(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 553**

(51) Int. CI.:
H04L 9/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **99907986 .6**
(96) Fecha de presentación: **09.02.1999**
(97) Número de publicación de la solicitud: **1060591**
(97) Fecha de publicación de la solicitud: **20.12.2000**

(54) Título: **Generador de secuencias pseudo-aleatorias y método asociado**

(30) Prioridad:
06.03.1998 US 36390

(45) Fecha de publicación de la mención BOPI:
28.03.2012

(45) Fecha de la publicación del folleto de la patente:
28.03.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
SMEETS, Bernhard, Jan, Marie

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Generador de secuencias pseudo-aleatorias y método asociado

La presente invención se refiere en general a la generación de secuencias de números pseudo-aleatorios usados, por ejemplo, en los procedimientos de cifrado. Más concretamente, la presente invención se refiere a un generador de secuencias de números pseudo-aleatorios, y a un método asociado, por el cual generar una secuencia de números pseudo-aleatorios que corresponde a una secuencia generada por un polinomio de rotación seleccionado.

Los elementos de memoria orientados a palabras se usan para almacenar palabras que forman la secuencia de números pseudo-aleatorios. Los tamaños de las palabras de memoria se seleccionan de manera que los tamaños de las partes de la secuencia generados por el generador de rotación durante iteraciones sucesivas de operaciones se pueden aumentar rápidamente, según se desea, para facilitar por ello la generación de la misma secuencia de números pseudo-aleatorios en tasas aumentadas, correspondiente a construcciones de generadores de rotación compatibles, alternativos.

La secuencia de números pseudo-aleatorios generada a través del funcionamiento de una realización de la presente invención se utiliza ventajosamente como parte de un sistema para cifrar datos a ser comunicados sobre un enlace de radio, tal como un enlace de radio formado entre un terminal móvil y una estación base de un sistema de comunicación celular. La secuencia de números pseudo-aleatorios generada a través del funcionamiento de una realización de la presente invención se utiliza también ventajosamente en comunicaciones de espectro expandido (por ejemplo, Acceso Múltiple por División de Código), en sistemas fluctuantes automatizados, en métodos de comprensión de señal de voz, y en sistemas de radar.

Antecedentes de la invención

Un sistema de comunicación es operable para comunicar información entre una estación de envío y una estación de recepción por medio de un canal de comunicación. En un sistema de comunicación cableado, el canal de comunicación está formado de una conexión fija entre las estaciones de envío y de recepción. Y, en un sistema de radiocomunicación, el canal de comunicación forma una parte del espectro de frecuencia electromagnético. Debido a que no se requiere una conexión física para formar el canal de comunicación entre las estaciones de envío y de recepción de un sistema de radiocomunicación, las comunicaciones son posibles cuando una conexión fija entre las estaciones de envío y de recepción sería poco práctica.

Un sistema de comunicación digital es un sistema de comunicación en el que la información a ser comunicada por una estación de envío a una estación de recepción está digitalizada. Un sistema de comunicación digital se puede implementar tanto en un sistema de comunicación cableado como en un sistema de comunicación radio. Un sistema de comunicación digital permite la utilización más eficiente del canal de comunicación que se extiende entre las estaciones de envío y de recepción, permitiendo por ello que la capacidad de comunicación del sistema de comunicación sea aumentada sobre aquélla de un sistema de comunicación analógico, convencional.

Las comunicaciones entre las estaciones de envío y de recepción algunas veces se desea que sean privadas en naturaleza. Es decir, las partes que envían y que reciben las señales de comunicación pretenden solamente que las partes de envío y de recepción sean capaces de acceder al contenido de la información de las señales de comunicación. Particularmente cuando el canal de comunicación es un canal de comunicación radio de un sistema de comunicación radio, la privacidad de las comunicaciones entre las estaciones de envío y de recepción llega a ser problemática. Como un canal de radio es inherentemente público en naturaleza, se puede detectar una señal de comunicación transmitida en el canal de comunicación de radio por cualquier estación de recepción, dentro del alcance de la señal de comunicación, y sintonizar al canal de radio. Una parte no autorizada, por ejemplo, es capaz de sintonizar un receptor de radio a la frecuencia del canal de radio en la que se transmite la señal de comunicación, para recibir por ello la señal de comunicación. Análogos problemas de seguridad también son motivo de preocupación en los sistemas de comunicación cableados en el caso de que una parte no autorizada consiga acceso al canal de comunicación cableado.

Una manera mediante la cual mejorar la seguridad de las comunicaciones en un sistema de comunicación es cifrar la información que forma una señal de comunicación en forma cifrada. Si solamente las partes autorizadas son capaces de descifrar la señal de comunicación cifrada, una parte no autorizada es incapaz de discernir el contenido de información de la señal de comunicación transmitida en el canal de comunicación. Por ello, la privacidad de las comunicaciones se asegura mejor.

Una señal de información digital es particularmente susceptible de un proceso de cifrado. Una señal de información digital está formada de secuencias de bits, y cada bit, si se desea, de la señal de información se puede codificar en forma cifrada en la estación de envío antes de su transmisión en el canal de comunicación. Una parte no autorizada, sin conocimiento de la manera por la que la señal de información se cifra es incapaz de descifrar una señal de recepción para recuperar el contenido de información de la señal transmitida. Solamente una estación de recepción capaz de descifrar la señal cifrada es capaz de recuperar el contenido de información de la señal de recepción.

Se usan varias maneras mediante las cuales cifrar la señal de información digital. Un esquema de cifrado típico, tal

como aquél usado en comunicaciones celulares, utiliza un proceso de cifrado por el cual los bit digitalizados de una señal de información se combinan con los bit de una secuencia pseudo-aleatoria generada por un generador de secuencias pseudo-aleatorias. El generador de las secuencias pseudo-aleatorias es operable en conjunto con una clave secreta que, en una técnica de cifrado simétrico, se conoce en la estación de envío y en una estación de recepción autorizada. La clave secreta se usa en la estación de recepción autorizada para descifrar la señal cifrada recibida en ese lugar, para recuperar por ello el contenido de información de la señal transmitida.

Las secuencias de números pseudo-aleatorios se derivan algunas veces mediante el cálculo de un polinomio de rotación. Las construcciones, si están implementadas en componentes físicos y componentes lógicos, que forman las secuencias de números pseudo-aleatorios de esta manera se conocen algunas veces como generadores de rotación. Los bit de salida generados por un generador de rotación forman las secuencias de números pseudo-aleatorios que se usan, *entre otras cosas*, para cifrar una señal de información. Un generador de rotación se refiere directamente a un polinomio primario, seleccionado sobre algún campo finito GF(q). Cuando q=2, el campo finito GF(2) se conoce como el caso binario y es de importancia particularmente en comunicaciones digitales. El número de polinomios primarios desde el cual un generador de rotación se puede derivar es limitado debido a muchas restricciones situadas en el polinomio. Especialmente en el caso binario cuando se requiere el polinomio para exhibir, para minimizar las operaciones de procesamiento necesarias para generar las salidas de allí, solamente unos pocos coeficientes distintos de cero, el número de polinomios adecuados que se pueden usar para formar un polinomio de rotación es limitado. El número de coeficientes distintos de cero de un polinomio se conoce como el peso del polinomio.

Existen tablas que enumeran polinomios primarios, tales como, para el caso binario de GF(2), los polinomios primarios con treo o cinco coeficientes distintos de cero y con grados de hasta cinco mil.

La aleatoriedad de las salidas, algunas veces conocidas aquí dentro como “n-tuplas”, generadas por un polinomio de rotación binario de peso=3 generalmente es pobre, de manera que para aumentar la aleatoriedad de las salidas, se requiere un polinomio de peso elevado. Pero, tal aleatoriedad mejorada sucede a costa del aumento de los requerimientos de procesamiento. Las tablas existentes no siempre se pueden usar para seleccionar un polinomio de rotación adecuado desde el cual derivar una secuencia de números pseudo-aleatorios ya que tales tablas existentes no muestran necesariamente todos los polinomios primarios con un número de coeficientes distintos de cero, por ejemplo, tres o cinco, seleccionados. Particularmente cuando se usan las secuencias de números pseudo-aleatorios para un proceso de cifrado, el conocimiento de los polinomios de rotación de un grado seleccionado sobre el campo finito GF(2) es valioso. No están disponibles métodos por los cuales derivar tal conocimiento. En su lugar, convencionalmente, se realiza un proceso de búsqueda, que incluye una prueba de primitivismo, tal como la prueba de Knuth Allanen.

Las láminas tomadas de un generador de rotación convencional son determinativas del tamaño de bits de las salidas, es decir, las n-tuplas, formadas por el generador. Como las capacidades de procesamiento mejoran con las generaciones sucesivas de los dispositivos de procesamiento operables a velocidades de procesamiento aumentadas, los generadores de rotación convencionales que tienen mayores números de láminas llegan a ser cada vez más prácticos. Un generador de rotación que tiene números de láminas aumentados es capaz de generar salidas de tamaño de bits más grande. Y, de ahí, que una secuencia de números pseudo-aleatorios se pueda generar más rápidamente.

Cuando una configuración del generador de rotación es compatible con un generador de rotación de otra configuración, la misma secuencia de números pseudo-aleatorios se genera por los generadores de cada configuración. Tal compatibilidad se requiere generalmente de manera que el aparato y los procesos que utilizan los generadores de rotación de las distintas configuraciones sean todos capaces de funcionar para producir los mismos resultados.

No obstante, no hay manera existente por la cual simplemente determinar la compatibilidad de las distintas configuraciones de los generadores de rotación. Convencionalmente, la compatibilidad entre configuraciones separadas se puede realizar solamente asignando un estado inicial de una configuración a aquélla de otra configuración. Pero tal asignación requiere que sea realizado un número significativo de operaciones. Los polinomios de rotación especiales, no obstante, permiten una transformación muy simple entre las configuraciones de los valores generados por un polinomio de rotación.

Además sería ventajoso proporcionar un generador de rotación de construcción simplificada y capaz de generar las secuencias de números pseudo-aleatorios correspondientes a un polinomio de rotación seleccionado pero capaz de conversión simple a las configuraciones alternativas, según se desee.

La publicación “Generadores de Secuencias de PN de rotación”, Actas del IEEE de Técnicas de Ordenadores E.y Digitales, vol. 136, nº 5, Parte E, 1 de septiembre de 1989 (1-09-1989), Smeets B J M y otros describe de manera general los generadores de rotación como un generador de secuencia de alta velocidad capaz de producir bloques de una serie de símbolos consecutivos en paralelo y que se pueden construir los polinomios de rotación para diversas secuencias de ruido pseudo-aleatorias distintas.

Las publicaciones de patentes FR 2721414 A 1 y WO 95/34971 revelan un generador de código cuasi-aleatorio en el que se usan los bits para sembrar la producción de una secuencia de autentificación en una tarjeta para ser validada. Un centro de gestión emite una palabra aleatoria que se almacena en una memoria (GS) del generador de código. La palabra entonces se codifica por el microprocesador para ser usada como una semilla para una secuencia de autentificación. Los bits de registro (SS, RI, AI) se dibujan aleatoriamente desde una memoria de acceso aleatorio base (MB) como una función de una parte de la palabra aleatoria. Los operadores Booleanos se usan para las operaciones que se llevan a cabo en los contenidos de algunos de los bits dibujados. Los resultados de estas operaciones se usan para llevar a cabo una renovación cuasi-aleatoria de los contenidos de los registros (SS, RI, AI). El contenido de ciertas partes del segundo registro (RI) se recupera y proporciona las direcciones de bit a una memoria fuente (MS) que contiene una clave de 1024 bits. Las operaciones binarias entonces se llevan a cabo en los bits extraídos y las partes del tercer registro (AI) proporcionando por ello los bits que forman la secuencia de autentificación.

Es a la luz de esta información de antecedentes relacionada con la generación de las secuencias de números pseudo-aleatorios que las mejoras significativas de la presente invención han evolucionado.

Resumen de la invención

La presente invención, por consiguiente, además proporciona ventajosamente un generador de rotación de construcción simplificada y capaz de generar las secuencias de números pseudo-aleatorios que corresponden a un polinomio de rotación seleccionado pero capaz de la conversión simple a las configuraciones alternativas, según se desee.

Las configuraciones de generadores de rotación se identifican las cuales, cuando se inician para ser de los estados iniciales seleccionados, generan n-tuplas que forman la misma secuencia de números pseudo-aleatorios. Las configuraciones identificadas tiene relaciones simples entre sí; es decir, las configuraciones se identifican mediante el cual la mera copia de los valores de estado iniciales en una relación seleccionada provoca el funcionamiento de las distintas configuraciones que generan las secuencias de números pseudo-aleatorios. Tal copia tiene una complejidad lineal en la dimensión de un espacio de estado, es decir, el grado del polinomio de generación, y no una complejidad cuadrática, convencionalmente requerida para asignar un estado inicial a un equivalente distinto.

En una implementación, las secuencias de números pseudo-aleatorios generadas por un generador de rotación de una realización de la presente invención se usan como un subcomponente para cifrar la información a ser transmitida por una estación de envío a una estación de recepción. En una implementación ejemplar, el sistema de comunicación forma un sistema de comunicación celular, y la información a ser comunicada entre un terminal móvil y la infraestructura de red del sistema de comunicación celular se cifra a través del uso de un número pseudo-aleatorio generado por el generador de rotación. El cifrado de una señal recibida, cifrada también se realiza análogamente con la utilización de la secuencia de números pseudo-aleatorios generada por un generador de rotación, para descifrar por ello la señal cifrada.

En otro aspecto de la presente invención, se proporciona un método eficiente por el cual generar eficientemente los bloques consecutivos de la secuencia de ruido pseudo-aleatoria en secuencias de máxima longitud y secuencias de larga duración particulares. Debido a que se utiliza una memoria orientada a palabras mediante la cual formar las secuencias de números pseudo-aleatorios, tales secuencias se generan rápidamente, sin requerimientos de cálculo significativos. Y, a través de la selección adecuada del tamaño de la palabra de memoria, se realizan las configuraciones alternativas de los generadores de rotación para permitir compatibilidad hacia arriba y retrocompatibilidad de las secuencias de números pseudo-aleatorios

En estos y otros aspectos, un método, y el aparato asociado, genera una secuencia de números pseudo-aleatorios. Un conjunto de elementos de memoria se forma en el cual cada elemento de memoria del conjunto almacena una palabra de memoria de un plano de palabra seleccionado allí dentro. Cada uno de los elementos de memoria se inicia con los valores de estado iniciales. Los valores de estado iniciales con los que se inicia cada uno de los elementos de memoria forman las palabras de memoria almacenadas allí dentro. Al menos una de las palabras de memoria almacenadas en al menos uno de los elementos de memoria se selecciona para formar una secuencia de salida. La secuencia de salida forma una parte de la secuencia de ruido pseudo-aleatoria. Al menos una nueva palabra de memoria se selecciona para ser almacenada en al menos uno de los elementos de memoria del conjunto de elementos de memoria. La nueva palabra de memoria se forma de la combinación seleccionada de las palabras de memoria almacenadas en los elementos de memoria del conjunto de elementos de memoria. La al menos una nueva palabra de memoria corresponde en longitud con la longitud de las palabras de memoria seleccionadas para formar la secuencia de salida.

Una apreciación más completa de la presente invención y del alcance de la misma se puede obtener a partir de los dibujos anexos que se resumen brevemente más adelante, la siguiente descripción detallada de las realizaciones preferentes en este momento de la invención, y las reivindicaciones adjuntas.

Breve descripción de los dibujos

La FIGURA 1 ilustra un diagrama de bloques funcional de un generador de rotación de una primera configuración,

operable para generar tres-tuplas como salidas.

La FIGURA 2 ilustra una tabla que enumera los valores en los elementos de retardo del generador de rotación mostrados en la Figura 1 y las salidas tres-tuplas formadas en iteraciones sucesivas del funcionamiento del generador de rotación.

La FIGURA 3 ilustra un diagrama de bloques funcional de un generador de rotación de una segunda configuración, operable para generar seis-tuplas como salidas.

La FIGURA 4 ilustra una tabla que enumera los valores en los elementos de retardo del generador de rotación mostrados en la Figura 3 y las salidas seis-tuplas formadas en iteraciones sucesivas del funcionamiento del generador de rotación.

La FIGURA 5 ilustra los valores de estado iniciales para las configuraciones de los generadores de rotación mostrados en las Figuras 1 y 3 y las asignaciones entre medias por las cuales ambas configuraciones pueden ser causadas para generar las secuencias de salida de números pseudo-aleatorios.

La FIGURA 6 ilustra las fin-tuplas de salida determinadas de dos maneras separadas.

La FIGURA 7 ilustra una tabla que muestra los polinomios de rotación de hasta el orden ciento veintisieteavo y los valores factibles de v calculados durante el funcionamiento de la realización de la presente invención.

La FIGURA 8 ilustra un diagrama de bloques funcional de un generador de rotación de una realización de la presente invención.

La FIGURA 9 ilustra la asignación de las palabras de memoria durante el funcionamiento del generador de rotación mostrado en la Figura 8.

La FIGURA 11 ilustra la manera por la que la nueva palabra de entrada se forma durante el funcionamiento del generador de rotación mostrado en la Figura 8.

La FIGURA 12 ilustra un diagrama de bloques funcional de un generador de rotación de otra realización de la presente invención.

La FIGURA 13 ilustra un diagrama de bloques funcional de otro generador de rotación de otra realización de la presente invención.

Descripción detallada

Con referencia primero a la Figura 1, un generador de rotación ejemplar, mostrado de manera general en 10, se muestra para ser formado de una pluralidad de elementos de retardo 12 y segregado en conjuntos de láminas v. Aquí, cada lámina de una longitud de lámina L_i, y cada lámina v incluye un bucle de realimentación 14 acoplado a los terminales de entrada de los elementos de suma 16. La de más a la derecha (según muestra la lámina v) se acopla además en un bucle de realimentación 18 a la lámina de más a la izquierda v.

Las derivaciones 22 se toman a partir de cada una de las láminas v y se proporcionan a un elemento de permutación que realiza la permutación, aquí la permutación de identidad, en las secuencias proporcionadas por las derivaciones 22. Las secuencias de salida formadas por el elemento de permutación 24 forman las fin-tuplas de salida generadas en las líneas 26, aquí representadas por S_{3j}, S_{3j+1}, S_{3j+2}.

La longitud L de cada lámina v se indica por L_i en donde i=0, 1, …, v-1. El conjunto de longitudes L_0 a L_{v-1} se determina por una fórmula conocida. De particular interés es cuando $L=L_0+L_1+\ldots+L_{v-1}$ satisface las ecuaciones:

$L=1 \bmod v$ (es decir el resto de L dividido por v es 1) o

$L=(v-1) \bmod v$.

De acuerdo con la primera ecuación señalada anteriormente, la permutación realizada por el elemento de permutación 24 se puede elegir que sea la permutación identidad, es decir, 0, 1, …, v-1 asigna a 0, 1, …, v-1. En tal caso, las longitudes L_i se cubren por la ecuación:

$L_0= \ldots =L_{v-2}=(L-1)/v$, $L_{v-1}=1+(L-1)/v$.

Las derivaciones de salida 22 se toman después de cada elemento de retardo (L-1)v-ésimo 12.

Con respecto a la segunda ecuación señalada anteriormente, la permutación se puede elegir que sea el “orden inverso”, es decir, 0, 1, …, v-1 asigna a v-1, v-2, …, 1, 0. Las longitudes L, en tal caso, se definen por la siguiente ecuación:

$L_0= \ldots =L_{v-2}=(L+1)/v$, $L_{v-1}=1+(L+1)/v$.

Las derivaciones de salida 22 tomadas a partir de cada lámina v se sitúan después de cada elemento de retardo p-ésimo 12 en donde p es un número que depende de el valor de v compatible más largo posible. Dos valores v y v' son compatibles si existe una simple asignación entre el estado inicial del generador de rotación 10 construido con v y el estado inicial del generado de rotación 10 construido con v' de manera que ambos generadores de rotación 10 generan la misma secuencia de salida. Es decir, la salida generada por el generador de rotación 10 satisface la ecuación:

$$s_j = f_1 s_{j-1} + f_2 s_{j-2} + \ldots + f_L s_{(j-L)}$$

en donde j=n, n+1, … para algún número n en donde el signo + es la suma en el campo finito GF(2) y $f(x)=1-f_1x^L - \ldots - f_{L-1}x^{L-1} - f_L x^L$.

La Figura 2 ilustra una tabla que enumera los valores en los elementos de retardo 12 en iteraciones sucesivas del funcionamiento del generador de rotación 10 en intervalos de nueve veces j=0-8. Las columnas de más a la derecha (según se muestran) de la tabla 28 enumeran las salidas generadas por el generador de rotación 10 en las líneas 22 y, debido a la permutación identidad realizada por el elemento de permutación 24, también en las líneas 26.

La Figura 3 ilustra un generador de rotación, también formado de grupos de láminas v, cada una que tiene elementos de retardo 12, bucles de realimentación 14, y elementos de suma 16. Un bucle de realimentación 18 también se forma entre la lámina v de más a la derecha (como se muestra) y la lámina v de más a la izquierda (como se muestra). Las derivaciones 22 de nuevo se toman fuera de las láminas v. Aquí, como el generador de rotación 10 incluye seis láminas v, el generador 10 incluye seis derivaciones 22. Un elemento de permutación 24 que realiza una permutación identidad y las salidas 26 de allí se muestran de nuevo.

La Figura 4 ilustra una tabla 34 que contiene un listado análogo al listado de la tabla 28 pero que aquí ilustra los valores de estado de los elementos de retardo 12 del generador de rotación de seis láminas mostrado en la Figura 3. Las columnas de más a la derecha (como se muestra) indican los valores derivados por las derivaciones 22 y también generados en las líneas 26. La comparación de las salidas, cuando se secuencian juntas, de los generadores de rotación 10 mostradas en las Figuras 1 y 3 y tabuladas en las tablas 28 y 34 indican su concepción común.

Cada lámina v del generador de rotación 10 mostrada en la Figura 1 incluye las conexiones de realimentación idénticas. Análogamente, cada lámina v del generador de rotación 10 mostrada en la Figura 3 también incluye conexiones de realimentación idénticas que se derivan a partir del polinomio de rotación f(x). El polinomio de rotación f(x) se puede volver a escribir en términos de una primera parte del polinomio y una segunda parte del polinomio, es decir:

$f(x)=1-f_1x^1 - \ldots - f_{L-1}x^{L-1} - x^L$, f_i es un elemento de GF(q).

$=b(x^v) - x^L$.

Cuando el polinomio f(x) se vuelve a caracterizar de esta manera, la realimentación en las láminas v se especifica por el polinomio b(x).

En el caso binario, es decir, cuando el campo finito es GF(2), f(x) se puede representar como:

$$f(x)=1+f_1x^1 + \ldots + f_{L-1}x^{L-1} + x^L .$$

Con respecto a un polinomio de rotación del grado séptimo, es decir:

$$f(x)=x^7 + x^6 + 1,$$

y del cual los generadores de rotación mostrados en las Figuras 1 y 3 implementan, el polinomio de rotación se puede volver a escribir como sigue:

$$f(x)=b(x^3) + x^7$$

donde $b(x)=1+x^2$. F(x) también se puede volver a escribir de otras maneras, de nuevo formada de dos partes de polinomio separadas tales como, por ejemplo:

$$f(x)=b(x^6) + x^7$$

donde b(x)=1+x y v=6.

A través de la selección adecuada de los valores de estado inicial de cada uno de los elementos de retardo 12 de los generadores de rotación mostrados en las Figuras 1 y 3, las configuraciones separadas de los generadores de rotación se pueden provocar para generar las mismas secuencias de números pseudo-aleatorios formados de sucesivas fin-tuplas generadas en las líneas 26 de las configuraciones respectivas de los generadores 10. Cuando un polinomio de rotación del grado L permite un generador de rotación 10, operable de acuerdo al mismo, y que

tiene v1 lámina so v2 láminas y que satisfacer una de las ecuaciones anteriormente mencionadas, es decir, 1=L mod v1=L mod v2 o v-1=L mod v1=L mod v2, la asignación simple de los valores de estado iniciales permite distintas configuraciones para producir la misma secuencia de números pseudo-aleatorios.

La Figura 5 ilustra la asignación para el polinomio de rotación de séptimo orden ejemplar. La parte más alta (como se muestra) ilustra los valores de estado iniciales, indicados por las letras a, b, c, d, e, f, y x en las tres láminas, Lámina 2, Lámina 1, y Lámina 0, del generador de rotación 10 mostrado en la Figura 1. La parte más baja (como se muestra) de la Figura ilustra los valores de estado iniciales asignados en las seis láminas v, Lámina 5, Lámina 4, Lámina 3, Lámina 2, Lámina 1, y Lámina 0 del generador de rotación 10 mostrado en la Figura 3. La asignación de los valores de estado iniciales como se ilustra permite las configuraciones separadas de los generadores de rotación 10 dibujados en las Figuras 1 y 3, respectivamente, para generar la misma secuencia de salida pseudo-aleatoria.

Cuando v1-1=L mod v1, v2-1=L mod v2, las asignaciones simples para los valores compatibles de v, que forman los generadores de rotación de las distintas configuraciones, se pueden determinar por la siguiente ecuación en la que p, es decir, el elemento de retardo p-ésimo 12, es un número que depende del valor de v compatible más grande posible:

$$p=(L+1-v_{max})/v,$$

donde v_{max} es el valor más grande compatible de v para un polinomio de rotación dado.

Por ejemplo, cuando el polinomio de rotación es del grado décimo séptimo, es decir, $f(x)=x^{17} + x^{12}+ 1$, entonces v_{max} =6 y p=4.

La Figura 6 ilustra las fin-tuplas de salida para los dos casos, definidos anteriormente. En la parte de más a la izquierda (como se muestra) de la Figura, los bits que forman las derivaciones de salida en cada lámina se toman a partir de la columna indicada por p mientras que la parte de más a la derecha (como se muestra) de la Figura muestra los bits de salida tomados desde una columna diferente debido al distinto valor de la pequeña v_{max}.

La Figura 7 ilustra una tabla de polinomios de rotación hasta el grado ciento veintisieteavo que se puede usar para generar los bloques de tres-tuplas binarias. Cada tres-tupla representa un número entero de ocho valores de manera que se pueden generar hasta sesenta y tres n-tuplas por un generador de rotación operable para derivar el mismo polinomio de rotación. La tabla dibujada en la Figura 7 además ilustra los valores factibles de las láminas v que forman distintas configuraciones de los generadores de rotación capaces de generar las mismas secuencias de números pseudo-aleatorios.

La Figura 8 ilustra un generador de rotación, mostrado generalmente en 100, de una realización de la presente invención. El generador de rotación 100 es funcionalmente equivalente a los generadores de rotación 10 mostrados en las Figuras 1 y 3, pero aquí se implementa a través del uso de la memoria orientada a palabras. Aquí, está formada una pila 102 de elementos de memoria. Cada uno de los elementos de memoria 104 es de una longitud de palabra seleccionada y la pila 102 está formada de un número seleccionado, M, de elementos de memoria 104.

El valor de M se determina de acuerdo con una de las siguientes ecuaciones:

$$M = 2 + (1 – 1)/v,$$

$$M = 1 + (L + 1)/v.$$

Los contenidos de los elementos de memoria 104 se actúan selectivamente a través del funcionamiento de un dispositivo de procesamiento 106, aquí operable para ejecutar las aplicaciones aquí representadas por un iniciador 108, un selector de secuencia de salida 112, y un selector de nuevas palabras de memoria 114. El iniciador 108 es operable para iniciar los elementos de memoria con las palabras de memoria de los valores de estado iniciales. El selector de secuencia de salida 112 es operable para provocar que una palabra de memoria seleccionada sea leída para formar una secuencia de salida n-tupla. Y, los selectores de nuevas palabras de memoria operables para seleccionar una nueva palabra de memoria a ser escrita para uno seleccionado o más elementos de memoria 104 durante el funcionamiento del generador 100.

La Figura 9 ilustra la asignación de las palabras de memoria durante el funcionamiento de una realización de la invención. Una vez que los elementos de memoria se han iniciado con los valores de estado iniciales a través del funcionamiento del iniciador 108, las palabras de memoria son desplazadas iterativamente de las maneras indicadas por las flechas 118 mostradas en la Figura. Una de las palabras de memoria se lee fuera de su elemento de memoria y forma la salida fin-tupla, a través del funcionamiento del generador de secuencia de salida 112. Y, una nueva palabra de entrada, formada de una combinación seleccionada de partes de las palabras de memoria almacenadas en las seleccionadas de los elementos de memoria 104 se inserta en un elemento de memoria disponible 104 a través del funcionamiento del selector de nuevas palabras de memoria 114. Como se ilustra, los contenidos de los elementos de las palabras de memoria en los elementos de memoria 104 se asignan en sentido columna. Y, a través del funcionamiento del selector de nuevas palabras de entrada 114, se inserta una nueva palabra de memoria en un elemento de memoria disponible 104. El sucesivo desplazamiento de las palabras de

memoria, sacado de las n-tuplas seleccionadas, y la formación de nuevas palabras de entrada permite que una secuencia de números aleatorios sea formada por ello. Debido a la orientación de las palabras del generador de rotación 100, las n-tuplas de salida de múltiples números de las palabras de memoria almacenadas en múltiples series de elementos de memoria 104 se pueden sacar durante cada iteración del funcionamiento del generador 100 si se desea aumentar los números de las salidas n-tuplas.

La Figura 11 ilustra la pila 102 de los elementos de memoria 104 mostrados previamente en las Figuras 9 y 10, aquí para ilustrar la manera por la cual el selector de nuevas palabras de memoria forma los valores de una nueva palabra de memoria a ser insertada en un elemento de memoria disponible. Una vez que una palabra de memoria se saca y forma una salida n-tupla, y como se indica por las flechas 128 y 132, se toman los valores de los últimos d elementos de cada lámina. Entonces, y como se indica por la flecha 134, la fila así formada se gira cíclicamente a través de una posición. Entonces, y como se indica por la flecha 136, se forma una realimentación complementaria. Y, la palabra así formada se desplaza hacia arriba de una manera en sentido columna, como se indica por la flecha 138.

La Figura 12 indica un generador de rotación 100 de otra realización de la presente invención. Aquí, de nuevo, se forma una pila 102 de elementos de memoria 104 en la que, de nuevo, las palabras de memoria de longitud M se almacenan en los elementos de memoria. Y, de nuevo, un dispositivo de procesamiento 106 es operable para ejecutar las aplicaciones representadas por el iniciador 108, el selector de secuencias de salida 112, y el selector de nuevas palabras de memoria 114. Aquí, más que desplazar los contenidos de las palabras de memoria durante cada iteración del funcionamiento del generador 100, un nuevo puntero de la palabra de entrada, aquí representado por la flecha 148, se mueve cíclicamente en medio de las M palabras de las que está formada la pila 102. Es decir, la ubicación de la nueva palabra de entrada se vuelve a identificar cíclicamente en medio de las palabras de memoria. Cuando el consumo bajo de potencia es una meta de funcionamiento significativa, reposicionar el puntero 148 consume menos potencia que desplazar cada palabra de memoria a través de la pila 102.

La Figura 13 ilustra un generador de rotación 100 de una realización, similar a aquél mostrado en la Figura 12, pero en el que solamente se utiliza un puntero actualizado cíclicamente 148 y solamente un conjunto de desplazamientos a un punto para la posición correcta de las palabras en la memoria donde los datos van a ser leídos o almacenados.

La implementación de un generador de rotación orientado a palabras se proporciona en la cual las secuencias de números pseudo-aleatorios están simplemente formadas meramente a través de las lecturas sucesivas de las palabras de memoria seleccionadas durante sucesivas iteraciones del funcionamiento del generador.

Las descripciones previas son de los ejemplos preferentes para la implementación de la invención, y el alcance de la invención no se debería limitar necesariamente por esta descripción. El alcance de la presente invención se define por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método para la generación de una secuencia de ruido pseudo-aleatoria de los valores generados por un polinomio de rotación, dicho método que comprende los pasos de:

- formar un conjunto de elementos de memoria (102), cada elemento de memoria (104) del conjunto (102) para el almacenamiento de una palabra de una longitud de palabra seleccionada allí dentro;

- iniciar (108) cada uno de los elementos de memoria (104) formados durante dicho paso de formación con los valores de estado iniciales, los valores de estado iniciales con los que cada uno de los elementos de memoria (104) se inicia formando la palabra almacenada allí dentro; y

- seleccionar (112) al menos una de las palabras almacenadas en al menos uno de los elementos de memoria (104) para formar una secuencia de salida (Palabra de Salida), la secuencia de salida que forma una parte de la secuencia de ruido pseudo-aleatoria;

caracterizado porque

el método además comprende el paso de:

- formar al menos una nueva palabra a ser almacenada en al menos uno de los elementos de memoria (104) del conjunto de elementos de memoria (102), la nueva palabra formada de una combinación seleccionada de palabras almacenadas en los elementos de memoria del conjunto de elementos de memoria, la al menos una nueva palabra que corresponde en longitud con la longitud de las palabras de memoria seleccionadas para formar la secuencia de salida.

2. El método de la reivindicación 1, en el que el polinomio de rotación es de un grado seleccionado, el grado seleccionado que es, al menos en parte, determinativo del número de elementos de memoria (104) del conjunto de elementos de memoria (102) formado durante dicho paso de formación.

3. El método de la reivindicación 2 en el que el número de elementos de memoria del conjunto de elementos de memoria (102) además es dependiente de la longitud de la palabra seleccionada de la que está formada cada una de las palabras de memoria.

4. El método de la reivindicación 3 en el que el número de elementos de memoria que forman el conjunto de elementos de memoria (102) es directamente proporcional al grado seleccionado y es inversamente proporcional a la longitud de la palabra seleccionada de la que está formada cada una de las palabras.

5. El método de la reivindicación 2 en el que el conjunto de elementos de memoria (102) formado durante dicho paso de formación comprende un grupo contiguo lógicamente de elementos de memoria (104), que forman una pila de palabras, al menos uno de los elementos de memoria (104) de la pila de elementos de memoria seleccionados para formar un elemento de memoria de salida, y en el que la al menos una de las palabras seleccionadas durante dicho paso de selección de la al menos una de las palabras comprende la al menos una palabra almacenada en el elemento de memoria de salida.

6. El método de la reivindicación 5 en el que los sucesivos del grupo contiguo lógicamente de elementos de memoria definen las columnas y en donde dicho método comprende el paso adicional de desplazar, en una forma por columnas, las palabras a través de la pila de los elementos de memoria.

7. El método de la reivindicación 6 en el que la al menos una palabra seleccionada durante dicho paso de selección de la al menos una nueva palabra comprende una palabra de valores correspondientes a los valores de realimentación generados por el polinomio de rotación del grado seleccionado.

8. El método de la reivindicación 1 que comprende el paso adicional de asignar en al menos un puntero actualizable cíclicamente (148) a al menso los seleccionados de los elementos de memoria.

9. El método de la reivindicación 8 en el que el al menos un puntero actualizable cíclicamente (148) asignado durante dicho paso de asignación identifica el al menos un elemento de memoria en el cual se almacena al menos una de las palabras seleccionadas durante dicho paso de selección.

10. El método de la reivindicación 9 en el que el al menos un puntero actualizable cíclicamente (148) asignado durante dicho paso de asignación identifica el al menos un elemento de memoria, seleccionado durante dicho paso de selección de la al menos una nueva palabra, en el cual la al menos una nueva palabra va a ser almacenada.

11. El método de la reivindicación 2 en el que la longitud de palabra seleccionada de la que cada una de las palabras almacenadas en cada uno de los elementos de memoria formados durante dicho paso de formación se selecciona de manera que al menos un múltiplo de la longitud de palabra seleccionada forma una longitud de palabra compatible, y en el que la al menos una de las palabras seleccionadas durante dicho paso de selección comprende al menos un múltiplo de una palabra única.

12. El método de la reivindicación 1 en el que dichos pasos de selección de al menos una de las palabras para formar la secuencia de salida y seleccionar la al menos una nueva palabra se realizan iterativamente.

13. Un generador de ruido pseudo-aleatorio (100, 106) para la generación de una secuencia de ruido pseudo-aleatoria de los valores generados por un polinomio de rotación, dicho generador de la secuencia de ruido pseudo-aleatoria que comprende:

- un conjunto de elementos de memoria (102), cada elemento de memoria (104) de dicho conjunto (102) para el almacenamiento de una palabra seleccionada de una longitud de palabra seleccionada allí dentro;

- un iniciador (108) para iniciar cada uno de los elementos de memoria (104) de dicho conjunto (102) con valores de estado iniciales, los valores de estado iniciales con los que cada uno de los elementos de memoria se inicia formando la palabra almacenada allí dentro; y

- un selector de la secuencia de salida (112) para la selección de al menos una de las palabras almacenadas en al menos uno de los elementos de memoria de dicho conjunto para formar una secuencia de salida, la secuencia de salida que forma una parte de la secuencia de ruido pseudo-aleatoria;

caracterizado porque el generador de ruido pseudo-aleatorio (100, 106) además comprende

- un selector de nuevas palabras (114) para formar al menos una nueva palabra a ser almacenada en al menos uno de los elementos de memoria de dicho conjunto, la nueva palabra formada de una combinación seleccionada de palabras almacenadas en los elementos de memoria del conjunto de elementos de memoria, la al menos una nueva palabra que corresponde en longitud con las palabras de longitud seleccionadas para formar la secuencia de salida.

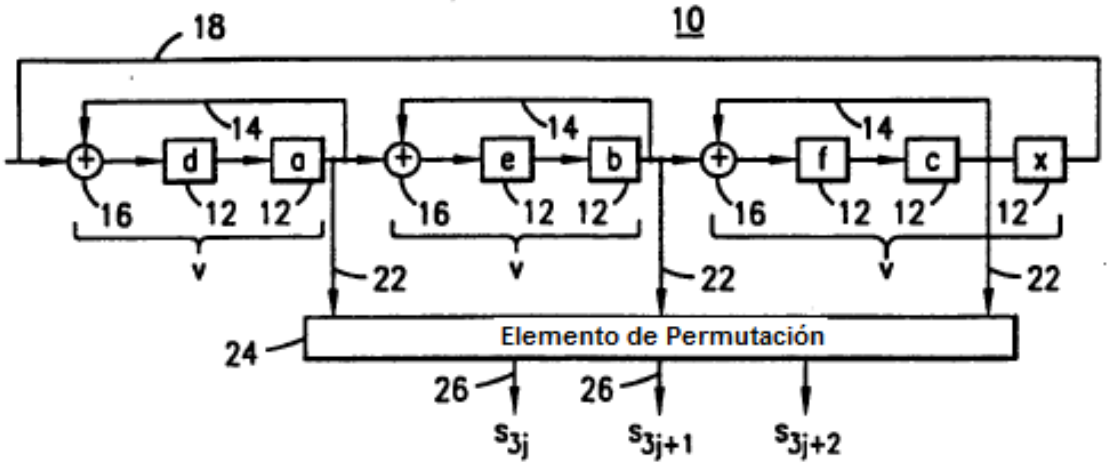

FIG. 1

28

	Lámina0	Lámina1	Lámina2	s_{3j}	s_{3j+1}	s_{3j+2}
j=0	1 0	1 0	0 1 0	0	0	1
j=1	0 1	0 1	1 0 1	1	1	0
j=2	0 0	0 0	1 1 0	0	0	1
j=3	0 0	0 0	1 1 1	0	0	1
j=4	1 0	0 0	1 1 1	0	0	1
j=5	1 1	0 0	1 1 1	1	0	1
j=6	0 1	1 0	1 1 1	1	0	1
j=7	1 0	1 1	1 1 1	0	1	1
j=8	1 1	1 1	0 1 1	1	1	1

FIG. 2

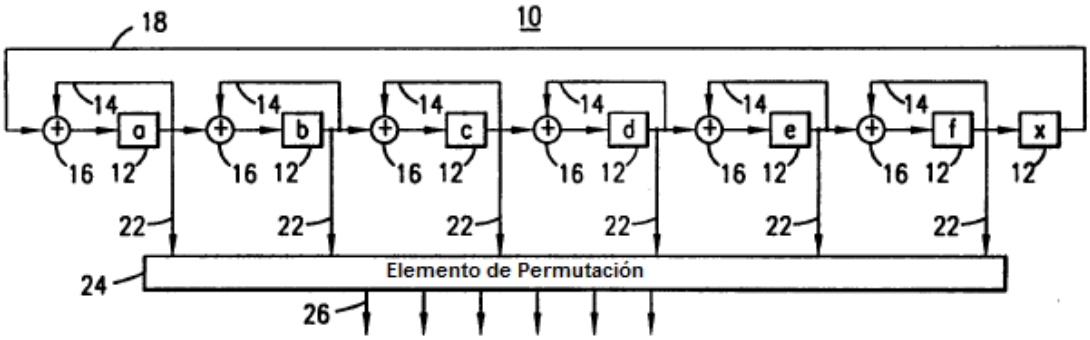
18
10
14
a
b
c
d
e
f
x
16
12
22
24
Elemento de Permutación
26

FIG. 3

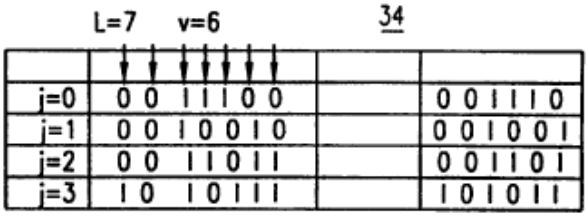
L=7
v=6
34
j=0
0 0 1 1 1 0 0
0 0 1 1 1 0
j=1
0 0 1 0 0 1 0
0 0 1 0 0 1
j=2
0 0 1 1 0 1 1
0 0 1 1 0 1
j=3
1 0 1 0 1 1 1
1 0 1 0 1 1

FIG. 4

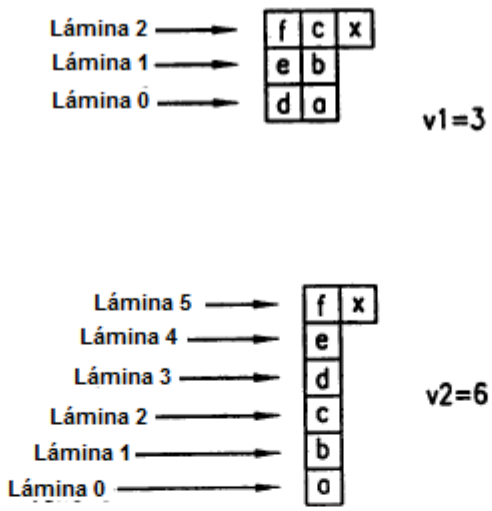
Lámina 2
Lámina 1
Lámina 0
f c x
e b
d a
v1=3
Lámina 5
Lámina 4
Lámina 3
Lámina 2
Lámina 1
Lámina 0
f x
e
d
c
b
a
v2=6

FIG. 5

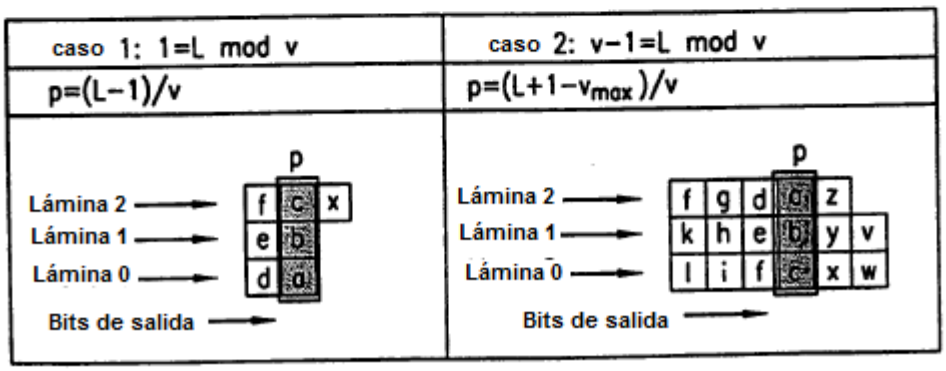
caso 1: 1=L mod v
p=(L−1)/v
p
Lámina 2
Lámina 1
Lámina 0
Bits de salida
f c x
e b
d a
caso 2: v−1=L mod v
p=(L+1−vmax)/v
p
Lámina 2
Lámina 1
Lámina 0
Bits de salida
f g d a z
k h e b y v
l i f c x w

FIG. 6

Polinomio de Rotación	valores v factibles (que son múltiples de 3) +: 1=L mod v, −: v−1=L mod v
x^7+x^6+1	3+,6+
$x^{17}+x^6+1$	3−,6−
$x^{17}+x^{12}+1$	3−6−,12
$x^{25}+x^{18}+1$	3−,6−,9,18
$x^{25}+x^{18}+1$	3+,6+,9,18
$x^{31}+x^6+1$	3+,6+
$x^{31}+x^{18}+1$	3+,6+,9,18
$x^{31}+x^{24}+1$	3+,6+,12,24
$x^{47}+x^{42}+1$	3−,6−,21,42
$x^{49}+x^{12}+1$	3+,6+,12+
$x^{55}+x^{24}+1$	3+,6+,12,24
$x^{65}+x^{18}+1$	3−,6−,9,18
$x^{71}+x^6+1$	3−,6−
$x^{71}+x^{18}+1$	3−,6−,9−,18−
$x^{71}+x^{36}+1$	3−,6−,9−,18−,36−
$x^{73}+x^{42}+1$	3+,6+,21,42
$x^{73}+x^{48}+1$	3+,6+,12+,24+,48
$x^{79}+x^{60}+1$	3+,6+,12,15,30,60
$x^{95}+x^{78}+1$	3−,6−,39,78
$x^{95}+x^{84}+1$	3−,6−,21−,42
$x^{97}+x^6+1$	3+,6+
$x^{97}+x^{12}+1$	3+,6+,12+
$x^{103}+x^{30}+1$	3+,6+,15,30
$x^{103}+x^{72}+1$	3+,6+,9,12,18,24,36,72
$x^{103}+x^{90}+1$	3+,6+,9,15,18,30,45,90
$x^{113}+x^{30}+1$	3−,6−,15,30
$x^{121}+x^{18}+1$	3+,6+,9,18
$x^{127}+x^{30}+1$	3+,6+,15,30
$x^{127}+x^{120}+1$	3+,6+,12,15,24,30,60,120
$x^{127}+x^{126}+1$	3+,6+,9+,18+,21+,42+,63+,126+

FIG. 7

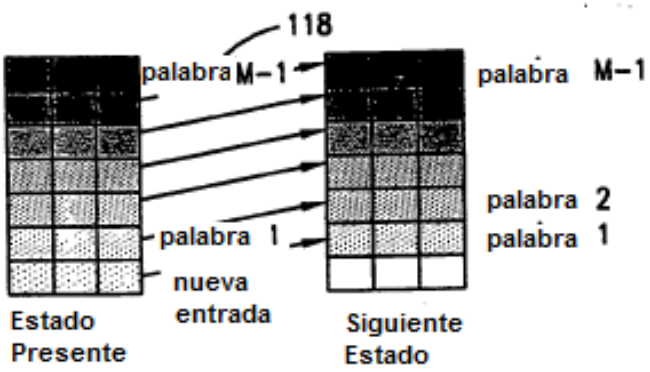
118
palabra M-1
palabra M-1
palabra 2
palabra 1
palabra 1
nueva entrada
Estado Presente
Siguiente Estado

FIG. 9

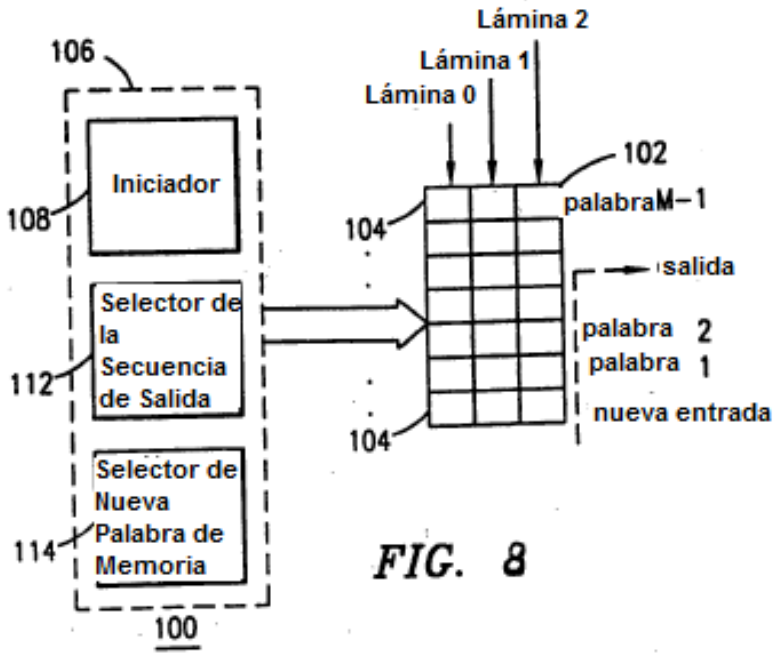
106
Iniciador
108
Selector de la Secuencia de Salida
112
Selector de Nueva Palabra de Memoria
114
100
Lámina 2
Lámina 1
Lámina 0
102
palabra M-1
104
salida
palabra 2
palabra 1
nueva entrada
104

FIG. 8

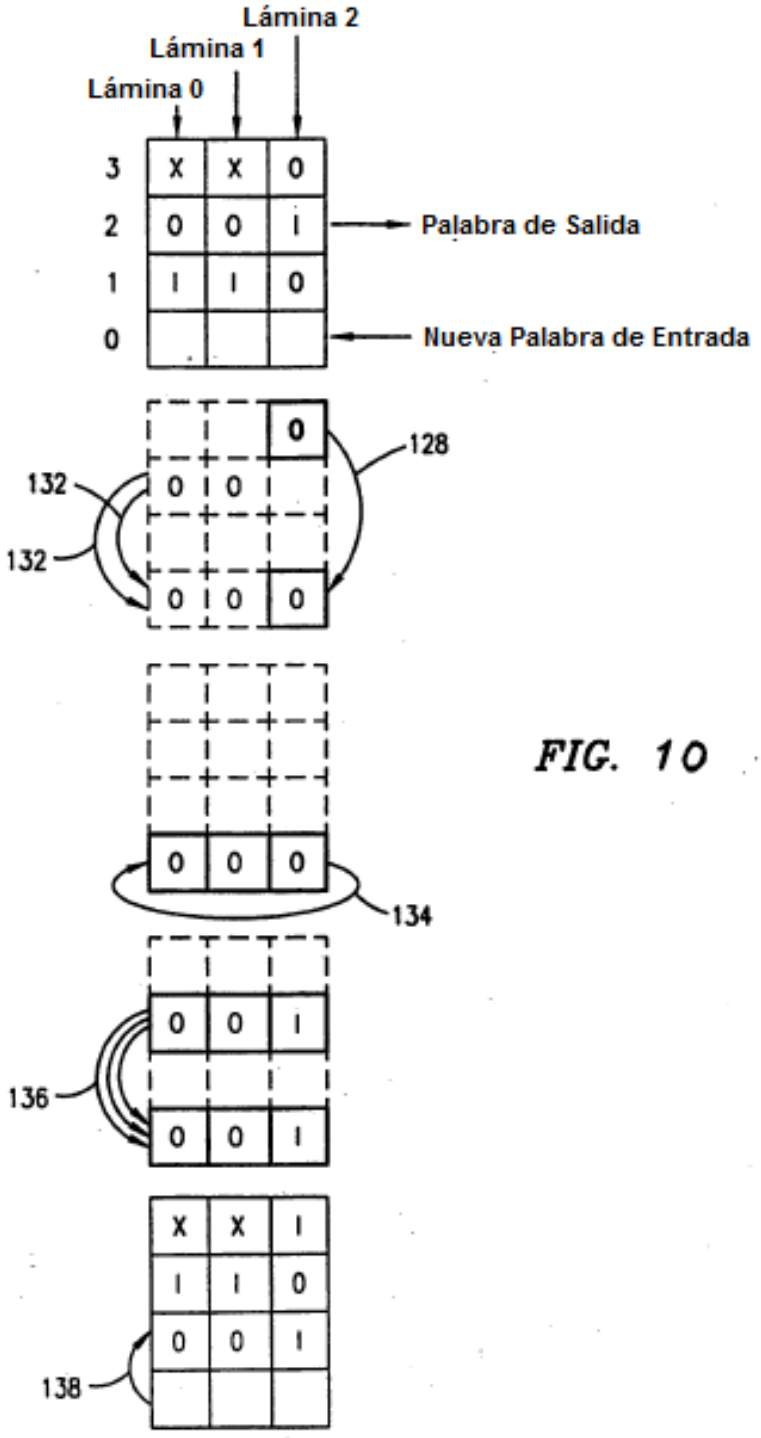
Lámina 2
Lámina 1
Lámina 0
3
2
1
0
Palabra de Salida
Nueva Palabra de Entrada
128
132
132
134
136
138

FIG. 10

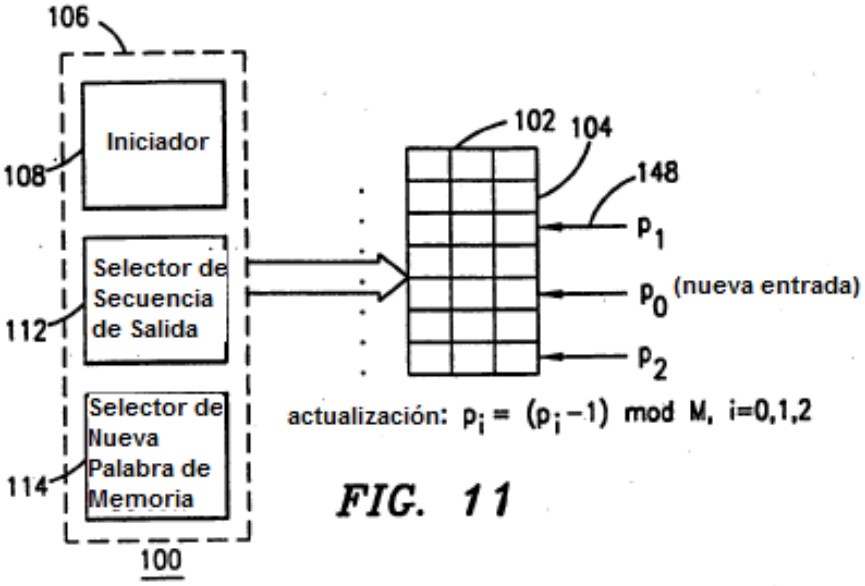
106
Iniciador
108
Selector de Secuencia de Salida
112
Selector de Nueva Palabra de Memoria
114
100
102
104
148
p_1
p_0 (nueva entrada)
p_2
actualización: $p_i = (p_i - 1) \bmod M$, i=0,1,2

FIG. 11

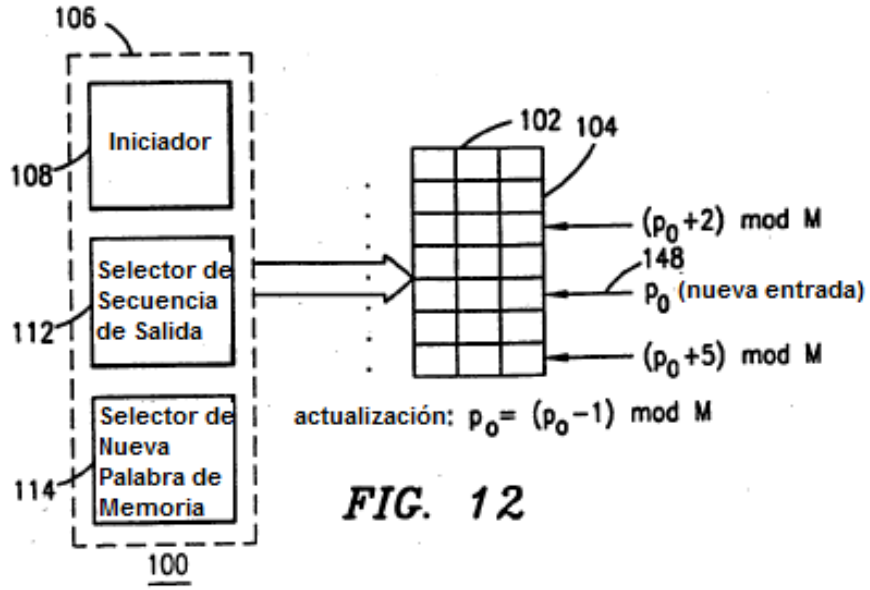
106
Iniciador
108
Selector de Secuencia de Salida
112
Selector de Nueva Palabra de Memoria
114
100
102
104
$(p_0+2) \bmod M$
148
p_0 (nueva entrada)
$(p_0+5) \bmod M$
actualización: $p_0 = (p_0 - 1) \bmod M$

FIG. 12