(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 354 136**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08776532 .7**
(96) Fecha de presentación : **26.06.2008**
(97) Número de publicación de la solicitud: **2100219**
(97) Fecha de publicación de la solicitud: **16.09.2009**

(54) Título: **Generador de bits.**

(30) Prioridad: **12.12.2007 IL 188089**

(45) Fecha de publicación de la mención BOPI:
10.03.2011

(45) Fecha de la publicación del folleto de la patente:
10.03.2011

(73) Titular/es: **NDS Limited**
Forrester & Boehmert Pettenkoferstrasse 20-22
80336 Munich, DE

(72) Inventor/es: **Kaluzhny, Uri**

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

DESCRIPCIÓN

CAMPO DE LA INVENCIÓN

La presente invención se refiere a generadores de bits aleatorios o pseudo-aleatorios, y en particular, a registros de desplazamiento con retroalimentación no lineal.

ANTECEDENTES DE LA INVENCIÓN

A modo de introducción, el uso de retrasos aleatorios, también conocidos como estados de espera aleatorios, es propuesto frecuentemente como una contramedida genérica contra análisis de canal lateral y ataques por fallos, bloqueando una CPU durante la ejecución de software incrustado. La eficiencia de un esquema de desencadenamiento de retrasos aleatorios mejora conforme incrementa la varianza de los estados de espera aleatorios. Sin embargo, los sistemas incorporan, típicamente, estados de espera aleatorios que están distribuidos uniformemente.

Se considera que las referencias siguientes representan también el estado de la técnica:

Patente US 6.167.553 concedida a Dent;
Patente US 6.785.389 concedida a Sella, et al.;
Solicitud de patente US publicada 2003/0085286 de Kelley, et al.;
Solicitud de patente US publicada 2004/0076293 de Smeets, et al.;
Solicitud de patente US publicada 2004/0205095 de Gressel, et al.;
Solicitud de patente US publicada 2006/0161610 de Goettfert, et al.;
Artículo titulado "Efficient Use of Random Delays" por Olivier Benoit y Michael Tunstall of Royal Holloway, Universidad de Londres;
Capítulo 6 del libro Applied Cryptography (CRC Press Series on Discrete Mathematics and Its Applications) por Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone.

Las divulgaciones de todas las referencias indicadas anteriormente y a lo largo de la presente especificación, así como las divulgaciones de todas las referencias indicadas en esas referencias, se incorporan a la presente memoria, por referencia.

RESUMEN DE LA INVENCIÓN

La presente invención busca proporcionar un registro de desplazamiento con retroalimentación mejorado.

De esta manera, se proporciona, según una realización preferente de la presente invención, un sistema que incluye un registro de desplazamiento con retroalimentación que tiene L etapas conectadas en serie, que incluyen una primera etapa y una etapa final, estando denotadas las etapas de 0 a L-1, desde la primera etapa a la etapa final, respectivamente, estando operativas las etapas para almacenar una pluralidad de bits, de manera que cada una de las etapas es operativa para almacenar uno de los bits, y un sub-sistema de retroalimentación no lineal, teniendo al menos algunas de las etapas una salida conectada operacionalmente al sub-sistema de retroalimentación no lineal, estando operativo el sub-sistema de retroalimentación no lineal para recibir una entrada desde una etapa n y una etapa 2n-1 de entre las etapas, incluyendo el sub-sistema de retroalimentación no lineal una primera puerta lógica AND, teniendo la primera puerta lógica AND una primera entrada conectada operacionalmente a la salida de la etapa n, una segunda entrada conectada operacionalmente a la salida de la etapa 2n+1, y una salida, teniendo el sub-sistema de retroalimentación no lineal una salida basada, al menos en parte, en un valor de la salida de la primera puerta lógica AND, un reloj conectado operacionalmente al registro de desplazamiento con retroalimentación, estando operativo el reloj para controlar el movimiento de los bits a lo largo de las etapas, un generador de bits que tiene una salida, estando operativo el generador de bits para generar una pluralidad de bits aleatorios/pseudo aleatorios para ser presentados en la salida del generador de bits, y una puerta lógica XOR principal que tiene una primera entrada y una segunda entrada y una salida, estando conectada operacionalmente la salida del generador de bits a la primera entrada de la puerta lógica XOR principal, estando conectada operacionalmente la salida del sub-sistema de retroalimentación no lineal a la segunda entrada de la puerta lógica XOR principal, estando conectada operacionalmente la salida de la puerta lógica XOR principal a la entrada de la primera etapa del registro con retroalimentación no lineal.

Además, según una realización preferente de la presente invención, el sub-sistema con retroalimentación no lineal está operativo para recibir una entrada desde una etapa m y una etapa 2m+1 de entre las etapas, el sub-sistema de retroalimentación no lineal incluye una segunda puerta lógica AND y una primera puerta lógica XOR, teniendo la segunda puerta lógica AND una primera entrada

conectada operacionalmente a la salida de la etapa m, una segunda entrada conectada operacionalmente a la salida de la etapa 2m+1, y una salida, la primera puerta lógica XOR del sub-sub-sistema de retroalimentación tiene una primera entrada conectada operacionalmente a la salida de la primera puerta lógica AND, y una segunda entrada conectada operacionalmente a la salida de la segunda puerta lógica AND, y la salida del sub-sistema de retroalimentación no lineal está basada, al menos en parte, en un valor de la salida de la primera puerta lógica XOR del sub-sistema de retroalimentación no lineal.

Además, según una realización preferente de la presente invención, el sub-sistema de retroalimentación no lineal está operativo para recibir una entrada desde una etapa k y una etapa 2k+1 de entre las etapas, el sub-sistema de retroalimentación no lineal incluye una tercera puerta lógica AND y una segunda puerta lógica XOR, teniendo la tercera puerta lógica AND que tiene una primera entrada conectada operacionalmente a la salida de la etapa k, una segunda entrada conectada operacionalmente a la salida de la etapa 2k+1, y una salida, la segunda puerta lógica XOR del sub-sub-sistema de retroalimentación tiene una primera entrada conectada operacionalmente a la salida de la primera puerta lógica XOR, y una segunda entrada conectada operacionalmente a la salida de la tercera puerta lógica AND, y la salida del sub-sistema de retroalimentación no lineal está basada, al menos en parte, en un valor de la salida de la segunda puerta lógica XOR del sub-sistema de retroalimentación no lineal.

Además, según una realización preferente de la presente invención, el generador de bits está operativo de manera que la salida del generador de bits está sesgada hacia un estado de las etapas del registro de desplazamiento con retroalimentación.

Además, según una realización preferente de la presente invención, el sistema incluye un planificador que tiene una entrada conectada operacionalmente a la puerta lógica XOR principal del registro de desplazamiento con retroalimentación, estando operativo el planificador para planificar una pluralidad de datos de estados de espera recibidos en la entrada del planificador.

También se proporciona, según todavía otra realización preferente de la presente invención, un sistema de estados de espera para almacenar una pluralidad de estados de espera, incluyendo un registro de desplazamiento con retroalimentación que tiene una pluralidad de etapas conectadas en serie que incluyen una primera etapa, estando operativas las etapas para almacenar una pluralidad de bits, de manera que cada una de las etapas está operativa para almacenar uno de los bits, y un sub-sistema de

retroalimentación no lineal, teniendo al menos una de las etapas una salida conectada operacionalmente al sub-sistema de retroalimentación no lineal, estando operativo el sub-sistema de retroalimentación no lineal para recibir una entrada desde al menos una de las etapas, estando operativo el sub-sistema de retroalimentación no lineal de manera que una salida del sub-sistema de retroalimentación no lineal es una función no lineal de la entrada del sub-sistema de retroalimentación no lineal, estando conectada operacionalmente la salida del sub-sistema de retroalimentación no lineal a la primera etapa, un reloj conectado operacionalmente al registro de desplazamiento con retroalimentación, estando operativo el reloj para controlar el movimiento de los bits a lo largo de las etapas, y un planificador que tiene una entrada conectada operacionalmente al registro de desplazamiento con retroalimentación, estando operativo el planificador para planificar una pluralidad de datos de estados de espera recibidos en la entrada del planificador.

También se proporciona, según todavía otra realización preferente de la presente invención, un procedimiento que incluye la provisión de un registro de desplazamiento con retroalimentación que tiene L etapas conectadas en serie que incluyen una primera etapa y una etapa final, estando denotadas las etapas de 0 a L-1 desde la primera etapa a la etapa final, respectivamente, estando operativas las etapas para almacenar una pluralidad de bits, de manera que cada una de las etapas está operativa para almacenar uno de los bits, y realizar lo siguiente una pluralidad de veces realizar una operación de puerta lógica AND con la salida de una etapa n y una etapa 2n+1 de entre las etapas como entrada, generar un bit aleatorio/pseudo-aleatorio, realizar una operación de puerta lógica XOR con el bit y un resultado de la operación de puerta lógica AND como entrada, desplazar los bits a lo largo de las etapas, e insertar un resultado de la operación de puerta lógica XOR en la primera etapa.

También se proporciona, según todavía otra realización preferente de la presente invención, un procedimiento que incluye la provisión de un registro de desplazamiento con retroalimentación que tiene una pluralidad de etapas conectadas en serie que incluyen una primera etapa y una etapa final, estando operativas las etapas para almacenar una pluralidad de bits, de manera que cada una de las etapas está operativa para almacenar uno de los bits, realizar lo siguiente una pluralidad de veces realizar una función no lineal sobre la salida de al menos una de las etapas, desplazar los bits a lo largo de las etapas, insertar un nuevo valor en la primera etapa, estando basado el nuevo valor en el resultado de la función no lineal, y planificar un estado de

espera en base a una salida del registro de desplazamiento con retroalimentación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención se entenderá y apreciará más completamente a partir de la descripción detallada siguiente, tomada en conjunción con los dibujos, en los que:

La Fig. 1 es una vista de un diagrama de bloques de un dispositivo de seguridad construido y operativo según una realización preferente de la presente invención;

La Fig. 2 es una vista de un diagrama de bloques de un planificador de estados de espera aleatorios para su uso con el dispositivo de seguridad de la Fig. 1;

La Fig. 3 es una primera realización preferente del planificador de estados de espera aleatorios de la Fig. 2;

Las Figs. 4a y 4b son vistas, en parte pictóricas, en parte diagramas de bloques, que ilustran la operación del planificador de estados de espera aleatorios de la Fig. 3;

La Fig. 5 es una segunda realización preferente del planificador de estados de espera aleatorios de la Fig. 2;

Las Figs. 6a y 6b son vistas, en parte pictóricas, en parte diagramas de bloques, que ilustran la operación del planificador de estados de espera aleatorios de la Fig. 5;

La Fig. 7 es una tercera realización preferente del planificador de estados de espera aleatorios de la Fig. 2;

La Fig. 8 es una vista, en parte pictórica, en parte diagrama de bloques, que ilustra la operación del planificador de estados de espera aleatorios de la Fig. 7; y

La Fig. 9 es una vista, en parte pictórica, en parte diagrama de bloques, de un generador de bits aleatorios para su uso con el dispositivo de seguridad de la Fig. 1.

DESCRIPCIÓN DETALLADA DE UNA REALIZACIÓN PREFERENTE

Se hace referencia ahora a la Fig. 1, que es una vista de un diagrama de bloques de un dispositivo 10 de seguridad construido y operativo según una realización preferente de la presente invención. El dispositivo 10 de seguridad incluye, preferentemente, un planificador 12 de estados de espera aleatorios para planificar una pluralidad de estados de espera.

El planificador 12 de estados de espera aleatorios incluye, preferentemente, un generador 14 de bits aleatorios, un registro de desplazamiento 16 con retroalimentación, una puerta lógica 18 OR-exclusivo (XOR) principal, un reloj 20 y un planificador 22.

Se hace referencia ahora a la Fig. 2, que es una vista de un diagrama de bloques del planificador 12 de estados de espera aleatorios para su uso con el dispositivo 10 de seguridad de la Fig. 1.

El registro de desplazamiento 16 con retroalimentación incluye, preferentemente, L etapas 24 conectadas en serie, implementadas, típicamente, como flip-flops, que incluyen una primera etapa 26 y una etapa final 28. Las etapas 24 se denotan, típicamente, de 0 a L-1, desde la primera etapa 26 a la etapa final 28, respectivamente. En otras palabras, las etapas están numeradas 0, 1, … L-2, L-1. Preferentemente, las etapas 24 están operativas para almacenar una pluralidad de bits, de manera que cada una de las etapas 24 está operativa para almacenar uno de los bits. Típicamente, cada una las etapas 24 incluye una entrada 30 y una salida 32 para conectar en serie las etapas 24. El contenido de las etapas 24 en un tiempo t se denomina el estado en el tiempo t.

Preferentemente, el registro de desplazamiento 16 con retroalimentación incluye un sub-sistema 34 de retroalimentación no lineal que está conectado operacionalmente a la salida 32 de las etapas 24, según sea apropiado. Generalmente, el sub-sistema 34 de retroalimentación no lineal solo necesita estar conectado operacionalmente a la salida 32 de las etapas 24 necesarias para el sub-sistema 34 de retroalimentación no lineal, tal como se explicará en mayor detalle con referencia a las Figs. 3, 5 y 7. Por lo tanto, el sub-sistema 34 de retroalimentación no lineal está operativo, típicamente, para recibir una entrada desde al menos alguna de las etapas 24. El sub-sistema 34 de retroalimentación no lineal tiene, preferentemente, una salida 36 que está conectada operacionalmente a la primera etapa 26 por medio de la puerta lógica 18 OR-exclusivo principal, tal como se describirá en mayor detalle,

más adelante.

Preferentemente, el sub-sistema 34 de retroalimentación no lineal está operativo para realizar una función F de retroalimentación Booleana, de manera que la salid del sub-sistema 34 de retroalimentación no lineal es una función no lineal de la entrada del sub-sistema 34 de retroalimentación no lineal. La función F de retroalimentación se describe en mayor detalle, más adelante.

Preferentemente, el reloj 20 está conectado operacionalmente al registro de desplazamiento 16 con retroalimentación no lineal. Generalmente, el reloj 20 está operativo para controlar el movimiento de los bits a lo largo de las etapas 24 y a través del sub-sistema 34 de retroalimentación no lineal.

Típicamente, el generador 14 de bits aleatorios tiene una salida 38. Preferentemente, el generador 14 de bits aleatorios está operativo para generar una pluralidad de bits aleatorios/pseudo-aleatorios para presentarlos en la salida 38 del generador 14 de bits aleatorios. El generador 14 de bits aleatorios se describe en mayor detalle, más adelante.

Preferentemente, la puerta lógica 18 OR-exclusivo principal tiene una entrada 40, una entrada 42 y una salida 44.

Preferentemente, la salida 38 del generador 14 de bits aleatorios está conectada operacionalmente a la entrada 42 de la puerta lógica 18 OR-exclusivo principal. Preferentemente, la salida 36 del sub-sistema 34 de retroalimentación no lineal está conectada operacionalmente a la entrada 40 de la puerta lógica 18 OR-exclusivo principal. Preferentemente, la salida 44 de la puerta lógica 18 OR-exclusivo principal está conectada operacionalmente a una entrada 46 del planificador 22 y a la entrada 30 de la primera etapa 26 del registro de desplazamiento 16 con retroalimentación.

Preferentemente, el planificador 22 está operativo para planificar una pluralidad de estados de espera según datos recibidos en la entrada 46 del planificador 22. Por ejemplo, cuando el dato en la entrada 46 es un “1”, entonces se planifica un estado de espera durante un periodo de tiempo determinado, típicamente, un ciclo de reloj.

Según una realización preferente alternativa de la presente invención, la entrada 46 del planificador 22 puede estar conectada operacionalmente a cualquiera de las salidas 32 de las etapas 24 o a la salida 36 del sub-sistema 34 de retroalimentación no lineal.

La operación del planificador 12 de estados de espera aleatorios se describe brevemente a continuación.

Preferentemente, durante cada unidad de tiempo (ciclo de reloj) se realizan las

siguientes operaciones. El sub-sistema 34 de retroalimentación no lineal realiza una función F no lineal sobre la salida de una o más de las etapas 24, descritas en mayor detalle con referencia a las Figs. 3-9. El generador 14 de bits aleatorios genera un bit aleatorio/pseudo-aleatorio. La puerta lógica 18 OR-exclusivo principal realiza una operación de puerta lógica OR-exclusivo (XOR) con el bit y un resultado de la función F del sub-sistema 34 de retroalimentación no lineal. El reloj 20 hace que los bits se desplacen a lo largo de las etapas 24, de manera que para cada etapa 24 desde 0 a L-2, el contenido S_i de la etapa i es movido a la etapa i+1. Un nuevo valor es insertado en la primera etapa 26 mediante la inserción de un resultado de la operación de la puerta lógica XOR (que está basado en un resultado de la función F no lineal) en la primera etapa 26. El planificador 22 planifica un estado de espera en base a la salida de la puerta lógica 18 OR-exclusivo principal (que está basada en la salida del sub-sistema 34 de retroalimentación no lineal y el generador 14 de bits aleatorios).

Típicamente, el planificador 12 de estados de espera aleatorios es implementado en hardware, usando puertas lógicas y/o chips disponibles comercialmente o circuitería y chips a medida. Sin embargo, las personas con conocimientos ordinarios en la materia apreciarán que el planificador 12 de estados de espera aleatorios puede ser implementado fácilmente en software o parcialmente en software y parcialmente en hardware.

Se hace referencia ahora a la Fig. 3, que es una primera realización preferente del planificador 12 de estados de espera aleatorios de la Fig. 2.

Según la primera realización preferente del planificador 12 de estados de espera aleatorios, típicamente, la función F de retroalimentación de la Fig. 2 tiene la forma:

$$F(S_0, S_1, \ldots S_{L-1}) = S_n \,\&\, S_{(2n+1)},$$

donde 2n+1 es menor de L, el número de etapas 24 en el registro de desplazamiento 16 con retroalimentación. En otras palabras, la salida de la función F de retroalimentación no lineal es un resultado de realizar una operación de puerta lógica AND sobre el valor de la salida de la etapa n-ava y el valor de la salida de la etapa (2n+1)-ava.

Por lo tanto, el sub-sistema 34 de retroalimentación no lineal está operativo, preferentemente, para recibir una entrada de la etapa n-ava y de la etapa (2n+1)-ava de entre las etapas 24. En el ejemplo de la Fig. 3, n es igual a 4, de manera que el sub-sistema 34 de retroalimentación no lineal está conectado operacionalmente a la salida 32 de la etapa 4 y la salida 32 de la etapa 9.

Preferentemente, el sub-sistema 34 de retroalimentación no lineal incluye una puerta lógica 48 AND. Típicamente, la puerta lógica 48 AND tiene: una entrada 50 conectada operacionalmente a la salida 32 de la etapa n-ava; una entrada 52 conectada operacionalmente a la salida 32 de la etapa (2n+1)-ava; y una salida 54. Generalmente, la salida 54 de la puerta lógica 48 AND está conectada operacionalmente a la entrada 40 de la puerta lógica 18 OR-exclusivo principal. Por lo tanto, la salida del sub-sistema 34 de retroalimentación no lineal está basada preferentemente, en el valor de la salida de la puerta lógica 48 AND.

Se hace referencia ahora a la Fig. 4a, que es una vista, en parte pictórica, en parte un diagrama de bloques, que ilustra la operación del planificador 12 de estados de espera aleatorios de la Fig. 3. La Fig. 4a muestra el estado de las etapas 24 del registro de desplazamiento 16 con retroalimentación de la Fig. 3, y cómo se calcula la función F de retroalimentación durante una pluralidad de tiempos, desde el tiempo t hasta el tiempo t+5.

Típicamente, el generador 14 de bits aleatorios (Fig. 3) está sesgado de manera que una pluralidad de bits 56 aleatorios/pseudo-aleatorios, presentados en la salida 38 (Fig. 3) del generador 14 de bits aleatorios, tiene una probabilidad muy alta de proporcionar el valor “0”. El sesgo del generador 14 de bits aleatorios se expone en mayor detalle con referencia a la Fig. 9. Por lo tanto, en algún momento en el tiempo, las etapas 24 están, típicamente, todas vacías. En otras palabras, S_i es igual a “0” para todo i. Al estado en el que todas las etapas 24 están vacías se le conoce también como el estado del registro de desplazamiento 16 con retroalimentación en estado vacío.

Si los bits 56 aleatorios/pseudo-aleatorios producidos por el generador 14 de bits aleatorios incluyen dos bits iguales a “1” separados por n etapas, la función F de retroalimentación devuelve un resultado 58 igual a “1” después de n ciclos de reloj. La Fig. 4a muestra que en el tiempo t, el estado de la etapa 4 y la etapa 9 son iguales a “1”. Por lo tanto, al realizar una operación de puerta lógica AND sobre la salida de la etapa 4 y la etapa 9 proporciona un “1” (el resultado 58). Suponiendo que el bit 56 aleatorio/pseudo-aleatorio es igual a “0”, un resultado 60 de realizar una operación XOR entre “1” y “0” proporciona “1”, que es ahora la nueva entrada a la primera etapa 26. De esta manera, se establece una secuencia periódica 62 de “1”s separados por n etapas, tal como se muestra en el tiempo t+5. Los “1” son usados, típicamente, para planificar estados de espera por el planificador 22 de la Fig. 3.

Se hace referencia ahora a la Fig. 4b, que es una vista, en parte pictórica, en

parte un diagrama de bloques, que ilustra la operación del planificador 12 de estados de espera aleatorios de la Fig. 3. La Fig. 4b muestra el estado de las etapas 24 del registro de desplazamiento 16 con retroalimentación de la Fig. 3 y cómo se calcula la función F de retroalimentación durante una pluralidad de tiempos, desde el tiempo t+5 al tiempo t+21.

En el tiempo t+5, el estado de la etapa 4 y de la etapa 9 son ambos iguales a “1”. En tal caso, el resultado 58 de la función de retroalimentación es igual a “1”.

Si el bit 56 aleatorio/pseudo-aleatorio es igual a “1”, lo cual es una ocurrencia rara, entonces el resultado 60 de realizar un XOR del resultado 58 con el bit 56 aleatorio/pseudo-aleatorio es igual a “0”. Por lo tanto, se rompe la secuencia periódica 62 y el estado del registro de desplazamiento 16 con retroalimentación estará vacío en el tiempo t+21.

Por lo tanto, el registro de desplazamiento 16 con retroalimentación resulta, típicamente, en una pluralidad de ráfagas aleatorias/pseudo-aleatorias de las secuencias periódicas 62. Cada secuencia periódica 62 tiene “1”s separados por n ciclos de reloj. El planificador 22 traduce, preferentemente, los “1”s a estados de espera. Las secuencias periódicas 62 comienzan y terminan, generalmente, aleatoriamente/pseudo-aleatoriamente, resultando en una alta varianza de los estados de espera.

El planificador 12 de estados de espera aleatorios de las Figs. 3, 4a y 4b proporciona, generalmente, la inicialización y la terminación de una secuencia periódica regular (la secuencia 62) como un evento raro. El planificador 12 de estados de espera aleatorios puede mejorarse incrementando la probabilidad de los “1”s en los bits 56 aleatorios/pseudo-aleatorios cuando el estado es vacío, sesgando de manera adecuada el generador 14 de bits aleatorios, tal como se describe con referencia a la Fig. 9. Además, el planificador 12 de estados de espera aleatorios puede mejorarse usando una función F de retroalimentación más compleja, tal como se describe con referencia a las realizaciones preferentes segunda y tercera, descritas con referencia a las Figs. 5-7.

Se hace referencia ahora a la Fig. 5, que es una segunda realización preferente del planificador de estados de espera aleatorios de la Fig. 2.

La segunda realización preferente del planificador 12 de estados de espera aleatorios es sustancialmente la misma que la primera realización preferente del planificador 12 de estados de espera aleatorios, descrita con referencia a la Fig. 3, exceptuando las diferencias siguientes que se describen a continuación.

Según la segunda realización preferente del planificador 12 de estados de espera aleatorios, la función F de retroalimentación de la Fig. 2, tiene, típicamente, la forma:

$$F(S_0, S_1, ...S_{L-1}) = [S_n \& S_{(2n+1)}] \text{ XOR } [S_m \& S_{(2m+1)}],$$

donde 2n+1 es menor que L, 2m+1 es menor que L y m no es igual a n.

En otras palabras, la salida de la función F de retroalimentación no lineal es, típicamente, un resultado de realizar: una primera operación de puerta lógica AND sobre el valor de la salida de la n-ava etapa y el valor de la salida de la (2n+1)-ava etapa; una segunda operación de puerta lógica AND sobre el valor de la salida de la etapa m-ava y el valor de la salida de la etapa (2m+1)-ava; realizar una operación XOR del resultado de la primera operación de puerta lógica AND con el resultado de la segunda operación de puerta lógica AND.

Por lo tanto, el sub-sistema 34 de retroalimentación no lineal está operativo, preferentemente, para recibir una entrada desde la etapa n-ava, la etapa (2n+1)-ava, la etapa m-ava, la etapa (2m+1)-ava, de entre las etapas 24. En el ejemplo de la Fig. 5, n es igual a 4 y m es igual a 6, de manera que el sub-sistema 34 de retroalimentación no lineal está conectado operacionalmente a la salida 32 de la etapa 4, la salida 32 de la etapa 6, la salida 32 de la etapa 9 y la salida 32 de la etapa 13.

Además de la puerta lógica 48 AND descrita anteriormente con referencia a la Fig. 3, el sub-sistema 34 de retroalimentación no lineal incluye, preferentemente, una puerta lógica 64 AND y una puerta lógica 66 XOR.

Preferentemente, la puerta lógica 64 AND incluye: una entrada 68 conectada operacionalmente a la salida 32 de la etapa m-ava; una entrada 70 conectada operacionalmente a la salida de la etapa (2m+1)-ava; y una salida 72.

La puerta lógica 66 XOR incluye generalmente: una entrada 74 conectada operacionalmente a la salida 72 de la puerta lógica 64 AND; una entrada 76 conectada operacionalmente a la salida 54 de la puerta lógica 48 AND; y una salida 78 conectada operacionalmente a la entrada 40 de la puerta lógica 18 OR-exclusivo principal.

Por lo tanto, la salida del sub-sistema 34 de retroalimentación no lineal está basada, preferentemente, en un valor de la salida de la puerta lógica 66 XOR.

Se hace referencia ahora a las Figs. 6a y 6b, que son vistas, en parte pictóricas, en parte diagramas de bloques, que ilustran la operación del planificador 12 de estados de espera aleatorios de la Fig. 5. Las Figs. 6a y 6b muestran el estado de las

etapas 24 del registro de desplazamiento 16 con retroalimentación de la Fig. 5 y cómo se calcula la función F de retroalimentación durante una pluralidad de tiempos, desde el tiempo t al tiempo t+20.

La Fig. 6a muestra en el tiempo t: una secuencia periódica 80 de “1”s, cada uno separado por n etapas; y una secuencia periódica 82 de “1”s, cada uno separado por m etapas.

Dependiendo de la elección de m y n y de la separación entre la secuencia periódica 80 y la secuencia periódica 82, las secuencias periódicas 80, 82 pueden actuar como secuencias periódicas separadas que terminan en una manera similar a la secuencia periódica 62 de la Fig. 4b y/o las secuencias periódicas 80, 82 pueden colisionar, tal como se describirá más adelante.

La función de retroalimentación en base al estado en el tiempo t+2 es calculada, típicamente, como se indica a continuación. Ambas operaciones de puerta lógica AND, basadas en el estado en el tiempo t+2, dan un resultado 84 de “1”. Al realizar una operación de puerta lógica XOR sobre los resultados 84, proporciona un resultado 86 de “0”. Al realizar una operación de puerta lógica XOR sobre el resultado 84 con el bit 56 aleatorio, proporciona un valor 88 igual a “0”.

En el tiempo t+3, para que las secuencias periódicas continúen, es necesario que el valor de la primera etapa 26 sea “1” y no “0”. El valor “1” en la primera etapa 26 sería parte tanto de la secuencia 80 n periódica como de la secuencia 82 m periódica.

Sin embargo, debido a un colisión de las secuencias periódicas 80 y 82, al calcular la función de retroalimentación a partir del estado en el tiempo t+2, calculado anteriormente, el valor 88 de la primera etapa 26 es “0” en el tiempo t+3, rompiendo, de esta manera, tanto la secuencia periódica 80 como la secuencia periódica 82. Las secuencias periódicas 80, 82 rotas, van pasando lentamente por las etapas 24 hasta que el estado del registro de desplazamiento 16 con retroalimentación (Fig. 3) está vacío en el tiempo 5+20 (Fig. 6b).

La adición del monomio S_m & $S_{(2m+1)}$ a la función F de retroalimentación, hace más complejo el patrón de la salida de la puerta lógica 18 OR-exclusivo principal (Fig.5). La adición de un tercer monomio, elegido adecuadamente, añade preferentemente la posibilidad de una tercera secuencia periódica creada a partir de las otras dos secuencias, tal como se describirá con referencia a las Figs. 7 y 8, más adelante. La posibilidad de crear una tercera secuencia en base a los restos de las otras dos secuencias, añade más “caos” a la salida del planificador 12 de estados de espera aleatorios.

Se hace referencia ahora a la Fig. 7, que es una tercera realización preferente del planificador 12 de estados de espera aleatorios de la Fig. 2.

La tercera realización preferente del planificador 12 de estados de espera aleatorios es sustancialmente la misma que la segunda realización preferente del planificador 12 de estados de espera aleatorios, descrito con referencia a la Fig. 3, exceptuando las siguientes diferencias, descritas a continuación.

Según la tercera realización preferente del planificador 12 de estados de espera aleatorios, la función F de retroalimentación de la Fig. 2 es una suma (que es un XOR) de varios monomios, de manera que F tiene, típicamente, la forma:

$$F(S_0, S_1, \ldots S_{L-1}) = \quad .$$

$$[S_k \,\&\, S_{(2k+1)}] \text{ XOR } [S_m \,\&\, S_{(2m+1)}] \text{ XOR } [S_n \,\&\, S_{(2n+1)}],$$

donde 2k+1 es menor de L, 2m+1 es menor de L, 2n+1 es menor de L y k, m y n son diferentes.

En otras palabras, la salida de la función F de retroalimentación no lineal es, típicamente, un resultado de realizar: una primera operación de puerta lógica AND sobre el valor de la salida de la etapa k-ava y el valor de la salida de la etapa (2k+1)-ava; una segunda operación de puerta lógica AND sobre el valor de la salida de la etapa m-ava y el valor de la salida de la etapa (2m+1)-ava; una tercera operación de puerta lógica AND sobre el valor de la salida de la etapa n-ava y el valor de la salida de la etapa (2n+1)-ava; y realizar una operación XOR de los resultados de la operaciones de puerta lógica AND entre sí.

Por lo tanto, el sub-sistema 34 de retroalimentación no lineal está operativo, típicamente, para recibir una entrada desde la etapa k-ava, la etapa (2k+1)-ava, la etapa m-ava, la etapa (2m+1)-ava, la etapa n-ava, la etapa (2n+1)-ava, de entre las etapas 24. En el ejemplo de la Fig. 7, k es igual a 8, n es igual a 4 y m es igual a 6, de manera que el sub-sistema 34 de retroalimentación no lineal está conectado operacionalmente a la salida 32 de las etapas 4, 6, 7, 8, 9, 13 y 17.

Con k, m, n elegidos adecuadamente y con una probabilidad adecuada elegida de “1”s que aparecen en el flujo de bits de entrada, se producirán ráfagas impredecibles de retrasos aleatorios. Para acercar más las ráfagas, unas a las otras, la probabilidad de aparición de “1”s en el flujo de bits de entrada se incrementa, por ejemplo, pero no se limita a, en una situación en la que el estado del registro de desplazamiento 16 con retroalimentación está vacío. Cuando se incrementa la

probabilidad de “1”s, por ejemplo, sesgando adecuadamente el generador 14 de bits aleatorios, la salida 38 del generador 14 de bits aleatorios puede estar conectada directamente a la entrada 30 de la primera etapa 26, circunvalando la puerta lógica 18 OR-exclusivo principal, de manera que el planificador 22 no planifica estados de espera en base a la salida del generador 14 de bits aleatorios.

En la función de retroalimentación anterior, pueden establecerse una secuencia k periódica de “1”s y/o una secuencia m periódica de “1”s y/o una secuencia n periódica de “1”s en el registro de desplazamiento 16 con retroalimentación. Las secuencias periódicas pueden existir separadamente o al mismo tiempo. Dependiendo de la elección de k, m y n y de la separación entre las secuencias periódicas, una secuencia periódica individual puede terminar debido a un “1” producido por el generador 14 de bits aleatorios en un tiempo determinado o dos o más de las secuencias periódicas pueden terminar debido a una colisión, tal como se ha explicado anteriormente con referencia a las Figs. 6a y 6b o dos secuencias pueden crear una tercera secuencia, tal como se describe en mayor detalle con referencia a la Fig. 8.

Además de la puerta lógica 48 AND, la puerta lógica 64 AND y la puerta lógica 66 XOR, descritas anteriormente con referencia a la Fig. 5, el sub-sistema 34 de retroalimentación no lineal incluye, preferentemente, una puerta lógica 90 AND y una puerta lógica 92 XOR.

La puerta lógica 90 AND tiene, típicamente: una entrada 94 conectada operacionalmente a la salida de la k-ava etapa; una entrada 96 conectada operacionalmente a la salida de la (2k+1)-ava etapa; y una salida 98.

La puerta lógica 92 XOR tiene, generalmente: una entrada 100 conectada operacionalmente a la salida 78 de la puerta lógica 66 XOR; una entrada 102 conectada operacionalmente a la salida 98 de la puerta lógica 90 AND; y una salida 104 conectada operacionalmente a la entrada 40 de la puerta lógica 18 OR-exclusivo principal.

Por lo tanto, la salida del sub-sistema 34 de retroalimentación no lineal está basada, preferentemente, en un valor de la salida de la puerta lógica 92 XOR del sub-sistema 34 de retroalimentación no lineal.

Las personas con conocimientos ordinarios en la materia apreciarán que la presencia de 1, 2 ó 3 monomios en la función F de retroalimentación es sólo a modo de ejemplo, y que pueden usarse cualquier número adecuado de monomios. Un monomio resulta, generalmente, en la creación y la terminación de una única secuencia periódica. Un segundo monomio elegido adecuadamente resulta

adicionalmente en que las secuencias colisionan y, por lo tanto, terminan. Un tercer monomio elegido resulta adicionalmente en que dos secuencias periódicas crean una tercera secuencia.

Las personas con conocimientos ordinarios en la materia apreciarán que pueden usarse cualquier número adecuado de etapas en el registro de desplazamiento 16 con retroalimentación.

Se hace referencia ahora a la Fig. 8, que es una vista, en parte pictórica, en parte un diagrama de bloques, que ilustra la operación del planificador 12 de estados de espera aleatorios de la Fig.7.

En el tiempo t, el estado del planificador 12 de estados de espera aleatorios (Fig. 7) incluye: una secuencia periódica 116 que tiene una separación de n (4 en el ejemplo de la Fig. 8); y una secuencia periódica 118 que tiene una separación de m (6 en el ejemplo de la Fig. 8).

En el tiempo t, la secuencia periódica 116 y la secuencia periódica 118 colisionan. La colisión de las secuencias periódicas 116, 118 interrumpe las secuencias y con el tiempo parece que las secuencias van a terminar.

Sin embargo, en el tiempo t+4, un valor 120 de la secuencia periódica 116 y un valor 122 de la secuencia periódica 118 coinciden con la entrada para la función de retroalimentación para la etapa k-ava y (2k+1)-ava (etapa 8 y 17 en el ejemplo de la Fig. 8), respectivamente. Por lo tanto, una salida 124 de la función F de retroalimentación es igual a “1” y la entrada a la primera etapa 26 es igual a “1”. Por lo tanto, se establece una nueva secuencia periódica 126 que tiene una separación de k.

De esta manera, las secuencias periódicas 116, 118, que se están terminando, se desarrollan en la nueva secuencia periódica 126.

Se hace referencia ahora a la Fig. 9, que es en parte pictórica, en parte un diagrama de bloques del generador 14 de bits aleatorios para su uso con el dispositivo 10 de seguridad de la Fig. 1.

Preferentemente, el generador 14 de bits aleatorios incluye un generador 114 de números aleatorios no sesgado para generar una pluralidad de bits 106 aleatorios/pseudo-aleatorios (ceros o unos) con una probabilidad igual de ceros y unos, tal como conocen las personas con conocimientos ordinarios en la materia.

Típicamente, el generador 14 de bits aleatorios incluye también un módulo 108 de pesaje de salida conectado operacionalmente al generador 114 de números aleatorios no sesgado. El módulo 108 de pesaje de salida está operativo, generalmente, para recibir los bits 106 aleatorios/pseudo-aleatorios y agrupar los bits

106 aleatorios/pseudo-aleatorios en grupos de P bits. Si todos los bits en un grupo son “1”s, el módulo 108 de pesaje de salida produce, preferentemente, un resultado 110 igual a “1”. Si el grupo incluye al menos un “0”, entonces el módulo 108 de pesaje de salida produce, preferentemente, un resultado 112 igual a “0”.

A continuación, los resultados 110, 112 son presentados, generalmente, en la salida 38 del generador 14 de bits aleatorios.

La probabilidad de que el generador 14 de bits aleatorios presente un “1” es igual a 2^{-P}.

Por lo tanto, la salida del generador 14 de bits aleatorios puede ser sesgada incrementando o decrementando P, según sea apropiado.

El valor de P puede tomar cualquier valor adecuado, por ejemplo, pero sin limitarse a, entre 5 y 15.

Típicamente, la salida del generador 14 de bits aleatorios es sesgada según el estado de las etapas 24 (Fig. 2) del registro de desplazamiento 16 con retroalimentación, de manera que cuando el estado es vacío, o casi vacío, el valor de P se reduce, y cuando el estado está poblado, el valor de P se incrementa al valor anterior de P. Típicamente, el estado se define como “casi vacío” cuando todos los valores de las etapas 24 son iguales a cero hasta, e incluyendo a, la mayor de: las etapas k-ava, m-ava o n-ava. Las personas con conocimientos ordinarios en la materia apreciarán que la definición de “casi vacío” puede ajustarse si la función F incluye más de 3 monomios.

Lo que sigue es un ejemplo no limitativo del planificador 12 de estados de espera aleatorios de la Fig. 2. El registro de desplazamiento 16 con retroalimentación incluye 30 etapas. El sub-sistema 34 de retroalimentación no lineal está configurado de manera que k=14, m=9, n=11. El valor P del generador 14 de bits aleatorios se fija a 7 cuando el estado es vacío y se fija a 13 cuanto el estado es poblado.

Las personas con conocimientos ordinarios en la materia apreciarán que el número de etapas y los valores de k, m, n y P pueden ser cualquier valor adecuado. Además, pueden añadirse más monomios a la función F de retroalimentación.

Típicamente, el planificador 12 de estados de espera aleatorios es implementado en hardware, usando chips y/o puertas lógicas disponibles comercialmente o circuitería y chips a medida. Sin embargo, las personas con conocimientos ordinarios en la materia apreciarán que el planificador 12 de estados de espera aleatorios puede ser implementado fácilmente en software o parcialmente en software y parcialmente en hardware.

Se apreciará que las diversas características de la invención que se describen, en aras de la claridad, en los contextos de realizaciones separadas, pueden ser proporcionadas también, en combinación, en una única realización. Por el contrario, diversas características de la invención que se describen, en aras de la brevedad, en el contexto de una única realización, pueden ser proporcionadas también de manera separada o en cualquier sub-combinación adecuada. Las personas con conocimientos ordinarios en la materia apreciarán también que la presente invención no está limitada por lo mostrado particularmente y descrito anteriormente, en esta memoria. Por el contrario, el alcance de la invención se define sólo por las reivindicaciones siguientes.

REIVINDICACIONES

1.- Sistema que comprende:

un registro de desplazamiento con retroalimentación que tiene:

L etapas conectadas en serie que incluyen una primera etapa y una etapa final, estando denotadas las etapas de 0 a L-1, desde la primera etapa a la etapa final, respectivamente, estando operativas las etapas para almacenar una pluralidad de bits, de manera que cada una de las etapas está operativa para almacenar uno de los bits; y

un reloj conectado operativamente al registro de desplazamiento con retroalimentación, estando operativo el reloj para controlar el movimiento de los bits a lo largo de las etapas;

un sub-sistema de retroalimentación no lineal, teniendo al menos algunas de las etapas una salida conectada operacionalmente al sub-sistema de retroalimentación no lineal,

caracterizado porque

el sub-sistema de retroalimentación no lineal está operativo para recibir una entrada desde una etapa n, una etapa 2n+1, una etapa m, una etapa 2m+1, una etapa k y una etapa 2k+1 de entre las etapas, siendo n, m y k diferentes, incluyendo el sub-sistema de retroalimentación no lineal (i) una primera puerta lógica AND, teniendo la primera puerta lógica AND: una primera entrada conectada operacionalmente a la salida de la etapa n; una segunda entrada conectada operacionalmente a la salida de la etapa 2n+1; y una salida; (ii) una segunda puerta lógica AND y una primera puerta lógica XOR, teniendo la segunda puerta lógica AND: una primera entrada conectada operacionalmente a la salida de la etapa m; una segunda entrada conectada operacionalmente a la salida de la etapa 2m+1; y una salida, teniendo la primera puerta lógica XOR: una primera entrada conectada operacionalmente a la salida de la primera puerta lógica AND; y una segunda entrada conectada operacionalmente a la salida de la segunda puerta lógica AND; una tercera puerta lógica

AND y una segunda puerta lógica XOR, teniendo la tercera puerta lógica AND: una primera entrada conectada operacionalmente a la salida de la etapa k; una segunda entrada conectada operacionalmente a la salida de la etapa 2k+1; y una salida, teniendo la segunda puerta lógica XOR: una primera entrada conectada operacionalmente a la salida de la primera puerta lógica XOR; una segunda entrada conectada operacionalmente a la salida de la tercera puerta lógica AND; y una salida, en el que el sub-sistema de retroalimentación no lineal tiene una salida basada, al menos en parte, en un valor de la salida de la segunda puerta lógica XOR, y

teniendo además el registro de desplazamiento con retroalimentación:

un generador de bits que tiene una salida, estando operativo el generador de bits para generar una pluralidad de bits aleatorios/pseudo-aleatorios para presentarlos en la salida del generador de bits; y

una puerta lógica XOR principal que tiene una primera entrada y una segunda entrada y una salida, estando conectada operacionalmente la salida del generador de bits a la primera entrada de la puerta lógica XOR principal, estando conectada operacionalmente la salida del subsistema de retroalimentación no lineal a la segunda entrada de la puerta lógica XOR principal, estando conectada operacionalmente la salida de la puerta lógica XOR principal a la entrada de la primera etapa del registro de desplazamiento con retroalimentación.

2.- Sistema según la reivindicación 1, en el que el generador de bits está operativo de manera que la salida del generador de bits esté sesgada según un estado de las etapas del registro de desplazamiento con retroalimentación.

3.- Sistema según cualquiera de las reivindicaciones 1-2, que comprende además un planificador que tiene una entrada conectada operacionalmente a la puerta lógica XOR principal o el registro de desplazamiento con retroalimentación, estando operativo el planificador para planificar una pluralidad de estados de espera según los datos recibidos en la entrada del planificador.

4.- Procedimiento que comprende:

proporcionar un registro de desplazamiento con retroalimentación que tiene L etapas conectadas en serie, que incluyen una primera etapa y una etapa final, estando denotadas las etapas de 0 a L-1, desde la primera etapa a la etapa final, respectivamente, estando operativas las etapas para almacenar una pluralidad de bits, de manera que cada una de las etapas está operativa para almacenar uno de los bits; y

realizar lo siguiente una pluralidad de veces:

realizar una operación de puerta lógica AND con la salida de una etapa n y una etapa 2n+1 de las etapas como entrada, proporcionando un primer resultado;

realizar una operación de puerta lógica AND con la salida de una etapa k y una etapa 2k+1 de las etapas como entrada, proporcionando un segundo resultado;

realizar una operación de puerta lógica AND con la salida de una etapa m y una etapa 2m+1 de las etapas como entrada, proporcionando un tercer resultado, siendo n, m y k diferentes;

realizar una operación de puerta lógica XOR usando el primer resultado, el segundo resultado y el tercer resultado como entrada, proporcionando un cuarto resultado;

generar un bit aleatorio/pseudo-aleatorio;

realizar una operación de puerta lógica XOR con el bit y el cuarto resultado como entrada, proporcionando un quinto resultado

desplazar los bits a lo largo de las etapas; e

insertar el quinto resultado en la primera etapa.

5.- Procedimiento según la reivindicación 4, que comprende además sesgar la generación del bit aleatorio/pseudo-aleatorio según un estado de las etapas del registro de desplazamiento con retroalimentación.

6.- Procedimiento según la reivindicación 4 y la reivindicación 5, que comprende además planificar una pluralidad de estados de espera según el quinto resultado.

FIG. 1

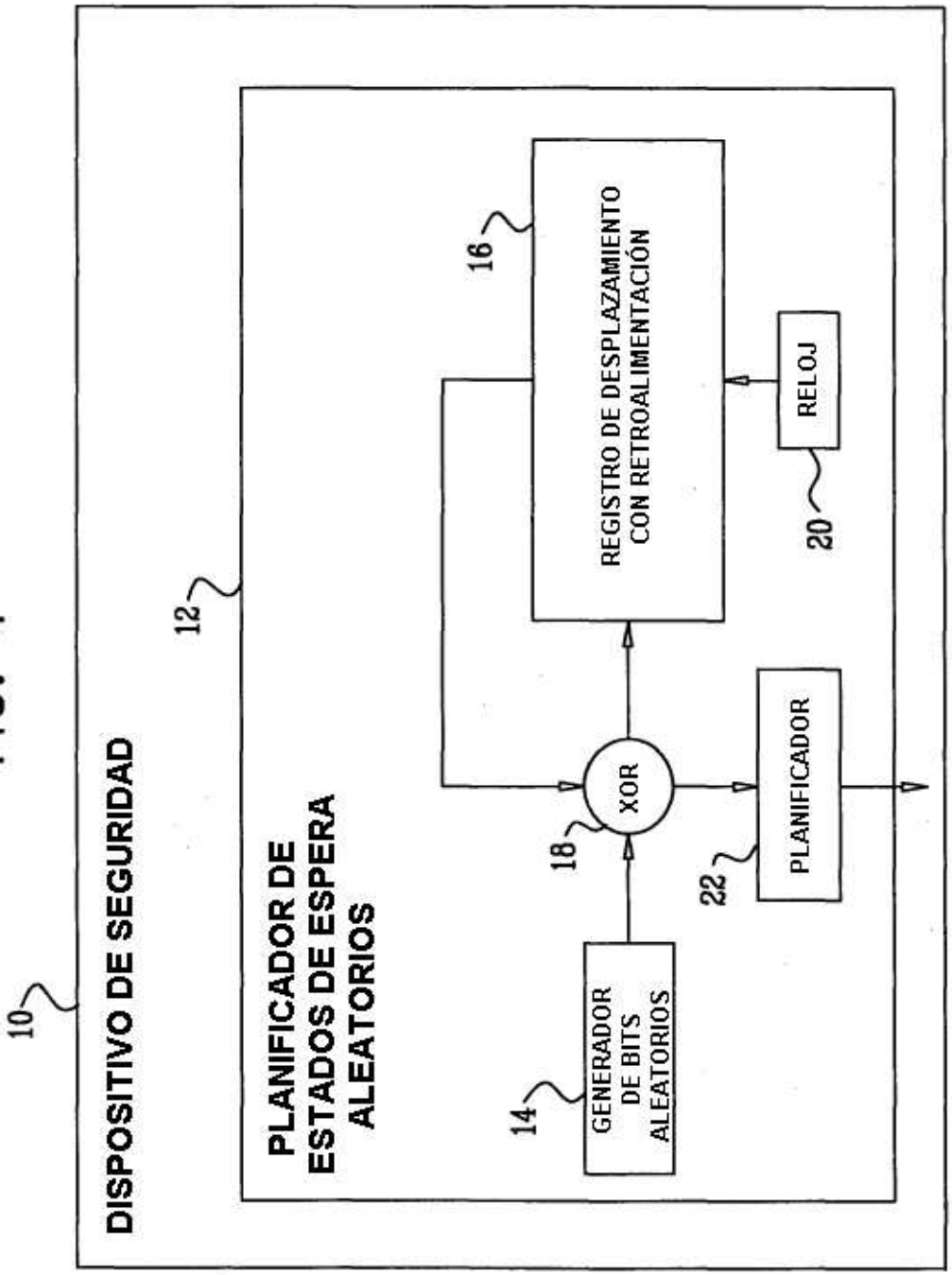

DISPOSITIVO DE SEGURIDAD
10
PLANIFICADOR DE ESTADOS DE ESPERA ALEATORIOS
12
GENERADOR DE BITS ALEATORIOS
14
XOR
18
REGISTRO DE DESPLAZAMIENTO CON RETROALIMENTACIÓN
16
RELOJ
20
PLANIFICADOR
22

FIG. 2

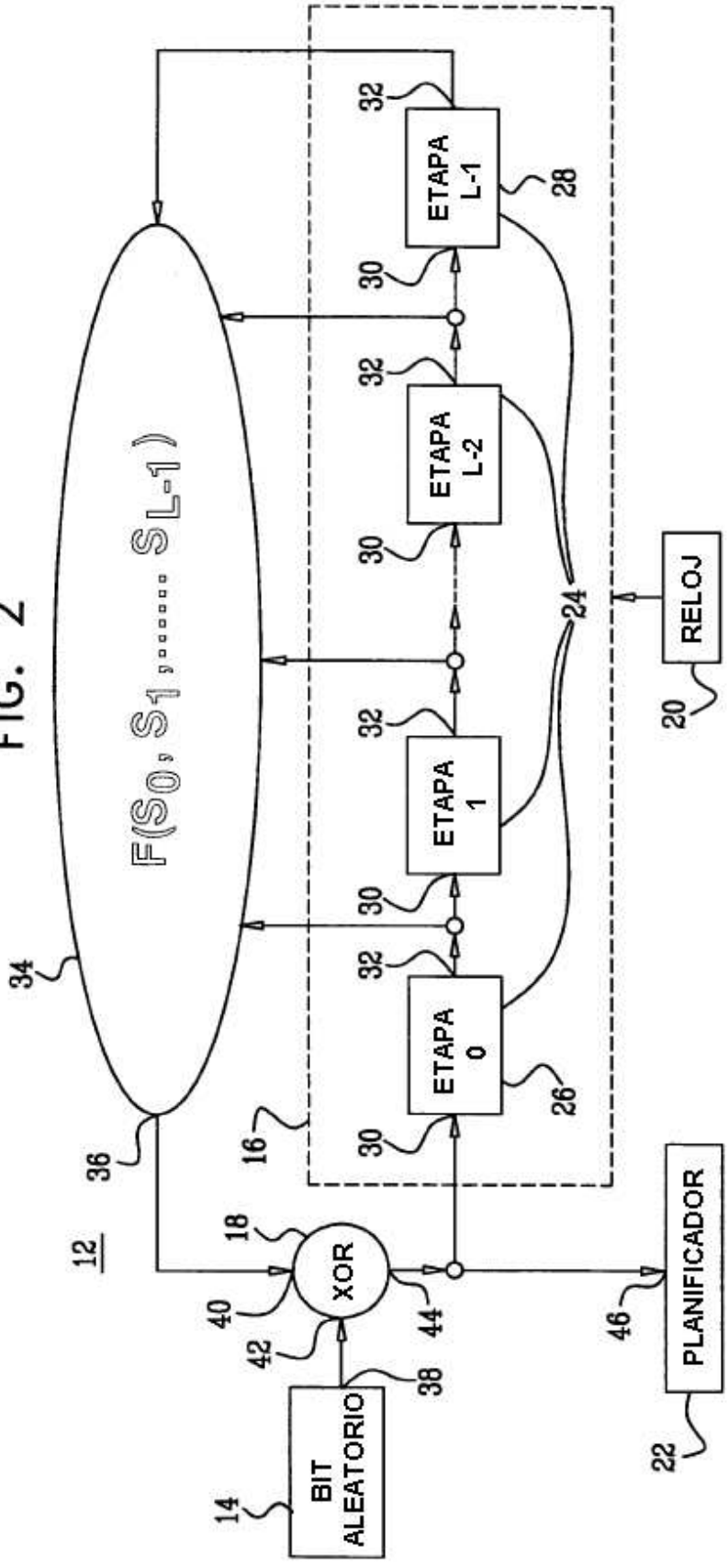
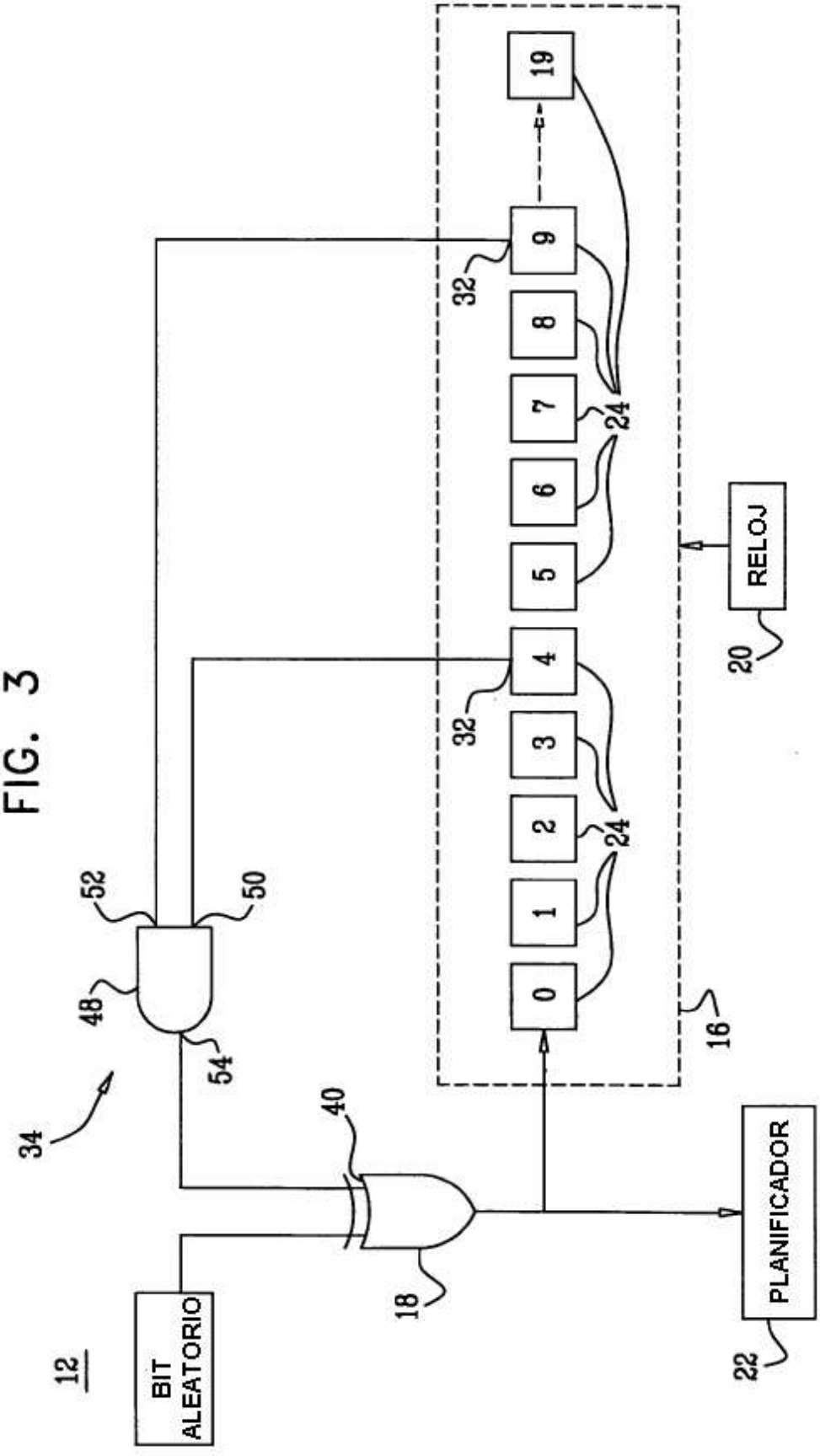

F(S0, S1 ..... SL-1)
34
36
12
16
18
XOR
40
42
44
38
BIT ALEATORIO
14
ETAPA 0
ETAPA 1
ETAPA L-2
ETAPA L-1
26
28
30
32
24
RELOJ
20
PLANIFICADOR
46
22

FIG. 3


12
BIT ALEATORIO
18
40
34
48
52
50
54
0
1
2
3
4
5
6
7
8
9
19
32
24
16
RELOJ
20
PLANIFICADOR
22

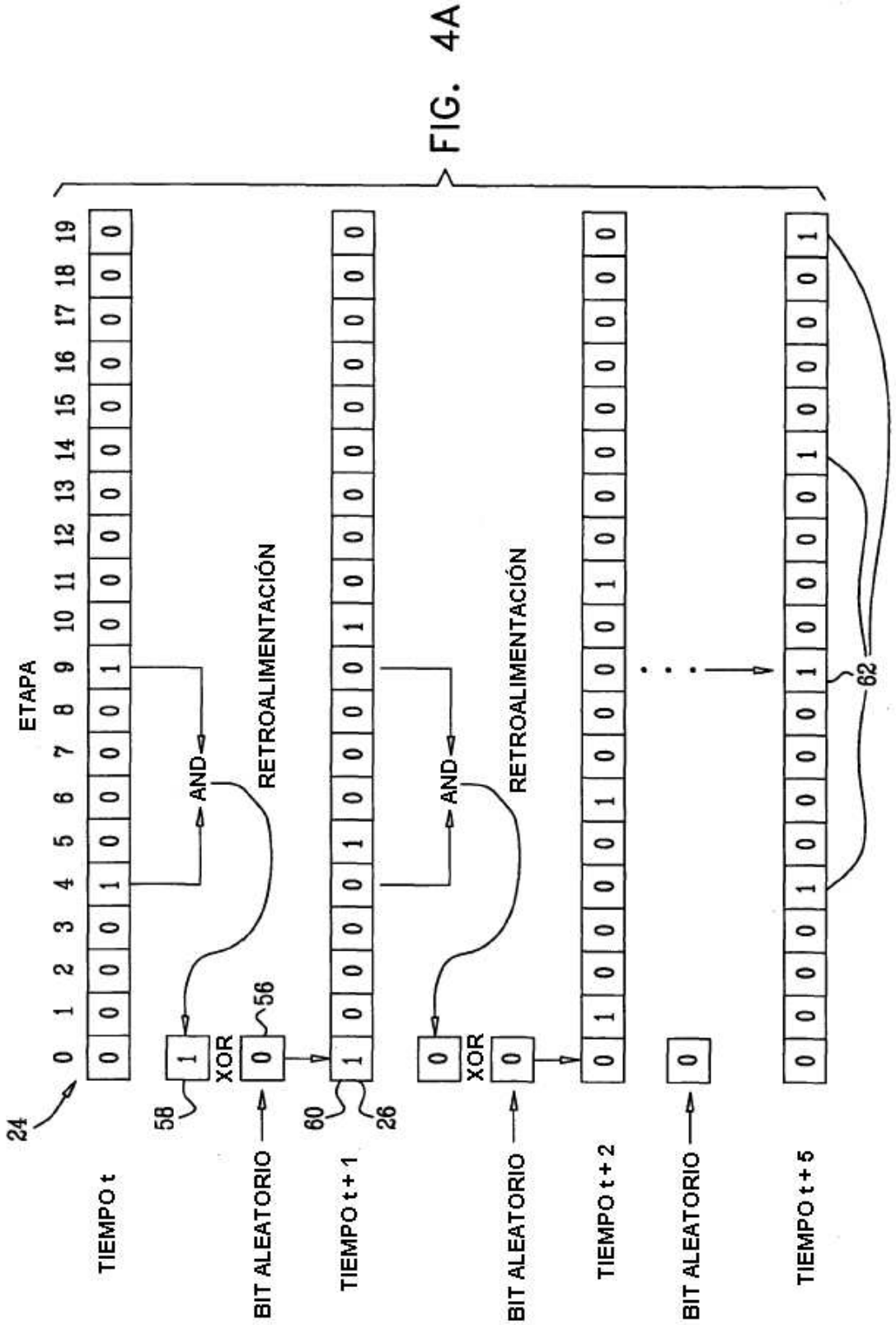

ETAPA
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
24
TIEMPO t
AND
RETROALIMENTACIÓN
58
XOR
56
BIT ALEATORIO
TIEMPO t+1
60
26
AND
RETROALIMENTACIÓN
XOR
BIT ALEATORIO
TIEMPO t+2
BIT ALEATORIO
TIEMPO t+5
62

FIG. 4A

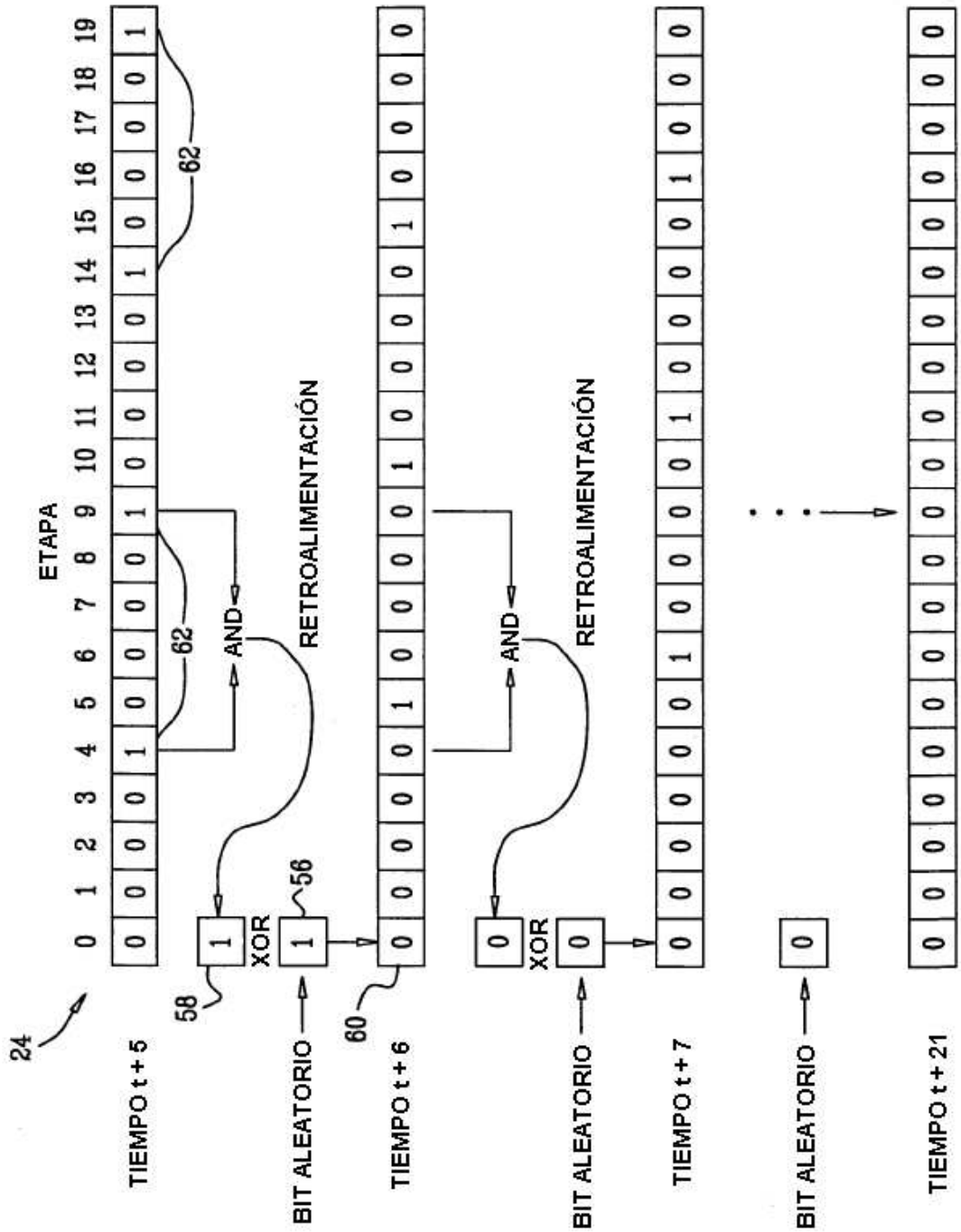
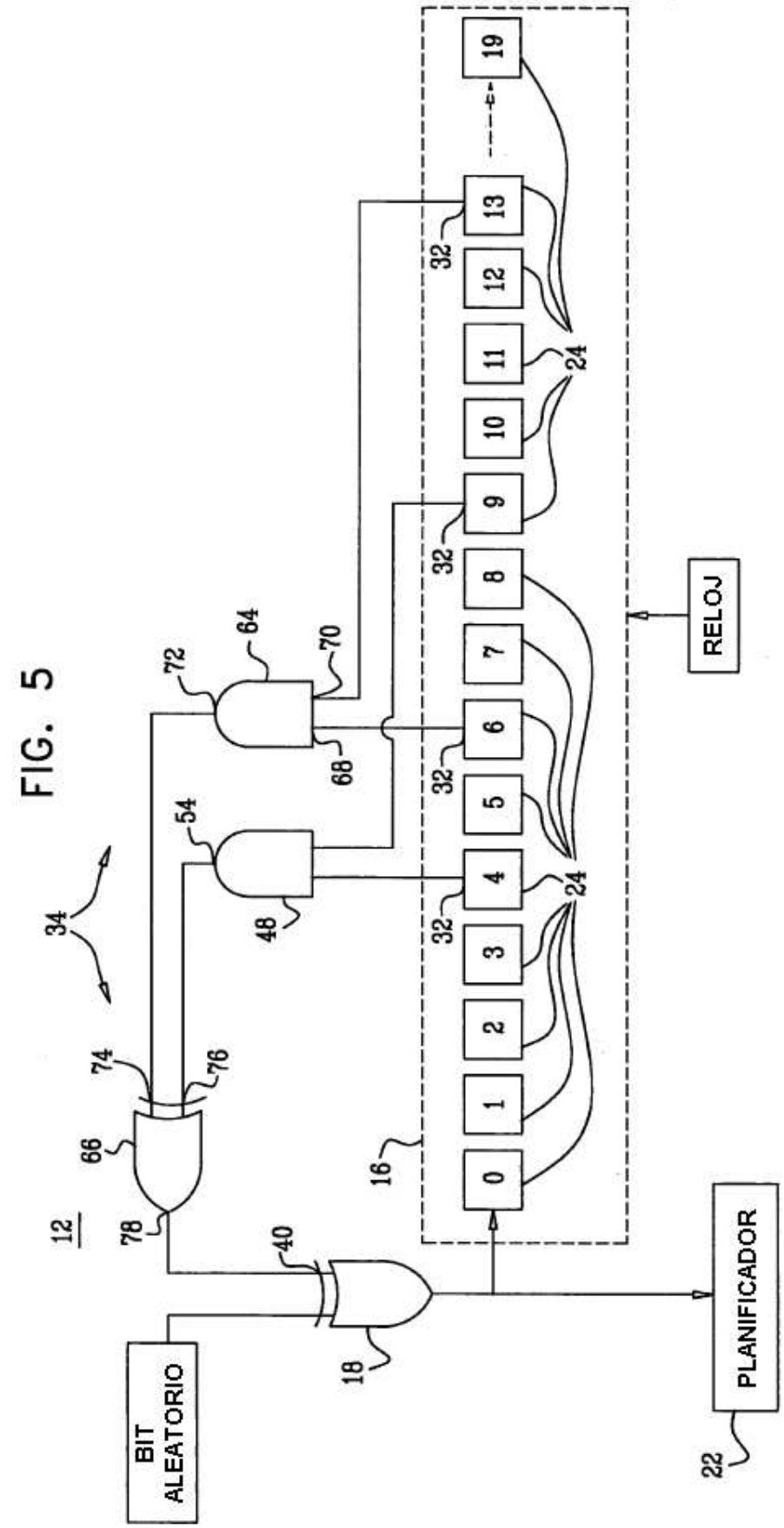

24
ETAPA
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
TIEMPO t+5
62
AND
RETROALIMENTACIÓN
58
XOR
56
BIT ALEATORIO
60
TIEMPO t+6
AND
RETROALIMENTACIÓN
XOR
BIT ALEATORIO
TIEMPO t+7
BIT ALEATORIO
TIEMPO t+21

FIG. 4B

FIG. 5


BIT ALEATORIO
PLANIFICADOR
RELOJ
12
16
18
22
34
40
48
54
64
66
68
70
72
74
76
78
24
32
0
1
2
3
4
5
6
7
8
9
10
11
12
13
19

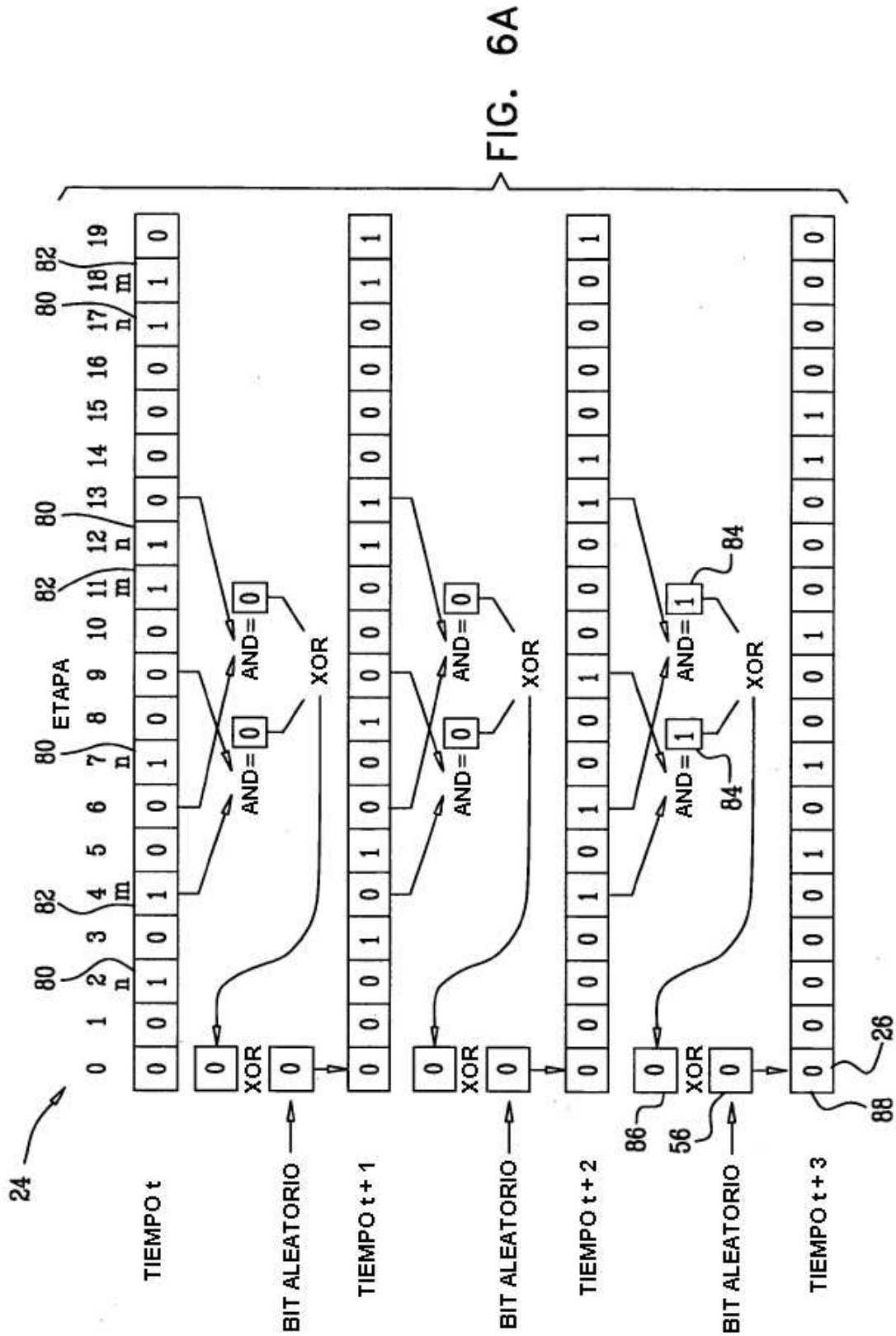

24
ETAPA
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
80 82 80 82 80 82 80
n m n m n m n
TIEMPO t
TIEMPO t+1
TIEMPO t+2
TIEMPO t+3
AND=
XOR
BIT ALEATORIO
84
86
56
88
26

FIG. 6A

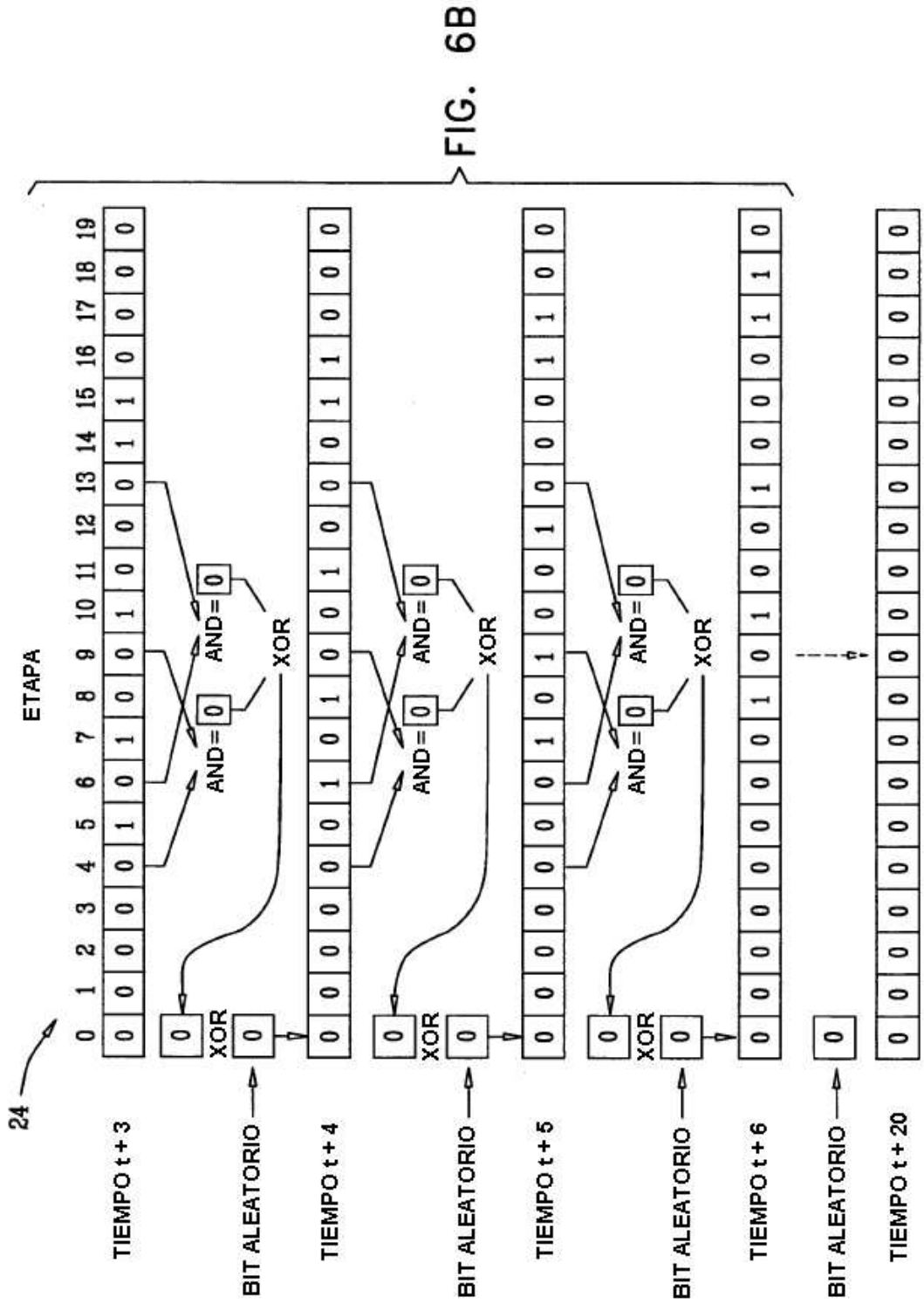
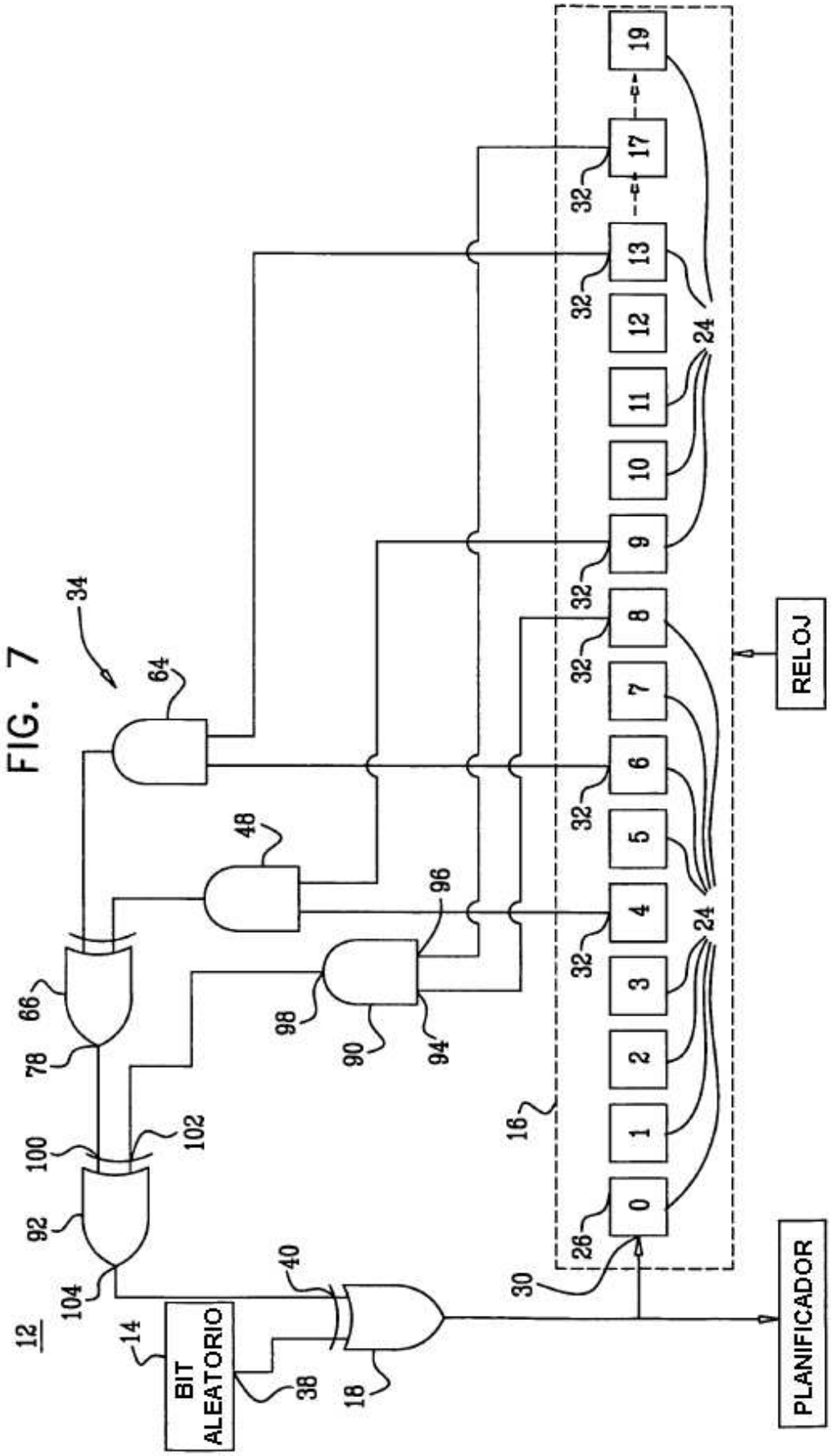

ETAPA
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
24
TIEMPO t+3
BIT ALEATORIO
TIEMPO t+4
BIT ALEATORIO
TIEMPO t+5
BIT ALEATORIO
TIEMPO t+6
BIT ALEATORIO
TIEMPO t+20
AND=
XOR

FIG. 6B

FIG. 7


12
14
BIT ALEATORIO
38
18
40
104
92
100
102
66
78
34
64
48
96
98
90
94
16
26
30
0
1
2
3
4
5
6
7
8
9
10
11
12
13
17
19
32
24
RELOJ
PLANIFICADOR

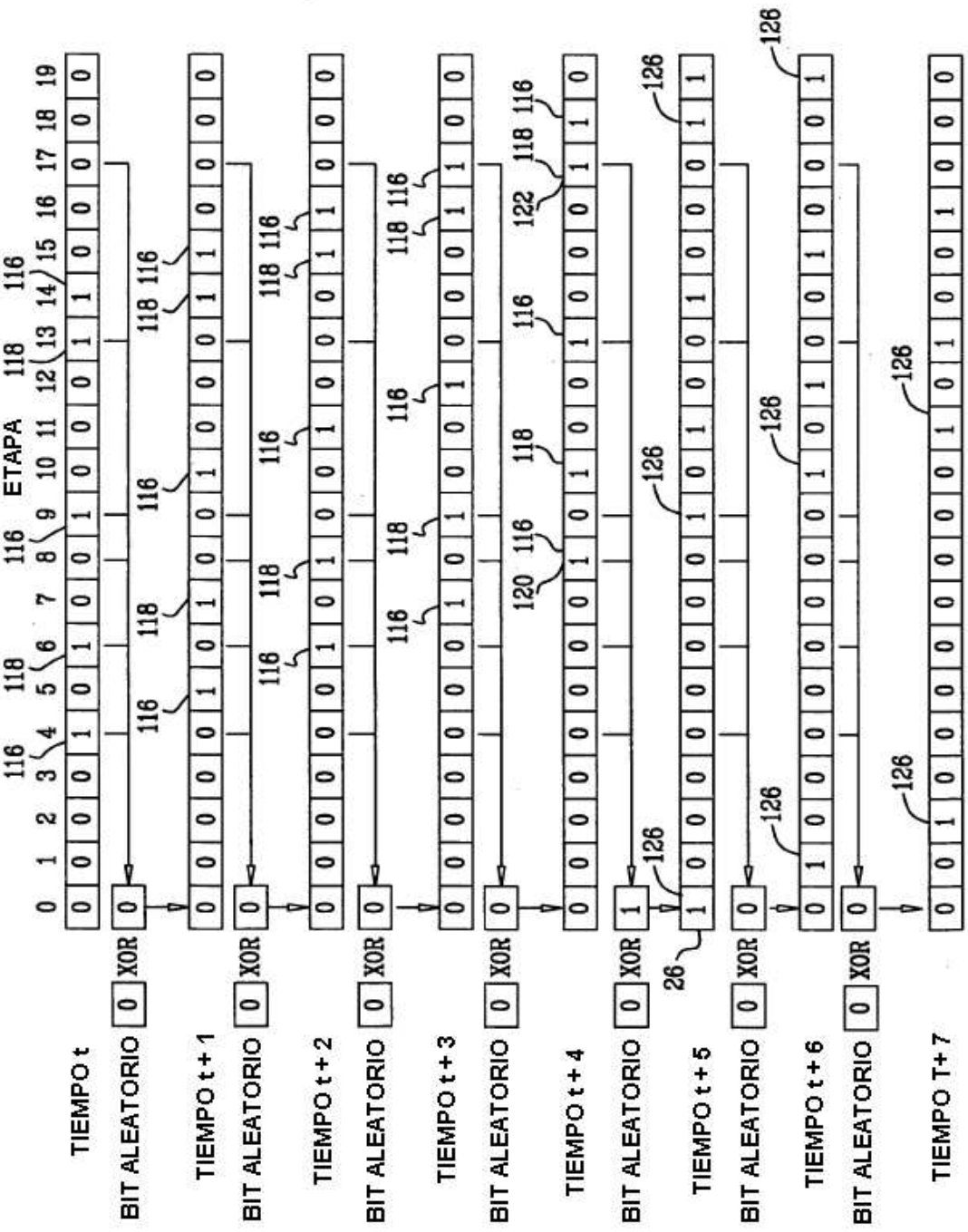
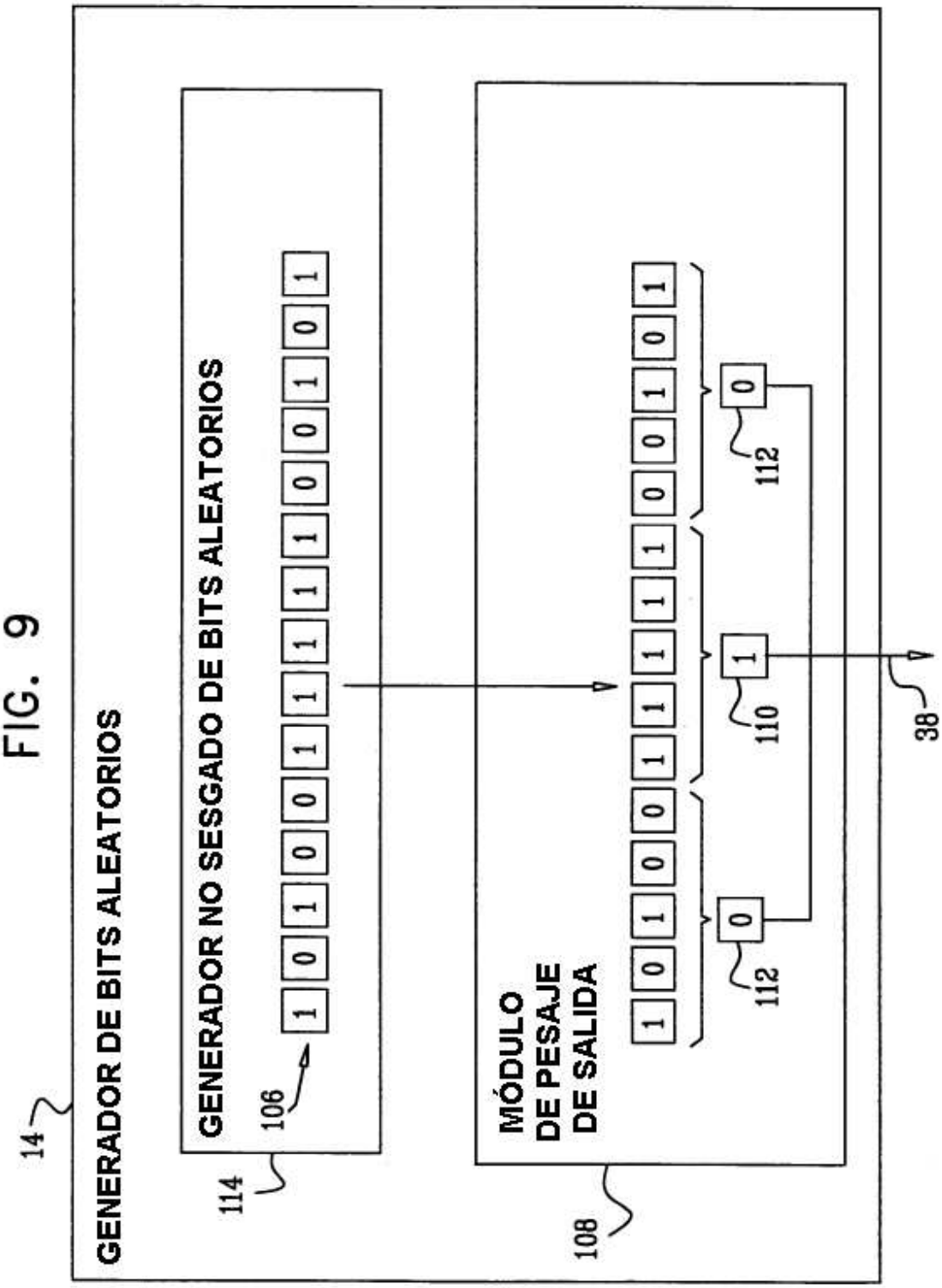

ETAPA
TIEMPO t
BIT ALEATORIO
XOR
TIEMPO t+1
TIEMPO t+2
TIEMPO t+3
TIEMPO t+4
TIEMPO t+5
TIEMPO t+6
TIEMPO T+7
116
118
120
122
126

FIG. 8

FIG. 9


GENERADOR DE BITS ALEATORIOS
14
GENERADOR NO SESGADO DE BITS ALEATORIOS
106
114
1 0 1 0 0 1 1 1 1 1 0 0 1 0 1
MÓDULO DE PESAJE DE SALIDA
108
1 0 1 0 0 1 1 1 1 1 0 0 1 0 1
112
112
110
38