(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 295 543**

(51) Int. Cl.:
H04K 1/00 (2006.01)
H04L 27/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03405655 .6**
(86) Fecha de presentación : **08.09.2003**
(87) Número de publicación de la solicitud: **1513279**
(87) Fecha de publicación de la solicitud: **09.03.2005**

(54) Título: **Cifrado de datos sobre la capa física de un sistema de transmisión de datos.**

(73) Titular/es: **ABB RESEARCH Ltd.**
Affolternstrasse 44
8050 Zürich, CH

(72) Inventor/es: **Dzung, Dacfey**

(74) Agente: **Ungría López, Javier**

(45) Fecha de publicación de la mención BOPI:
16.04.2008

(45) Fecha de la publicación del folleto de la patente:
16.04.2008

DESCRIPCIÓN

Cifrado de datos sobre la capa física de un sistema de transmisión de datos.

Campo de la invención

La invención se refiere a técnicas de códigos cifrados para transmisión de datos. Se parte de un método de cifrado de datos sobre la capa física de un sistema de transmisión de datos como se describe en el preámbulo de la reivindicación 1.

Antecedentes de la invención

Las señales de transmisión inalámbrica de datos en general, lo mismo que las señales de comunicación de línea de energía, son fácilmente interceptadas por receptores apropiados, que necesitan técnicas de cifrado de datos para conseguir un determinado nivel de confidencialidad. El cifrado digital se aplica habitualmente a los bits transmitidos al nivel de conexión entre datos o a capas de protocolo más altas de la pila de protocolos de comunicación. Las técnicas de códigos de cifrado de bloques permutan bloques de bits de un modo dependiente de la clave, mientras que los cifrados de flujos generan primero un flujo de clave binario pseudo-aleatorio dependiente de la clave, que entonces se opera en XOR con la secuencia de bits del texto sin retocar para producir el texto cifrado. Un procedimiento de gestión de claves separado asegura que el remitente y el receptor legitimado conocen, ambos, la clave secreta y pueden establecer así un trayecto de transmisión de datos confidencial. Un escucha sin acceso a la clave no puede recuperar fácilmente el texto sin retocar desde un texto cifrado interceptado.

La realización de códigos cifrados sobre un nivel cierto de protocolo superior lo hace específico en aplicación o servicio. Otros servicios que marchan sobre la parte alta de capas de protocolo inferiores sin cifrar permanecen sin proteger o debe implementarse su propio cifrado. Además, algunos bits de datos, por ejemplo para sincronización, direccionamiento y otras funciones de control pueden permanecer sin cifrar. Los escuchas que utilizan los llamados "rádares" son capaces de esta forma de sincronizar paquetes de datos interceptados, leer información de control, y obtener el texto de cifrado binario, que puede entonces ser analizado criptográficamente por separado.

La realización del cifrado de datos en el nivel de protocolo más bajo del proceso de transferencia de información, es decir, la capa de comunicación física o capa de modem donde tiene lugar la modulación digital, resuelve las desventajas mencionadas antes. La Patente estadounidense 6.157.679 describe un método para cifrar señales de 2^4-QAM de portador simples de radiofrecuencia (RF) por transmisión de los símbolos de la constelación de QAM directa y secuencialmente. La alteración se basa en un flujo de clave binario y supone una conjugación de complejos de símbolos de QAM, es decir permutación del signo de sus componentes. El cambio de signo es fácil de poner en práctica ya que no supone cálculos. Sin embargo, como sucede con QAM de dominio universal, la interferencia intersímbolos de los símbolos de QAM introduce complicaciones para sincronización y ecualización de canales para el receptor al que se destinan, incluso sin cifrado de los símbolos de QAM.

La Patente estadounidense 4.924 516 (1990 AT&T) muestra un método de cifrado de QAM de canal simple que supone modificación de fase y ganancia de los símbolos QAM según una secuencia pseudoaleatoria.

Descripción de la invención

Es, por tanto, un objetivo de la invención proporcionar una técnica de cifrado de datos que evite que los escuchas sincronicen paquetes de datos interceptados y facilite al mismo tiempo la ecualización de canales por el receptor al que se destinan. Estos objetivos se consiguen por un método de cifrado de datos según la reivindicación 1, y por un modem para descifrar los datos según la reivindicación 7. Además se ponen de manifiesto modos de realización preferidos en las reivindicaciones de patente adjuntas.

En la técnica de código de cifrado de la invención, se combina un cifrado de datos en la capa física de comunicación con esquemas de transmisión de Orthogonal Frecuency Division Multiplex (OFDM). El OFDM es una técnica de modulación digital particularmente adaptada a canales o bandas de transmisión con características dependientes de la frecuencia (por ejemplo señal-a-ruido) tal como transmisión inalámbrica o de línea de energía. En contraste con QAM de portador simple, la modulación OFDM supone una superposición de varios sub-canales o sub-portadores, donde se evita la interferencia entre sub-portadores y se facilita la ecualización de sub-portadores por un prefijo cíclico.

En otras palabras, la invención introduce el cifrado sobre la capa física de protocolo, es decir, directamente sobre el nivel de modulación digital del esquema de modulación OFDM. Los símbolos de OFDM para ser transmitidos comprenden varios símbolos de Quadrature Amplitude Modulated (QAM) subyacentes que son alterados de manera determinada por una clave de cifrado. Específicamente, el concepto de cifrado de flujo se modifica de manera que una secuencia del flujo de clave generalizada es concatenada con las secuencias de los citados símbolos de QAM subyacentes. La generación de la secuencia de flujo de clave tiene la ventaja de los métodos conocidos para generar flujos de claves binarios criptográficamente seguros. El presente cifrado es fácil de ponerse en práctica.

En la presente invención, se insertan, cifran y transmiten periódicamente símbolos de OFDM de entrenamiento exactamente lo mismo que los símbolos ordinarios de OFDM de datos. En el receptor, los símbolos de OFDM de entrenamiento recibidos se evalúan para facilitar la sincronización y evaluación del canal.

En una variante preferida de la invención, la citada secuencia de flujo de clave consiste en elementos seleccionados aleatoriamente de un conjunto de valores distintos de K>2. Esto permite alteraciones más variadas de los símbolos de QAM subyacentes que el simple cambio de signo o una conjugación de complejos, además de obstruir los intentos de adquisición de la señal por parte de un escucha.

En otro modo de realización preferido de la invención, la operación de cifrado consiste en una sencilla multiplicación de complejos con los elementos de la secuencia de flujo de clave, que se puede llevar a cabo eficazmente por los procesadores de señales digitales utilizados típicamente para poner en práctica modems de OFDM. (Los esquemas de cifrado binarios tradicionales requieren manipulaciones a nivel de bit que no pueden realizarse eficazmente sobre tales procesadores). Si los elementos de la secuencia de flujo de clave son de igual amplitud, la amplitud de los símbolos de QAM y por tanto la energía transmitida de los correspondientes subcanales se deja sin cambiar.

En el caso de una modulación de 2^m QAM subyacente que supone 2^m puntos de constelación (o símbolos de QAM potenciales), estos últimos se distribuyen simétricamente en cuatro cuadrantes del plano del complejo. Si la operación es entonces igual a una rotación congruente, cada símbolo alterado es de nuevo un punto de constelación regular. El número K de elementos del complejo distintos de la secuencia del flujo de clave se establece por tanto preferiblemente en 4 y los elementos mismos son múltiplos de $\pi/2$. Otra posible constelación de QAM consiste en 16 puntos igualmente espaciados sobre un círculo, es decir, una modulación de fase pura. Aquí K=16 (raíces de unidad) también conserva los puntos de constelación originales.

En un modo de realización de la invención, alternativo, preferido, la operación del cifrado consiste en una permutación pseudoaleatoria de los puntos de la constelación, es decir, los símbolos de QAM se intercambian por otros símbolos de QAM. Con el fin de no trastornar la asignación de energía a los sub-canales, la permutación tiene lugar preferiblemente entre subconjuntos de puntos de constelación con igual amplitud.

Breve descripción de las figuras

El material objetivo de la invención quedará explicado con más detalle en el texto siguiente con referencia a los modos de realización ejemplo preferidos que quedan representados en los dibujos adjuntos, en los que:

La Figura 1 muestra esquemáticamente un diagrama de bloques del transmisor.

La Figura 2 muestra esquemáticamente un diagrama de bloques del receptor.

Los símbolos de referencia utilizados en las figuras y sus significados están enumerados en forma resumida en la lista de símbolos de referencia. En principio, se proporcionan partes idénticas con los mismos símbolos de referencia en las figuras.

Descripción detallada de los modos de realización preferidos

La Figura 1 muestra un diagrama de bloques del transmisor para construir un símbolo de OFDM cifrado con N-subcanales según la invención. Los bits de datos, que comprenden bits de la capa física por sincronización y evaluación de canal en adición a bits del nivel superior, se preparan en paquetes en la fuente de datos 10 y entran en serie y son divididos en bloque de datos de m_n bits (n = 0 ... N-1) por un vectorizador de OFDM 11. Estos bloques se procesan en paralelo en una unidad de establecimiento de una correspondencia de QAM 12, siendo asignado cada bloque a un número del complejo z_n, es decir, haciéndose una proyección a un símbolo de QAM o punto de la constelación según el esquema de 2^m-QAM y posiblemente aumentado proporcionalmente en una ganancia g_n. El número m_n de bits y la ganancia g_n pueden depender del índice n de sub-portador, si se utilizan una carga de bits dependiente de la frecuencia optimizada y esquemas de asignación de ganancia.

En la siguiente etapa del cifrado, la secuencia de números de complejo z_n se opera en una unidad de cifrado 13 por multiplicación por una secuencia de flujo de clave evaluada por complejo {kn} generalizada y se obtiene una secuencia de texto cifrado v_n, es decir

$$v_n = k_n \cdot z_n$$

La generación de {kn}, una secuencia K-aria pseudoaleatoria, PSR, con un valor de K de por ejemplo K = 4 u 8, en el generador de flujo de clave 18, se describe después. Para el caso presente de OFDM, la selección preferida de{$[k_n\}$ tiene la forma

$$k_n = e^{j\varphi_n}$$

donde φ_n es una secuencia K-aria pseudoaleatoria con $0 \leq \varphi_n < 2\pi$. La señal separada en tiempo de OFDM se genera entonces como una superposición de los N sub-portadores modulados, es decir:

$$x_k = \sum_{n=0}^{N-1} v_n \cdot e^{j2\pi \frac{nk}{N}}$$

que se calcula de la manera más eficaz con una Transformación de Fourier Inversa en IFFT 14. La adición del llamado prefijo cíclico en un sumador de prefijos 15 reduce la interferencia entre sub-portadores en el receptor. Por último, tiene lugar una conversión de digital a analógico y posiblemente un mezclado o traducción de frecuencia a la frecuencia real del portador, en un mezcladora y convertidor de digital a analógico (D/A) 16, lo que da por resultado la señal transmitida x(t).

Como se ha mencionado antes, el cifrado es proporcionado por la secuencia de flujo de clave K-aria $\{k_n\}$ o $\{\varphi_n\}$. Los flujos de clave son secuencias pseudoaleatorias, que son determinadas unívocamente por una clave de cifrado, deben ser de gran longitud (periodo) e impredecibles (dado un extracto de la secuencia) por cualquiera que no conozca la clave de cifrado. La generación de flujos de clave binarios para cifrados de flujos binarios es ya conocida.

Para la presente aplicación, una secuencia de flujo de clave K-aria $\{\varphi_n\}$ puede obtenerse sencillamente por utilización $\log_2 K$ bits de salida sucesivos de un generador de flujo de clave binario. Estos bits se dirigen a una tabla con K entradas que contiene el establecimiento de una correspondencia a valores de φ_n o a $\mathrm{Re}(k_n) = \cos(\varphi_n)$ y $\mathrm{lm}(k_n) = \mathrm{sen}(\varphi_n)$. Con selecciones razonables de las entradas de la tabla, secuencias binarias criptográficamente buenas conducen entonces a $\{\varphi_n\}$ K-aria. Obviamente el tamaño de la clave de codificación que determina el flujo de clave $\{\varphi_n\}$ debe ser grande para evitar ataques de fuerza bruta y comprender preferiblemente 128 bits o más. Además, el período del flujo de clave debe cubrir un gran número de símbolos de OFDM, en que para cada símbolo de OFDM con N sub-portadores o N símbolos de QAM z_n, son consumidos $N\text{-}\log_2(K)$ bits del flujo de clave binario. El índice n en $\{k_n\}$ debe por tanto contar sobre muchos de tales símbolos de OFDM.

La selección óptima de los niveles K de φ_n (asignados equidistantemente entre 0 y 2π) depende de m_n, o más precisamente de los puntos de la constelación de los símbolos 2^mQAM z_n. Por ejemplo la constelación de puntos regulares $2^2 = 4$ sería congruentemente rotada con niveles $K = 2^2 = 4$ de φ_n (es decir, 0, $\pi/2$, $3\pi/2$), de aquí que $K = 4$ deberá ser suficiente para cifrar estos símbolos z_n de QAM. Por otra parte puede ser preferible un valor más alto de K con el fin de obstruir cualquier sincronización de portador de bucle abierto intentada por un escucha.

La Figura 2 muestra el diagrama de bloques de un receptor que en principio invierte simplemente las etapas realizadas por el transmisor. La señal analógica recibida y(t) se mezcla descendentemente y se digitaliza en la unidad de mezclado descendente y convertidor (26) análogico a digital (A/D) y se hace pasar a través del eliminador de prefijo cíclico 25. El transformador de Fourier rápido 24 calcula los símbolos y_n (n = 0 ... N-1) que se descifran entonces en el descifrador 23 con ayuda de la secuencia de flujo de clave {kn} proporcionada por el generador de flujo de clave 28. Por último se lleva a cabo la desconfiguración y serialización en la unidad de desconfigurado y serializador de símbolos 21.

Una función h_n de transferencia de canal representa una posible distorsión de la señal recibida y_n a la enésima frecuencia del subportador por las características de propagación del canal. Según esto, una estimación del receptor $\hat{v}_n$ de la secuencia del texto cifrado es aproximada por

$$y_n = h_n \cdot \hat{v}_n$$

y la distorsión se corrige en el ecualizador 30, es decir, la operación combinada

$$\hat{z}_n = k_n^{-1} \cdot \frac{y_n}{h_n} = e^{-j\varphi_n} \frac{y_n}{h_n}$$

ecualiza y descifra el símbolo de QAM $\hat{z}_n$ que puede entonces introducirse como alimentación al desconfigurador de QAM 22 para recuperar finalmente los bits de datos transmitidos. Esto requiere que el receptor conozca la clave de cifrado/descifrado y también la información de sincronización precisa.

La sincronización para obtener esta información de reloj y evaluación de la función h_n de transferencia de canal son las dos tareas auxiliares cruciales del receptor. Como se representa en la Figura 2, estas tareas se llevan a cabo por un sincronizador/evaluador de canal 32. Este último correlaciona la señal recibida con las réplicas conocidas de símbolos de OFDM 31 de “entrenamiento” que el transmisor inserta periódicamente en la secuencia de símbolos de OFDM de “datos”. Según la presente invención, se propone también el cifrado de símbolos de OFDM de entrenamiento 31

utilizados para soporte de la sincronización y evaluación de canal, es decir, cualquier símbolo de entrenamiento insertado por el transmisor será cifrado por una alteración basada en k_n de la misma manera que los símbolos portadores de datos normales. El receptor que tiene conocimiento tanto del flujo de clave $\{k_n\}$ como de los símbolos de OFDM de entrenamiento sin cifrar 31 es capaz de generar las señales de entrenamiento cifradas que varían con el tiempo y utilizar éstas para sincronización y evaluación de canal de la manera habitual. Sin embargo, un escucha que no conoce la clave del cifrado no será capaz de sincronizar la señal interceptada. Esto proporciona un fuerte nivel adicional de protección. Preferiblemente, se asegura que el cifrado de un texto sin retocar conocido de flujo de clave $\{k_n\}$, tal como en particular, los símbolos de entrenamiento 31, no volverá a usarse para cifrar otros datos.

En resumen, la presente invención se refiere a un método para cifrar modulación de OFDM, por multiplicación de sus símbolos de QAM subyacentes por una secuencia de flujo de clave generalizada evaluada por complejo. La realización del cifrado sobre la capa física asegura que todos los servicios y aplicaciones que marchan sobre el modem de OFDM estarán protegidos frente a escuchas. Se propone también la inclusión en el cifrado de los símbolos de entrenamiento utilizados para la sincronización y evaluación de canal. Solamente el receptor legitimado que conoce la clave del cifrado es capaz, por tanto, de sincronizar y desmodular correctamente la señal recibida mientras que los piratas no podrán ni capturar la señal cifrada.

Lista de designaciones

10 fuente de datos

11 vectorizador de OFDM

12 unidad de establecimiento de una correspondencia

13 unidad de cifrado

14 transformador de Fourier rápido inverso IFFT

15 sumador de prefijos

16 mezclador y convertidor de digital a analógico (A/D)

18 generador de flujo de clave

21 serializador de símbolos

22 unidad de des-establecimiento de correspondencia de QAM

23 descifrador

24 transformador de Fourier rápido FFT

25 eliminador de prefijo cíclico

26 mezclador descendente y convertidor de analógico a digital (A/D)

28 generador de flujo de clave

31 símbolos de OFDM de “entrenamiento”

32 sincronizador/evaluador de canales.

REIVINDICACIONES

1. Un Método de cifrado de datos sobre la capa física de un sistema de transmisión de datos que comprende las etapas de

- proporcionar una secuencia de flujo de clave $\{k_n\}$,
- establecer una correspondencia de cada secuencia de bloques de datos con un símbolo z_n de QAM
- alterar cada uno de los símbolos z_n de QAM según un elemento k_n de la secuencia de flujo de clave $\{K_n\}$, creando con ello símbolos v_n cifrados,

caracterizado porque

- los símbolos cifrados v_n son asignados a $N \geq 2$ sub-portadores distintos de un esquema de transmisión Orthogonal Frecuency Division Multiplex OFDM,
- en un transmisor, se insertan periódicamente símbolos (31) de OFDM de entrenamiento, se alteran según elementos de la secuencia de flujo de clave (kn) y se transmiten
- en un receptor, los símbolos de OFDM (31) de entrenamiento se cifran de acuerdo con elementos de la secuencia de flujo de clave $\{k_n\}$ y se comparan con los símbolos de entrenamiento cifrados transmitidos (31) recibidos por un sincronizador/evaluador de canales (32), y porque
- de allí se deduce una función h_n de transferencia de canal o información de sincronización.

2. El método según la reivindicación 1 **caracterizado** porque la secuencia de flujo de clave {kn} es una secuencia K-aria con K>2, siendo elegido cada elemento K_n de la secuencia de flujo de clave $\{k_n\}$ de valores de K distintos.

3. El método según la reivindicación 2, **caracterizado** porque los símbolos z_n de QAM se multiplican con elementos k_n de la secuencia de flujo de clave $\{k_n\}$.

4. El método según la reivindicación 3, **caracterizado** porque los elementos k_n son de la forma $k_n = e^{j\varphi n}$.

5. El método según la reivindicación 4, donde los símbolos z_n de QAM forman un conjunto de 2^m puntos de constelación distintos, **caracterizado** porque K=4 y φ_n es un múltiplo de $\pi/2$.

6. El método según la reivindicación 2, **caracterizado** porque K iguala al número de puntos de la constelación distintos, y porque los símbolos z_n de QAM se permutan entre ellos.

7. Un modem para descifrado, en un receptor, de los datos cifrados sobre la capa física de un sistema de transmisión de datos de Orthogonal Frecuency Division Multiplex, OFDM, siendo cifrados los citados datos por alteración, en un transmisor, de cada secuencia de símbolos z_n de QAM y símbolos de OFDM de entrenamiento (31), de acuerdo con un elemento k_n de una secuencia de flujo de clave $\{k_n\}$, creando así símbolos cifrados v_n para ser transmitidos al receptor, donde los símbolos cifrados v_n son asignados a $N \geq 2$ sub-portadores distintos de un esquema de transmisión Orthogonal Frecuency División Multiplex, comprendiendo el modem un sincronizador/evaluador de canal (32) para comparar los símbolos (31) de OFDM de entrenamiento cifrados transmitidos recibidos con los símbolos (31) de OFDM de entrenamiento cifrados creados por alteración, en el receptor, los símbolos (31) de OFDM de entrenamiento de acuerdo con los elementos de la secuencia de flujo de clave $\{k_n\}$ y para deducir de allí una función de transferencia de canal h_n o información de sincronización.

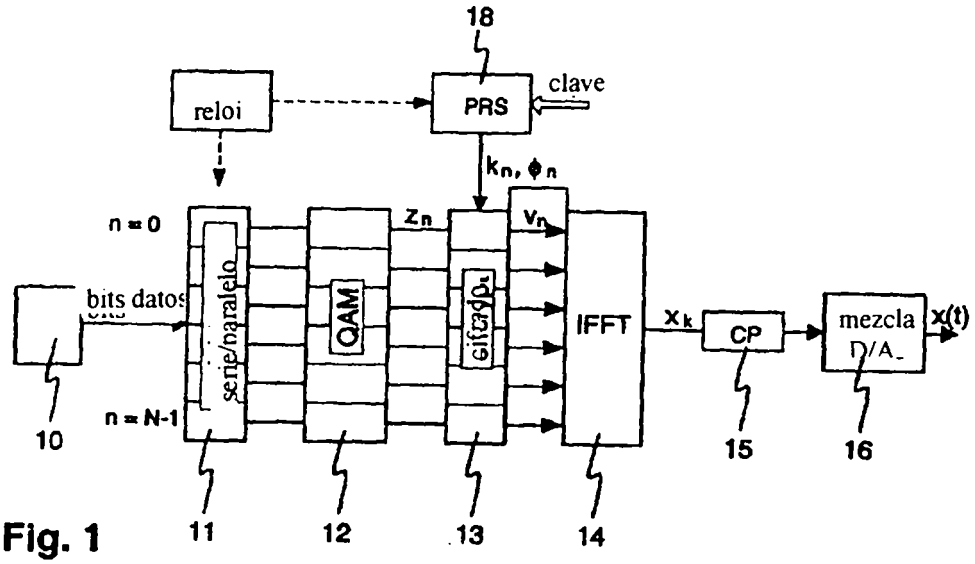
18
reloi
PRS
clave
k_n, ϕ_n
n = 0
z_n
v_n
bits datos
serie/paralelo
QAM
cifrado
IFFT
x_k
CP
mezcla D/A
x(t)
n = N-1
10
11
12
13
14
15
16

Fig. 1

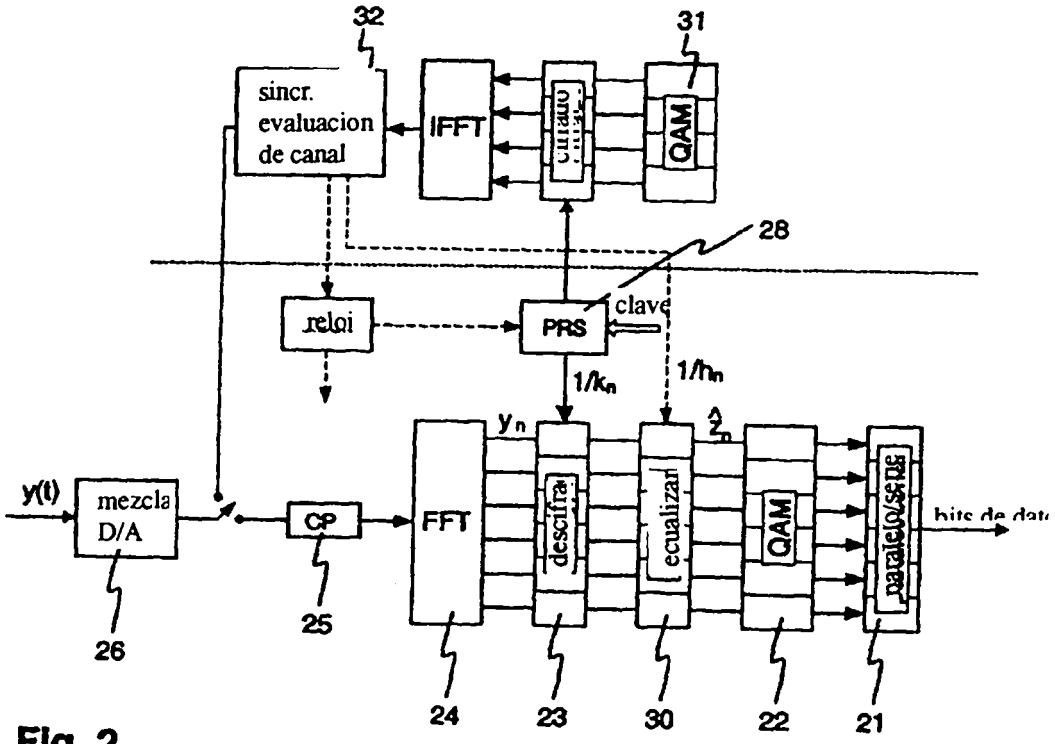
32
31
sincr. evaluacion de canal
IFFT
cifrado
QAM
28
reloi
PRS
clave
$1/k_n$
$1/h_n$
y_n
z_n
y(t)
mezcla D/A
CP
FFT
descifrar
ecualizar
QAM
paralelo/serie
bits de dat
26
25
24
23
30
22
21

Fig. 2