(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 355 828**

(51) Int. Cl.:
G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04786246 .1**
(96) Fecha de presentación : **02.08.2004**
(97) Número de publicación de la solicitud: **1784718**
(97) Fecha de publicación de la solicitud: **16.05.2007**

(54) Título: **Generación de una secuencia de datos pseudoaleatoria.**

(45) Fecha de publicación de la mención BOPI:
31.03.2011

(45) Fecha de la publicación del folleto de la patente:
31.03.2011

(73) Titular/es: **FRANCE TELECOM**
6 place d'Alleray
75015 Paris, FR
Université de Caen Basse Normandie

(72) Inventor/es: **Sibert, Hervé y**
Gouget, Aline

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

GENERACIÓN DE UNA SECUENCIA DE DATOS PSEUDOALEATORIA

Campo técnico de la invención

La invención se refiere al campo de la codificación/decodificación y en particular, se refiere a un sistema y un método de generación de una secuencia de datos pseudoaleatoria.

La invención encuentra una aplicación muy ventajosa en la que permite crear secuencias de bits destinadas al cifrado simétrico, para el cual las operaciones de cifrado y descifrado utilizan una misma clave secreta. Se inscribe dentro del método clásico denominado de cifrado simétrico flotante para el cual son idénticas la operación de cifrado y de la operación de descifrado. El cifrado simétrico se suele utilizar en todos los tipos de comunicaciones, tales como las comunicaciones móviles (GSM, UMTS,…), Internet (SSL…), las tarjetas con circuito integrado (tarjetas bancarias), etc.

Antecedentes de la invención

El método más extendido de cifrado flotante consiste en generar una secuencia cifradora de forma independiente del mensaje a cifrar haciendo llamada, con un objeto de economía material, a registros de desplazamiento con retroacción lineal.

El principal inconveniente de los registros de desplazamiento con retroacción lineal es su linealidad. En efecto, el conocimiento de un número de bits de salida del registro igual a la longitud de registro así como del polinomio de retroacción asociado al registro permite conocer los bits de salida así como todos los estados posteriores del registro.

Además, con el fin de “destruir” la linealidad de los registros de desplazamiento con retroacción lineal, es de utilidad combinar la salida de varios registros así como, ocasionalmente, su estado interno, con la ayuda de una función booleana no lineal, por ejemplo.

La Figura 6 representa un tal generador 100 denominado “*shrinking generator*” (generador pseudoaleatorio), descrito en la solicitud de patente europea EP 0 619 659, que presenta un primer registro de desplazamiento con retroacción lineal 111a, un segundo registro de desplazamiento con retroacción lineal 111b y un medio 112 para seleccionar la salida del generador 100.

De este modo, en cada desplazamiento, los dos registros 111a y 111b están desplazados simultáneamente y la salida del dispositivo 100 es igual a la salida del segundo registro 111b si la salida del primer registro 111a es “1” y si no es así, no hay ningún bit a la salida.

El *shrinking generator* permite combinar no solamente las salidas de dos registros de desplazamiento con retroacción lineal sino también, más generalmente, cualquier par de secuencias de bits. Este generador pseudoaleatorio forma parte de una clase de métodos de cifrado simétrico flotante, en donde un registro de desplazamiento con retroacción lineal controla a otro. La idea objetivo es hacer variar el número de desplazamientos, de una parte, entre los diferentes registros utilizados y, de otra parte, entre dos bits consecutivos, con el fin de destruir la linealidad de los registros.

Una variante del *shrinking generator*, denominada “*self-shrinking generator” (generador pseudoaleatorio automático)*, se basa en el mismo principio pero a partir, esta vez, de un solo registro. Los bits de salida del registro son objeto de lectura dos a dos y el primer bit controla la salida del segundo, de modo que la salida del sistema es el segundo bit si el primero es “1” y si no es así, no existe ningún bit de salida.

Los inconvenientes del empleo de registros de desplazamiento con retroacción lineal solamente son numerosos. El principal es la debilidad debida a la linealidad del dispositivo. Cuando se combinan registros por una función booleana, también aparecen inconvenientes. Al nivel material, proceden de la complejidad de la realización de la función. Además, esta función está fijada y es posible atacarla.

De otra parte, métodos estadísticos han puesto en evidencia algunos puntos débiles del *shrinking generator* y de otros métodos de cifrado con control de reloj. En particular, dentro del *shrinking generator*, el número de desplazamientos efectuados por los dos registros varía entre dos bits de salida, pero tiene el mismo valor para los dos registros.

Finalmente, un último inconveniente del *shrinking generator* es su debilidad con respecto al número de bits salidos sobre el número de bits calculados que es igual, como media, a 1/4. Esta relación es la misma para el *self-shrinking generator*, que presenta la mayor parte de las vulnerabilidades del *shrinking generator*.

Objetivo y resumen de la invención

La invención tiene por objetivo subsanar estos inconvenientes y simplificar la generación de una secuencia de datos pseudoaleatoria de calidad adecuada.

Otro objetivo es dar a conocer un método y un generador que permiten tener una relación entre el número de bits salidos y el número de bits calculados superior a 1/4.

Otro objetivo de la invención es realizar un generador muy eficaz y de bajo coste.

Estos objetivos se alcanzan gracias a un método de generación de una secuencia de datos pseudoaleatoria, ejecutado por un generador de secuencia de datos pseudoaleatoria, utilizándose dicha secuencia de datos pseudoaleatoria como una secuencia cifradora en un método de cifrado a flote y siendo generada a partir de un método de búsqueda de al menos un motivo de búsqueda de un bit dentro de una secuencia de datos inicial de N bits, desplazando una ventana de la magnitud de 1 bit en la secuencia de datos inicial, estando situada esta ventana en una posición inicial determinada. La secuencia de datos inicial se genera por un medio que comprende un registro de desplazamiento con retroacción lineal.

De este modo, el método según la invención se refiere a un método no lineal de generación de datos pseudoaleatorios y basado en la detección de motivos que permiten combinar, de manera no lineal, uno o varios flujos de bits para obtener un nuevo flujo de bits.

Este método, muy sencillo de realizar, presenta una complejidad intrínseca para poder obtener una secuencia de datos pseudoaleatoria de calidad adecuada.

El procedimiento de búsqueda comprende las etapas siguientes:

- establecer el bit de la ventana en un motivo de búsqueda;

- detectar el motivo de búsqueda en dicha secuencia de datos inicial desplazando la ventana en la secuencia de datos inicial;

- determinar un motivo de salida de k bits según una operación que depende del desarrollo de la etapa anterior, estando dicho motivo determinado:

● según una primera ley, si la ventana se desplaza una sola vez antes de detectar el motivo de búsqueda en la secuencia de datos inicial, atribuyendo dicha primera ley un valor denominado de salida al motivo de salida y

● según una segunda ley, si no es así, que atribuye al motivo de salida el resultado de la adición, de módulo dos, entre el valor denominado de salida y el valor 1;

- desplazar la ventana de 1 bit, desde el bit actual al bit siguiente y

- repetir las etapas anteriores de forma sucesiva para constituir la secuencia de datos pseudoaleatoria mediante concatenación de los motivos de salida.

Las etapas de detección de dicho motivo de búsqueda y de determinación de dicho motivo de salida se realizan mediante una secuencia de operaciones que comprenden un primer conjunto de reglas que permiten definir al menos un modo de desplazamiento para desplazar la ventana en dicha secuencia de datos inicial para detectar el motivo de búsqueda.

La secuencia de operaciones comprende, además, un segundo conjunto de reglas que determinan las condiciones de parada de desplazamiento de la ventana en dicha secuencia de datos inicial.

Al menos una regla de dicho conjunto de reglas genera una actualización del motivo de búsqueda y/o de dicho motivo de salida, en función del desplazamiento y/o del contenido de la ventana.

La secuencia de operaciones se puede repetir hasta que se cumpla una condición previamente determinada.

En una forma de realización preferida, la secuencia de operaciones se modifica después de cada ejecución.

Según una particularidad de la invención, la secuencia de operaciones permanece invariable después de cada ejecución y permite, por medio de la ventana de 1 bit, recorrer dicha secuencia de datos inicial, de manera continua bit a bit, para detectar un motivo de búsqueda de 1 bit y para determinar un motivo de salida de 1 bit.

Según un primer modo de realización de la invención, la secuencia de operaciones comprende las etapas siguientes:

- establecer el bit de una ventana en el motivo de búsqueda;

- desplazar la ventana de un bit desde el bit actual al bit siguiente;

- actualizar el motivo de salida según una primera ley, si el contenido de la ventana es igual al del motivo de búsqueda;

- actualizar el motivo de salida según una segunda ley, si el contenido de la ventana no es igual al bit del motivo de búsqueda;

- desplazar la ventana, bit a bit, hacia los bits siguientes en tanto que el contenido de la ventana no sea igual al bit del motivo de búsqueda;

- desplazar la ventana en un bit, desde el bit actual al bit siguiente y

- hacer salir el motivo de salida.

Según el primer modo de realización, la primera ley atribuye un valor determinado b al motivo de salida y la segunda ley realiza una adición de módulo dos entre dicho valor determinado b y el valor 1 y atribuye el resultado de dicha adición al motivo de salida.

Según un segundo modo de realización de la invención, la primera ley realiza una adición de módulo dos entre un valor determinado b y el valor E del motivo de búsqueda y atribuye el resultado de dicha adición al motivo de salida y la segunda ley realiza una adición de módulo dos entre dicho valor determinado b, el valor E del motivo y de búsqueda y el valor 1 y atribuye el resultado de dicha adición al motivo de salida.

Según una aplicación del método de la presente invención, cada bit de dicha secuencia de datos pseudoaleatoria está combinado con un bit correspondiente de una secuencia de datos de un mensaje a cifrar mediante una adición de módulo dos para constituir una secuencia de datos cifrada.

La invención se refiere, además, a un dispositivo de codificación que comprende un generador de una secuencia de datos pseudoaleatoria, estando dicho dispositivo de codificación adaptado para realizar un cifrado simétrico flotante utilizando la secuencia de datos pseudoaleatoria generada como secuencia cifradora, presentando dicho generador un medio de búsqueda para buscar al menos un motivo de búsqueda dentro de una secuencia de datos inicial de N bits, desplazando una ventana de magnitud de 1 bit de un medio de detección del medio de búsqueda en la secuencia de datos inicial, situándose la ventana en una posición inicial determinada.

El medio de búsqueda del generador comprende, además, un medio de determinación y un medio de repetición y se caracteriza porque:

- el medio de determinación es capaz de establecer el bit de la ventana en un motivo de búsqueda;

- el medio de detección es capaz de detectar el motivo de búsqueda en dicha secuencia de datos inicial desplazando dicha ventana en dicha secuencia de datos inicial;

- el medio de determinación es capaz de determinar un motivo de salida de un bit según una operación que depende del desarrollo de la detección de dicho al menos un motivo de búsqueda, estando determinado el motivo de salida:

● según una primera ley, si la ventana se desplaza, una sola vez, antes de detectar el motivo de búsqueda en la secuencia de datos inicial, dicha primera ley atribuye un valor denominado de salida al motivo de salida y

● según una segunda ley, de lo contrario, dicha segunda ley atribuye al motivo de salida el resultado de la adición, de módulo dos, entre el valor denominado de salida y el valor 1;

- el medio de detección es capaz de desplazar la ventana, en un bit, desde el bit actual al bit siguiente y

- el medio de repetición es adecuado para generar la secuencia de datos pseudoaleatoria mediante concatenación de los motivos de salida.

El medio de detección contiene dicha ventana destinada a desplazarse en dicha secuencia de datos inicial y un primer medio de control para controlar el desplazamiento de dicha ventana en dicha secuencia de datos inicial.

El medio de determinación presenta un segundo medio de control para actualizar dicho motivo de búsqueda y/o dicho motivo de salida.

El generador comprende, además, un medio inicial para generar la secuencia de datos inicial de N bits.

El medio inicial comprende un registro de desplazamiento con retroacción lineal.

La invención se refiere, además, a un dispositivo de codificación que presenta una puerta lógica ‘o exclusiva’ y un generador según las características anteriores.

La invención se refiere, además, a un sistema asegurado que comprende al menos dos entidades, cada una de las cuales presenta un dispositivo de codificación.

Breve descripción de los dibujos

Otras particularidades y ventajas de la invención se deducirán de la lectura de la descripción realizada, a continuación, a título indicativo pero no limitativo, haciendo referencia a los dibujos adjuntos, en los que:

- la Figura 1 ilustra un ejemplo muy esquemático de un generador de una secuencia de datos pseudoaleatoria según la invención;

- la Figura 2 representa un sistema de uso seguro que contiene generadores según se representa en la Figura 1;

- la Figura 3 ilustra un ejemplo de un método de búsqueda para la generación de la secuencia de datos pseudoaleatoria, según la invención;

- las Figuras 4 a 5 representan modos de realización particulares del método según la invención y

- la Figura 6 es una vista muy esquemática de un generador según la técnica anterior.

Descripción detallada de modos de realización

En conformidad con la invención, la Figura 1 ilustra un ejemplo muy esquemático de un generador 1 de una secuencia de datos pseudoaleatoria 3.

El generador 1 comprende un medio de búsqueda 5 para buscar al menos un motivo de búsqueda 7 dentro de una secuencia de datos inicial 9 de N bits. Éste o estos motivos de búsqueda figuran entre un conjunto de motivos de búsqueda.

En lo que sigue en esta descripción se denomina un “motivo” cualquier palabra constituida únicamente por 0 y 1. Por ejemplo, 0, 11, 000, 1010, 00111 son motivos de longitudes respectivas, 1, 2, 3, 4 y 5. Por otro lado, un motivo “vacío” es una palabra nula.

La secuencia de datos inicial de N bits (siendo N un número entero) se genera por un medio inicial 11 que puede comprender un registro de desplazamiento con retroacción lineal de periodo máximo.

Un registro de desplazamiento con retroacción lineal es una tabla de bits de longitud definida (el registro) provista de una combinación lineal, representada por un polinomio denominado polinomio de retroacción de los elementos componentes de la tabla. En cada desplazamiento, el bit de índice más elevado es objeto de salida, siendo todos los demás bits desplazados en un índice y el bit de índice más pequeño toma el valor de la combinación lineal antes del desplazamiento.

En una forma de realización preferida, el polinomio de retroacción puede ser, por ejemplo, un polinomio primitivo correspondiente a un registro de desplazamiento lineal de periodo máximo o bien, un polinomio de la forma $Q=(x^2+1)P$, siendo P un polinomio primitivo.

El medio de búsqueda 5 del generador 1 comprende un medio de detección 13, un medio de determinación 15 y un medio de repetición 17.

El medio de detección 13 está destinado a detectar al menos un motivo de búsqueda 7 de r bits dentro de la secuencia de datos inicial, en donde r es igual a 1. El medio de determinación 15 define el conjunto de motivos de búsqueda al que pertenece el motivo de búsqueda 7 detectado por el medio de detección 13.

El medio de detección comprende una ventana 19 destinada a desplazarse en la secuencia de datos inicial 9 y un primer medio de control 21 para controlar el desplazamiento de la ventana 19 en la secuencia de datos inicial 9.

La ventana 19 está situada en una posición inicial determinada en la secuencia de datos inicial 9 y presenta una magnitud determinada de 1 bit. Por ejemplo, una ventana 19 de magnitud t (siendo t un número entero inferior a N) situada en la secuencia de datos inicial 9 es una máscara que puede desplazarse en esta secuencia 9 dejando aparecer, en cada desplazamiento, exactamente t bits de la secuencia 9.

El medio de determinación 15 está en interacción con el medio de detección 13 a través de un enlace 23. Este medio de determinación 15 está destinado a determinar un motivo de salida 25 de k bits (siendo k igual a 1), según una operación que depende del desarrollo de la búsqueda del motivo de búsqueda 7.

En efecto, el medio de determinación 15 presenta un segundo medio de control 27 para definir o actualizar el conjunto de motivos de búsqueda y/o el motivo de salida 25.

Por otro lado, el medio de repetición 17 está unido a los medios de detección 13 y de determinación 15 a través de los enlaces 29 y 31, respectivamente.

De este modo, el medio de repetición 17 puede intercambiar señales con los medios de detección 13 y de determinación 15 para reiniciar las operaciones de detección y de determinación, por ejemplo, después de haber recibido, del medio de determinación 15, la señal de que acaba de salir un motivo de salida 25, siendo esta última una condición de parada previamente determinada no cumplida. El medio de repetición 17 puede, además, comprobar la condición de parada gracias a los intercambios de señales con los medios de detección 13 y de determinación 15. Esto permite generar una sucesión de motivos de salida 25 que constituyen, mediante concatenación, la secuencia de datos pseudoaleatoria 3.

Se entenderá que el medio de repetición 17 puede, además, estar integrado en el primero o segundo medio de control 21 o 27 de los medios de detección 13 y de determinación 15.

La Figura 2 representa un sistema de uso seguro 31 que comprende al menos dos entidades conectadas entre sí

mediante una red de comunicación 35 de tipo Internet, GSM, UMTS, etc.

El ejemplo de esta figura presenta una primera entidad 33a conectada, a través de la red de comunicación 35 a una segunda entidad 33b.

La primera entidad 33a (respectivamente, la segunda entidad 33b) comprende un primer terminal 37a (respectivamente un segundo terminal 37b), un primer dispositivo de codificación 39a (respectivamente un segundo dispositivo de codificación 39b) y un primer módem 41a (respectivamente un segundo módem 41b), pudiendo ser los módems 41a y 41b cualquier dispositivo que permita la realización de una interfaz para la red de comunicación 35.

Cada uno de los primero y segundo dispositivos de codificación 39a, 39b comprende un generador 1 de una secuencia de datos pseudoaleatoria 3 tal como se describió anteriormente y una puerta lógica “o exclusiva” 43.

Cada dispositivo de codificación 39a, 39b, está destinado a realizar un cifrado o un descifrado a flote, que consiste en cifrar o descifrar un mensaje bit a bit.

Según este ejemplo, el primer dispositivo de codificación 39a realiza una operación de cifrado. De este modo, la secuencia de datos pseudoaleatoria 3 denominada secuencia cifradora, está combinada por la puerta O exclusiva 43 con cada bit de posición correspondiente de un mensaje no cifrado 45 enviado por el primer terminal 37a para obtener un texto cifrado 47 que, a continuación, se envía por el primer módem 41a a la segunda entidad 33b. De este modo, la operación de cifrado consiste en añadir, bit a bit, una secuencia cifradora 3 en texto no cifrado del mensaje 45 para obtener el texto cifrado 47.

El segundo dispositivo de codificación 39b realiza una operación de descifrado que consiste en añadir, bit a bit, esta misma secuencia cifradora 3 al texto cifrado 47, enviado por la primera entidad 33a para reformar el mensaje al texto no cifrado 45.

De este modo, las operaciones de cifrado y de descifrado son idénticas.

Las Figuras 3 a 5 ilustran el procedimiento de generación de datos pseudoaleatoria según la invención.

Este método consiste en generar la secuencia de datos pseudoaleatoria 3 a partir de un método de búsqueda de al menos un motivo de búsqueda dentro de la secuencia de datos inicial 9.

De este modo, la determinación de los elementos de la secuencia de datos pseudoaleatoria, según la invención, depende del motivo buscado y del registro histórico o de la manera en la que se ha realizado la búsqueda.

La Figura 3 ilustra un ejemplo de un método de búsqueda para la generación de la secuencia de datos pseudoaleatoria 3, según la invención.

La etapa E1 se refiere a la detección de al menos un motivo de búsqueda 7 de 1 bit definido entre un conjunto de motivos de búsqueda dentro de la secuencia de datos inicial 9.

La etapa E2 se refiere a la determinación de un motivo de salida 25 de 1 bit, según una operación que depende del desarrollo de la etapa precedente E1.

En efecto, la determinación del motivo de salida 25 depende del motivo de búsqueda 7 y del registro histórico de la búsqueda, en particular del número de etapas o de iteraciones efectuadas antes de encontrar el motivo de búsqueda 7 en cuestión dentro de la secuencia de datos inicial 9.

Estas etapas de detección E1 del motivo de búsqueda 7 y de determinación E2 del motivo de salida 25 se realizan mediante una secuencia de operaciones.

Esta secuencia de operaciones presenta un primer conjunto de reglas implantadas por el primer medio de control 21 del generador 1, que permiten definir al menos un modo de desplazamiento para desplazar una ventana 19 en la secuencia de datos inicial 9 para detectar el motivo de búsqueda 7.

De una manera general, una ventana 19, de magnitud no nula, se desplaza en la secuencia de datos inicial 9. Al principio del método de búsqueda, la ventana 19 se encuentra en una posición inicial en la secuencia inicial 9 (por ejemplo, puede estar al principio de la secuencia inicial 9). El bit que se encuentra en la ventana 19 se utilizará para determinar el motivo de salida 25.

El primer conjunto de reglas puede definir el sentido de desplazamiento, la amplitud del desplazamiento o la forma de desplazamiento de la ventana 19, por ejemplo un desplazamiento cíclico en una parte de la secuencia de datos inicial 9.

A título de ejemplo, el primer conjunto de reglas puede presentar una regla r_1 definida de la manera siguiente:

r_1 = “desplazar en un bit hacia la derecha”.

Además, la secuencia de operaciones presenta un segundo conjunto de reglas implantadas por el segundo medio

de control 27 del generador 1, que determinan las condiciones de parada de desplazamiento de la ventana 19 a través de la secuencia de datos inicial 9.

El segundo conjunto de reglas puede presentar una pluralidad de reglas que se deben aplicar según un orden determinado, antes de que el generador 1 entregue el motivo de salida 25. De este modo, la entrega por el generador 1 de una sucesión de motivos de salida 25 permite constituir la secuencia de datos pseudoaleatoria 3.

A título de ejemplo, el segundo conjunto de reglas presenta una regla r_2 definida de la manera siguiente:

r_2 = “en tanto que el contenido de ventana 19 no sea un motivo del conjunto de motivos de búsqueda 7, desplazar la ventana 19 según la regla r_1”, en donde r_1 es una regla del primer conjunto de reglas.

Además, otra regla perteneciente a este segundo conjunto de reglas puede generar una actualización del conjunto de motivos de búsqueda 7 y/o del motivo de salida 25 según una ley binaria dada y en función del desplazamiento y/o del contenido de la ventana 19.

De este modo, los motivos de búsqueda 7 dependen del contenido de la ventana 19 o de las ejecuciones precedentes de la secuencia de operaciones que presentan los primero y segundo conjuntos de reglas.

Además, el motivo de salida 25 puede depender del contenido de la ventana 19 o también depender de las ejecuciones precedentes de la secuencia de operaciones que presentan los primero y segundo conjuntos de reglas.

Por otro lado, la etapa E3 del método de búsqueda consiste en repetir las dos etapas precedentes E1 y E2, de forma sucesiva, para constituir, mediante concatenación, la secuencia de datos pseudoaleatoria 3 a partir de una sucesión de motivos de salida 25.

Se entenderá que la sucesión de operaciones se puede repetir hasta que se cumpla una condición previamente determinada. Esta condición puede ser el contenido de una ventana 19 de la secuencia de datos inicial 9, si esta última está acabada. Además, es posible repetir la sucesión de operaciones hasta que se cumpla una condición definida por el usuario.

Por otro lado, con el fin de mejorar todavía más la calidad de la secuencia de datos pseudoaleatoria 3, es posible modificar la sucesión de operaciones después de cada ejecución.

De este modo, este método consiste en recorrer un flujo inicial de bits (secuencia de datos inicial 9) con la ayuda de una ventana 19, de modo que cada bit de salida de la secuencia de datos pseudoaleatoria 3 dependa de al menos una búsqueda de uno o varios motivos 7 dentro de este flujo inicial 9. Además, los motivos 7 a buscar dependen, ellos mismos, del contenido y/o del desplazamiento de la ventana 19.

Las Figuras 4 a 5 representan modos de realización particulares del método según la invención.

Según estos ejemplos, la sucesión de operaciones permanece invariable después de cada ejecución, la ventana 19 es de “magnitud uno” (es decir, que cada ventana comprende 1 bit), el conjunto de motivos de búsqueda contiene al menos un motivo de búsqueda 7 y los motivos de búsqueda 7 y de salida 25 son también de magnitud uno.

Además, la amplitud de desplazamiento de la ventana 19 es igual a una unidad, es decir que cada ventana 19 se desplaza en un bit en cada iteración, por ejemplo, desde el bit actual al bit siguiente (es decir, de izquierda a derecha).

De este modo cada secuencia de datos inicial 9 puede ser objeto de lectura de una forma continua, es decir bit a bit, lo que hace a los modos de realización muy sencillos de poner en práctica.

En todo lo que sigue, se indicará el valor del motivo de búsqueda 7 por E, el valor del motivo de salida 25 por s y el valor de la ventana 19 por f, f_1 y f_2.

Inicialmente, los motivos de búsqueda 7 y de salida 25 son inicializados atribuyendo un bit vacío a cada uno de ellos, es decir $E \leftarrow \phi$ y $s \leftarrow \phi$, siendo ϕ el conjunto vacío. Asimismo, se definen valores binarios o constantes, indicados por b, b_1 y b_2 que permanecen fijos en cada aplicación de la sucesión de operaciones de estos modos de realización.

Según la invención, una sola ventana 19 se desplaza en la secuencia de datos inicial 9. Puede estar inicialmente fijada en el primer bit de la secuencia de datos inicial 9.

La sucesión de operaciones del primer modo de realización puede definirse de la manera siguiente:

- imponer como única regla del primer conjunto de reglas la regla $r_{1,1}$ = “desplazar en un bit hacia la derecha”,

- imponer como reglas del segundo conjunto de reglas las siguientes:

$r_{2,1}$ = “poner el bit f de la ventana en el motivo de búsqueda *(E ← f)*”,

$r_{2,2}$ = “desplazar la ventana una vez según la regla $r_{1,1}$”,

$r_{2,3}$ = “si el contenido de la ventana es igual al bit E del motivo de búsqueda, entonces actualizar el motivo de salida $s \leftarrow b$”,

$r_{2,4}$ = “si el contenido de la ventana no es igual al bit E del motivo de búsqueda, entonces actualizar el motivo de salida $s \leftarrow b \oplus 1$”,

$r_{2,5}$ = “en tanto que el contenido f de la ventana no sea un motivo de búsqueda, desplazar la ventana según la regla $r_{1,1}$”,

$r_{2,6}$ = “desplazar la ventana una vez según la regla $r_{1,1,}$

- aplicar, en su orden, las reglas $r_{2,1}$, $r_{2,2}$, $r_{2,3}$, $r_{2,4}$, $r_{2,5}$ y $r_{2,6,}$ y

- hacer salir el motivo s de salida.

En efecto, el organigrama de la Figura 4 representa el desarrollo de la sucesión de operaciones anteriores.

La etapa E11 consiste en poner el bit de la ventana 19 en el motivo de búsqueda 7.

La etapa E12 consiste en desplazar la ventana 19 de un bit, desde el bit actual al bit siguiente.

La etapa E13 es una prueba que compara el contenido de la ventana 19 con el contenido del motivo de búsqueda 7.

La etapa E14 consiste en actualizar el motivo de salida 25 según una primera ley, si el contenido de la ventana 19 es igual al contenido del motivo de búsqueda 7. Según este ejemplo, la primera ley corresponde a la atribución del valor determinado b al motivo de salida 25 ($s \leftarrow b$).

La etapa E15 consiste en actualizar el motivo de salida 25 según una segunda ley, si el contenido de la ventana 19 no es igual al bit del motivo de búsqueda 7. Según este ejemplo, la segunda ley corresponde a realizar una adición de módulo dos entre el valor determinado b y el valor “1” y atribuye el resultado de esta adición al motivo de salida 25 $\left(s \leftarrow b \oplus 1\right)$.

Las etapas E16 y E17 constituyen un bucle que consiste en desplazar la ventana 19, bit a bit, hacia los bits siguientes en tanto que el contenido de la ventana 19 no sea igual al bit del motivo de búsqueda 7.

La etapa E18 consiste en desplazar la ventana 19 en un bit, desde el bit actual al bit siguiente.

Por último, la etapa E19 consiste en hacer salir del generador 1 el motivo de salida.

De forma esquemática, la sucesión de operaciones puede resumirse de este modo: se lee el bit E actual en la secuencia de datos inicial 9, luego se desplaza hacia la derecha en la secuencia 9 hasta encontrar el bit E. Si solamente se desplaza en un índice para encontrar el bit E, entonces es objeto de salida b y si no es así, la salida es $b \oplus 1$. A continuación, se desplaza, en un bit, hacia la derecha antes de reiniciar.

Por supuesto, el organigrama puede comprender un test de parada (no representado en la figura para mayor simplificación) para determinar si se cumple una condición previamente definida.

A título de ejemplo, estas etapas pueden repetirse para constituir la secuencia de datos pseudoaleatoria hasta que la ventana 19 salga de la secuencia de datos inicial 9.

La Figura 5 es un organigrama que ilustra el desarrollo de la secuencia de operaciones de un segundo modo de realización.

El organigrama de esta figura se distingue del organigrama de la Figura 4 solamente por las etapa E24 y E25.

En efecto, en la etapa E24, la primera ley corresponde a realizar una adición de módulo dos entre el valor determinado b y el valor E del motivo de búsqueda 7 y atribuye el resultado de esta adición al motivo de salida 25 $\left(s \leftarrow b \oplus E\right)$.

Por el contrario, en la etapa E25, la segunda ley corresponde a realizar una adición de módulo dos entre el valor determinado b, el valor E del motivo de búsqueda 7 y el valor “1” y atribuye el resultado de esta adición al motivo de salida 25 $s \leftarrow b \oplus E \oplus 1$.

De este modo, la sucesión de operaciones del segundo modo de realización se puede definir de la manera siguiente:

- imponer como única regla del primer conjunto de reglas la regla $r_{1,1}$ = “desplazar en un bit hacia la derecha”,

- imponer como reglas del segundo conjunto de reglas las siguientes:

$r_{2,1}$ = “poner el bit f de la ventana en el motivo de búsqueda ($E \leftarrow f$)”,

$r_{2,2}$ = “desplazar la ventana una vez según la regla $r_{1,1}$”,

$r_{2,3}$ = “si el contenido de la ventana es igual al bit E del motivo de búsqueda, entonces actualizar el motivo de salida $s \leftarrow b \oplus E$”,

$r_{2,4}$ = “si el contenido de la ventana no es igual al bit E del motivo de búsqueda, entonces actualizar el motivo de salida $s \leftarrow b \oplus E \oplus 1$”,

$r_{2,5}$ = “en tanto que el contenido f de la ventana no sea un motivo de búsqueda, desplazar la ventana según la regla $r_{1,1}$”,

$r_{2,6}$ = “desplazar la ventana una vez según la regla $r_{1,1}$”,

- aplicar, en su orden, las reglas $r_{2,1}$, $r_{2,2}$, $r_{2,3}$, $r_{2,4}$, $r_{2,5}$ y $r_{2,6}$, y

- hacer salir el motivo s de salida.

De forma esquemática, la sucesión de operación del segundo modo de realización puede resumirse así: se lee el bit E actual en la secuencia de datos inicial 9 y luego se desplaza hacia la derecha en la secuencia hasta encontrar el bit E. Si solamente se desplaza en un índice para encontrar E, entonces se tiene a la salida $b \oplus E$ y si no es así, se tiene a la salida $b \oplus E \oplus 1$. Se desplaza, a continuación, en un bit hacia la derecha antes de reiniciar.

Estos modos de realización son sencillos de realizar. Además, su relación entre el número de bits salidos y el número de bits calculados es, como media de 1/3 cuando, por ejemplo, el medio inicial 11, que proporciona la secuencia de datos inicial 9, es un registro de desplazamiento con retroacción lineal.

De este modo, el método según la invención permite crear una secuencia de bits pseudoaleatoria de calidad adecuada, que puede utilizarse para el cifrado simétrico del tipo de cifrado simétrico flotante.

En efecto, cada bit de la secuencia de datos pseudoaleatoria 3 puede combinarse con un bit correspondiente de una secuencia de datos de un mensaje 45 a cifrar mediante una adición de módulo 2 para formar una secuencia de datos cifrada 47 (véase Figura 2).

REIVINDICACIONES

1.- Método de generación de una secuencia de datos pseudoaleatoria (3), ejecutado por un generador (1) de secuencia de datos pseudoaleatoria, utilizándose dicha secuencia de datos pseudoaleatoria (3) como una secuencia cifradora en un método de cifrado a flote y siendo generada a partir de un método de búsqueda de al menos un motivo de búsqueda (7) de un bit en una secuencia de datos inicial (9) de N bits desplazando una ventana (19), del tamaño de un bit, en dicha secuencia de datos inicial (9), estando dicha ventana situada en una posición inicial determinada y siendo dicha secuencia de datos generada por un medio que presenta un registro de desplazamiento con retroacción lineal, comprendiendo dicho método de búsqueda las etapas siguientes:

- poner (E11) el bit de la ventana en un motivo de búsqueda;

- detectar (E12, E13) dicho motivo de búsqueda (7) en dicha secuencia de datos inicial (9) desplazando dicha ventana (19) en dicha secuencia de datos inicial (9);

- determinar (E14–E17) un motivo de salida (25) de un bit, según una operación que depende del desarrollo de la etapa precedente, estando dicho motivo de salida determinado:

● según una primera ley (E14), si la ventana se desplaza, una sola vez, antes de detectar el motivo de búsqueda en la secuencia de datos inicial, atribuyendo dicha primera ley un valor denominado de salida al motivo de salida y

● segunda una segunda ley (E15) si no lo es, dicha segunda ley atribuye al motivo de salida el resultado de la adición del módulo dos entre el valor denominado de salida y el valor 1;

- desplazar (E18) la ventana de un bit, desde el bit actual al bit siguiente y

- repetir las etapas precedentes, de manera sucesiva, para formar la secuencia de datos pseudoaleatoria (3) mediante concatenación de los motivos de salida (25).

2.- Método según la reivindicación 1, caracterizado porque el valor denominado de salida es igual:

- a un valor determinado o

- al resultado de la adición del módulo dos entre un valor determinado y el motivo de búsqueda.

3.- Método según la reivindicación 1 o 2, caracterizado porque las etapas de detección (E1) de dicho motivo de búsqueda (7) y de determinación (E2) de dicho motivo de salida (25) se realizan mediante una sucesión de operaciones que presenta un primer conjunto de reglas que permiten definir al menos un modo de desplazamiento para desplazar la ventana (19) en dicha secuencia de datos inicial (9) para detectar dicho al menos un motivo de búsqueda (7).

4.- Método según la reivindicación 3 caracterizado porque la sucesión de operaciones presenta, además, un segundo conjunto de reglas que determinan las condiciones de parada del desplazamiento de dicha ventana (19) en dicha secuencia de datos inicial (9).

5.- Método según la reivindicación 4, caracterizado porque al menos una de las reglas de dicho segundo conjunto de reglas genera una actualización del motivo de búsqueda y/o del motivo de salida, en función del desplazamiento y/o del contenido de dicha ventana.

6.- Método según una cualquiera de las reivindicaciones 3 y 4, caracterizado porque la sucesión de operaciones se repite hasta que se cumpla una condición previamente determinada.

7.- Método según una cualquiera de las reivindicaciones 3 y 4, caracterizado porque la sucesión de operaciones se modifica después de cada ejecución.

8.- Método según una cualquiera de las reivindicaciones 3 y 4, caracterizado porque la sucesión de operaciones permanece invariable después de cada ejecución.

9.- Método según una cualquiera de las reivindicaciones 1 a 8, caracterizado porque cada bit de dicha secuencia de datos pseudoaleatoria está combinado con un bit correspondiente de una secuencia de datos de un mensaje a cifrar mediante una adición de módulo 2 para formar una secuencia de datos cifrada.

10.- Dispositivo de codificación (39) que comprende un generador de una secuencia de datos pseudoaleatoria (3), estando dicho dispositivo de codificación adaptado para realizar un cifrado a flote utilizando la secuencia de datos pseudoaleatoria generada como secuencia cifradora, comprendiendo dicho generador un medio inicial (11) para generar una secuencia de datos inicial de N bits, que presenta un registro de desplazamiento con retroacción lineal y un medio de búsqueda (5) para buscar al menos un motivo de búsqueda (7) de un bit dentro de la secuencia de datos inicial (9) de N bits, desplazando una ventana de magnitud de un bit de un medio de detección del medio de búsqueda en dicha secuencia de datos inicial, situándose dicha ventana en una posición inicial determinada, presentado dicho medio de búsqueda (5), además, un medio de determinación (15) y un medio de repetición (17) y siendo de tal modo que:

- el medio de determinación (15) es capaz de poner el bit de la ventana en un motivo de búsqueda;

- el medio de detección (13) es capaz de detectar el motivo de búsqueda (7) en dicha secuencia de datos inicial (9) desplazando dicha ventana en dicha secuencia de datos inicial;

- el medio de determinación (15) es capaz determinar un motivo de salida (25) de un bit de magnitud según una operación que depende del desarrollo de la detección de dicho al menos un motivo de búsqueda (7), estando dicho motivo de salida determinado:

● según una primera ley, si la ventana se desplaza, una sola vez, antes de detectar dicho al menos un motivo de búsqueda en la secuencia de datos inicial, atribuyendo dicha primera ley un valor denominado de salida al motivo de salida y

● según una segunda ley, si no lo es, atribuyendo dicha segunda ley al motivo de salida el resultado de la adición del módulo entre el valor denominado de salida y el valor 1;

- el medio de detección es capaz de desplazar la ventana en un bit, desde el bit actual al bit siguiente y

- el medio de repetición (17) es capaz de generar la secuencia de datos pseudoaleatoria (3) mediante la concatenación de los motivos de salida (25).

11.- Dispositivo de codificación según la reivindicación 10, caracterizado porque el valor denominado de salida es igual:

- a un valor determinado o

- al resultado de la adición del módulo dos entre un valor determinado y el motivo de búsqueda.

12.- Dispositivo de codificación según la reivindicación 10 o 11, caracterizado por el medio de detección (13) presenta un primer medio de control (21) para controlar el desplazamiento de dicha ventana en dicha secuencia de datos inicial.

13.- Dispositivo de codificación según la reivindicación 12, caracterizado porque el medio de determinación (15) presenta un segundo medio de control (27) para actualizar el denominado motivo de búsqueda y/o el denominado motivo de salida.

14.- Dispositivo de codificación (39), según una cualquiera de las reivindicaciones 10 a 13 que presenta, además, una puerta lógica O exclusiva (43).

15.- Sistema asegurado que presenta al menos dos entidades (33a, 33b) caracterizado porque cada una de dichas al menos dos entidades (33a, 33b) presenta un dispositivo de codificación (39a, 39b), según la reivindicación 14.

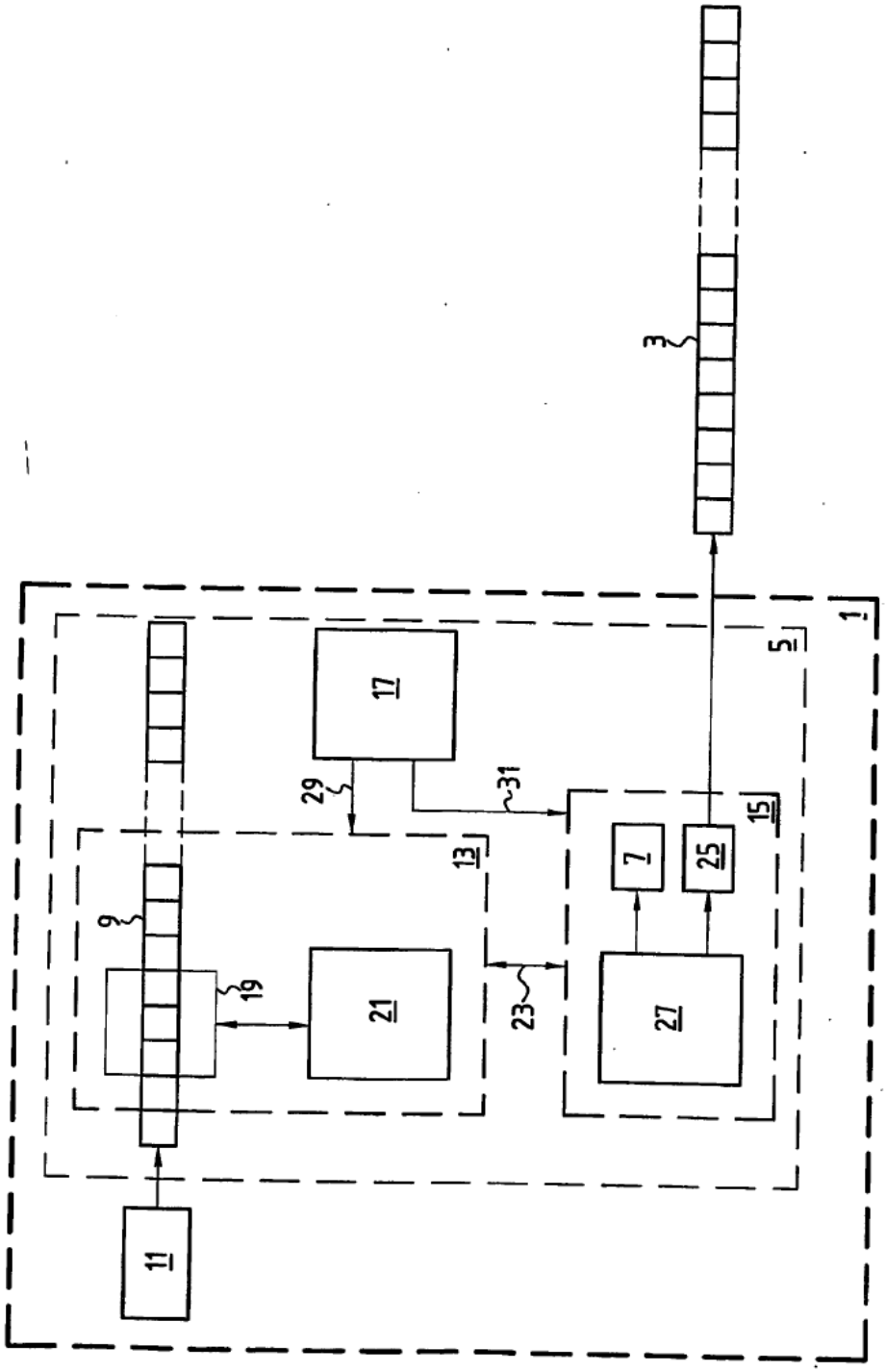

FIG.1

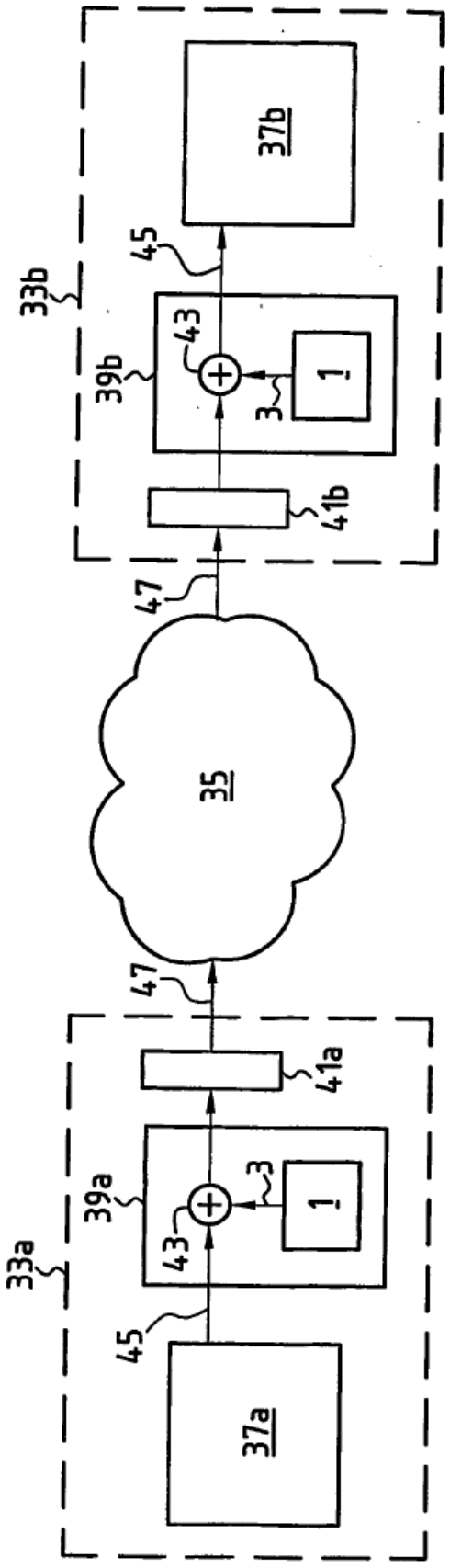

FIG.2

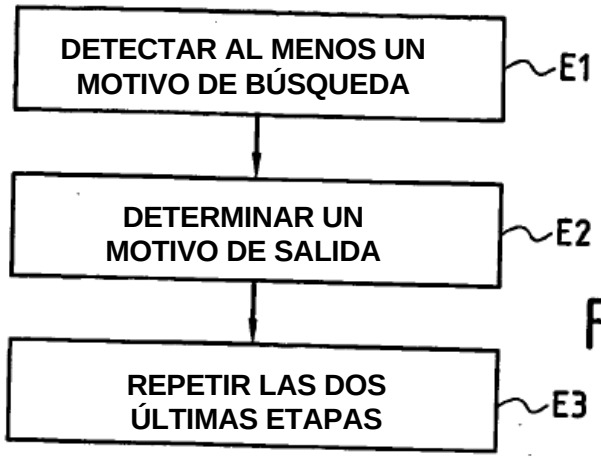
DETECTAR AL MENOS UN MOTIVO DE BÚSQUEDA
E1
DETERMINAR UN MOTIVO DE SALIDA
E2
REPETIR LAS DOS ÚLTIMAS ETAPAS
E3

FIG.3

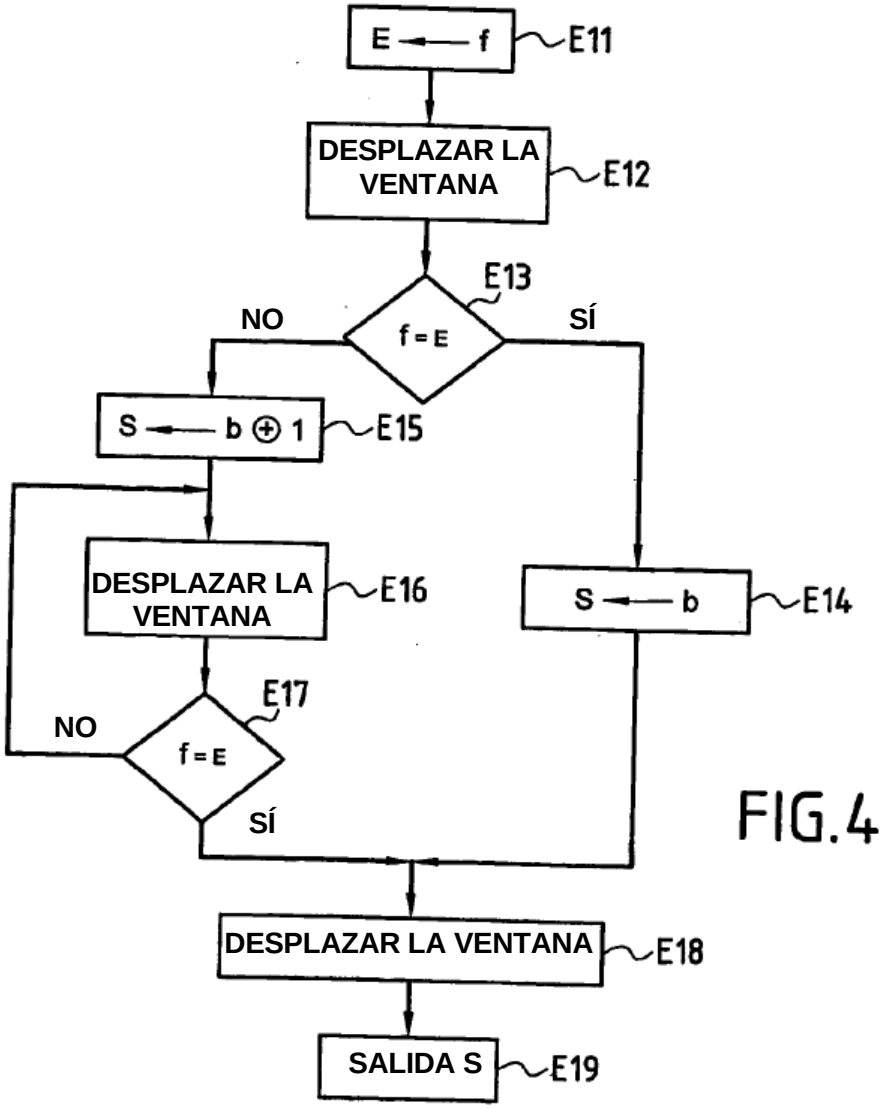
E ← f
E11
DESPLAZAR LA VENTANA
E12
E13
f = E
NO
SÍ
S ← b ⊕ 1
E15
DESPLAZAR LA VENTANA
E16
S ← b
E14
E17
f = E
NO
SÍ
DESPLAZAR LA VENTANA
E18
SALIDA S
E19

FIG.4

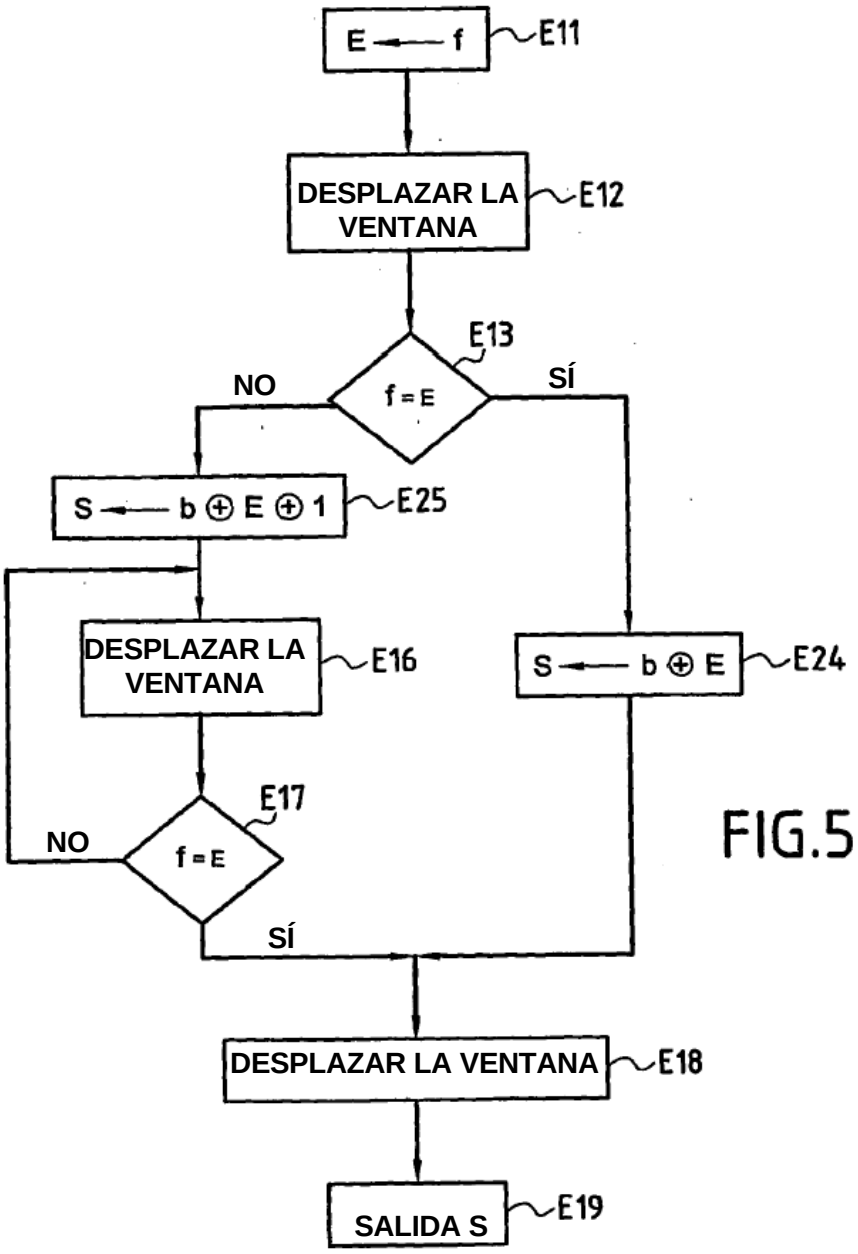

FIG.5

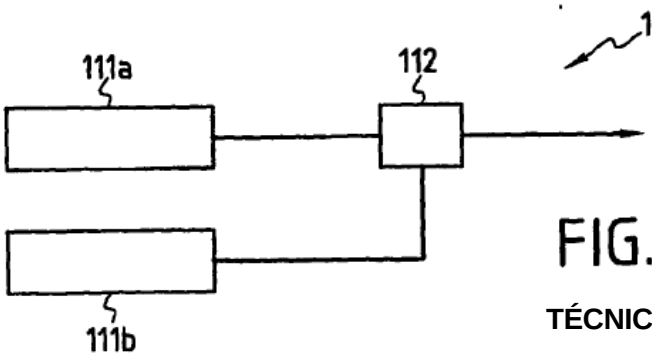

FIG. 6

TÉCNICA ANTERIOR