en una sucesión de supertramas de dimensión 2. Cada una de estas supertramas está formada por un único bloque ( $p = 1$ ) que comprende por ejemplo en el canal de señalización una trama de sincronización que contiene la palabra de gestión de sincronización de la supertrama y en el canal de tráfico asociado  $n$  tramas de datos de tráfico cifrados.

De acuerdo con una segunda hipótesis, la palabra de gestión de sincronización de la supertrama tiene un tamaño  $S_{SY}$  superior o igual al tamaño  $S_{trama}$  de una trama. Sin restringir la generalidad de esta hipótesis, la palabra de gestión de sincronización debe ser transmitida en tramas identificables y separables de las tramas de tráfico del flujo de datos cifrados, siendo solventado el caso contrario segmentando las tramas del flujo de datos cifrados en otras tantas tramas ad hoc. De acuerdo con un ejemplo simple, se supone que  $S_{SY} = p \times S_{trama}$  y la palabra de gestión de sincronización resulta de la concatenación de  $p$  tramas de sincronización para una supertrama dada.

El flujo efectivamente transmitido de acuerdo con el primer método de asociación consiste entonces en una sucesión de supertramas. Cada una de estas supertramas está formada por  $p$  bloques de dimensión 1 que comprenden cada uno una respectiva trama de sincronización seguida de  $n - 1$  tramas de tráfico, reemplazando las tramas de sincronización, respectivamente en los  $p$  bloques de la supertrama, que concatenadas según su orden de emisión constituyen la palabra de gestión de sincronización, a  $p$  tramas de tráfico.

El flujo efectivamente transmitido de acuerdo con el segundo método de asociación consiste también en una sucesión de supertramas. Cada una de estas supertramas está formada por un único bloque ( $p = 1$ ) de dimensión 2 que comprende en el canal de señalización la palabra de gestión de sincronización seguida en el canal de tráfico por  $n$  tramas de tráfico.

Así, de acuerdo con la técnica anterior, cualesquiera que sean las hipótesis sobre el tamaño  $S_{SY}$  de la palabra de gestión de sincronización y el primer o segundo método de asociación, la sincronización criptográfica es posible aproximadamente después de cada ocurrencia de una supertrama, una vez conocida la palabra de gestión de sincronización. Esto conduce aproximadamente a un período entre sincronizaciones igual a  $T_{\text{sinc}} = (n \cdot p \cdot S_{\text{trama}})/B$ .

La medición de la rapidez  $T_{\text{sinc}}$  de sincronización criptográfica para un ejemplo real pone en evidencia las limitaciones de la técnica anterior: con  $B = 2400$  bit/s,  $S_{\text{trama}} = 54$  bits,  $n = 24$ ,  $p = 3$ , se obtiene  $T_{\text{sinc}} = 1,62$  s; con  $B = 2400$  bit/s,  $S_{\text{trama}} = 54$  bits,  $n = 24$ ,  $p = 4$ , se obtiene  $T_{\text{sinc}} = 2,16$  s.

Estos valores de período entre sincronizaciones  $T_{\text{sinc}}$  son satisfactorios para una comunicación punto a punto en una red telefónica de establecimiento de llamada lento, del orden de algunos segundos. Estos no obstante son incompatibles con constantes de tiempo de sincronización rápida, típicamente del orden de 0,3 a 1 segundo como máximo, necesarios en redes de radiocomunicación para móviles que ponen en práctica funciones de transferencia intercelular, de entrada tardía o de derecho preferente. Éstas, además, son muy superiores a la duración típica de un fonema en una señal de palabra que está cifrada en el flujo de datos cifrados. Estos valores de período entre sincronizaciones  $T_{\text{sinc}}$  son así incompatibles con exigencias de comunicaciones seguras interoperables que impliquen simultáneamente a equipos terminales de usuario a través de redes heterogéneas. La necesidad de sincronización rápida puede ser ilustrada por una teleconferencia segura multiusuario que implique a equipos tales como un terminal de usuario de una red de cable RNIS o IP, un terminal móvil de una red de radiocomunicación celular GSM o UMTS y/o un terminal móvil de una red de radiocomunicación celular profesional PMR.

Por otra parte, se conoce un procedimiento de sincronización descrito en la solicitud de patente EP 1209844 que añade tramas de sincronización suplementarias en el flujo de datos cifrados. La adición de estas tramas de sincronización suplementarias modifica la banda pasante necesaria inicialmente en el flujo de datos cifrados y no satisface a una necesidad de sincronización rápida de manera optimizada. Además, este procedimiento de sincronización destruye el sincronismo del flujo de datos cifrados y por tanto la sincronización lenta anterior lo que impone que todos los receptores traten las tramas de sincronización suplementarias y constituye una limitación de interoperabilidad de la seguridad. Por consiguiente, este procedimiento es inapropiado para asegurar una sincronización rápida coexistente con una sincronización lenta preexistente, de la cual saca partido.

Un objetivo de la invención es superar los inconvenientes precedentes de la técnica anterior, por una sincronización de un equipo con un flujo de datos en tiempo real que permita una sincronización rápida coexistente con una sincronización lenta, sin aumentar la banda pasante inicial necesaria para el flujo de datos.

Para conseguir este objetivo, un procedimiento de sincronización aplicado a un flujo de datos estructurado en supertramas formadas cada una por bloques de tramas, comprendiendo cada bloque en una supertrama una parte de sincronización lenta y al menos una trama de tráfico, siendo las partes de sincronización lenta en la supertrama diferentes entre sí y resultantes al menos de una descomposición de una palabra de gestión de sincronización, está caracterizado de acuerdo con la reivindicación.

La palabra de gestión de sincronización es conservada sin cambio de orden ni descomposición de las partes de sincronización lenta. Por ejemplo, el reagrupamiento de las partes de sincronización lenta de acuerdo con un orden predeterminado, como por ejemplo una concatenación, ayuda a la reproducción de una palabra de gestión de sincronización. De acuerdo con la invención, la conservación de las partes de sincronización lenta permite a cualquier equipo actual continuar funcionando con la sincronización lenta, sin ninguna modificación en el equipo actual. Las partes de sincronización lenta procedentes de la palabra de gestión de sincronización son introducidas en la supertrama de acuerdo con uno u otro de los primero y segundo métodos de asociación conocidos. Las partes de sincronización suplementarias son similares a las partes de sincronización lenta, es decir las partes de sincronización suplementarias son respectivamente idénticas a, o un poco diferentes de, las partes de sincronización lenta, y son añadidas de acuerdo con la invención a una supertrama por sustitución de bits de trama de tráfico y por tanto por robos de ciertas tramas de tráfico enteras y/o por robos de ciertos bits de tramas de tráfico.

Las partes de sincronización suplementarias dan la posibilidad a un equipo de funcionar con una sincronización más rápida que la sincronización lenta, cuando se constata que esto es útil, como por ejemplo durante una transferencia (handover) de célula para un terminal móvil o una estación de base en una red de radiocomunicación celular. La sincronización rápida coexiste con la sincronización lenta preexistente sin conducir a ninguna modificación de los equipos actuales que únicamente funcionan con la sincronización lenta.

La invención es particularmente interesante para una sincronización criptográfica de equipo en un flujo de datos cifrados en tiempo real, estructurado en supertramas, en el cual el cifrado depende igualmente de la palabra de gestión de sincronización y del recorte inicial de cada supertrama en bloques de tamaño idéntico y que incluyen cada uno una respectiva parte de sincronización lenta y una o varias tramas de tráfico.

Sea un número entero  $k = \text{Ceiling}(p/2)$  para un número  $p$  de bloques en la supertrama. El operador Ceiling es igual al argumento  $p/2$  si éste es entero y es igual al entero inmediatamente superior al argumento, si no lo es. Por ejemplo, se tiene  $k = 2$  para  $p = 3$  y  $k = 2$  para  $p = 4$ . La duración entre dos sincronizaciones rápidas sucesivas de acuerdo con el procedimiento de la invención puede ser sensiblemente como mucho  $T_{\text{sinc}} = (n k S_{\text{trama}})/B$  y por tanto inferior al período  $T_{\text{sinc}} = (n p S_{\text{trama}})/B$  para la sincronización lenta de acuerdo con la técnica anterior.

El procedimiento de la invención permite una sincronización rápida sensiblemente en como mucho  $k = 2$  bloques para una supertrama formada por 3 bloques o por 4 bloques, al tiempo que preserva la sincronización lenta en la supertrama. Dicho de otro modo, el procedimiento de la invención permite una sincronización rápida en menos de  $k n = 2 n$  tramas, y una sincronización lenta en menos de  $3 n$  tramas para una supertrama formada por 3  $n$  tramas o en menos de  $4 n$  tramas para una supertrama formada por 4  $n$  tramas, siendo  $n$  el número de tramas por bloque.

De acuerdo con una realización de la invención, una de las partes de sincronización suplementarias reemplaza a una trama de tráfico en un bloque de la supertrama. En particular, las partes de sincronización suplementarias pueden reemplazar respectivamente a tramas de tráfico en los bloques de la supertrama, a razón de una trama de tráfico por bloque, quedando entonces entrelazadas las partes de sincronización lenta y las partes de sincronización suplementarias. En un receptor que recibe el flujo de datos estructurado en supertramas, durante la reconstitución de la palabra de gestión de sincronización, el número de bloques consecutivos observados en la supertrama puede ser todavía reducido hasta ser inferior sensiblemente a la mitad del número de bloques en la supertrama.

Si las partes de sincronización lenta son introducidas en la supertrama de acuerdo con el primer método de asociación, el número de tramas de tráfico robadas en la supertrama pasa de  $p$  a  $2p$ , lo que corresponde a una tasa de eliminación de tramas de tráfico del flujo de datos doblada con respecto a la técnica anterior. Si las partes de sincronización lenta son introducidas en la supertrama de acuerdo con el segundo método de asociación, el número de tramas de tráfico robadas en la supertrama pasa de 0 a  $p$ , lo que corresponde a una tasa de eliminación de tramas del flujo de datos igual a  $1/n$ , en lugar de 0 de acuerdo con la técnica anterior.

De acuerdo con otras realizaciones de la invención, una de las partes de sincronización suplementarias reemplaza a bits predeterminados en tramas de tráfico predeterminadas en un bloque de la supertrama, es decir estas tramas de tráfico solamente son alteradas parcialmente por la parte de sincronización suplementaria. Las partes de sincronización suplementarias pueden tener subpartes que tienen un tamaño en bits inferior al tamaño de las tramas de tráfico y que están repartidas en sustitución de bits predeterminados en todas las tramas de tráfico en la supertrama, o de ciertas tramas de tráfico que tienen rangos predeterminados en un bloque predeterminado o en bloques predeterminados de la supertrama.

En comparación con la sincronización lenta dependiente de la palabra de gestión de sincronización y sistemáticamente presente en cada supertrama del flujo de datos estructurado, otra ventaja del procedimiento de la invención es que las partes de sincronización suplementarias, de las que depende la sincronización rápida, que depende igualmente de las partes de sincronización lenta, pueden ser transmitidas opcionalmente en cada supertrama, en función de las necesidades de los equipos.

La invención se refiere igualmente a una secuencia de sincronización en una supertrama de un flujo de datos estructurado en supertramas formadas cada una por bloques de tramas digitales, comprendiendo cada bloque en una supertrama una parte de sincronización lenta y al menos una trama de tráfico, siendo las partes de sincronización lenta en la supertrama diferentes entre sí y resultantes al menos de una descomposición de una palabra de gestión de sincronización. La secuencia de sincronización está caracterizada de acuerdo con la reivindicación 12.

La invención se refiere también a un emisor de acuerdo con la reivindicación 15 y a un receptor de acuerdo con la reivindicación 16 por ejemplo en un equipo terminal fijo y/o móvil o en un equipo pasarela entre dos redes de telecomunicación heterogéneas en materia de sincronización.

Otras características y ventajas de la presente invención se pondrán de manifiesto de modo más claro con la lectura de la descripción que sigue de varias realizaciones de la invención, dadas a título de ejemplos no limitativos, refiriéndose a los dibujos anejos correspondientes, en los cuales:

- la figura 1 es un diagrama de bloques esquemático de un emisor de un equipo terminal y de un receptor RE de otro equipo terminal para la puesta en práctica del procedimiento de sincronización criptográfica de la invención;

- la figura 2 es un algoritmo de etapas del procedimiento de sincronización criptográfica;
- las figuras 3 y 5 muestran la estructura de supertramas en un flujo de datos cifrados con una sincronización lenta de acuerdo con el primer método de asociación respectivamente para un primer y un segundo ejemplos de acuerdo con la técnica anterior;
- 5 - las figuras 4 y 6 muestran la estructura de supertramas en un flujo de datos cifrados respectivamente según las figuras 3 y 5 y completada de acuerdo con una primera realización de la invención;
- las figuras 7 y 9 muestran la estructura de supertramas en un flujo de datos cifrados de acuerdo con el segundo método de asociación respectivamente para el primer y el segundo ejemplos de acuerdo con la técnica anterior;
- 10 - las figuras 8 y 10 muestran la estructura de supertramas en un flujo de datos cifrados con una sincronización lenta respectivamente según las figuras 7 y 9 y completada de acuerdo con un segunda realización de la invención; y
- las figuras 11, 12 y 13 muestran la estructura de supertramas en un flujo de datos cifrados con una sincronización lenta de acuerdo con el primer método de asociación para el primer ejemplo y completada de acuerdo con otras realizaciones de la invención por robos de bits en ciertas tramas de tráfico, respectivamente en ciertos bloques.

15 Refiriéndose a la figura 1, un equipo que pone en práctica el procedimiento de acuerdo con la invención es por ejemplo un terminal móvil o una estación de base de una red de radiocomunicación celular terrestre o aeronáutica o por satélites, o también de tipo radio terrestre profesional TETRA, o bien también un terminal fijo tal como un puesto o una instalación telefónica digital, un ordenador o una red local servida por una red digital de tipo RNIS o IP.

20 En un emisor EM del equipo terminal, un flujo de datos en claro, por ejemplo una señal de palabra digital SP producida por un codificador de palabra CP es cifrada en un flujo de datos cifrados digitales FDC en un cifrador CH. El cifrado de la señal de palabra es periódico a una frecuencia de trama de tráfico y función de secuencias criptográficas que dependen de una palabra de gestión de sincronización SY y de una clave de cifrado secreta K asociada al equipo terminal.

25 La palabra de gestión de sincronización SY es generada y mantenida por un generador de sincronización GS que produce partes de sincronización lenta y partes de sincronización suplementarias que resultan al menos de una descomposición de la palabra de gestión de sincronización SY para aplicarlas en una secuencia de sincronización criptográfica de acuerdo con la invención a una frecuencia de supertrama en una unidad de inserción de sincronización UIS. La unidad UIS produce un flujo de datos cifrados sincronizados FDCS que a continuación es modulado para ser transmitido a través de un canal de transmisión CT hacia el receptor RE de otro equipo terminal. El flujo de datos digitales FDCS es estructurado en supertramas ST de las cuales una o en general varias contienen, cada una, una

30 secuencia de sincronización criptográfica que sirve a la vez para el sincronismo con los receptores de equipos terminales que solamente tengan necesidad de una sincronización lenta preexistente SL de manera conocida en dependencia de la palabra de gestión de sincronización SY, y para el sincronismo con los receptores de equipos terminales que especialmente tengan necesidad de una sincronización rápida SR en dependencia de las partes de sincronización lenta y de las partes de sincronización suplementarias. En la figura 1, se ha supuesto que el receptor RE comprende un circuito de recuperación de sincronización CRS que recupera, tanto la sincronización lenta SL, como la

35 sincronización rápida SR, aunque circuitos de recuperación de sincronización en receptores de otros equipos terminales que pueden comunicar con el emisor EM estén concebidos para recuperar solamente la sincronización lenta SL o la sincronización rápida SR.

40 En la unidad UIS, la transmisión de partes de sincronización lenta en el flujo de datos cifrados FDC es realizada de manera conocida "sobre la marcha", en el período de bloque en una supertrama, ya sea de acuerdo con el primer método de asociación por robos de tramas de tráfico y así la sustitución periódica de tramas de tráfico por partes de sincronización lenta del mismo tamaño, o bien de acuerdo con el segundo método de asociación por introducción periódica de las partes de sincronización lenta de igual tamaño, en un canal lógico, por ejemplo un canal de señalización, asociado a otro canal lógico, tal como un canal de tráfico, que transporta las tramas de tráfico del flujo de

45 datos cifrados FDC.

La inserción de las partes de sincronización suplementarias en el flujo de datos cifrados FDC es realizada de acuerdo con la invención por robos de tramas de tráfico, o bien por robos de bits de tramas de tráfico, es decir por sustitución de tramas de tráfico o bien de bits de tramas de tráfico por partes de sincronización suplementarias en cada supertrama en el flujo de datos cifrados FDC.

50 En lo que sigue de la descripción se hará referencia a dos ejemplos de estructura de supertrama ST.

De acuerdo con el primer ejemplo mostrado en las figuras 3, 4, 7, 8, 11, 12 y 13 una supertrama está compuesta por  $p = 3$  bloques y cada bloque comprende  $n = 24$  tramas numeradas  $T_1$  a  $T_{24}$  en el primer bloque y  $T_{25}$  a  $T_{48}$  en el segundo bloque y  $T_{49}$  a  $T_{72}$  en el tercer bloque. La palabra de gestión de sincronización SY tiene un tamaño de  $p S_{\text{trama}} = 3 S_{\text{trama}}$ , donde  $S_{\text{trama}}$  es el tamaño de una trama,  $p = 3$  partes de sincronización lenta A, B y C (rectángulos rayados hacia la derecha) a priori diferentes entre sí y de tamaño idéntico al de una trama de tráfico que resultan en su totalidad o al menos principalmente de una descomposición de la palabra de gestión de sincronización SY.

De acuerdo con un segundo ejemplo mostrado en las figuras 5, 6, 9 y 10, una supertrama está compuesta por  $p = 4$  bloques y cada bloque comprende  $n = 24$  tramas numeradas  $T_1$  a  $T_{24}$  en el primer bloque,  $T_{25}$  a  $T_{48}$  en el segundo bloque,  $T_{49}$  a  $T_{72}$  en el tercer bloque y  $T_{73}$  a  $T_{96}$  en el cuarto bloque. La palabra de gestión de sincronización SY tiene un tamaño de  $4 S_{\text{trama}}$ ,  $p = 4$  partes de sincronización lenta A, B, C y D (rectángulos rayados hacia la derecha) a priori diferentes entre sí y de tamaño idéntico al de una trama de tráfico que resultan en su totalidad o al menos principalmente de una descomposición de la palabra de gestión de sincronización SY.

Las partes A, B y C o A, B, C y D facilitadas por el generador GS pueden ser simplemente partes consecutivas de la palabra de gestión de sincronización SY cuya concatenación reconstruye la palabra SY, o bien estas partes consecutivas pero según un orden diferente de aquél en la palabra SY. De acuerdo con otras variantes, cada una de las partes A, B y C, o A, B, C y D está compuesta por varias sucesiones de bits de tamaños idénticos o diferentes inferiores al tamaño de una trama, tomados según un orden predeterminado en la palabra de gestión de sincronización SY; por ejemplo las partes A, B y C están respectivamente compuestas de bits de pesos pequeños, de bits de pesos grandes y de bits de pesos grandes de la palabra SY. Las partes A, B y C o A, B, C y D pueden comprender en pequeña proporción elementos, por ejemplo elementos de redundancia, o prefijos o sufijos, que no pertenecen a la palabra de gestión de sincronización SY. Las partes A, B y C o A, B, C y D resultan así al menos de una descomposición predeterminada de la palabra de gestión de sincronización y así son deducidas de una función predeterminada aplicada a la palabra de gestión de sincronización SY. En otras palabras, cada una de las partes A, B y C o A, B, C y D puede comprender, pero no exclusivamente, una o varias porciones respectivas consecutivas o no consecutivas de la palabra SY, y la reunión de todas estas porciones en las partes A, B y C o A, B, C y D está comprendida en la palabra SY.

Una primera realización del procedimiento de sincronización de la invención es relativa al primer método de asociación en lo que concierne a la inserción de las partes de sincronización lenta. El procedimiento comprende etapas E1 a E6 mostradas en la figura 2.

Refiriéndose al primer ejemplo de supertrama ST, el generador de sincronización GS produce a partir de la palabra de gestión de sincronización SY las  $p = 3$  partes de sincronización lenta A, B y C de tamaño idéntico y las aplica a la unidad UIS para insertarlas en el flujo de datos cifrados FDC de acuerdo con el primer método de asociación en la etapa E1. La unidad de inserción de sincronización UIS efectúa un robo periódico de  $p = 3$  tramas en el flujo FDC sustituyendo tres tramas de tráfico  $T_1$ ,  $T_{25}$  y  $T_{49}$  respectivamente por las partes de sincronización lenta A, B y C en la etapa E2. Las partes A, B y C en el flujo FDCS están designadas por A1, B25 y C49 en la supertrama mostrada en la figura 3. Por convenio, el inicio de la supertrama de dimensión 1 en el flujo de datos cifrados sincronizados FDCS puede ser definido por la primera parte A1 dependiente del inicio de la palabra SY. Las partes A1, B25 y C49 que constituyen la información de sincronización criptográfica son así transmitidas en la banda pasante total necesaria para la transmisión del flujo de datos cifrados FDC. Las tramas de tráfico reemplazadas  $T_1$ ,  $T_{25}$  y  $T_{49}$  no son transmitidas entonces.

La unidad de inserción de sincronización UIS puede comprender funcionalidades análogas por ejemplo a las del codificador de voz paramétrico descrito en la solicitud de patente internacional WO 20054/024786 y que sirve para insertar un flujo de información secundario, en concepto de flujo de sincronización criptográfico ABC, en un flujo de información principal, como flujo de datos cifrados FDC, que tiene un caudal más elevado. Esto supone que las tramas del flujo de datos cifrados FDC sean tramas cifradas de acuerdo con el modo OFB o CTR anteriormente citado o un modo con las propiedades similares al modo CTR. Un generador de máscaras de tramas en el codificador de voz selecciona, entre las  $p \times n$  tramas de tráfico en cada supertrama del flujo de datos cifrados FDC, aquellas  $T_1$ ,  $T_{25}$  y  $T_{49}$  en las cuales solamente hay que insertar las partes de sincronización lenta A1, B25 y C49.

Las etapas E1 y E2 son realizadas de una manera conocida.

De acuerdo con la invención, el generador de sincronización GS genera y mantiene igualmente partes de sincronización suplementarias a la frecuencia de supertrama, en la etapa E3 que puede ser simultánea a la etapa E1. El generador GS produce a partir de la palabra de gestión de sincronización  $p = 3$  partes de sincronización suplementarias a, b y c respectivamente similares a las partes de sincronización lenta A, B y C de tamaño idéntico al de una trama de tráfico. El término "similares" significa que las partes de sincronización suplementarias a, b y c pueden ser idénticas respectivamente a las partes de sincronización lenta A, B y C, o bien pueden ser en una pequeña proporción diferentes

respectivamente de las partes A, B y C. En esta última variante, las partes a, b y c comprenden por ejemplo prefijos o sufijos que son respectivamente diferentes de los de las partes A, B y C. Las sensibles diferencias entre las partes de los pares (A, a), (B, b) y (C, c) no contravienen en el receptor a la reconstitución de la palabra de origen SY a partir de una secuencia de tipo AcB, cBa, BaC, aCb, CbA o bAC, como se verá en lo que sigue de la descripción.

5 Finalmente, en la etapa E4 intermedia entre las etapas E1-E3 y E2-E5, el generador GS entrelaza las partes de sincronización lenta A, B y C con las partes de sincronización suplementarias a, b y c para constituir una secuencia de sincronización criptográfica AcBaCb.

10 La secuencia cab (rectángulos rayados cruzados) deducida de la palabra de sincronización SY es aplicada siendo entrelazada con las partes A, B y C a la unidad UIS para ser igualmente insertada en el flujo de datos cifrados FDC, en la etapa E5. En la práctica, las etapas E2 y E5 están entrelazadas de conformidad con el entrelazamiento de las secuencias ABC y cab. La unidad de inserción de sincronización UIS efectúa un robo periódico de  $p = 3$  tramas en el flujo FDC sustituyendo tres tramas de tráfico  $T_{12}$ ,  $T_{36}$  y  $T_{60}$  respectivamente por las partes c, a y b que son designadas por C12, A36 y B60 en la supertrama mostrada en la figura 4. La secuencia de sincronización criptográfica AcBaCb es así transmitida en la banda pasante total necesaria para la transmisión del flujo de datos cifrados FDC, en la etapa E6.

15 Las tramas de tráfico reemplazadas  $T_1$ ,  $T_{12}$ ,  $T_{25}$ ,  $T_{36}$ ,  $T_{49}$  y  $T_{60}$  no son transmitidas.

20 En la supertrama de dimensión 1 del flujo de datos cifrados sincronizados FDCS, el entrelazamiento de las partes A, B y C con las partes c, a y b en la secuencia de sincronización criptográfica AcBaCb es tal que una parte de sincronización suplementaria c que depende sensiblemente del final de la palabra de gestión de sincronización SY es insertada en la supertrama después de otra parte de sincronización lenta A que depende del inicio de la palabra de gestión de sincronización. En otras palabras, bits de peso grande de la palabra de gestión de sincronización SY preceden a bits de pesos pequeños de la palabra de gestión de sincronización SY con el fin de que en el receptor RE el conocimiento de una parte de sincronización lenta SY y de dos partes de sincronización suplementarias, o el conocimiento de dos partes de sincronización suplementarias y una parte de sincronización lenta, sirva para reconstruir la palabra de gestión de sincronización SY  $\equiv ABC$ ,  $\equiv abc$  en entero. Esta característica es útil para el circuito de recuperación de sincronización CRS en el receptor RE de otro equipo terminal que tenga necesidad de una sincronización rápida SR para encontrar siempre la palabra de gestión de sincronización en tres partes consecutivas de la secuencia de sincronización criptográfica recibida, o sea AcB, cBa, BaC, aCb, CbA y bAc. La detección de una secuencia AcB, cBa, BaC, aCb, CbA, bAc resulta de la observación de, cómo mucho, 2 bloques consecutivos de la supertrama ST. Estos bloques consecutivos de la supertrama son por tanto en número estrictamente inferior al número

25 de 3 bloques en la supertrama y contribuyen a reconstituir las mismas informaciones que la secuencia ABC en el receptor RE.

30 El orden de inserción de las partes de sincronización suplementarias c, a y b optimiza la rapidez de reconstitución de la palabra de gestión de sincronización SY. En el receptor, el reconocimiento de las partes c, a y b puede ser similar pero distinto del reconocimiento de las partes de la secuencia ABC: por ejemplo, es conveniente la utilización de diferentes prefijos pseudoaleatorios determinados en el inicio de las partes A, B, C, a, b y c; es conveniente también la utilización de prefijos no todos idénticos.

35 Aunque cada parte de sincronización suplementaria c, a o b pueda reemplazar a cualquier trama de tráfico comprendida en el primero, segundo o tercer bloque en la supertrama, es preferible que las tramas de tráfico  $T_{12}$ ,  $T_{36}$  y  $T_{60}$  reemplazadas por las partes de sincronización suplementaria c, a y b estén temporalmente situadas sensiblemente en la mitad respectivamente de los bloques de la supertrama, como aparece en la figura 4. Estas posiciones temporales de las partes c, a y b sensiblemente centrales en los bloques reducen al mínimo el período medio de recuperación de la sincronización rápida. En efecto, en los peores casos, cuando la sincronización rápida es activada en el receptor RE justo después de la detección de una cualquiera de las tramas de sincronización A1, C12, B25, A36, C49 y B60 que aseguran en combinación la sincronización lenta preexistente de acuerdo con la técnica anterior y la sincronización rápida de acuerdo con la invención, el circuito de recuperación de sincronización CRS en el receptor observa como mucho la mitad de la supertrama ST, es decir como mucho las tramas en durante 1,5 períodos de bloque de acuerdo con este primer ejemplo de supertrama, para recuperar una de las secuencias AcB, cBa, BaC, aCb, CbA, bAc y reconstituir las mismas informaciones que la palabra de gestión de sincronización SY  $\equiv ABC$ .

40

45

50 Como ilustración, para el caudal  $B = 2400$  bit/s de los flujos FDC y FDCS y parámetros  $S_{\text{trama}} = 54$  bits,  $n = 24$ ,  $p = 3$  y por tanto  $k = 2$ , el período de sincronización rápida es  $T'_{\text{sinc}} = (n \cdot 1,5 \cdot S_{\text{trama}})/B = 0,81$  s para un posicionamiento temporal de las partes de sincronización suplementarias c, a y b sensiblemente central en los bloques de la supertrama, como muestra la figura 6. En el peor de los casos, si dos partes de sincronización suplementarias, por ejemplo c y a, son insertadas en extremidades opuestas en bloques consecutivos de la supertrama, en sustitución de la trama de tráfico  $T_1$  que sucede a la trama de sincronización lenta A1 y en sustitución de la trama de tráfico  $T_{48}$  que precede a la trama de sincronización lenta C49, el período de sincronización rápida se extiende como mucho en aproximadamente dos bloques, o sea menos de  $2n$  tramas, o sea  $T'_{\text{sinc}} < (2 \cdot n \cdot S_{\text{trama}})/B = 1,08$  s. En todos los casos, el período de

55

sincronización rápida es netamente inferior al período de sincronización lenta de la palabra de gestión de sincronización  $SY \equiv ABC$  extendido como mucho en  $3n$  tramas, o sea  $T_{\text{sync}} = (3 n S_{\text{trama}})/B = 1,62 \text{ s}$ .

Se hará referencia ahora al segundo ejemplo de supertrama ST para la primera realización del procedimiento de sincronización de la invención.

5 El generador de sincronización GS produce a partir de la palabra de gestión de sincronización SY a la frecuencia de supertrama,  $p = 4$  partes de sincronización lenta A, B, C y D y  $p = 4$  partes de sincronización suplementarias a, b, c y d de tamaño idéntico, en las etapas E1 y E3. Las partes de sincronización suplementarias a, b, c y d son respectivamente similares a las partes de sincronización lenta A, B, C y D. En la etapa E4, el generador GS entrelaza las partes de sincronización lenta A, B, C y D con las partes de sincronización suplementarias a, b, c y d para constituir una secuencia de sincronización criptográfica AcBdCaDb.

10 La secuencia AcBdCaDb resultante de un entrelazamiento de orden 2 de las partes de sincronización lenta y de las partes de sincronización suplementarias es aplicada a la unidad UIS que la inserta en el flujo de datos cifrados FDC de acuerdo con el primer método de asociación, en las etapas E2 y E5. La unidad de inserción de sincronización UIS efectúa un robo periódico de  $2p = 8$  tramas en el flujo FDC reemplazando cuatro tramas de tráfico  $T_1, T_{25}, T_{49}$  y  $T_{73}$  respectivamente por las partes de sincronización lenta A, B, C y D que son designadas por A1, B25, C49 y D73 en la supertrama mostrada en la figura 6, y reemplazando cuatro tramas de tráfico  $T_{12}, T_{36}, T_{60}$  y  $T_{84}$  respectivamente por las partes de sincronización suplementarias c, d, a y b que son designadas por C12, D36, A60 y B84 (rectángulos con rayas cruzadas) en la supertrama mostrada en la figura 6.

20 En comparación con la supertrama mostrada en la figura 5 que únicamente comprende la palabra de gestión de sincronización  $SY = ABCD$  y relativa a la sincronización lenta SL de acuerdo con la técnica anterior, la invención añade las  $p = 4$  partes de sincronización suplementarias, c, d, a y b. La secuencia de sincronización criptográfica AcBdCaDb es así transmitida en la banda pasante total necesaria para la transmisión del flujo de datos cifrados FDC, en la etapa E6. Las tramas de tráfico reemplazadas  $T_1, T_{12}, T_{25}, T_{36}, T_{49}, T_{60}, T_{73}$  y  $T_{84}$  no son transmitidas.

25 La secuencia de sincronización criptográfica AcBdCaDb presenta características análogas a la secuencia AcBaCb. El circuito de recuperación de sincronización CRS en el receptor RE de otro equipo terminal que tenga necesidad de una sincronización rápida SR encuentra siempre la palabra de gestión de sincronización  $SY \equiv ABCD$  en como mucho cinco partes consecutivas de la secuencia de sincronización criptográfica recibida, o sea AcBd, cBdCa, BdCa, dCaDb, CaDb, aDbAc, DbAc, bAcBd, al tiempo que preserva la secuencia de sincronización lenta ABCD. La detección de una secuencia AcBd, cBdCa, BdCa, dCaDb, CaDb, aDbAc, DbAc, bAcBd permite reconstituir las mismas informaciones de sincronización que la secuencia ABCD en el receptor RE.

30 Las posiciones temporales de las partes de sincronización suplementarias c, d, a y b son preferentemente sensiblemente centrales en los bloques con el fin de optimizar la rapidez de reconstitución de la palabra de sincronización  $ABCD \equiv SY$  y reducir al mínimo el período medio de recuperación de la sincronización rápida en el circuito de recuperación de sincronización CRS del receptor.

35 Tomando de nuevo los mismos valores de caudal y de parámetros pero con  $p = 4$ , el período de sincronización rápida  $T'_{\text{sync}}$  se extiende como mucho en dos bloques, o sea menos de  $2n$  tramas:

$$T'_{\text{sync}} \leq (n k S_{\text{trama}})/B = (24 \times 2 \times 54) / 2400 = 1,08 \text{ s}$$

El período de sincronización rápida es todavía inferior al período de sincronización lenta de la palabra de gestión de sincronización  $SY \equiv ABCD$  extendida en  $4n$  tramas, o sea  $T_{\text{sync}} = (n 4 S_{\text{trama}})/B = 2,16 \text{ s}$ .

40 Otras secuencias de sincronización criptográfica presentan características análogas a las secuencias precedentes AcBaCb y AcBdCaDb. Así, en el orden d, a, b y c, las partes de sincronización suplementarias son entrelazadas con las partes de sincronización lenta A, B, C y D para formar la secuencia de sincronización rápida AdBaCbDc en el flujo de datos cifrados, al tiempo que preserva la secuencia de sincronización lenta preexistente ABCD.

45 De modo más general, el número de partes de sincronización lenta y el número de partes de sincronización suplementarias pueden ser superiores a cuatro, cualquiera que sea el número  $n$  de tramas por bloque.

Una segunda realización del procedimiento de sincronización de la invención es relativa al segundo método de asociación en lo que concierne a la inserción de las partes de sincronización lenta. El procedimiento comprende etapas análogas a las etapas E1 a E6 mostradas en la figura 2 y se describe a continuación igualmente refiriéndose al primer y al segundo ejemplos de estructura de supertrama ST.

50 De acuerdo con la técnica anterior, el generador de sincronización GS produce a partir de la palabra de gestión de sincronización SY las  $p = 3$  partes de sincronización lenta A, B y C de acuerdo con el primer ejemplo, o las  $p = 4$

partes de sincronización lenta A, B, C y D de acuerdo con el segundo ejemplo, en la etapa E1. Estas partes de sincronización lenta son de tamaños idénticos, y aplicadas a la unidad de inserción de sincronización UIS. En lugar de degradar sensiblemente la fonía por la inserción de las partes de sincronización lenta en el canal de tráfico de acuerdo con el primer método de asociación y por tanto por ocupación de recursos útiles para la comunicación, la unidad UIS inserta las partes de sincronización lenta A, B y C, o A, B, C y D, en otro canal lógico asociado al canal de tráfico que transporta el flujo de datos cifrados FDC, de acuerdo con el segundo método de asociación.

Por ejemplo, de acuerdo con la solicitud de patente internacional WO 2004/014019, el canal de tráfico está compuesto por intervalos de tiempo de un primer tipo multiplexados por división de tiempo TDMA ("Time Division Multiple Access" en inglés) ocupados por las tramas de tráfico, como en la primera realización, y el otro canal lógico es un canal de señalización formado por al menos un intervalo de tiempo de un segundo tipo ocupado por las partes de sincronización lenta. En el canal de señalización es introducida igualmente una información de retardo representativa del desvío temporal entre un intervalo de tiempo del segundo tipo y una trama de tráfico que es transmitida cuando una parte de sincronización lenta es transmitida. Las partes de sincronización lenta pueden ser transmitidas en el canal de señalización cuando recursos de éste están disponibles.

Por ejemplo, cuando el emisor EM está en un equipo terminal tal como un móvil de una red celular, el canal de tráfico es un canal lógico de tráfico ascendente o descendente TCH (de "Traffic CHannel" en inglés) establecido en una frecuencia predeterminada y multiplexado temporalmente con otros canales lógicos: canales de tráfico atribuidos a otros móviles y al menos a un canal de señalización. El canal de señalización es un canal de control lento de tipo SACCH ("Slow Associated Control CHannel" en inglés) que transporta las partes de la palabra de gestión de sincronización A, B y C o A, B, C y D, y así asegura una sincronización lenta del canal de tráfico asociado, sin alterar el canal de tráfico por robos de trama. Así, en las figuras 7 y 9, se supone por convenio que el inicio de la supertrama de dimensión 2, correspondiente a un multiplexado de canales de orden 2, en el flujo de datos cifrados sincronizados FDCS y por tanto el inicio del primer bloque están definidos por la primera parte de sincronización lenta A dependiente del inicio de la palabra SY y que ocupa un intervalo de tiempo A1 del canal de señalización que precede a la primera trama de tráfico T<sub>1</sub>. Al inicio de los bloques siguientes a n = 24 tramas de tráfico, la segunda parte B ocupa un intervalo de tiempo B25 del canal de señalización que precede a la primera trama de tráfico T<sub>25</sub> del segundo bloque de la supertrama y la tercera parte C ocupa un intervalo de tiempo C49 del canal de señalización que precede a la primera trama de tráfico T<sub>49</sub> del tercer bloque de la supertrama, y para la supertrama de acuerdo con el segundo ejemplo (véase la figura 9), la cuarta parte D ocupa un intervalo de tiempo D73 del canal de señalización que precede a la primera trama de tráfico T<sub>73</sub> del cuarto bloque de la supertrama.

Las partes A1, B25 y C49, o A1, B25, C49 y D73, representativas de la información de sincronización criptográfica es así transmitida fuera de la banda pasante necesaria para la transmisión del flujo de datos cifrados FDC que no es alterado.

Para asociar las partes de sincronización lenta fuera de la banda del flujo de datos cifrados, la unidad de inserción de sincronización UIS puede comprender funcionalidades análogas por ejemplo a las de la parte de recepción del terminal móvil de acuerdo con la solicitud de patente internacional WO 2004/014019, y especialmente del circuito de tratamiento de señal que hay que emitir en esta parte de recepción.

De acuerdo con la invención, el generador de sincronización GS genera igualmente a partir de la palabra de gestión de sincronización SY a la frecuencia de supertrama, en la etapa E3, y mantiene p = 3 partes de sincronización suplementarias a, b y c respectivamente similares a las partes de sincronización lenta A, B y C, o p = 4 partes de sincronización suplementarias a, b, c y d respectivamente similares a las partes de sincronización lenta A, B, C y D, y de tamaño idéntico al de una trama de tráfico. En la etapa E4 intermedia entre las etapas E1-E3 y E4-E5, el generador GS entrelaza las partes de sincronización lenta A, B y C o A, B, C y D, con las partes de sincronización suplementarias a, b y c, o a, b, c y d (rectángulos con rayas cruzadas), para constituir una secuencia de sincronización criptográfica AcBaCb según la figura 8, o AcBdCaDb según la figura 10.

La secuencia cab, o cdba, deducida de la palabra de gestión de sincronización SY y entrelazada con las partes A, B y C, o A, B, C y D, es aplicada a la unidad UIS para insertarla en el flujo de datos cifrados FDC por robo periódico de trama de tráfico en la etapa E5, como en la primera realización. Para insertar las partes de sincronización suplementarias a, b y c o a, b, c y d en la banda del flujo de datos cifrados, la unidad de inserción de sincronización UIS puede comprender funcionalidades análogas por ejemplo a las del codificador de voz paramétrico que incluye un generador de máscaras de tramas de tráfico y descrito en la patente internacional WO 2004/024786.

Así, lo que se ha descrito para la primera realización en lo que concierne a las partes de sincronización suplementarias a, b y c, o a, b, c y d es válido para la segunda realización. Como se ve en la figura 8, en acuerdo con la figura 4 según el primer ejemplo, las tres tramas de tráfico T<sub>12</sub>, T<sub>36</sub> y T<sub>60</sub> son reemplazadas respectivamente por las partes c, a y b designadas por C12, A36 y B60; estas partes están situadas temporalmente sensiblemente en la mitad

respectivamente de los bloques de la supertrama y están entrelazadas con las partes A1, B25 y C49, estando las partes A1, B25 y C49 repartidas fuera de la banda en la supertrama como muestra igualmente la figura 7 de la técnica anterior; el circuito de recuperación de sincronización CRS en el receptor RE que recibe el canal de tráfico y el canal de señalización detecta secuencias de sincronización rápida AcB, cBa, BaC, aCb, CbA, bAc que cada una le permiten reconstituir las mismas informaciones que la secuencia ABC. De acuerdo con el segundo ejemplo mostrado en la figura 10, en acuerdo con la figura 6, las cuatro tramas de tráfico  $T_{12}$ ,  $T_{36}$ ,  $T_{60}$  y  $T_{84}$  son reemplazadas respectivamente por las partes c, d, a y b designadas por C12, D36, A60 y B84; estas partes están situadas temporalmente sensiblemente en la mitad respectivamente de los bloques de la supertrama y están entrelazadas con las partes A1, B25, C49 y D73, estando las partes A1, B25, C49 y D73 repartidas fuera de la banda en la supertrama como muestra igualmente la figura 9 de la técnica anterior; el circuito de recuperación de sincronización CRS detecta secuencias de sincronización rápida AcBd, cBdCa, BdCa, dCaDb, CaDb, aDbAc, DbAc, bAcBd, que cada una le permiten reconstituir las mismas informaciones que la secuencia ABCD.

La sincronización rápida es posible al menos en 25 tramas según la figura 8, como según la figura 4, y en el peor de los casos en como mucho 47 tramas si dos partes de sincronización suplementarias, por ejemplo c y a, están insertadas en extremidades opuestas en bloques consecutivos de la supertrama. De una manera similar, la sincronización rápida es posible en al menos 36 tramas según la figura 10, como según la figura 6, y en el peor de los casos en como mucho 72 tramas.

La secuencia de sincronización criptográfica AcBaCb o AcBdCaDb asegura también la coexistencia de la sincronización lenta preexistente SL y de la sincronización rápida SR.

La invención no está limitada a las dos realizaciones descritas anteriormente, sino que abarca otras realizaciones algunas de las cuales se presentan a continuación. El número de partes que componen una secuencia de sincronización criptográfica puede ser superior a ocho.

Se hará referencia ahora a las figuras 11, 12 y 13 que son relativas al primer método de asociación en lo que concierne a las partes de sincronización lenta (rectángulos rayados hacia la derecha). Sin embargo, todo lo que se precisa a continuación concerniente a la repartición de partes de sincronización lenta en el flujo de datos cifrados FDC por robos de bits de tráfico es igualmente válido para otros ejemplos y para el segundo método de asociación.

En las figuras 11, 12 y 13, la sincronización lenta preexistente depende de  $p = 3$  partes A, B y C deducidas de la palabra de gestión de sincronización SY según el primer ejemplo. El generador de sincronización GS genera las partes de sincronización suplementarias a, b y c que son respectivamente similares a las partes de sincronización lenta A, B y C. Sin embargo, las partes de sincronización suplementarias a, b y c son a su vez divididas en subpartes (rectángulos con rayas cruzadas) cuyo tamaño es inferior al tamaño  $S_{\text{trama}}$  de las tramas de tráfico con el fin de que la sincronización rápida solamente sea puesta en práctica de modo intermitente, por ejemplo en ciertas tramas de tráfico, o solamente en ciertos bloques de tramas en todas o solamente algunas supertramas. En función especialmente de las características del flujo de datos cifrados que haya que preservar en el transcurso de la transmisión entre el emisor EM y el receptor RE, la sincronización rápida puede ser reducida al mínimo en número de tramas afectadas por robos de bits para insertar las partes de sincronización suplementarias.

De acuerdo con la figura 11, las partes de sincronización suplementarias c, a y b presentan conjuntamente tantas subpartes como tramas de tráfico en una supertrama ST, o sea  $p(n-1)$  subpartes. La unidad de inserción de sincronización UIS inserta en cada trama de tráfico una subparte de sincronización suplementaria en sustitución de bits que tienen rangos predeterminados en la trama de tráfico. Así, las subpartes que reemplazan a bits de tráfico en las tramas de tráfico de los primero, segundo y tercero bloques resultan de fragmentaciones respectivamente de las partes de sincronización suplementarias c, a y b con el fin de insertar la secuencia de sincronización criptográfica AcBaCb en el flujo de datos cifrados FDC. La inserción de las partes c, a y b según la figura 11 preserva parcialmente todas las tramas de tráfico, y la sincronización rápida es posible en al menos 25 tramas y en como mucho 47 tramas.

La realización de acuerdo con la figura 12 difiere de la figura 11 en el número de subpartes de las partes de sincronización suplementarias que es inferior al número  $p(n-1)$  de tramas de tráfico en una supertrama ST. Las partes c, a y b están respectivamente repartidas en sustitución de bits que tienen rangos predeterminados en tramas de tráfico que a su vez tienen rangos predeterminados en los bloques de la supertrama. De acuerdo con el ejemplo de la figura 11, bits al final de las tres primeras tramas de tráfico que suceden a una parte de sincronización lenta A1, B25, C49 en los tres bloques son reemplazados por subpartes de las respectivas partes de sincronización suplementarias c, a y b y las otras tramas de tráfico son mantenidas sin ningún robo de bits.

Refiriéndose a la figura 13 y en comparación con las figuras 11 o 12, en lugar de repartir las partes de sincronización suplementarias c, a y b en todas o en ciertas tramas de tráfico de todos los bloques de una supertrama ST, la unidad de inserción de sincronización UIS inserta subpartes de las partes de sincronización suplementarias en

sustitución de bits que tienen rangos predeterminados en todas o en ciertas tramas de tráfico de un solo bloque de una supertrama ST, por ejemplo el primer bloque de ésta.

Para las realizaciones según las figuras 11, 12 y 13, cuando el modelo de fuente del flujo de datos que hay que cifrar prevé diferentes clases de bits en función de su sensibilidad con respecto a la calidad de codificación de la señal de palabra de la que procede el flujo de datos cifrados FDC, los bits o algunos bits de las partes de sincronización suplementarias reemplazan a los bits menos sensibles de tramas de tráfico. Los bits menos sensibles en las tramas de tráfico pueden ser elegidos entre aquéllos que contribuyen menos a la calidad objetiva o subjetiva de la señal de palabra descifrada por el codificador-descodificador utilizado en el receptor y que pertenecen a una clase de bits de protección predeterminada para la codificación del canal entre el emisor y el receptor.

Como ilustración, para un caudal  $B = 2400$  bit/s de los flujos FDC y FDCS y parámetros  $S_{\text{trama}} = 54$  bits,  $n = 24$  y  $p = 3$ , el período de sincronización rápida es en el mejor de los casos  $T'_{\text{sinc}} = (n - 1 S_{\text{trama}})/B = 0,54$  s para  $3 \times 54$  bits robados en el primer bloque para insertar las partes de sincronización suplementarias según la figura 13, y en el peor de los casos  $T'_{\text{sinc}} = (n - 2 S_{\text{trama}})/B = 1,08$  s para  $n = 54$  bits robados por bloque para insertar las partes de sincronización suplementarias según las figuras 11 o 12.

Cualquiera que sea la realización, la secuencia de sincronización criptográfica que entrelaza las partes de sincronización lenta y las partes de sincronización suplementarias asegura a la vez la sincronización lenta SL y la sincronización rápida SR.

El procedimiento de acuerdo con la invención encuentra aplicaciones especialmente en el ámbito de las telecomunicaciones seguras. Éste está adaptado a la sincronización criptográfica entre equipos terminales, fijos y/o móviles, que operan en redes heterogéneas interconectadas cuyas constantes temporales de sincronización difieren.

Una aplicación típica concierne a la sincronización criptográfica de flujos de datos cifrados en tiempo real entre un terminal fijo y un terminal móvil. El terminal fijo solamente es compatible con una sincronización criptográfica lenta. El terminal móvil necesita además una sincronización criptográfica rápida, por ejemplo con ocasión de una transferencia intercelular ("handover" en inglés), para no interrumpir una conversación establecida entre los dos terminales.

En una comunicación de fonía cifrada, si la fuente de tráfico cifrado es un codificador de voz que pone en práctica tramas de silencio, el emisor del flujo de datos de tráfico cifrados puede imponer que la sincronización rápida sea insertada al menos en supertramas o bloques que correspondan a ventanas temporales de silencio.

En una comunicación cifrada que implique a varias redes de telecomunicación heterogénea interconectadas, el procedimiento de la invención es ventajosamente puesto en práctica en todas las redes  $x$  que necesiten una sincronización rápida, al tiempo que se preserva la sincronización lenta necesaria en las otras redes interconectadas. Para esto, el procedimiento de la invención es puesto en práctica en cualquier terminal conectado a una red interconectada que necesite una sincronización rápida, como por ejemplo un terminal radio móvil en una red de radiocomunicación celular. El procedimiento es puesto en práctica igualmente en equipos de telecomunicación que realizan una pasarela entre una red de radiocomunicación celular y una red de telecomunicación fija tal como una red de telecomunicación conmutada o una red de paquetes de tipo internet o intranet. Así, el flujo de datos cifrados que proviene de un terminal de sincronización lenta, por ejemplo un terminal de una red fija de tipo RNIS, puede ser aumentado con robos de trama suplementarios que aseguran la sincronización rápida, como por ejemplo un terminal móvil de una red de radiocomunicación celular. En el sentido inverso, el flujo que contiene las tramas de sincronización lenta y las tramas de sincronización rápida emitido por un terminal rápido, es tratado a la vez por el receptor de un terminal de sincronización rápida que reconoce la sincronización rápida y la sincronización lenta, y por el receptor de un terminal de sincronización lenta que reconoce la sincronización lenta y trata las tramas de sincronización rápida como tramas de tráfico que han sufrido una interferencia.

## REIVINDICACIONES

1. Procedimiento de sincronización aplicado a un flujo de datos (FDCS) estructurado en supertramas (ST) formadas cada una por bloques de tramas, comprendiendo cada bloque en una supertrama (ST) una parte de sincronización lenta (A, B, C) y al menos una trama de tráfico ( $T_2$  a  $T_{24}$  o  $T_1$  a  $T_{24}$ ), siendo las partes de sincronización lenta (A, B, C) en la supertrama (ST) diferentes entre sí y resultantes al menos de una descomposición de una palabra de gestión de sincronización (SY), caracterizado en la supertrama (ST) por una sustitución (E5) de bits de tramas de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) en la supertrama (ST) por partes de sincronización suplementarias (a, b, c) cada una de las cuales es como mucho en una pequeña proporción diferente de una respectiva parte de sincronización lenta (A, B, C) para permitir, durante una recepción de la supertrama (ST), una reconstitución de la palabra de gestión de sincronización (SY) por observación de bloques consecutivos en la supertrama (ST) en número estrictamente inferior al número de bloques en la supertrama (ST).
2. Procedimiento de acuerdo con la reivindicación 1, según el cual al menos una parte de sincronización suplementaria (c; d) dependiente sensiblemente del final de la palabra de gestión de sincronización es insertada en la supertrama (ST) después de otra parte de sincronización lenta (A) dependiente del inicio de la palabra de gestión de sincronización.
3. Procedimiento de acuerdo con las reivindicaciones 1 o 2, según el cual una de las citadas partes de sincronización suplementarias (a, b, c) reemplazan a una trama de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) en un bloque de la supertrama (ST).
4. Procedimiento de acuerdo con las reivindicaciones 1 o 2, según el cual las partes de sincronización suplementarias (a, b, c) reemplazan respectivamente a tramas de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) en bloques de la supertrama (ST), a razón de una trama de tráfico por bloque.
5. Procedimiento de acuerdo con la reivindicación 4, según el cual las tramas de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) reemplazadas por las partes de sincronización suplementarias (a, b, c) están temporalmente situadas sensiblemente en la mitad de los bloques de la supertrama (ST).
6. Procedimiento de acuerdo con las reivindicaciones 1 o 2, según el cual una de las partes de sincronización suplementarias reemplazan a bits predeterminados en tramas de tráfico predeterminadas en un bloque de la supertrama (ST).
7. Procedimiento de acuerdo con las reivindicaciones 1 o 2, según el cual las partes de sincronización suplementarias tienen subpartes que tienen un tamaño inferior al tamaño de las tramas de tráfico y que están repartidas en sustitución de bits predeterminados en tramas de tráfico en la supertrama (ST).
8. Procedimiento de acuerdo con las reivindicaciones 1, 2 o 7, según el cual las partes de sincronización suplementarias tienen subpartes que tienen un tamaño inferior al tamaño de las tramas de tráfico y que están repartidas en sustitución de bits en tramas de tráfico que tienen rangos predeterminados en bloques predeterminados de la supertrama (ST).
9. Procedimiento de acuerdo con las reivindicaciones 1, 2 o 7, según el cual las partes de sincronización suplementarias tienen subpartes que tienen un tamaño inferior al tamaño de las tramas de tráfico y que están repartidas en sustitución de bits de tramas de tráfico incluidas en un bloque de la supertrama (ST).
10. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 6 a 9, caracterizado porque bits de tramas de tráfico en la supertrama (ST) reemplazados por las partes de sincronización suplementarias son los bits menos sensibles de tramas de tráfico.
11. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 10, según el cual el número de bloques consecutivos observados en la supertrama (ST) durante la reconstitución de la palabra de gestión de sincronización (SY) es inferior sensiblemente a la mitad del número de bloques en la supertrama (ST).
12. Supertrama (ST) que comprende una secuencia de sincronización y está formada por bloques de tramas digitales, comprendiendo cada bloque en la supertrama (ST) una parte de sincronización lenta (A, B, C) y al menos una trama de tráfico ( $T_2$  a  $T_{24}$  o  $T_1$  a  $T_{24}$ ), siendo las partes de sincronización lenta en la supertrama (ST) diferentes entre sí y resultantes al menos de una descomposición de una palabra de gestión de sincronización (SY), caracterizada porque comprende partes de sincronización suplementarias (a, b, c) de las cuales cada una es como mucho en una pequeña proporción diferente de una respectiva parte de sincronización lenta (A, B, C) y que están repartidas en sustitución de bits de tramas de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) en la supertrama (ST), para permitir, durante una recepción de la supertrama

(ST), una reconstitución de la palabra de gestión de sincronización (SY) por observación de bloques consecutivos en la supertrama (ST) en número estrictamente inferior al número de bloques en la supertrama (ST).

13. Supertrama (ST) de acuerdo con la reivindicación 12, del tipo AcBaCb en la cual a, b y c designan partes de sincronización suplementarias respectivamente en pequeñas proporciones diferentes de partes de sincronización lenta A, B y C y entrelazadas con estas últimas en la supertrama (ST).

14. Supertrama (ST) de acuerdo con la reivindicación 12, del tipo AcBdCaDb o AdBaCbDc en la cual a, b, c y d designan partes de sincronización suplementarias respectivamente en pequeñas proporciones diferentes de partes de sincronización lenta A, B, C y D y entrelazadas con estas últimas en la supertrama (ST).

15. Emisor (EM) apto para emitir un flujo de datos (FDCS) estructurado en supertramas (ST) formadas cada una por bloques de tramas, comprendiendo cada bloque en una supertrama (ST) una parte de sincronización lenta (A, B, C) y al menos una trama de tráfico ( $T_2$  a  $T_{24}$  o  $T_1$  a  $T_{24}$ ), siendo las partes de sincronización lenta (A, B, C) en la supertrama (ST) diferentes entre sí y resultantes al menos de una descomposición de una palabra de gestión de sincronización (SY), caracterizado porque comprende un medio (GS, UIS) para reemplazar bits de tramas de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) en la supertrama (ST) por partes de sincronización suplementarias (a, b, c) de las cuales cada una es como mucho en pequeña proporción diferente de una respectiva parte de sincronización lenta (A, B, C) para permitir, por un receptor (RE) de la supertrama (ST), una reconstitución de la palabra de gestión de sincronización (SY) por observación de bloques consecutivos en la supertrama (ST) en número estrictamente inferior al número de bloques en la supertrama (ST).

16. Receptor (RE) apto para recibir un flujo de datos (FDCS) estructurado en supertramas (ST) formadas cada una por bloques de tramas, comprendiendo cada bloque en una supertrama (ST) una parte de sincronización lenta (A, B, C) y al menos una trama de tráfico ( $T_2$  a  $T_{24}$  o  $T_1$  a  $T_{24}$ ), siendo las partes de sincronización lenta (A, B, C) en la supertrama (ST) diferentes entre sí y resultantes al menos de una descomposición de una palabra de gestión de sincronización (SY), caracterizado porque comprende un medio (CRS) para reconstituir la palabra de gestión de sincronización (SY) por observación de bloques consecutivos en la supertrama (ST) en número estrictamente inferior al número de bloques en la supertrama (ST) en la cual partes de sincronización suplementarias (a, b, c) de las cuales cada una es como mucho en una pequeña proporción diferente de una respectiva parte de sincronización lenta (A, B, C), reemplazan a bits de tramas de tráfico ( $T_{12}$ ,  $T_{36}$ ,  $T_{60}$ ) en la supertrama (ST).

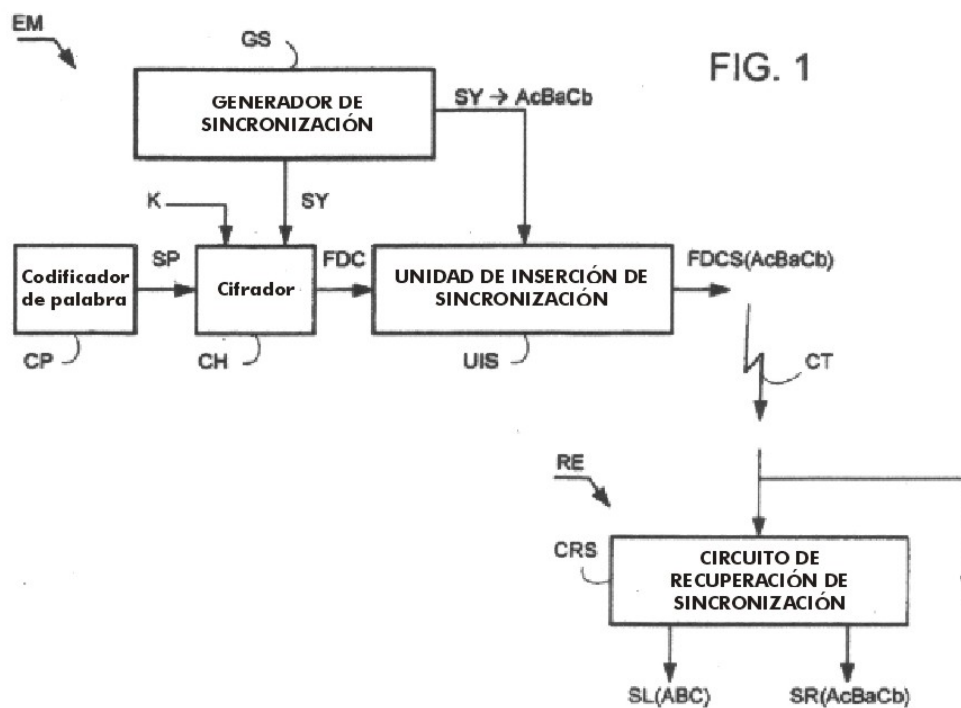


FIG. 2

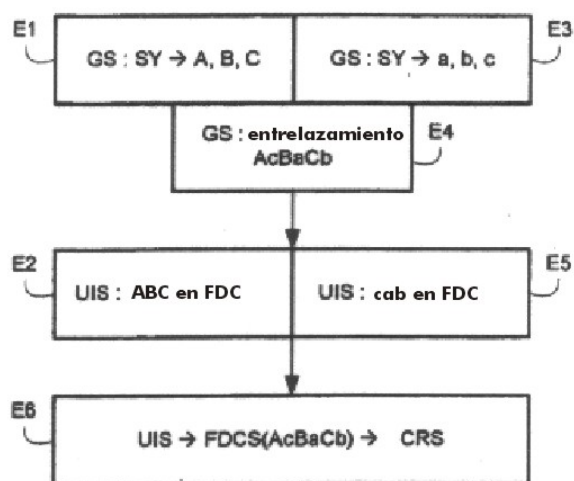


FIG. 3

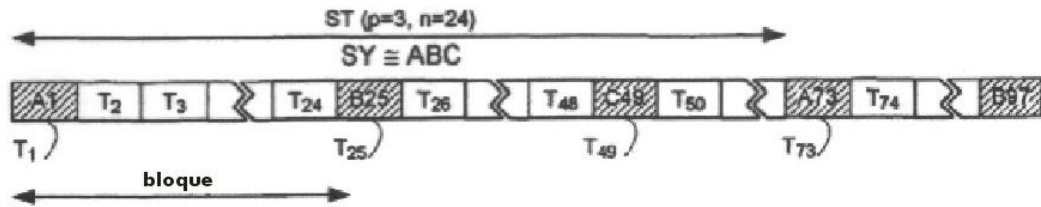


FIG. 4

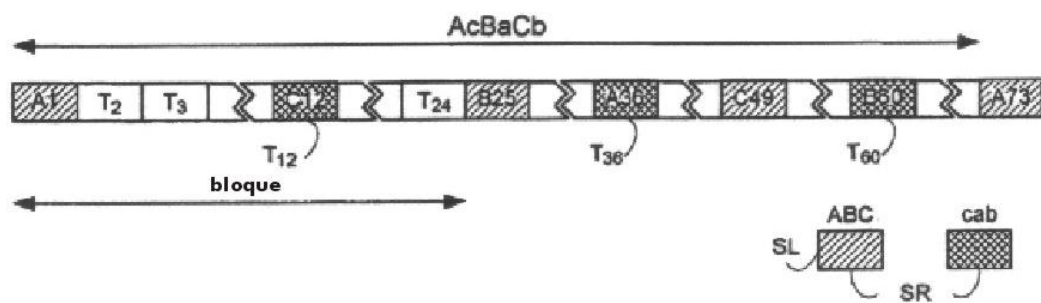


FIG. 5

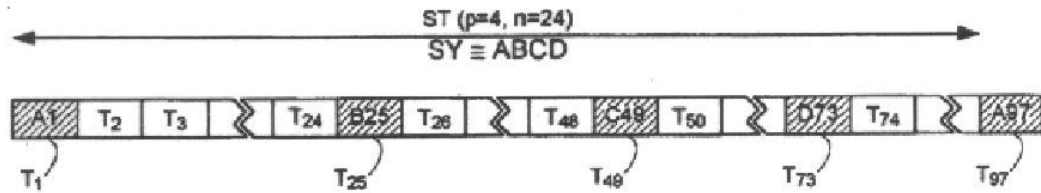


FIG. 6

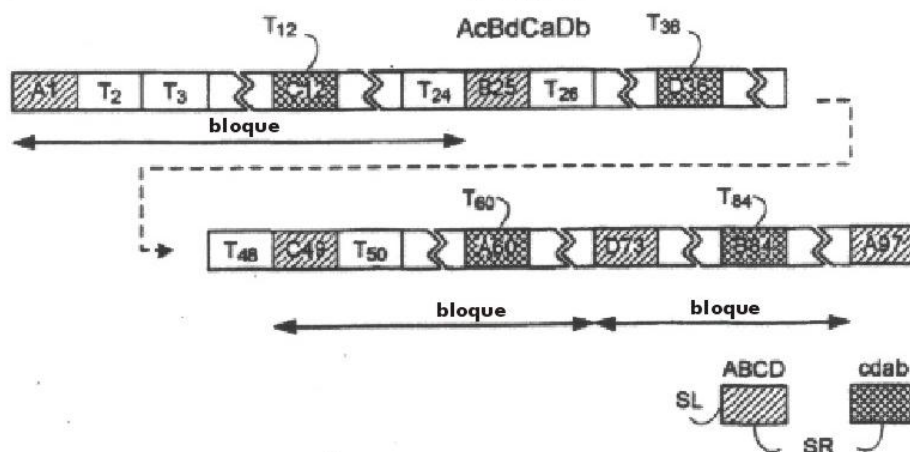


FIG. 7

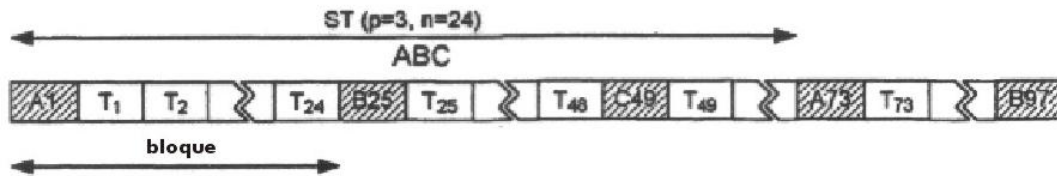


FIG. 8

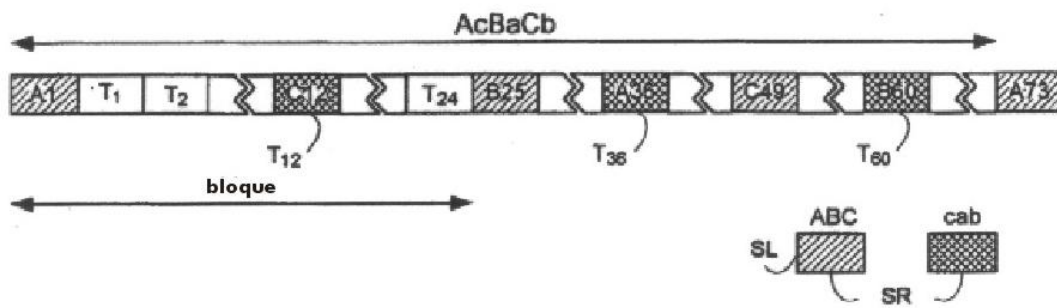


FIG. 9

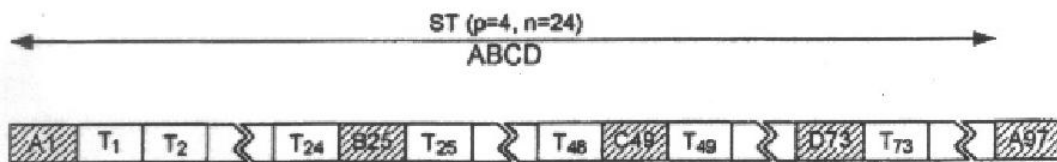


FIG. 10

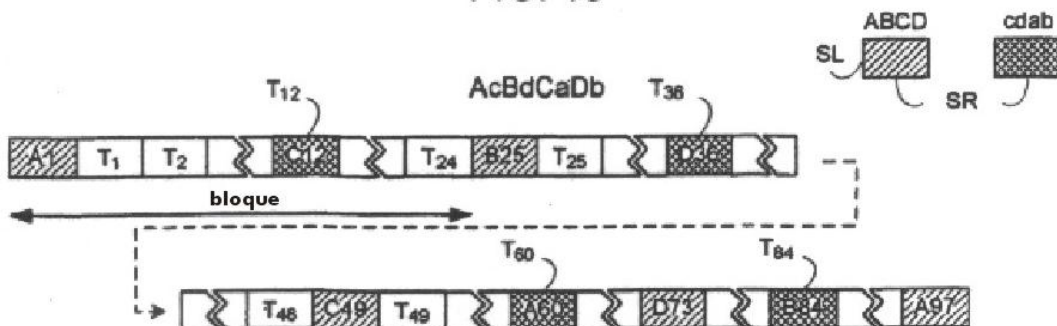


FIG. 11

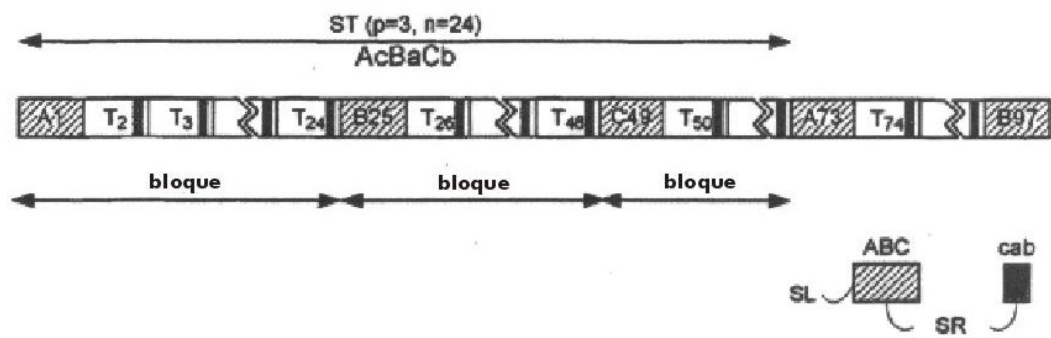


FIG. 12

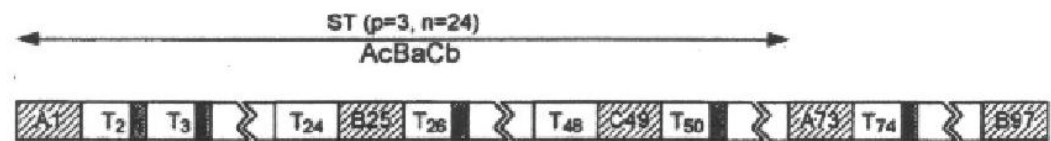


FIG. 13

