(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 271 730**

(51) Int. Cl.:
H04L 9/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04009133 .2**
(86) Fecha de presentación : **21.05.1998**
(87) Número de publicación de la solicitud: **1458130**
(87) Fecha de publicación de la solicitud: **15.09.2004**

(54) Título: **Método y aparato para generar una corriente de cifra.**

(30) Prioridad: **10.10.1997 US 949027**

(45) Fecha de publicación de la mención BOPI:
16.04.2007

(45) Fecha de la publicación del folleto de la patente:
16.04.2007

(73) Titular/es:
INTERDIGITAL TECHNOLOGY CORPORATION
3411 Silverside Road, Concord Plaza
Suite 105, Hagley Building
Wilmington, Delaware 19810, US

(72) Inventor/es: **Ozluturk, Faith M.**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método y aparato para generar una corriente de cifra.

Antecedentes de la invención

Campo de la invención

Esta invención se refiere, en general, a la transmisión segura de comunicaciones digitales de voz y datos. Más concretamente, la invención se refiere a un cifrador continuo con una pluralidad de registros de desplazamiento con realimentación lineal que generan grandes secuencias seudo-aleatorias de bits y con múltiples claves de seguridad.

Descripción de la técnica anterior

El acceso múltiple por diferenciación de código (CDMA) es un tipo de sistema de comunicaciones de espectro ensanchado en el que cada unidad de abonado se distingue del resto de unidades de abonado merced a la posesión de un código único. Para comunicar con una unidad de abonado en particular, un equipo de transmisión comunica el código único con la transmisión, y el receptor usa el mismo código para descodificar la transmisión.

Los códigos únicos usados por un sistema de comunicaciones CDMA para transmitir comunicaciones de voz y datos tienen características de ruido y son aleatorios. Puesto que las secuencias aleatorias se generan mediante elementos lógicos determinísticos estándar, dichas secuencias de bits son predecibles y repetibles. El uso de estas secuencias binarias aleatorias, repetibles, es lo que permite una fácil modulación con cualquier señal portadora de información. Estas secuencias aleatorias predecibles se denominan secuencias seudo-aleatorias.

Cada transmisor de un sistema de comunicaciones CDMA incluye un generador de cifrado continuo que usa una clave para cifrar las comunicaciones de voz y datos. En el receptor, un generador de cifrado continuo idéntico descifra las comunicaciones cifradas recibidas usando la misma clave.

Tal como se conoce en la técnica anterior, el generador de cifrado continuo más simple es el registro de desplazamiento con realimentación lineal. Un registro de desplazamiento con una longitud en bits finita se temporiza con una frecuencia fija. Una puerta "O exclusiva" genera la señal de entrada en serie merced a la aplicación de algunos bits del registro de desplazamiento a dicha puerta. El circuito, entonces, pasa por una serie de estados, que se repiten, eventualmente, después de un número finito de impulsos de temporización. Pero el cifrado continuo generado mediante registros de desplazamiento con realimentación lineal está relacionado con la longitud del registro de desplazamiento y con los bits que se combinen en la puerta "O exclusiva" para generar la entrada siguiente. Si se desea un cifrador continuo complejo, tiene que usarse un registro de desplazamiento costoso, con una longitud inconveniente.

El documento "Pseudo Random Bit Generators in Stream-Cipher Crytography" (Generadores de bits seudo-aleatorios en Criptografía de cifrado continuo), de Zeng *et al*, publicado el 1 de febrero de 1991 en el Volumen 24, nº 2, páginas 8-17, de Computer, describe diversos circuitos que usan registros de desplazamiento con realimentación lineal para crear cifradores continuos.

En consecuencia, hay necesidad de un método sencillo para aumentar la complejidad de los cifradores continuos con objeto de aumentar la seguridad de los mensajes cifrados.

Compendio de la invención

Un circuito generador de cifrado continuo para uso en sistemas de comunicaciones inalámbricos incluye, al menos, dos circuitos de registro de desplazamiento con realimentación lineal (LFSR), acoplados, uno de cuyos circuitos LFSR se usa para controlar la temporización del otro. Esta combinación de circuitos LFSR genera un cifrado continuo con una complejidad lineal y un periodo muy grandes. La salida total está equilibrada con respecto a las salidas individuales de los circuitos LFSR. El circuito generador de cifrado continuo puede usarse con una configuración de múltiples etapas, en cuyo caso la seguridad se mejora en gran medida, puesto que la complejidad lineal y el periodo de la salida del cifrador continuo aumentan exponencialmente.

En consecuencia, un objeto de la presente invención consiste en ofrecer un método para generar secuencias seudo-aleatorias con mayor complejidad.

Otros aspectos y ventajas resultarán evidentes a los expertos en la técnica a partir de la lectura de la descripción detallada de las realizaciones preferidas.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques de un transmisor de espectro ensanchado convencional;

la figura 2 es un diagrama de bloques de un receptor de espectro ensanchado convencional;

la figura 3 es un diagrama de temporización de una secuencia de seudo-ruido (PN) usada en las figuras 1 y 2;

la figura 4 es un diagrama que muestra un generador de corriente de cifra convencional;

la figura 5 es un diagrama de bloques de una realización del transmisor de espectro ensanchado de la presente invención;

la figura 6 es un diagrama de bloques de una primera realización del generador de corriente de cifra de la presente invención;

la figura 7 es un diagrama de flujo de los pasos para generar una corriente de cifra en la primera realización de la presente invención;

la figura 8 es un diagrama de bloques de una realización del receptor de espectro ensanchado de la presente invención; y

la figura 9 es una segunda realización del generador de corriente de cifra de la presente invención.

Descripción de las realizaciones preferidas

Las realizaciones preferidas se describen con referencia a las figuras de los dibujos, en las que números similares representan, en todas ellas, elementos similares.

Un transmisor 10 de espectro ensanchado típico de la técnica anterior, como se muestra en la figura 1, incluye un convertidor analógico-digital (A/D) 12 y un conmutador 14. El convertidor A/D 12 recibe una señal analógica de voz, digitaliza la señal y transmite la señal digitalizada al conmutador 14. El conmutador 14 recibe la señal digital de voz del convertidor A/D 12 y una señal digital de datos de un terminal de datos (no mostrado). Los expertos en la técnica entenderán con facilidad que el terminal de datos puede incluir un telefax, un ordenador o cualquier otro tipo de dispositivo electrónico que pueda emitir o recibir datos digitales. El conmutador 14 conecta el transmisor 10 de espectro ensanchado con una entrada para datos digitales, que pueden ser de voz o no. En lo que sigue, tanto los datos digitales de voz como los que no sean de voz se denominan, de manera general, datos digitales.

Un mezclador 16 combina datos del conmutador 14 con la corriente de cifra creada por el generador 17 de corriente de cifra, que tiene, al menos, una clave 18. Después de combinar la corriente de cifra con los datos, el mezclador 16 transmite los datos digitales cifrados a un ensanchador 20, que puede ser un mezclador. Una secuencia seudo-aleatoria, creada por el generador 30 de secuencias seudo-aleatorias, se aplica a un primer terminal del ensanchador 20. El generador 30 de secuencias seudo-aleatorias y el ensanchador 20 se muestran incluidos en un codificador 40 de espectro ensanchado.

El ensanchador 20 desempeña una función de ensanchamiento de espectro de frecuencias al multiplicar los datos por la secuencia seudo-aleatoria en el dominio del tiempo, lo que equivale a envolver el espectro bimodal de la secuencia de datos con el espectro, aproximadamente rectangular, de la secuencia seudo-aleatoria en el dominio de la frecuencia. La salida del ensanchador 20 se aplica a un filtro 50 de pasa-bajos, cuya frecuencia de corte es igual a la frecuencia de bits (Fcr) de la secuencia seudo-aleatoria del sistema. La salida del filtro 50 de pasa-bajos se aplica, entonces, a un terminal de un mezclador 60 y se convierte a una frecuencia más elevada, determinada por la frecuencia de portadora Fc aplicada a su otro terminal. A continuación, la señal aumentada en frecuencia es hecha pasar por un filtro 70 de paso de banda. El filtro 70 tiene un ancho de banda igual al doble de la frecuencia de bits de la secuencia seudo-aleatoria y una frecuencia central igual a la frecuencia central del ancho de banda del canal del sistema de espectro ensanchado. La salida del filtro 70 se aplica a la entrada de un amplificador 80 de RF, cuya salida activa una antena 90.

En la figura 2 se muestra un receptor 100 de espectro ensanchado de la técnica anterior. Una antena 110 recibe la señal de espectro ensanchado transmitida, que es filtrada mediante un filtro 120 de paso de banda. El filtro tiene un ancho de banda igual al doble de la frecuencia de bits de la secuencia seudo-aleatoria, y una frecuencia central igual a la frecuencia central del ancho de banda del canal del sistema de espectro ensanchado. Subsiguientemente, la salida del filtro 120 se reduce en frecuencia mediante un mezclador 130, posiblemente en dos etapas, para formar una señal de banda de base, usando un oscilador local con una frecuencia constante que sea, aproximadamente, la misma que la frecuencia Fc de portadora del transmisor 10. Luego, se recupera el ancho de banda original de la salida del mezclador 130 aplicando dicha salida a un primer terminal del correlacionador 140, mientras que se aplica la misma secuencia seudo-aleatoria entregada al ensanchador 20, o una secuencia similar, a un segundo terminal del correlacionador 140. La secuencia seudo-aleatoria se crea merced a un generador 150 de código de correlación. El correlacionador 140 y el generador 150 de código de correlación están incluidos en un descodificador 160 de espectro ensanchado, como se muestra en la figura 2.

Más concretamente, se apreciará que la secuencia seudo-aleatoria usada en el receptor 100 de un sistema de comunicaciones de espectro ensanchado tiene que estar sincronizada con la secuencia seudo-aleatoria usada en el transmisor 10. La salida del correlacionador 140 se aplica a un mezclador 170. El generador 172 de corriente de descifrado genera la misma corriente de cifra que el generador 17 del corriente de cifra, para descifrar los datos digitales cifrados. En la

técnica anterior, la clave 18 usada en el transmisor 10 es la misma que la clave 174 usada en el receptor 100. La clave 174 de recepción se aplica al generador 172 de corriente de cifra para descifrar los datos digitales cifrados. La salida del mezclador 170 se aplica a un filtro 180 de pasa-bajos, cuya frecuencia de corte es la frecuencia de entrada de datos en el transmisor 10 de espectro ensanchado. La salida del filtro 180 de pasa-bajos es una réplica de la entrada de datos de voz o digitales mostrada en la figura 1.

La secuencia digital seudo-aleatoria mostrada en la figura 3 es una secuencia de ensanchamiento convencional. La secuencia, típicamente, alcanza dos valores constantes, (±1), a lo largo del tiempo. La secuencia se usa para aumentar el ancho de banda de la señal que se transmita y para recuperar el ancho de banda original de la señal que se reciba. El cifrado continuo se crea mediante un generador 17 de corriente de cifra como el mostrado en la figura 4. Una corriente de datos cifrados puede descifrarse si se conoce la clave 18 de la corriente de cifra original y se reproduce en el receptor. Los bits son creados mediante el generador 17 de corriente de cifra, y los bits de datos se aplican a una puerta "O exclusiva" para cifrar los datos. La corriente de datos original se recupera cuando se aplican los datos cifrados a una puerta "O exclusiva" con la misma corriente de cifra, como se muestra mediante la ecuación 1:

$$b_i \oplus c_i \oplus c_i = b_i \qquad \text{Ecuación (1)}$$

en la que b_i es la corriente de datos original y c_i es la corriente de cifra original.

Como es bien conocido en la técnica anterior, el generador 17 de corriente de cifra más simple es el registro 34 de desplazamiento con realimentación lineal. El registro 34 de desplazamiento comprende un número finito de bits, 33, 35, 37, o una longitud en bits finita, y es temporizado mediante un circuito de temporización 32 con una frecuencia fija predeterminada. Una combinación de bits 35, 37 de LFSR se aplica a una puerta "O exclusiva" 38 con objeto de generar el siguiente bit de entrada al LFSR 34. Los coeficientes de un polinomio primitivo determinan los bits a aplicar a la puerta "O exclusiva". Una puerta "O exclusiva" 36 combina la salida del LFSR 34 y la corriente 39 de datos digitales con el fin de cifrar los datos. El LFSR, entonces, pasa por una serie de estados, que se repiten, eventualmente, después de un número finito de impulsos de temporización generados por el circuito de temporización 32.

Un LFSR 34 de tres bits convencional, como se muestra en la figura 4, es un ejemplo de generador 17 de corriente de cifra. Un registro de desplazamiento con n bits tiene un periodo igual a 2^n-1. En consecuencia, el periodo del registro 34 de desplazamiento de tres bits es igual a siete. Cada valor inicial cero o uno cargado en cada bit del registro 34 constituye una clave, excepto en el caso en que todo sean ceros. Por ejemplo, si la clave es 111, el registro 34 de desplazamiento generará los valores siguientes:

Carga inicial	→	111
		011
		001
		100
		010
		101
		110
Repetición	→	111
		011
		-
		-
		-

El LFSR 34 de tres bits mostrado tiene un periodo muy pequeño (es decir, igual a siete). En consecuencia, un LFSR de este tamaño no permite una transmisión de datos muy segura.

En la figura 5 se muestra un transmisor 200 de espectro ensanchado hecho de acuerdo con la presente invención. El transmisor 200 incluye todos los componentes del transmisor 10 de espectro ensanchado mostrado en la figura 1, que funcionan de la misma manera, a excepción del generador 220 de corriente de cifra y de las claves 210, que se explicarán con mayor detalle en lo que sigue. Aunque la figura 5 muestra un transmisor 200 para transmitir un canal, pueden combinarse múltiples canales y, luego, cifrarse mediante el generador 220 de corriente de cifra.

Con referencia a la figura 6, el generador 220 de corriente de cifra incluye dos circuitos LFSR, (L_1, L_2). La salida del segundo circuito LFSR, L_2, se usa para controlar la temporización del primer circuito LFSR, L_1. Por ejemplo, la salida del segundo LFSR, L_2, preferiblemente, está conectada con una puerta "Y" 222, que está conectada con la entrada de temporización del primer LFSR, L_1. La puerta "Y" 222 podría sustituirse por una puerta "NO-Y". En lugar de la puerta "Y" 222 pueden usarse, también, otras puertas, tales como "O", "NO-O", "O exclusiva", etc., o una combinación de puertas. Las puertas "O exclusiva" 38 permiten la realimentación de los registros L_1, L_2 de desplazamiento. El generador 220 de corriente de cifra incluye, también, una puerta "O exclusiva" 224, conectada con las salidas de

los LFSR L_1, L_2. La puerta "O exclusiva" 224 combina las salidas de los LFSR L_1, L_2, y, a continuación, emite la corriente de cifra. Los estados iniciales de los dos LFSR L_1, L_2 son las dos claves compartidas por el generador 220 de corriente de cifra y el generador 320 de corriente de descifrado. De modo preferido, el generador 320 de corriente de descifrado, que se explicará con más detalle en lo que sigue, es similar al generador 220 de corriente de cifra. El generador 220 de corriente de cifra y el generador 320 de corriente de descifrado se usan, preferiblemente, en modo síncrono (a diferencia del modo auto-síncrono), porque el modo auto-síncrono es susceptible de propagar errores, como consecuencia de errores de bits individuales, comunes en transmisiones inalámbricas. En cifradores continuos auto-síncronos, los datos digitales cifrados se usan como parte de la clave para cifrar los bits de datos siguientes. El problema con este enfoque consiste en que si un bit se altera durante su transmisión y se descifra de modo incorrecto, dicho bit alterará, también, los bits siguientes, ya que se usa, también, como clave de cifrado para los bits de datos siguientes.

Todos los esquemas de cifrado distintos a una tabla de consulta de un solo uso son periódicos. Para que se produzca una transmisión segura, el generador 220 de corriente de cifra y el generador 320 de corriente de descifrado tienen que tener un periodo tan largo como sea posible. Los dos LFSR L_1, L_2 generan el periodo máximo si los coeficientes de derivación para la realimentación corresponden a un polinomio primitivo. Una secuencia de este tipo se denomina secuencia de longitud máxima (secuencia m).

Aunque no es necesario, en una realización, el periodo máximo se consigue cuando los periodos de las salidas individuales de los dos LFSR L_1, L_2, sean primos entre sí (los periodos de las salidas individuales no tienen un divisor común). Por ejemplo, si el primer LFSR, L_1, tiene una longitud en bits igual a tres, el periodo de la salida individual es igual a siete. Si el segundo LFSR, L_2, tiene una longitud en bits de dos, el periodo de la salida individual es igual a tres. Por lo tanto, los periodos de salida no tienen un divisor común.

Un polinomio primitivo, bien conocido en álgebra de cuerpos finitos, genera un periodo igual a 2^L-1 si dicho polinomio es de grado L. Un grupo de polinomios forman un cuerpo finito. Un cuerpo finito tiene, al menos, un elemento primitivo, de tal modo que todos los elementos distintos a cero del cuerpo sean potencias de este elemento primitivo. Un polinomio que tenga como raíz un elemento primitivo se denomina polinomio primitivo. Por lo tanto, cuando los circuitos LFSR L_1, L_2 tengan longitudes L_{E1} y L_{E2}, respectivamente, las salidas del generador 220 de corriente de cifra y del generador 320 de corriente de descifrado, tienen el periodo:

$$\text{Periodo de salida} \approx 2^{L_{E1}+L_{E2}} \qquad \text{Ecuación (2)}$$

Cuando las longitudes de los dos LFSR, L_1, L_2, sean del orden de ~20, el periodo del cifrado continuo es $\sim 10^{12}$ bits. Ello significa que puede cifrarse una corriente de datos de 32 kbits/s durante un año, de manera continua, sin que se repita el cifrado de corriente.

La complejidad lineal del generador 220 de corriente de cifra es igual a la longitud del LFSR más corto que pueda generar la salida del generador 220 de corriente de cifra. Dicha complejidad lineal se usa, con frecuencia, como medida de la aleatoriedad de la salida del generador 220 de corriente de cifra. La complejidad lineal de este generador 220 de corriente de cifra es del orden de

$$\text{Complejidad lineal} = (2^{L_{E1}})L_{E2} + (2^{L_{E2}})L_{E1} \qquad \text{Ecuación (3)}$$

Si la salida del generador 220 de corriente de cifra tuviera que obtenerse mediante un solo LFSR equivalente, el registro tendría que tener una longitud superior a 20 millones de etapas (para L_{E1} y L_{E2} ~20, como antes).

Se dice que un generador 220 de corriente de cifra está equilibrado si su salida es igual a la salida de cada circuito LFSR interno L_1, L_2, con la misma probabilidad. Preferiblemente, el valor de salida será el mismo que la salida de cualquiera de los circuitos LFSR L_1, L_2, es decir, una probabilidad igual a 0,5. Es importante prever un cifrador que esté equilibrado porque es más fácil violar cifradores que no lo estén. Si se consideran las combinaciones de las salidas de los circuitos LFSR L_1, L_2 y la salida del generador 220 de corriente de cifra, puede verse que la corriente de cifra está perfectamente equilibrada y, la mitad del tiempo, es similar a cada salida LFSR L1, L2.

El estado inicial del generador 220 de corriente de cifra se determina mediante las dos claves K_1 y K_2, que son los estados iniciales de los dos LFSR, L_1, L_2, respectivamente. Para protegerse contra ataques de inserción, las claves K_1 y K_2 tienen que modificarse con frecuencia (preferiblemente, al menos, una vez por periodo del cifrador). Cuanto mayor sea el número de combinaciones de las claves K_1 y K_2, más segura será la transmisión. El número de combinaciones de clave de este ejemplo es

$$\text{Combinaciones de clave} \approx 2^{L_{E1}+L_{E2}} \qquad \text{Ecuación (4)}$$

que es un número extremadamente grande.

El generador 220 de corriente de cifra de la presente invención tiene las ventajas siguientes: 1) su complejidad lineal es muy grande; 2) su periodo es muy grande; 3) su salida está equilibrada con respecto a las salidas de los dos circuitos LFSR L_1, L_2; 4) puede realizarse con un mínimo de equipos; y 5) usa dos claves, K_1 y K_2, lo que aumenta su seguridad.

Por ejemplo, como se muestra en la figura 6, se supone que el primer circuito LFSR, L_1, tiene una longitud en bits de 3 y el segundo circuito LFSR, L_2, tiene una longitud en bits de 2. Además, se supone que la clave K_1 es "111", y la clave K_2, "11". Las claves K_1 y K_2 se cargan en L_1 y L_2, respectivamente. La tabla 1 siguiente proporciona los estados de los circuitos LFSR L_1, L_2, las salidas de los circuitos LFSR L_1, L_2, y la corriente de cifra de varios ciclos de temporización consecutivos.

TABLA 1

Ciclo de temporización	Estado L_1	Estado L_2	Salida de L_1	Salida de L_2	Corriente de cifra
1	111	11	1	1	0
2	011	01	1	1	0
3	001	10	1	0	1
4	001	11	1	1	0
5	100	01	0	1	1
6	010	10	0	0	1
7	010	11	0	1	1
8	101	01	1	1	0
9	110	10	0	0	1
10	110	11	0	1	1
11	111	01	1	1	0
12	011	10	1	0	1
13	011	11	1	1	0
14	001	01	1	1	0
15	100	10	0	0	1
16	100	11	0	1	1
17	010	01	0	1	1
18	101	10	1	0	1
19	101	11	1	1	0
20	110	01	0	1	1
21	111	10	1	0	1
22	111	11	1	1	0
23	011	01	1	1	0
24	001	10	1	0	1
25	001	11	1	1	0

En la tabla 1 puede verse que el periodo de la corriente de cifra es de 21 impulsos de temporización, que es el producto de los periodos individuales de los circuitos LFSR $L_1(7)$ y $L_2(3)$.

La corriente de cifra puede generarse, también, usando lógica, como se muestra en el diagrama de flujo de la figura 7. Los estados iniciales, las dos claves K_1 y K_2, se cargan en registros o ubicaciones de memoria (S1). Si en ese momento la salida del segundo circuito LFSR, L_2, es igual a "1" (S2), se actualiza (S3) el valor del primer circuito LFSR, L_1, y, luego, se actualiza (S4) el segundo circuito LFSR, L_2. Pero si en ese momento la salida del circuito LFSR L_2 es cero (S2), entonces, el circuito LFSR L_1 no se actualiza, y se actualiza (S4), solamente, el circuito LFSR L_2. Las salidas de los circuitos LFSR L_1, L_2 son aplicadas, entonces, a una puerta "O exclusiva", que emite la corriente de cifra (S5). A continuación, se repiten los pasos (S2) a (S5).

Un receptor 300 de espectro ensanchado realizado de acuerdo con la presente invención, tal como se muestra en la figura 8, incluye todos los componentes del receptor 100 de espectro ensanchado de la figura 2, que funcionan de la misma manera, a excepción del generador 310 de corriente de descifrado y de las claves 320.

Tanto el generador 220 de corriente de cifrado como el generador 320 de corriente de descifrado pueden usarse con una configuración de múltiples etapas, como se muestra en la figura 9, en cuyo caso la seguridad se mejora en gran medida, puesto que la complejidad lineal y el periodo aumentan exponencialmente.

Si L1~L2~L, entonces, la complejidad lineal de la configuración multietapa, de N etapas, es de, aproximadamente, $\approx 2L2^{LN}$, y el periodo de la salida se convierte en, aproximadamente, $\approx 2^{2LN}$. El algoritmo de cifrado continuo explicado en lo que antecede puede usarse con una estructura en cascada como la de la figura 9, a fin de aumentar adicionalmente su seguridad. Las etapas pueden tener longitudes, en bits, iguales o diferentes. En la forma en cascada, las etapas anteriores generan impulsos de temporización para las etapas siguientes. Como se muestra en la figura 9, la salida del primer circuito LFSR, L_1, de la etapa 1, y la salida del segundo circuito LFSR, L_2, de la etapa 2, están acopladas con una puerta "Y" a fin de formar una señal digital que se usa como temporizador para el primer circuito LFSR, L_1, de la etapa 2. De modo similar, la salida del segundo circuito LFSR, L_2, de la etapa 1 se convierte en el temporizador del segundo circuito LFSR, L_2, de la etapa 2. Pueden añadirse más etapas de idéntica manera. Un LFSR está temporizado cuando la señal de su entrada de temporización cambia de 0 a 1. Aunque, en cada etapa, los LFSR L_1, L_2 tienen, preferiblemente, las mismas longitudes en bits, dichas longitudes pueden ser, también, diferentes.

Aunque la invención se ha descrito con referencia detallada a ciertas realizaciones específicas, tales detalles pretenden ser instructivos, en lugar de restrictivos. Los expertos en la técnica apreciarán que pueden hacerse muchas variaciones en la estructura y el modo de operación sin salirse del ámbito de esta invención, tal como se describe en las enseñanzas de este documento.

REIVINDICACIONES

1. Un generador de corriente de cifra que incluye un primer (L1) y un segundo (L2) registros de desplazamiento con realimentación lineal, cada uno con una entrada y una salida de temporización, teniendo el generador de cifrado continuo salidas que se combinan con el fin de generar dicha corriente de cifra, **caracterizándose** dicho generador de cifrado continuo porque la salida de dicho segundo registro (L2) se combina con una señal de temporización, la salida del segundo registro y la señal de temporización, combinadas, se aplican a la entrada de temporización de dicho primer registro (L1) y la señal de temporización se aplica, directamente, a la entrada de temporización de dicho segundo registro (L2).

2. El generador de corriente de cifra de la reivindicación 1, **caracterizado** porque dichos primero (L1) y segundo (L2) registros tienen longitudes diferentes.

3. El generador de corriente de cifra de las reivindicaciones 1 o 2, **caracterizado** porque el periodo de dicho primer registro (L1) es primo en relación con el periodo de dicho segundo registro (L2).

4. El generador de corriente de cifra de cualquiera de las reivindicaciones precedentes, **caracterizado** porque la salida de dicho primer registro (L1) de desplazamiento con realimentación lineal y la salida de dicho segundo registro (L2) de desplazamiento con realimentación lineal se combinan mediante una puerta “O exclusiva”.

5. El generador de corriente de cifra de cualquiera de las reivindicaciones precedentes, **caracterizado** porque dicho primer registro (L1) de desplazamiento con realimentación lineal recibe la salida de dicho segundo registro (L2) de desplazamiento con realimentación lineal por medio de una puerta “Y” o una puerta “NO-Y”.

6. El generador de corriente de cifra de cualquiera de las reivindicaciones precedentes, **caracterizado** porque comprende una serie de primeros (L1) y segundos (L2) registros de desplazamiento con realimentación lineal, asociados, en el que las salidas de dichas series generan dicha corriente de cifra, y en el que cada dicho primer registro (L1) de desplazamiento con realimentación lineal respectivo está previsto de modo que reciba realimentación a partir de cada dicho segundo registro (L2) de desplazamiento con realimentación lineal respectivo.

7. El generador de corriente de cifra de la reivindicación 6, **caracterizado** porque cada uno de dichos primeros registros (L1) de desplazamiento con realimentación lineal tiene una longitud, en bits, diferente de la de cada uno de dichos segundos registros (L2) de desplazamiento con realimentación lineal.

8. El generador de corriente de cifra de la reivindicación 7, **caracterizado** porque cada uno de los primeros registros (L1) de desplazamiento con realimentación lineal tiene la misma longitud en bits, y cada uno de los segundos registros (L2) de desplazamiento con realimentación lineal tiene la misma longitud en bits.

9. El generador de corriente de cifra de la reivindicación 1, **caracterizado** porque comprende N primeros registros (L1) de desplazamiento con realimentación lineal y M segundos registros (L2) de desplazamiento con realimentación lineal, en el que la salida del enésimo primer registro (L1) de desplazamiento con realimentación lineal y la salida del emésimo segundo registro (L2) de desplazamiento con realimentación lineal se combinan mediante una puerta “O exclusiva”.

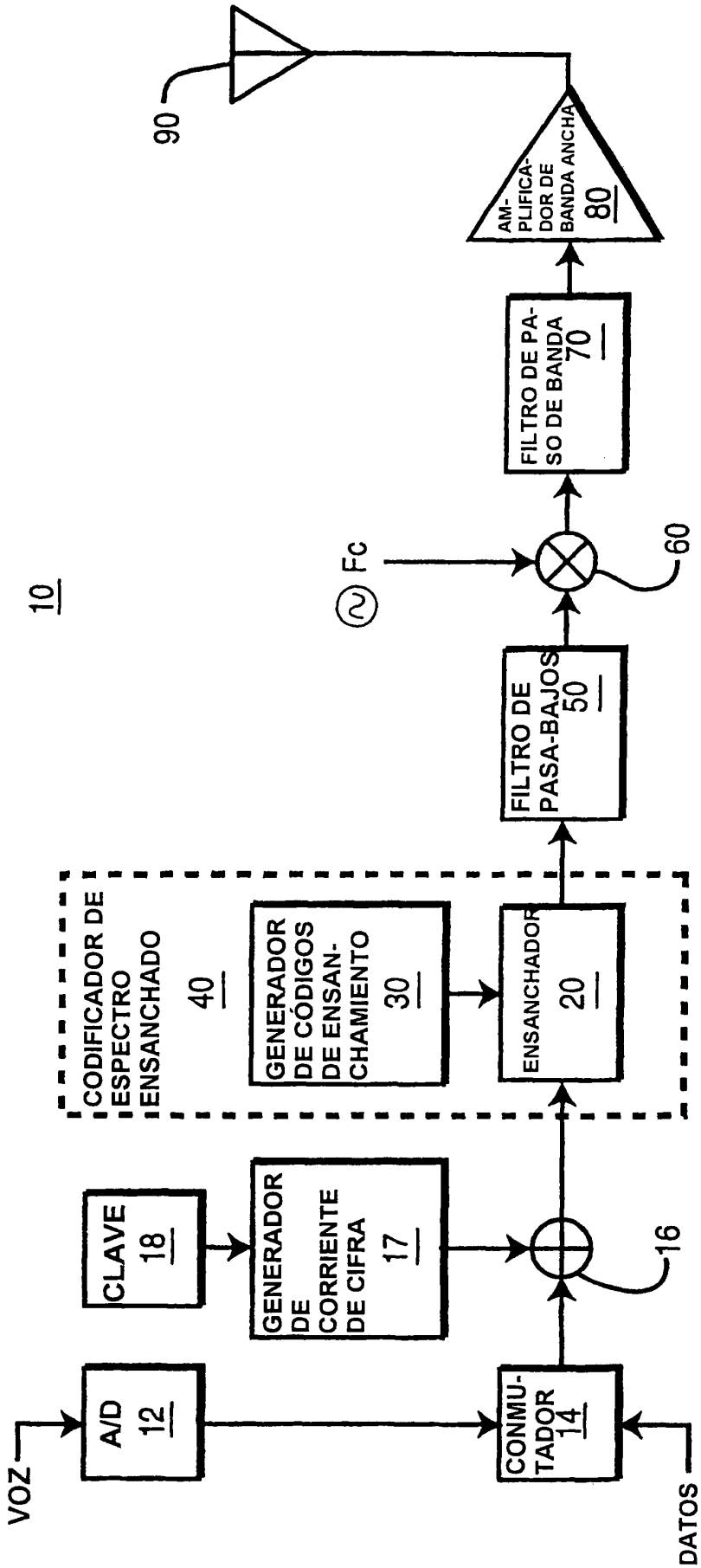

FIG. 1
TÉCNICA ANTERIOR

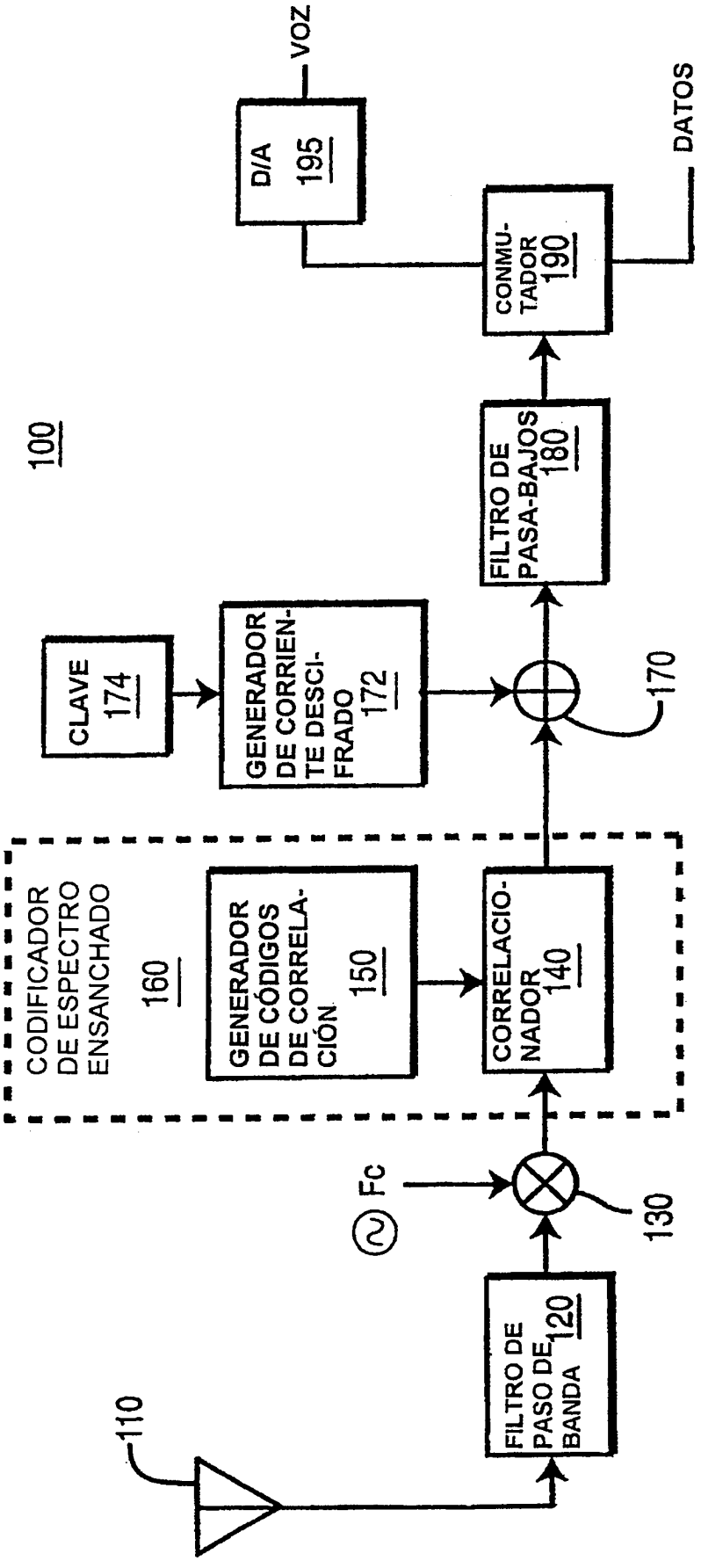
100
110
FILTRO DE PASO DE BANDA 120
Fc
130
CODIFICADOR DE ESPECTRO ENSANCHADO 160
GENERADOR DE CÓDIGOS DE CORRELACIÓN 150
CORRELACIONADOR 140
CLAVE 174
GENERADOR DE CORRIENTE DESCIFRADO 172
170
FILTRO DE PASA-BAJOS 180
CONMUTADOR 190
D/A 195
VOZ
DATOS

FIG. 2

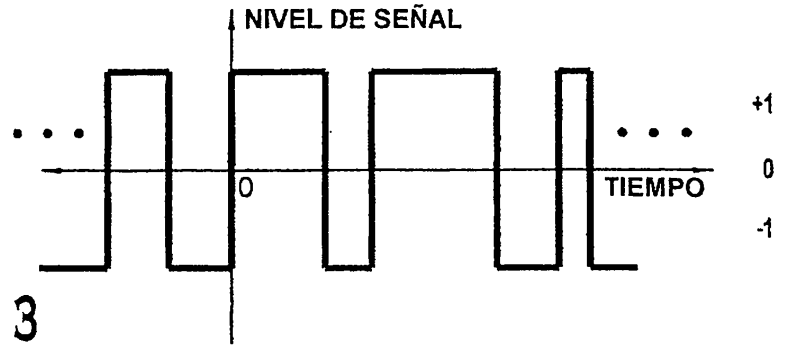

FIG. 3
TÉCNICA ANTERIOR

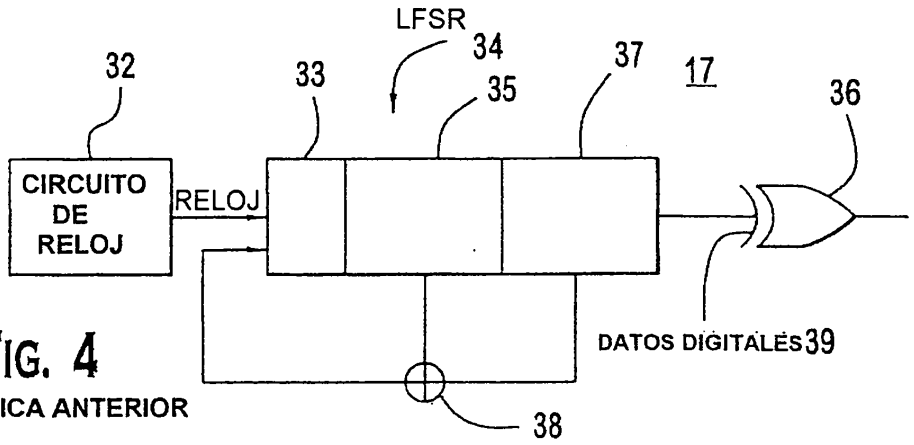

FIG. 4
TÉCNICA ANTERIOR

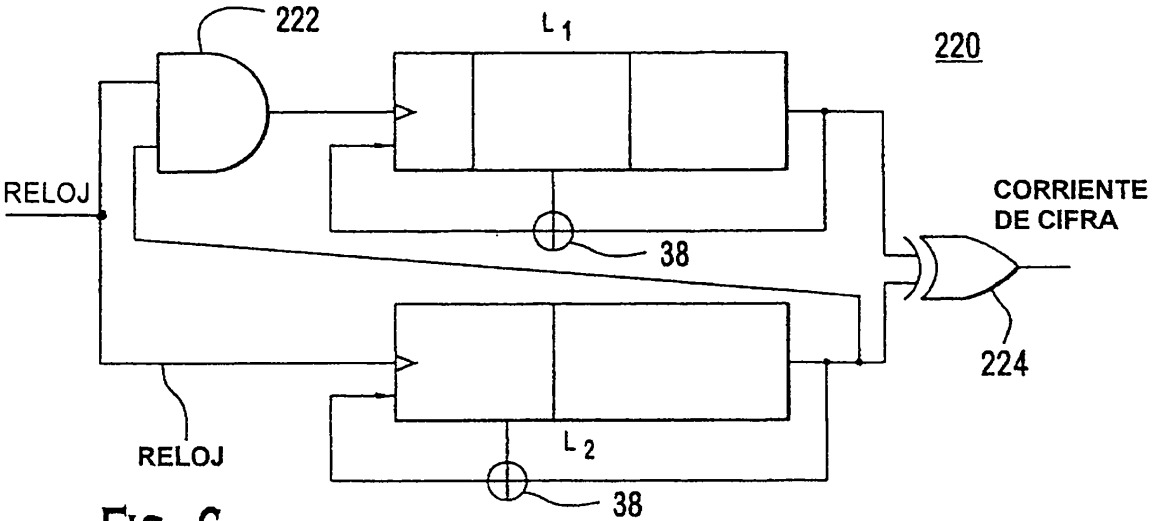

FIG. 6

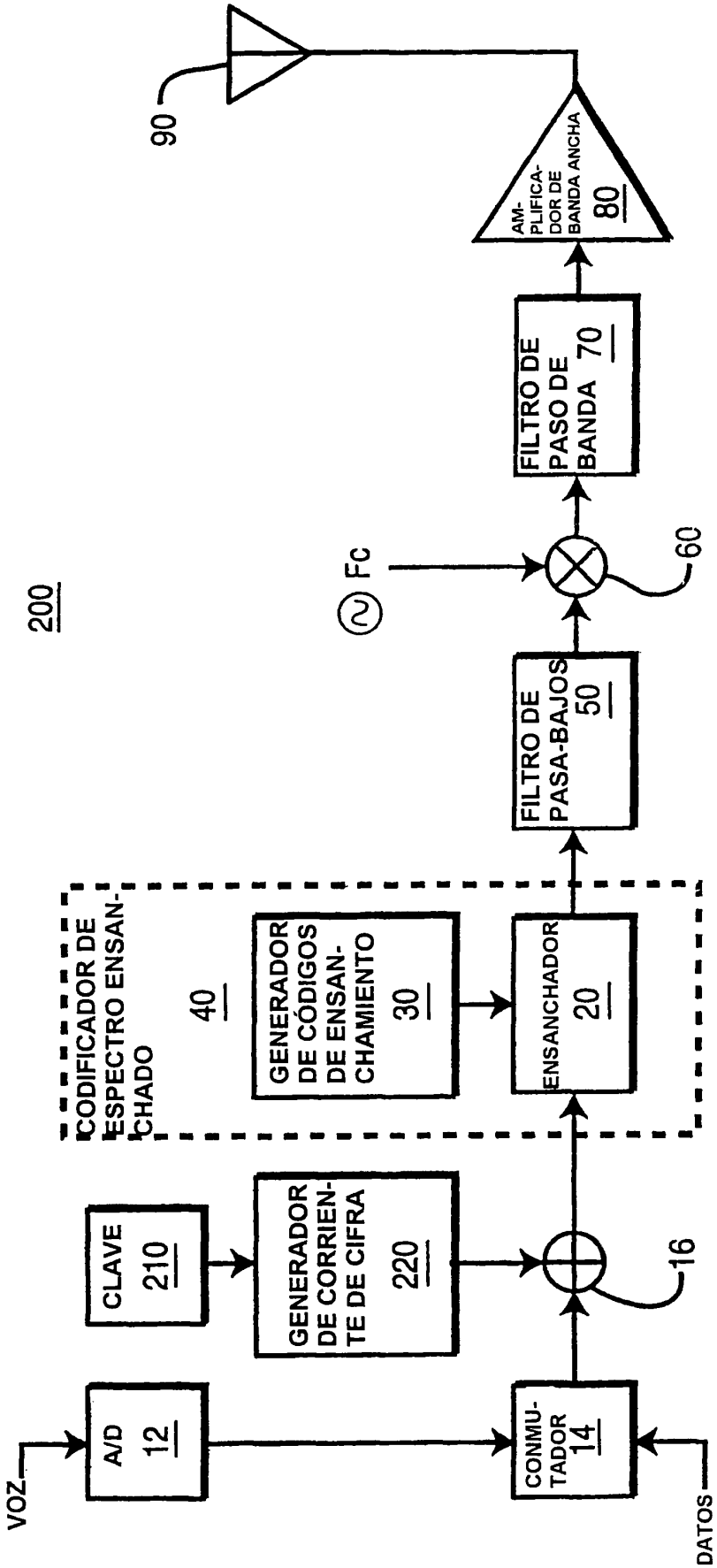
200
VOZ
A/D 12
CLAVE 210
GENERADOR DE CORRIENTE DE CIFRA 220
CODIFICADOR DE ESPECTRO ENSANCHADO 40
GENERADOR DE CÓDIGOS DE ENSANCHAMIENTO 30
ENSANCHADOR 20
CONMUTADOR 14
DATOS
16
FILTRO DE PASA-BAJOS 50
Fc
60
FILTRO DE PASO DE BANDA 70
AMPLIFICADOR DE BANDA ANCHA 80
90

FIG. 5

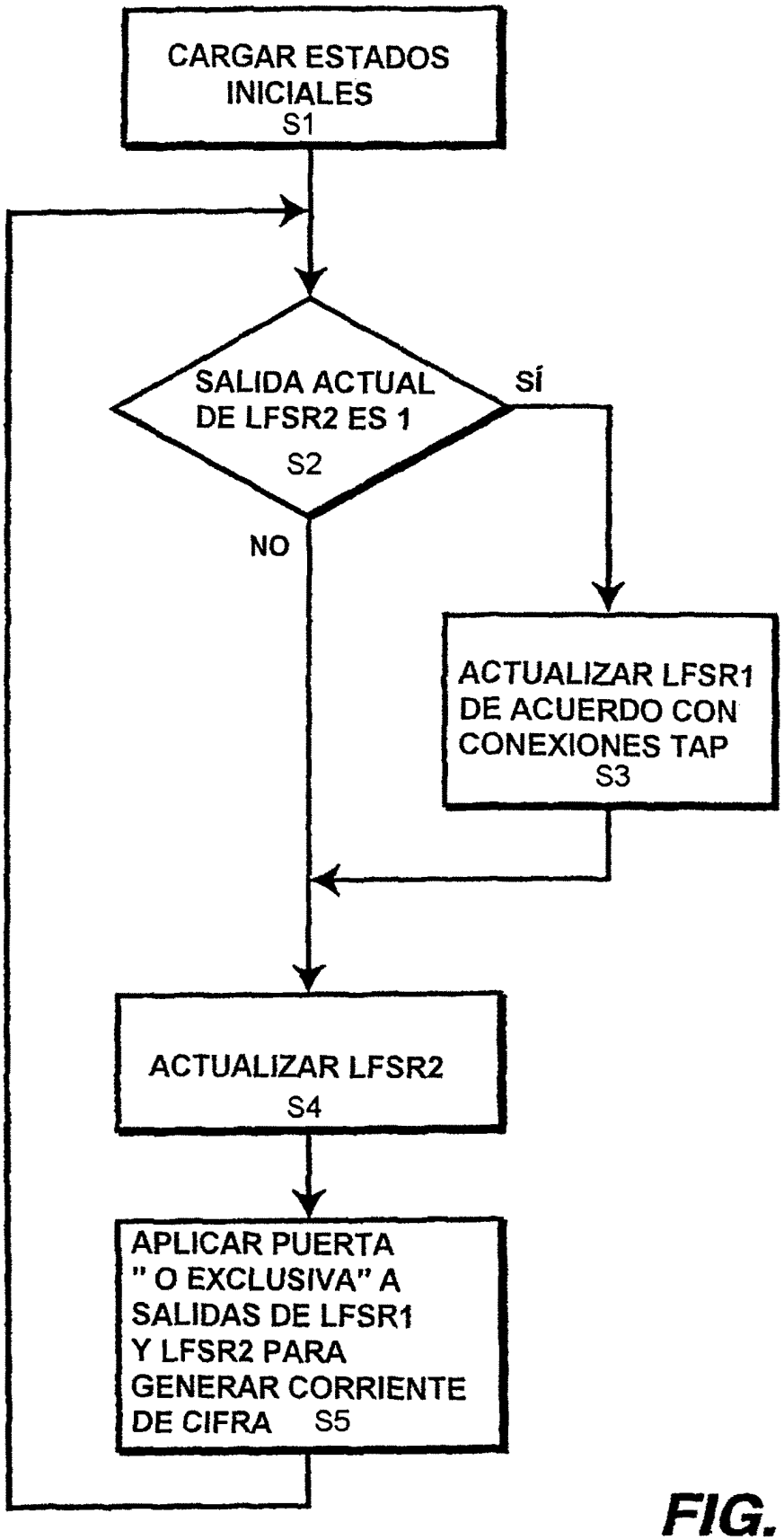
CARGAR ESTADOS INICIALES
S1
SALIDA ACTUAL DE LFSR2 ES 1
S2
SÍ
NO
ACTUALIZAR LFSR1 DE ACUERDO CON CONEXIONES TAP
S3
ACTUALIZAR LFSR2
S4
APLICAR PUERTA " O EXCLUSIVA" A SALIDAS DE LFSR1 Y LFSR2 PARA GENERAR CORRIENTE DE CIFRA
S5

FIG. 7

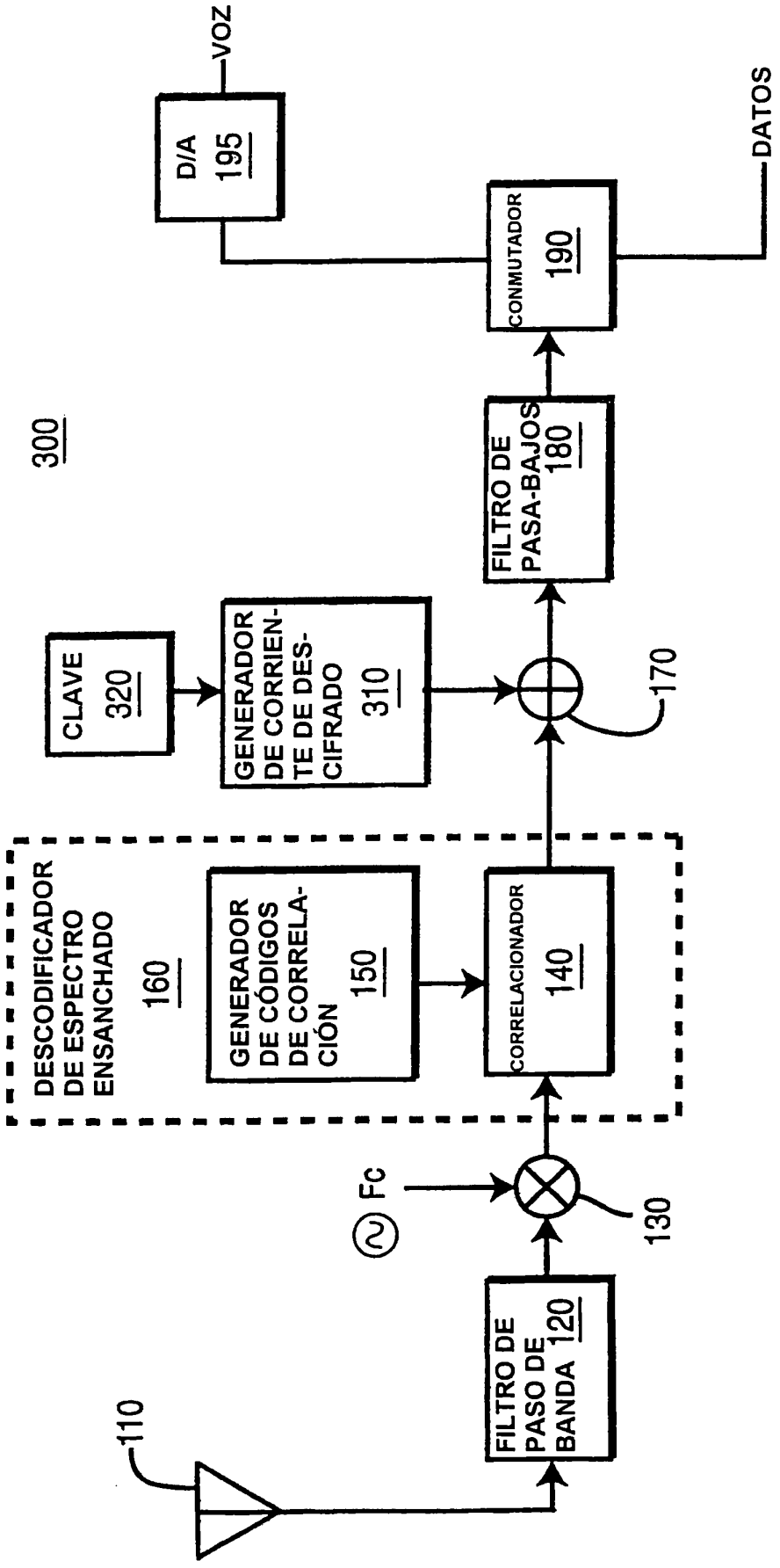
300
110
FILTRO DE PASO DE BANDA 120
Fc
130
DESCODIFICADOR DE ESPECTRO ENSANCHADO 160
GENERADOR DE CÓDIGOS DE CORRELACIÓN 150
CORRELACIONADOR 140
CLAVE 320
GENERADOR DE CORRIENTE DE DESCIFRADO 310
170
FILTRO DE PASA-BAJOS 180
CONMUTADOR 190
D/A 195
VOZ
DATOS

FIG. 8

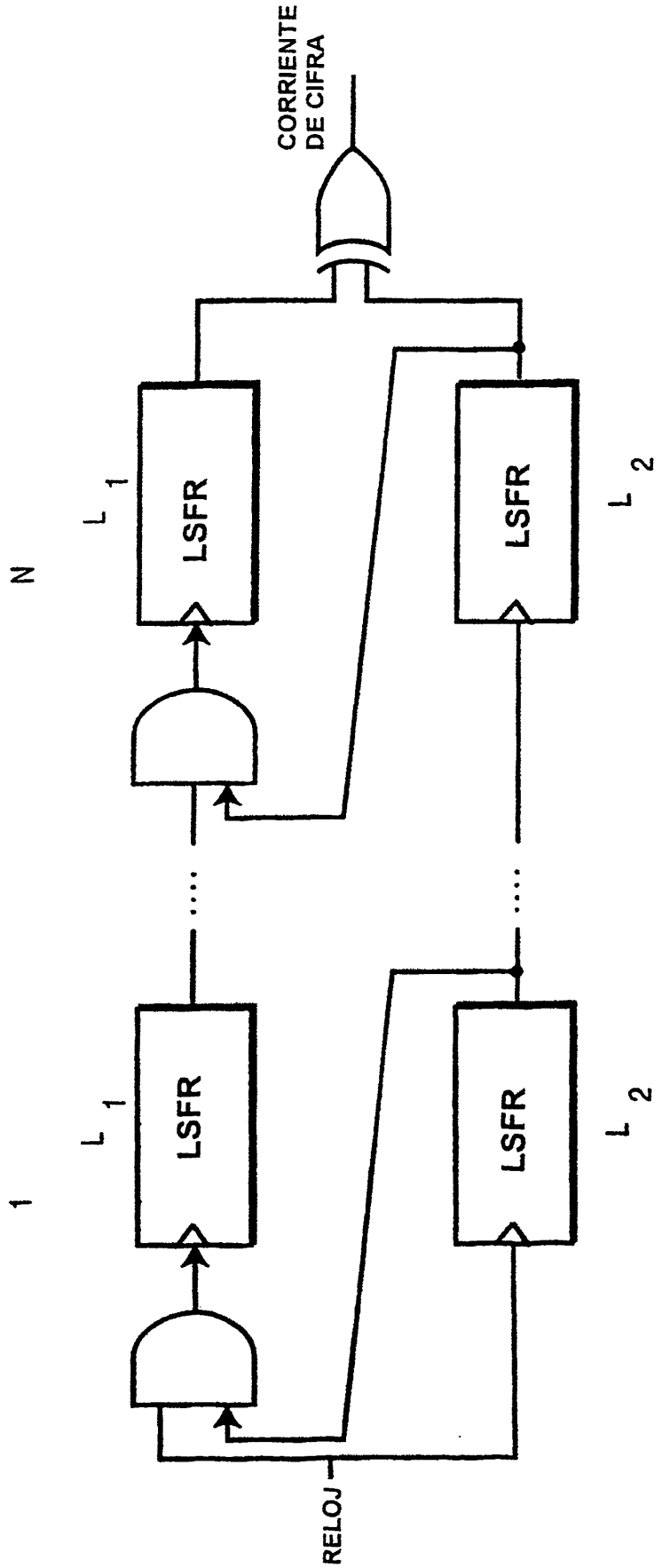

FIG. 9