(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 679**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09732686 .2**
(96) Fecha de presentación: **11.03.2009**
(97) Número de publicación de la solicitud: **2271980**
(97) Fecha de publicación de la solicitud: **12.01.2011**

(54) Título: **Dispositivo y procedimiento para generar una secuencia de bits aleatorios**

(30) Prioridad:
14.04.2008 DE 102008018678

(45) Fecha de publicación de la mención BOPI:
10.07.2012

(45) Fecha de la publicación del folleto de la patente:
10.07.2012

(73) Titular/es:
Siemens Aktiengesellschaft
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:
DICHTL, Markus

(74) Agente/Representante:
Zuazo Araluze, Alexander

DESCRIPCIÓN

Dispositivo y procedimiento para generar una secuencia de bits aleatorios.

La invención se refiere a dispositivos y procedimientos para generar bits aleatorios y secuencias de bits aleatorios. Ello sirve por ejemplo para implementar un generador de números aleatorios.

En aplicaciones relevantes para la seguridad se necesitan a menudo números aleatorios, que se presentan en forma digital como secuencias de bits aleatorios. Por ejemplo en procedimientos de autentificación asimétricos es necesario generar y utilizar números aleatorios. En particular en tags RFID (etiquetas de identificación por radiofrecuencia) con funcionalidad de seguridad han de generarse los correspondientes números aleatorios con un coste del hardware especialmente bajo. Es deseable al respecto utilizar solamente circuitos lógicos digitales, que pueden implementarse económicamente.

En el pasado se utilizaron generadores de números aleatorios por ejemplo utilizando fuentes de ruido analógicas, cuyas señales se digitalizan. No obstante, los circuitos híbridos analógico/digitales son costosos de implementar.

Un generador de números aleatorios que prácticamente presenta exclusivamente circuitos lógicos digitales se describe en el documento WO 2006/015624 A1. En esta solicitud de patente internacional se propone utilizar fluctuaciones de fase aleatorias de osciladores anulares constituidos a partir de puertas (gatter) digitales. No obstante, según el documento WO 2006/015624 A1 solamente son adecuados osciladores anulares muy especiales, a saber, osciladores anulares Fibonacci o Galois con características especiales para su utilización en un generador de números aleatorios. En un circuito eléctrico así constituido se parte de que los osciladores anulares no deben presentar ningún punto fijo. Esta condición puede representarse en particular para circuitos oscilantes Fibonacci o Galois mediante ecuaciones matemáticas, que deben cumplirse según el documento WO 2006/015624 A1. Por lo tanto en la correspondiente implementación ha de comprobarse primeramente si un oscilador anular presenta puntos fijos. Por ello es un inconveniente que la posibilidad de elección de circuitos oscilantes adecuados sea muy limitada.

El documento Keerat Brar y colab.: “True Random Number Generators” (generadores de números aleatorios auténticos), Course Cryptography and Computer Network Security ECE646, Fall 2007, George Manson University, Department of Electrical and Computer Engineering, Fairfax, Virginia, USA, páginas 1-5, diciembre 2007, da a conocer un oscilador anular Fibonacci con una ruta de realimentación, con ayuda del cual pueden generarse números pseudo-aleatorios.

El documento WO 2009/109959 A1 da a conocer un sistema para generar números pseudo-aleatorios con un circuito oscilante anular, que puede presentar diversas configuraciones y un componente de aleatorización que alterna entre las configuraciones del circuito oscilante anular en función de un flujo de números pseudo-aleatorios.

Es por lo tanto una tarea de la presente invención lograr un dispositivo mejorado para generar bits aleatorios.

Esta tarea se resuelve mediante un dispositivo con las características de la reivindicación 1.

Según ello presenta un dispositivo para generar una secuencia de bits aleatorios un circuito oscilante anular digital con al menos una primera ruta de realimentación y una segunda ruta de realimentación. Entonces se realiza en instantes que pueden predeterminarse una conmutación entre las rutas de realimentación y en un nodo de salida del circuito oscilante anular puede tomarse una señal aleatoria con una evolución aleatoria del nivel de la señal. El circuito oscilante anular presenta además un nodo de entrada y está configurado tal que cuando tiene lugar un cambio de estado de una señal de arranque lógica acoplada al nodo de entrada, tiene lugar una oscilación.

En circuitos oscilantes anulares digitales está realimentado por lo general un número impar de puertas lógicas (gatter). Esto significa que la salida de una de las puertas lógicas está combinada con la entrada de otra puerta lógica. De esta manera pueden resultar oscilaciones que bajo determinadas condiciones asumen formas de señal no predecibles, es decir, representan señales aleatorias. Se prevé ahora disponer de varias rutas de realimentación posibles entre las que puede conmutarse. De esta manera pueden lograrse una característica aleatoria mejorada para la señal aleatoria. Mediante la conmutación, que provoca características de oscilación variables en el oscilador anular, pueden generarse así bits aleatorios sin un gran coste.

Debido a procesos térmicos o de mecánica cuántica, dentro de los componentes semiconductores utilizados para implementar el oscilador, resultan por ejemplo fluctuaciones de fase o jitter, que provocan evoluciones internas aleatorias de la señal o del potencial. Los componentes lógicos, por ejemplo un número impar de circuitos inversores, pueden estar acoplados, por ejemplo para formar un oscilador anular, en forma de cascada para constituir un anillo. Por lo general depende la frecuencia de oscilación básica de la cantidad de circuitos inversores o lógicos utilizados. Debido a los distintos retardos que se presentan en el tratamiento de la señal por causa de los distintos componentes lógicos, no resulta por lo general una fase constante, sino una fluctuación de fase o jitter, con lo que a menudo se presentan formas de señal irregulares.

No obstante, no puede partirse básicamente de que también para largos periodos exista siempre una "curva de oscilación" absolutamente aleatoria. Cada circuito oscilante anular presenta en su curva de señal, tras su activación o arranque, evoluciones aleatorias en el tiempo del nivel de la señal, que básicamente pueden desembocar, desde luego también después de un proceso de estabilización de la señal, en una curva determinística.

Mediante la conmutación de las rutas de realimentación, se evita no obstante que el transitorio de arranque se estabilice por ejemplo en un punto fijo. Puede modificarse por ejemplo, controlada por impulsos o periódicamente, la correspondiente realimentación del circuito oscilante anular. Incluso cuando el concepto básico del correspondiente oscilador anular tiende a oscilaciones periódicas y esto parece por lo tanto a priori inadecuado para generar señales aleatorias, se logra mediante la conmutación que tales oscilaciones potencialmente periódicas se vean perturbadas. Se establece así de esta manera siempre un comportamiento de la oscilación aleatorio no periódico, a partir del que puede obtenerse una gran entropia para la generación a continuación de valores de bits aleatorios. Es posible entonces utilizar también osciladores anulares Fibonacci o Galois más cortos, con lo que se reduce el costo de hardware y de implementación. Una conmutación tiene lugar por ejemplo tal que se conmuta entre al menos dos realimentaciones Galois o Fibonacci distintas.

El dispositivo para generar una secuencia de bits aleatorios tiene por lo tanto en particular la ventaja de que es fácil de implementar y no tienen que realizarse cálculos como los que son necesarios según el estado de la técnica para excluir un punto fijo. Como circuitos oscilantes anulares puede tomarse así un surtido mayor de osciladores. Además, los osciladores anulares generales, que se encuentran en uno o en otro estado de servicio en función de la realimentación ajustada, tienen la ventaja de que incluso cuando se alcanza el punto fijo, lo cual no es nocivo en el dispositivo propuesto para generar una secuencia de bits aleatorios en cuanto a la calidad de la aleatoriedad, el consumo de energía desciende fuertemente. Esto es así en particular en una implementación de las correspondientes configuraciones de circuitos en tecnología CMOS.

La conmutación entre rutas de realimentación posibilita la utilización de sólo unos pocos componentes lógicos conectados en serie. De esta manera se logra un ahorro de energía adicional. Se prevé por ejemplo en un ejemplo de ejecución solamente un equipo de conmutación adicionalmente, que en instantes predeterminados realiza una conmutación de la ruta de realimentación. Esto puede realizarse por ejemplo en función de una señal de conmutación. La señal de conmutación corresponde preferiblemente a un impulso externo, con el que se realiza periódicamente una conmutación entre las rutas de realimentación.

Mediante la implementación especialmente económica, que preferiblemente presenta exclusivamente componentes digitales, es especialmente favorable una realización a modo de un circuito FPGA. Bajo FPGA se entienden circuitos integrados programables en la técnica digital. Los FPGAs pueden programarse "en campo" mediante una configuración de estructuras internas que pueden formar puertas lógicas (FPGA = Field Programable Gate Array, conjunto de puertas programable en campo". Evidentemente puede realizarse el correspondiente dispositivo para generar números aleatorios también como circuito integrado específico de la aplicación (ASIC = Application Specific Integrated Circuit), por ejemplo en CMOS. El dispositivo, mejorado respecto a las configuraciones usuales de circuitos para generar señales aleatorias, puede también constituirse a partir de componentes discretos, cuando por ejemplo se sustituye o reestructura un generador de bits aleatorios anterior ya utilizado, para aumentar la aleatoriedad de la señal generada.

En una forma constructiva del dispositivo, está previsto un elemento de memoria intermedia acoplado al nodo de salida, que en función de la señal aleatoria memoriza un nivel de señal lógico.

Es posible por ejemplo configurar un elemento de memoria intermedia como flip-flop, que al pasar por un valor lógico de umbral que previamente puede determinarse cambia su estado interno memorizado. Los flip-flops conocidos cambian por ejemplo de estado lógico memorizado internamente con cada flanco de señal ascendente o descendente de la señal aleatoria acoplada. Es decir, siempre que la señal aleatoria oscile de manera irregular entre dos niveles lógicos, aporta el elemento de memoria intermedia un valor de bit aleatorio, que depende de la cantidad, que no puede determinarse, de por ejemplo flancos ascendentes o descendientes de la señal aleatoria. Por ejemplo puede memorizar el elemento de memoria intermedia un nivel lógico correspondiente a la señal aleatoria.

Puede pensarse al respecto que el elemento de memoria intermedia, como por ejemplo un flip-flop, memorice en función de una señal de exploración un nivel lógico correspondiente a la señal aleatoria. Una señal de exploración, por ejemplo una señal de impulso externa, da lugar a que en determinados instantes el nivel de la señal aleatoria sea detectado por el elemento de memoria intermedia y bien se utilice como bit aleatorio o también provoque una inversión de nivel lógico memorizado en el elemento de memoria intermedia. La señal de conmutación para conmutar entre las rutas de realimentación puede presentar preferiblemente una frecuencia más elevada que la señal de exploración. No obstante, también puede pensarse que la señal de arranque, la señal de conmutación y la señal de exploración tengan la misma frecuencia y sean síncronas o decaladas en el tiempo entre si. Esto último tiene la ventaja de que no son necesarios equipos distintos de generación de señal para las señales.

La correspondiente señal de arranque para el rearranque del oscilador anular puede aportarla por ejemplo un equipo generador de señales rectangulares, que genera una señal de arranque con niveles lógicos cambiantes. En este sentido se arranca de nuevo regularmente el circuito oscilante anular utilizado y muestra un comportamiento aleatorio en el transitorio de arranque.

En una forma constructiva preferente del dispositivo, se prevé un equipo de control que por ejemplo origina según una programación la toma de un valor de bit aleatorio en el nodo de salida o elemento de memoria intermedia y/o la generación de la señal de arranque y/o de la señal de conmutación.

La generación de una secuencia de bits aleatorios puede realizarse en particular mediante inversión de un flip-flop conectado al nodo de salida en cada paso de 0 a 1 de la señal aleatoria, pudiendo determinarse los bits aleatorios también mediante muestreo o exploración periódicos del nivel lógico memorizado transitoriamente de este flip-flop.

La invención prevé también la utilización de un circuito oscilante anular digital con al menos una primera ruta de realimentación y una segunda ruta de realimentación. Entonces se conmuta la correspondiente ruta de realimentación en instantes predeterminados y en un nodo de salida del oscilador anular puede tomarse una señal aleatoria con una curva de nivel lógico aleatoria. Esto sirve para generar al menos un bit aleatorio.

En un perfeccionamiento de la invención se propone un generador de números aleatorios con un dispositivo, antes descrito, para generar una secuencia de bits aleatorios. El mismo puede utilizarse por ejemplo en un chip de RFID. El chip presenta entonces un dispositivo para generar una secuencia de bits aleatorios y un equipo criptográfico, utilizándose varios bits aleatorios derivados de la señal aleatoria del equipo criptográfico para realizar una autentificación criptográfica, para generar una firma criptográfica y/o para generar una clave criptográfica.

La invención se refiere además a un procedimiento para generar una secuencia de bits aleatorios según la reivindicación 17.

Según ello se propone un procedimiento para generar una secuencia de bits aleatorios en el que en función de la evolución de un nivel lógico de una señal aleatoria tomada de un circuito oscilante anular digital, se determinan valores de bits aleatorios, presentando el circuito oscilante anular digital utilizado al menos una primera ruta de realimentación y una segunda ruta de realimentación. En instantes predeterminados se realiza una conmutación entre las rutas de realimentación. Entonces puede tomarse en un nodo de salida del circuito oscilante anular una señal aleatoria con una evolución del nivel lógico aleatoria. El circuito oscilante anular presenta además un nodo de entrada y está configurado tal que cuando tiene lugar un cambio de estado de una señal lógica de arranque acoplada al nodo de entrada, tiene lugar una oscilación.

En una variante del procedimiento se realizan entonces las siguientes etapas del procedimiento: Activación de un circuito oscilante anular digital, conmutación entre la primera y la segunda ruta de realimentación y toma de uno o varios valores de nivel lógico de una señal aleatoria oscilante generada por el circuito oscilante anular.

El correspondiente procedimiento puede implementarse por ejemplo mediante programación adecuada de circuitos lógicos digitales, como por ejemplo FPGAs. La activación del circuito oscilante anular puede realizarse por ejemplo mediante conexión o acoplamiento de una tensión de alimentación adecuada al correspondiente circuito. Además es posible una activación correspondiente a la respectiva implementación del circuito oscilante anular acoplando una señal de control o de arranque adecuada. Bajo activación se entiende un proceso que da como resultado una oscilación del circuito oscilante anular, preferiblemente partiendo de un estado inicial predeterminado de las puertas lógicas utilizadas.

Entonces puede activarse varias veces el circuito oscilante anular para generar varios valores de bits aleatorios. Las etapas del procedimiento propuestas pueden entonces realizarse independientemente entre si en el tiempo. En particular los procesos de conmutación entre las rutas de realimentación acentúan entonces la aleatorización en la evolución del nivel lógico.

Tal como ya se ha descrito en cuanto al dispositivo para generar una secuencia de bits aleatorios, puede explorarse la señal aleatoria varias veces y modificarse, en función del correspondiente valor del nivel lógico de la señal aleatoria, un nivel lógico de un bit aleatorio. Esto puede lograrse por ejemplo mediante un elemento de memorización intermedia, tal como se ha descrito previamente.

Otras configuraciones ventajosas de la invención son objeto de las reivindicaciones subordinadas, así como de los ejemplos de ejecución descritos a continuación.

A continuación se describirá más en detalle la invención con referencia a las figuras adjuntas y en base a algunos ejemplos de ejecución. Se muestra al respecto en

figura 1 un ejemplo de ejecución de un generador de números aleatorios;

figura 2 una primera forma constructiva de un circuito oscilante anular;
figura 3 la evolución de una señal aleatoria de la primera forma constructiva de un circuito oscilante anular;
figura 4 una segunda forma constructiva de un circuito oscilante anular;
figura 5 la evolución de una señal aleatoria de la segunda forma constructiva de un circuito oscilante anular;
figura 6 una tercera forma constructiva de un circuito oscilante anular; y
figura 7 un diagrama secuencial a modo de ejemplo de un procedimiento para generar secuencias de bits aleatorios.

En las figuras se han dotado los elementos iguales o que tienen igual función de las mismas referencias, salvo que se indique otra cosa.

En la figura 1 se representa a modo de ejemplo un generador de números aleatorios 1. El generador de números aleatorios 1 presenta un circuito oscilante anular 2 con un nodo de entrada 3 y un nodo de salida 4. En las siguientes figuras 2, 4 y 6 se muestran por ejemplo más en detalle ejemplos de ejecución de osciladores anulares.

Por ejemplo puede realizarse un oscilador anular conectando en cascada varios inversores. Los inversores o también otros componentes lógicos sirven entonces como elementos de retardo, provocando oscilaciones no predecibles de los distintos tiempos de retardo variaciones de oscilación no previsibles, las llamadas jitter. Las oscilaciones de retardo se basan por lo general en distintos factores de ruido internos y externos, como por ejemplo la implementación de hardware de los componentes y las oscilaciones de la intensidad, tensión y/o temperatura. Si el tiempo de retardo es extremadamente corto, tal como es el caso en inversores o puertas lógicas, aportan estas fluctuaciones no predecibles evoluciones aleatorias del nivel lógico de la señal básicamente oscilante que puede tomarse en el nodo de salida 4 como señal aleatoria OS.

El oscilador anular 2 presenta además una conexión 5 para una señal de conmutación CT1. Internamente tiene el circuito oscilante anular, tal como ya se ha indicado antes, componentes lógicos conectados en serie o en cascada, que no obstante pueden realimentarse a través de al menos dos rutas de realimentación distintas. En función de la señal de conmutación CT1 se modifica la ruta de realimentación en el oscilador anular 2. Con ello se logra una aleatorización adicional, ya que al variar la correspondiente ruta de realimentación se realiza una perturbación de la evolución de la señal que resulta.

El circuito oscilante anular 2 puede activarse o bien arrancarse mediante una señal de arranque ST adecuada, que está acoplada al nodo de entrada 3. Es básicamente posible que el circuito oscilante anular 2, debido a su estructura interna, presente un punto fijo, es decir, que existan estados estables, en los que los componentes lógicos presentan estados lógicos que ya no varían con el tiempo. No obstante, hasta alcanzar un tal punto fijo tiene lugar una variación prácticamente aleatoria del correspondiente nivel lógico que puede tomarse. Además, por lo general se evita por completo mediante la conmutación y con ello LA variación de la topología de conexión del oscilador anular 2, que resulte un estado estable dentro del oscilador anular.

La señal aleatoria OS se lleva por ejemplo a un elemento de memoria intermedia 8, por ejemplo un equipo flip-flop. El equipo flip-flop 8, por ejemplo un equipo flip-flop D, recibe en una entrada de datos la señal aleatoria y aporta en una salida de datos un nivel lógico memorizado transitoriamente como bit aleatorio ZB. Puesto que la señal aleatoria OS fluctúa en el tiempo y oscila aleatoriamente, puede pensarse por ejemplo que acoplando una señal de exploración, por ejemplo en forma de una señal de impulso externo CLK a una entrada de impulsos del flip-flop 8, el valor actual en el instante de exploración, es decir, por ejemplo cuando existe un flanco de subida o de caída en el impulso, de la señal aleatoria OS se capte o bien memorice transitoriamente.

La correspondiente señal de exploración o de impulso CLK se aporta en la representación a modo de ejemplo de la figura 1 mediante un equipo de control 6. El equipo de control 6 genera igualmente una señal de conmutación CT1 adecuada, que se conduce para conmutar la ruta de realimentación en el circuito oscilante anular 2 a su conexión 5 y una señal de control CT2 para controlar un generador de señal rectangular 7, que aporta la señal de arranque ST al nodo de entrada 3 del oscilador anular 2.

Mediante por ejemplo una conmutación periódica entre las rutas de realimentación y con ello entre las características de oscilación inherentes del circuito oscilante anular 2, dejan de ser críticos los puntos fijos que potencialmente existan en cuanto al número aleatorio o bien la generación de bits aleatorios. Previendo varias posibilidades de acoplamiento o bien rutas y la conmutación entre las mismas, sólo se tiene en cuenta por lo general el comportamiento en el transitorio de arranque, que no se realiza determinísticamente, al tomar la señal aleatoria OS. En este sentido es adecuado para su utilización como circuito oscilante anular todo oscilador anular convencional que se modifique tal que se prevean varias rutas alternativas de realimentación, entre las que puede conmutarse.

Puede pensarse en distintos modos de servicio en cuanto a la ejecución del generador de números aleatorios 1. Por ejemplo, tal como antes se ha descrito, puede captarse en cualquier instante de exploración la señal aleatoria OS mediante el elemento de memoria intermedia 8 y emitirse como bit aleatorio ZB. Éste se introduce por ejemplo en un

registro deslizante 9. Tras un número predeterminado de instantes de exploración, se tiene así una secuencia de bits aleatorios en el registro deslizante 9. Alternativamente, aún cuando no se representa explícitamente en la figura 1, puede controlarse también el registro deslizante mediante la señal de exploración CLK. En una salida 11 del generador de números aleatorios 1 puede tomarse entonces un numero aleatorio ZZ codificado en binario, cuyas posiciones binarias pueden leerse por ejemplo por impulsos.

Alternativamente puede estar configurado el elemento de memoria intermedia o flip-flop 8 también tal que en cada paso 0-1 o también 1-0 de la señal aleatoria OS, se modifique el valor internamente memorizado para el bit aleatorio ZB en el elemento de memoria intermedia 8. Con ello se utiliza como elemento aleatorio adicional la cantidad de fluctuaciones u oscilaciones de la señal aleatoria OS para generar un bit aleatorio. En función de la señal de exploración o de impulso CLK se emite entonces el estado de nivel lógico generado aleatoriamente en el elemento de memoria intermedia 8 como bit aleatorio ZB.

Puede pensarse además en poner a cero o bien arrancar de nuevo antes de cada generación de bits aleatorios el circuito oscilante anular 2, para reducir el peligro de alcanzar un punto fijo. Preferiblemente se prescribe al poner a cero o inicializar el circuito oscilante anular que el estado inicial, es decir, el nivel lógico de todos los componentes lógicos y digitales que se utilizan en el circuito oscilante anular 2, no correspondan al estado del punto fijo.

A continuación se describen más en detalle, circuitos oscilantes anulares a modo de ejemplo con rutas de realimentación conmutables, adecuados para su utilización en un dispositivo para generar secuencias de bits aleatorios.

En la figura 2 se representa un circuito oscilante anular 2, que presenta dieciséis componentes lógicos 12-17 conectados en serie. Entonces está realizado el componente lógico cero como puerta NAND 12 y los demás componentes lógicos 13-17 como etapas inversoras. Esta configuración es equivalente a 16 puertas inversoras dispuestas en serie. Las correspondientes señales de salida se denominan W0-W15. El primer componente lógico 12, es decir, la puerta lógica NAND, tiene dos entradas 37 y 38, de las cuales la segunda entrada 38 esta unida con el nodo de entrada 3 del oscilador anular 2. Al nodo de entrada 3 esta acoplada una señal de arranque ST. En la salida 39 de la puerta lógica NAND puede tomarse la señal aleatoria OS, que está conducida al nodo de salida 4 del oscilador anular 2.

La señal de salida W15 del último, es decir, del inversor número quince 27, está conducida como una señal exterior de realimentación R15, a la entrada 37 de la puerta lógica NAND 12. Además de esta ruta de realimentación exterior R, se toman en las salidas del primer inversor 13, del tercer inversor 15, del quinto inversor 17, del octavo inversor 20, del undécimo inversor 23 y del décimocuarto inversor 26 las correspondientes señales de salida W1, W3, W5, W8, W11 y W14 y se encuentran disponibles como señales potenciales de realimentación R1, R3, R5, R8, R11 y R14.

Las señales de realimentación R1, R3, R5 y R11 se suman mediante sumadores 29, 30, 31, 33 a la señal de realimentación exterior R15 y constituyen así rutas de realimentación, fijas e invariables. Las señales de realimentación R8 y R14 igualmente existentes pueden conectarse mediante un equipo de conmutación 28 igualmente como rutas de realimentación. Para ello están conducidas las señales de realimentación R8 y R14 a entradas 34, 35 de un equipo de conmutación 28, que en función de la señal de conmutación CT1 que llega a través de la entrada de conmutación 5 al circuito oscilante anular 2, aporta en su salida 51 una señal de realimentación RS conmutada. La señal de realimentación conmutada RS se suma mediante un sumador 32 a la ruta de realimentación exterior R15, que está acoplada con la señal de realimentación R11 a través del sumador 33. Los componentes representados como sumadores 29, 30, 31, 32, 33 corresponden a componentes XOR lógicos.

El equipo de conmutación 28 puede estar concebido un ejemplo como multiplexor. Es posible así conmutar mediante el equipo de conmutación 28 entre ambas rutas de realimentación R8 y R14. Mediante una conmutación durante el funcionamiento del circuito oscilante anular, es decir, mientras tiene lugar una oscilación o fluctuación, por lo general aleatoria, en la ruta de señalización debido a la cadena de componentes lógicos 12-27, se ve perturbada la misma, con lo que se provoca otra aleatorización de la señal aleatoria OS existente en particular en la salida del primer componente lógico 12. El oscilador anular representado en la figura 2 corresponde esencialmente a un oscilador anular Fibonacci de la longitud 16, que puede representarse con la siguiente función de realimentación:

WO = NOT(W15 XOR [(W14 AND CT2) OR (W8 AND NOT CT2)] XOR W3
XOR W11 XOR W5 XOR W11 XOR W1), con Wi + 1 = NOT Wi.

La señal aleatoria OS tiene debido a ello prácticamente un comportamiento totalmente aleatorio.

En la figura 3 se representa por ejemplo la evolución de la señal aleatoria OS para un oscilador anular implementado con FPGA según la figura 2. Al respecto se ha partido de que tiene lugar una conmutación entre ambas rutas de realimentación posibles R8 y R14 cada 10 ns. Esto puede implementarse por ejemplo mediante una realización adecuada de la señal de conmutación CT1. Por ejemplo puede equiparse la entrada de conmutación 36 del

multiplexor o del equipo de conmutación 28 con la correspondiente señal de impulsos como señal de conmutación. La evolución de la señal representada en la figura 3 se representa en función del tiempo t en ns. La señal está indicada como evolución de la tensión en cualesquiera unidades.

Se observa que no se ve ninguna evolución periódica o determinística de la señal. Mediante la conmutación entre las distintas rutas de señal de realimentación se perturba cualquier comportamiento de oscilación que resulte tal que, tal como se representa en la figura 3, resulte una evolución aleatoria de la señal. Tal como antes se ha descrito, puede tomarse mediante una toma adecuada o memorización intermedia de esta señal aleatoria OS un bit aleatorio correspondiente.

En la figura 4 se representa una segunda forma de ejecución de un oscilador anular 200. El oscilador anular 200 es igualmente un oscilador anular Fibonacci, desde luego realizado con siete inversores. Entonces está realizado el primer inversor de nuevo como puerta lógica NAND 12, a la que están conectados seis inversores 13-18 conectados en serie. En cuanto a las denominaciones de la señal, rige lo indicado para la figura 2. Básicamente es similar la estructura del oscilador anular 200 a la del oscilador anular representado en la figura 2, por lo que no entraremos de nuevo en detalle en los mismos elementos.

En la salida del primer inversor o bien puerta lógica NAND 12 puede tomarse la señal aleatoria OS y llevarse al nodo de salida 4. En las salidas de los inversores 13, 15, 17 y 18 pueden tomarse las correspondientes señales de realimentación R1, R3, R5 y R6. La última señal de realimentación R6 sirve como señal de realimentación exterior y se lleva a la entrada 37 de la puerta lógica NAND 12. Además, pueden conmutarse entre sí las rutas de realimentación R1 y R2 mediante el equipo de conmutación 28, con lo que básicamente resultan distintas arquitecturas del oscilador anular Fibonacci. La señal de realimentación R3 se suma fijamente mediante un sumador o bien una puerta lógica XOR 30 a la señal de realimentación exterior R6.

En función de una señal de conmutación CT1 se suma bien la señal de realimentación R1 o la señal de realimentación R5 como señal de realimentación conmutada RS igualmente a la señal de realimentación R6 exterior a través de un sumador o bien una puerta lógica XOR 29. Resultan así de nuevo dos posibles rutas de realimentación, que bien conducen de la salida del primer inversor 13 a la entrada 37 de la puerta lógica NAND o bien una ruta de realimentación que conduce desde la salida del quinto inversor a la entrada 37 de la puerta lógica NAND 12.

Mediante cambio del nivel de la señal de arranque RS, puede activarse el oscilador anular 200 y comienza una oscilación aleatoria. Puesto que sólo están previstos siete inversores o componentes lógicos, resulta básicamente una frecuencia muy elevada para las oscilaciones, que pueden tomarse por ejemplo a la salida de la puerta lógica NAND como señal aleatoria. Para evitar que resulten oscilaciones estables o puntos fijos, se conmuta con una frecuencia relativamente alta entre las rutas de realimentación. Esto puede ajustarse mediante ajuste de los períodos o del ritmo de los impulsos o bien de la frecuencia de la señal de conmutación CT1.

En la figura 5 se representa la evolución de la señal análogamente a la figura 3 para la señal aleatoria OS del oscilador anular 200. La curva representada en la figura 5 corresponde al caso en el que cada 100 ns se conmuta entre ambas rutas de realimentación alternativas R1 y R3. Puede observarse que resulta por ejemplo en la gama entre 50 y 120 ns una oscilación casi periódica. No obstante, conmutando en cada caso a la otra ruta de realimentación, es decir, modificando las características de oscilación del oscilador anular Fibonacci que resulta, por ejemplo a 125 ns, se perturba este comportamiento casi periódico, con lo que resulta una entropía relativamente elevada en la evolución de la señal que resulta aleatoriamente. Mediante la conmutación por ejemplo periódica, resulta un complejo comportamiento no periódico de la señal aleatoria OS que, tal como se ha descrito antes, es adecuado para generar valores de bits aleatorios.

Investigaciones de la entidad solicitante han dado como resultado que en particular en circuitos oscilantes anulares que prevén 7 o más de 7 componentes lógicos, es posible una realización fiable aleatoria de la señal. No obstante preferiblemente han de preverse más de 10 componentes lógicos conectados en serie.

En la figura 6 se representa otro ejemplo de implementación de un oscilador anular 201. Allí están previstas ocho puertas lógicas NAND 40-47 en cascada. En cada caso a una de las entradas de las puertas lógicas NAND 40-47 está acoplada la señal de arranque ST. Al respecto se ha utilizado la señal aleatoria OS existente a la salida de la puerta lógica NAND cero 40 igualmente como señal de realimentación interna R0. Otra señal de realimentación R1 a la salida de la primera puerta lógica NAND 41 realiza otra ruta de realimentación además de la ruta de realimentación exterior, que resulta mediante la señal de realimentación R6. Las correspondientes señales de realimentación están sumadas mediante puertas lógicas XOR 48, 49.

Además están previstas dos posibles rutas de realimentación alternativas, que resultan mediante las señales R4, R5 existentes a la salida de la cuarta y quinta puerta lógica NAND 44, 45. Como señal de realimentación RS conmutable, que aporta un multiplexor 28 en función de la señal de conmutación CT1, resulta así una realimentación mediante la señal de realimentación R4 ó R5. Mediante la señal de arranque y la utilización de puertas lógicas

NAND como componentes lógicos, puede activarse o iniciarse el circuito oscilante anular 201 cuando hay un cambio de 0 a 1, es decir, cuando hay un flanco lógico ascendente de la señal de arranque ST.

En la figura 7 se representa esquemáticamente a modo de ejemplo un diagrama secuencial de un procedimiento para generar secuencias de bits aleatorias. Tal como ya se ha descrito, es en particular adecuado un oscilador anular según los ejemplos de ejecución de las figuras 2, 4 ó 6 para generar señales aleatorias. Así se aporta en una etapa de preparación S0 opcional el correspondiente oscilador anular, que está configurado tal que puede conmutarse entre varias rutas de realimentación.

En etapas del proceso S11, S12 y S13 que discurren básicamente independientes entre sí en el tiempo, se arranca el correspondiente oscilador anular, por ejemplo el representado en la figura 2 (etapa S11). La señal aleatoria OS se explora (etapa S12), para deducir de ello un valor de bit aleatorio, que tiene lugar en la etapa siguiente S2. En paralelo a ello en el tiempo, se realiza continuamente en instantes predeterminados una conmutación entre las rutas de realimentación potencialmente existentes en la etapa S13.

A partir de determinados bits aleatorios, o bien de los derivados de la señal aleatoria OS, por ejemplo en la etapa S2, puede confeccionarse a continuación en la etapa S3 una secuencia de bits aleatorios. Esta secuencia de bits aleatorios corresponde a un número aleatorio codificado binariamente, que queda disponible para otras aplicaciones.

Tal como ya se ha indicado, pueden realizarse independientemente en el tiempo el arranque del oscilador anular, la exploración de la señal aleatoria OS y la conmutación entre distintas rutas de realimentación. Es posible realizar la conmutación con más frecuencia que una exploración de la señal aleatoria. Tal como ya se ha mostrado y descrito en relación con la figura 1, son posibles varias variantes de la exploración y obtención del bit aleatorio individual. Básicamente debería elegirse la frecuencia de conmutación para el cambio de una primera a una segunda ruta de realimentación tal que mientras tanto no tenga lugar ninguna oscilación periódica estable. Esto puede averiguarse por ejemplo mediante experimentos o simulaciones previos. Básicamente se ha partido de que cuantos menos componentes lógicos existan en el circuito oscilante anular, tanto mayor debe ser la frecuencia de conmutación necesaria, para interrumpir y perturbar oscilaciones periódicas que potencialmente aparezcan.

La invención, en forma de los generadores de números aleatorios, osciladores anulares y secuencias de procedimiento presentados a modo de ejemplo, logra una generación fiable de números aleatorios con un coste en hardware extremadamente bajo. Las secuencias de bits aleatorios o números aleatorios alcanzan una elevada calidad estadística y pueden utilizarse por ejemplo en procedimientos de codificación o bien algoritmos de autentificación, en particular también en chips RFID.

REIVINDICACIONES

1. Dispositivo (1) para generar una secuencia de bits aleatorios con un circuito oscilante anular digital (2) que presenta al menos una primera ruta de realimentación (R8) y una segunda ruta de realimentación (R14) y que está configurado tal que se realiza en instantes que pueden predeterminarse una conmutación entre las rutas de realimentación (R8, R14) y en un nodo de salida (4) del circuito oscilante anular (2) puede tomarse una señal aleatoria (OS) con una evolución aleatoria del nivel de señal,
caracterizado porque el circuito oscilante anular (2) presenta además un nodo de entrada (3) y está configurado tal que cuando tiene lugar un cambio de estado de una señal de arranque lógica (ST) acoplada al nodo de entrada (3), tiene lugar una oscilación.

2. Dispositivo (1) según la reivindicación 1,
en el que está previsto un equipo de conmutación (28) que en instantes predeterminados realiza una conmutación de la ruta de realimentación (RS).

3. Dispositivo (1) según la reivindicación 2,
en el que el equipo de conmutación (28) conmuta en función de una señal de conmutación (CT1) entre las rutas de realimentación (R8, R14).

4. Dispositivo (1) según una de las reivindicaciones 1 - 3,
en el que se realiza periódicamente una conmutación.

5. Dispositivo (1) según una de las reivindicaciones 1 - 4,
en el que el circuito oscilante anular (2) presenta varios elementos lógicos (12-27) conectados en serie.

6. Dispositivo (1) según la reivindicación 5,
en el que están previstos al menos siete componentes lógicos (12-27) conectados en serie.

7. Dispositivo (1) según la reivindicación 5 ó 6,
en el que los componentes lógicos (13-27) son inversores.

8. Dispositivo (1) según una de las reivindicaciones 1 - 7,
tal que el dispositivo (1) presenta un elemento de memoria intermedia (8) acoplado al nodo de salida (4), que en función de la señal aleatoria (OS) memoriza un nivel lógico.

9. Dispositivo (1) según la reivindicación 7 u 8,
en el que el elemento de memoria intermedia (8) memoriza un nivel lógico correspondiente a la señal aleatoria (OS) en función de una señal de exploración (CLK).

10. Dispositivo (1) según la reivindicación 9,
tal que el dispositivo (1) presenta un equipo de generación de la señal de exploración (6), que en instantes predeterminados genera un cambio de estado lógico de la señal de exploración (CLK).

11. Dispositivo (1) según una de las reivindicaciones 1 - 10,
tal que el dispositivo (1) presenta un equipo de generación de señal rectangular (7) acoplado al nodo de entrada (3), que genera la señal de arranque (ST) con niveles lógicos cambiantes.

12. Dispositivo (1) según una de las reivindicaciones 1 - 11,
tal que el dispositivo (1) presenta un equipo de control (5) que según una programación origina la toma de un valor de bit aleatorio en el nodo de salida (4) o elemento de memoria intermedia (8) y/o la generación de la señal de arranque (ST) y/o de la señal de conmutación (CT1).

13. Dispositivo (1) según una de las reivindicaciones 1 - 12,
en el que el circuito oscilante anular (2) está realizado a modo de un oscilador anular Galois u oscilador anular Fibonacci.

14. Dispositivo (1) según una de las reivindicaciones 1 - 13,
tal que el dispositivo (1) esta implementado como circuito FPGA.

15. Chip RFID con un dispositivo (1) según una de las reivindicaciones 1 - 14 y un equipo criptográfico,
en el que se utilizan varios bits aleatorios (ZB) obtenidos de la señal aleatoria (OS) por el equipo criptográfico para realizar una autentificación criptográfica, para generar una firma criptográfica y/o para generar una clave criptográfica.

16. Generador de números aleatorios con un dispositivo (1) según una de las reivindicaciones 1 – 14,

en el que se captan varios valores de nivel lógico de la señal aleatoria (OS) tomados en el nodo de salida (4) o de niveles lógicos (ZB) memorizados por un elemento de memoria intermedia (8) como valores de bits de un número aleatorio (ZZ).

17. Procedimiento para generar una secuencia de bits aleatorios, en el que en función de la evolución de un nivel lógico de una señal aleatoria (OS) tomada de un circuito oscilante anular digital (2), se determinan valores de bits aleatorios (ZB), presentando el circuito oscilante anular digital (2) al menos una primera ruta de realimentación (R8) y una segunda ruta de realimentación (R14) y en instantes predeterminados se realiza una conmutación entre las rutas de realimentación (R8, R14), pudiendo tomarse en un nodo de salida (4) del circuito oscilante anular (2) una señal aleatoria (OS) con una evolución del nivel lógico aleatoria,
caracterizado porque el circuito oscilante anular (2) presenta además un nodo de entrada (3) y está configurado tal que cuando tiene lugar un cambio de estado de una señal lógica de arranque (ST) acoplada al nodo de entrada (3), tiene lugar una oscilación.

18. Procedimiento según la reivindicación 17,
en el que se realizan las siguientes etapas:
- activación (S1) de un circuito oscilante anular digital (2);
- conmutación (S2) entre la primera y la segunda ruta de realimentación (R8, R14);
- toma (S2, S21) de uno o varios valores de nivel lógico de una señal aleatoria (OS) oscilante generada por el circuito oscilante anular (2).

19. Procedimiento según la reivindicación 17 ó 18,
en el que el circuito oscilante anular (2) se activa varias veces para generar varios valores de bits aleatorios.

20. Procedimiento según una de las reivindicaciones 17 – 19,
en el que se conmuta periódicamente entre las rutas de realimentación (R8, R14).

21. Procedimiento según una de las reivindicaciones 17 – 20,
en el que en función de la evolución de la señal aleatoria (OS) se determina un valor de bit aleatorio (S21, S22).

FIG 1

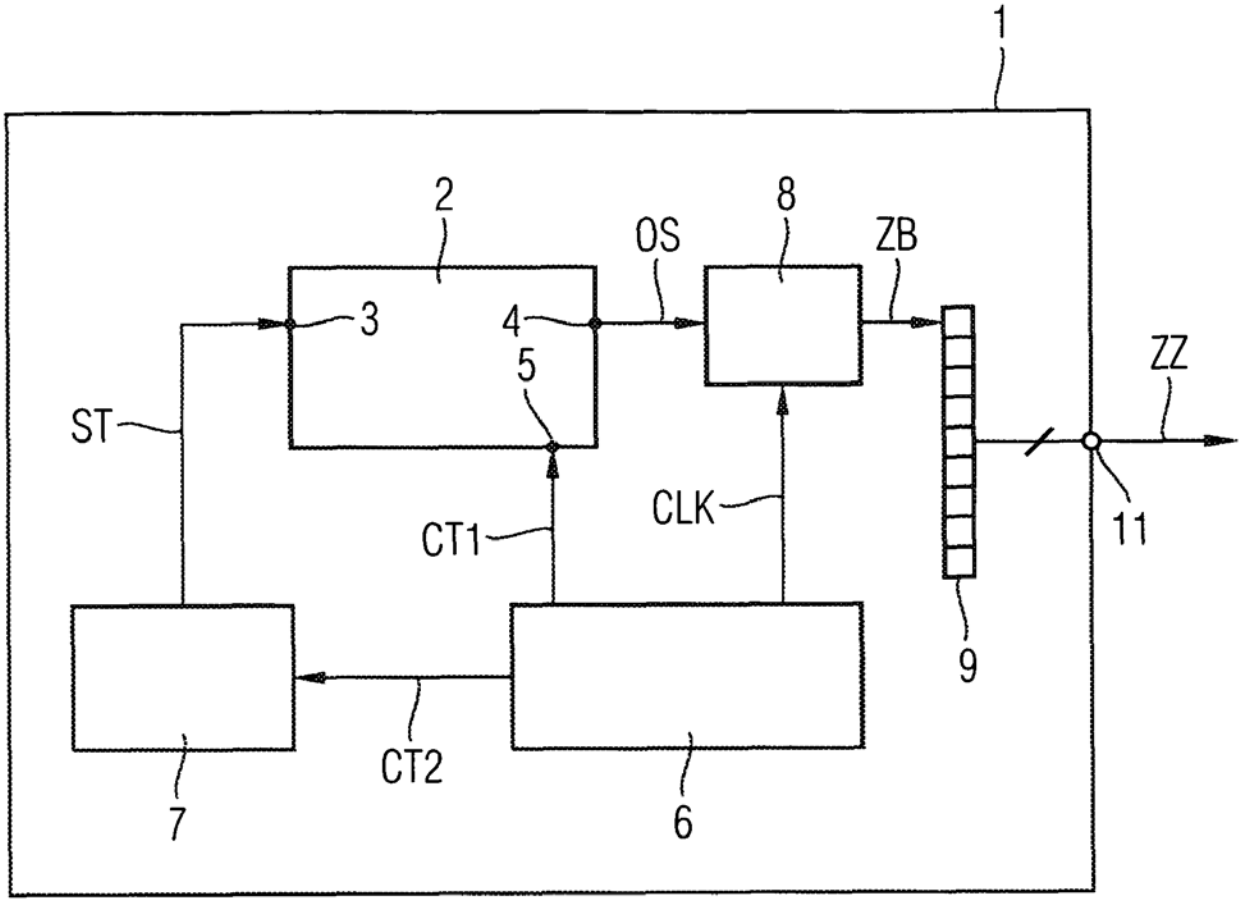


FIG 2

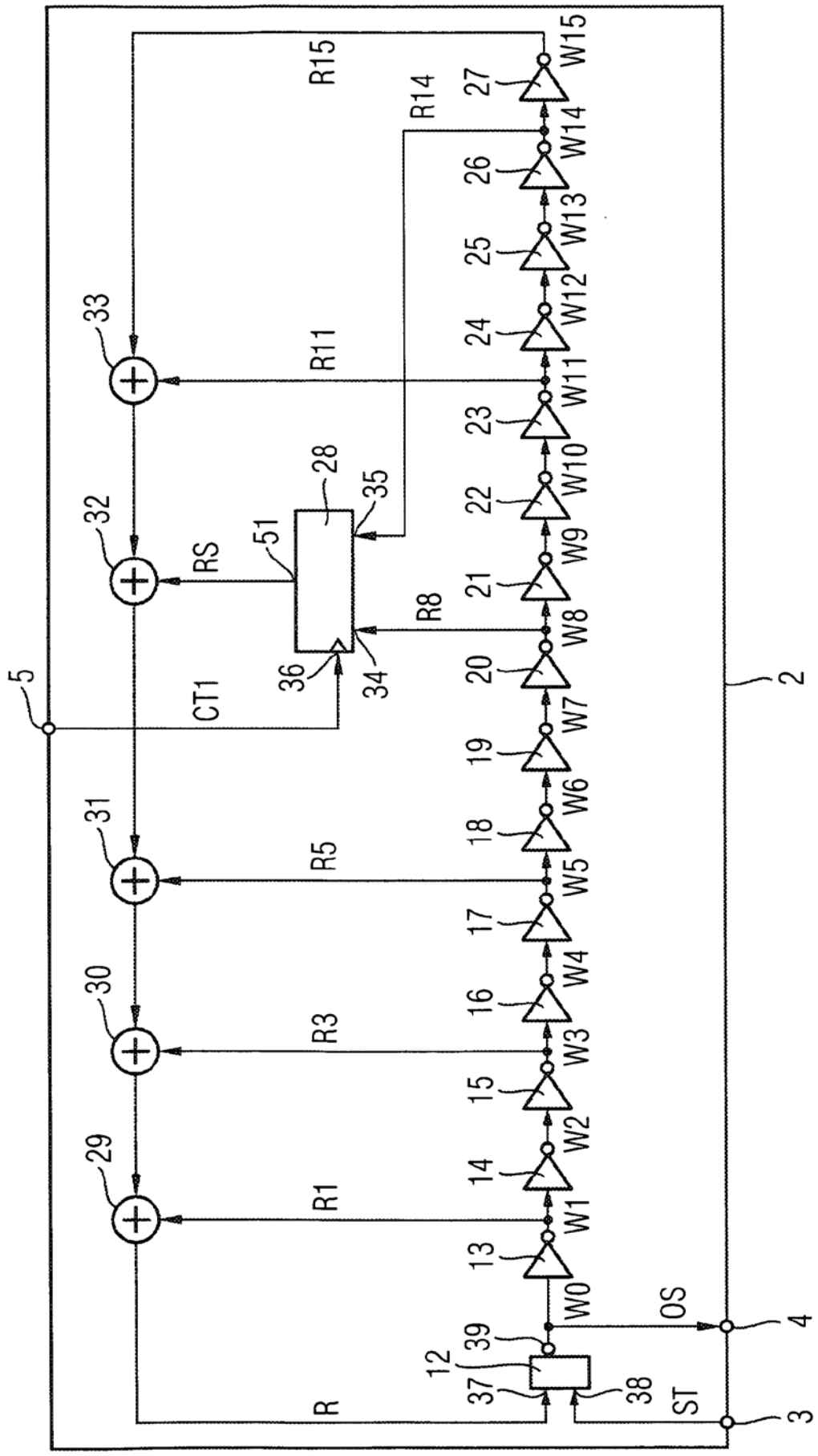

W0
W1
W2
W3
W4
W5
W6
W7
W8
W9
W10
W11
W12
W13
W14
W15
R
R1
R3
R5
R8
R11
R14
R15
RS
CT1
OS
ST
2
3
4
5
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
51

FIG 3

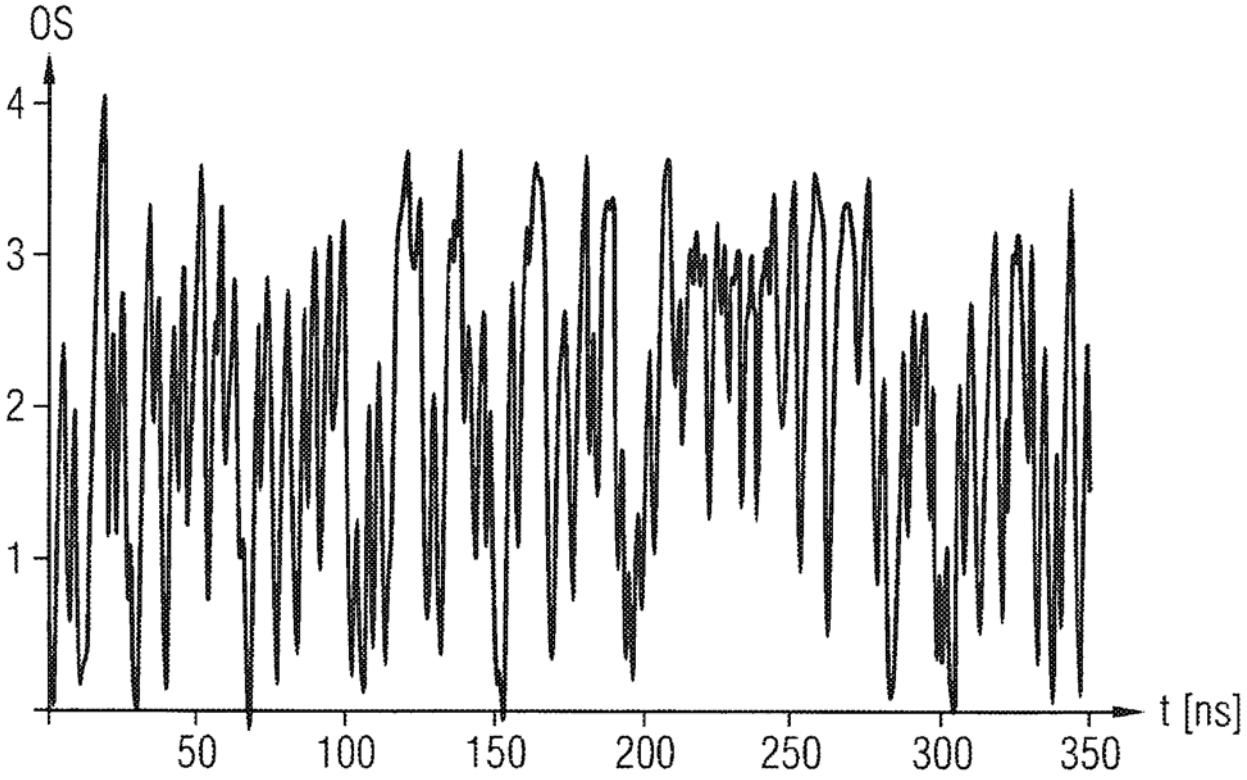


FIG 4

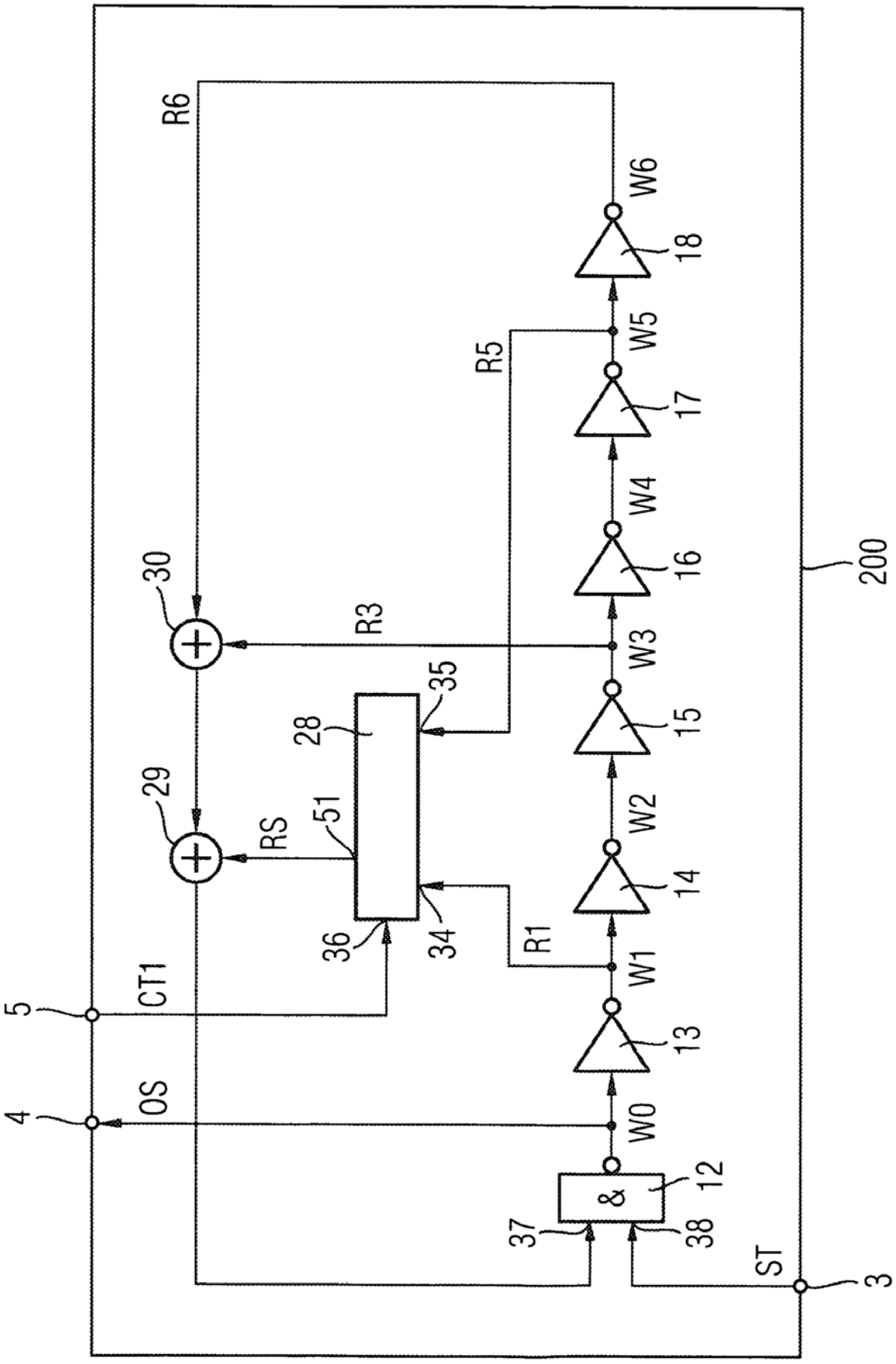

R6
W6
18
W5
R5
17
W4
16
30
R3
W3
35
28
15
29
RS
51
W2
14
36
34
R1
W1
CT1
5
13
OS
4
W0
12
&
37
38
ST
3
200

FIG 5

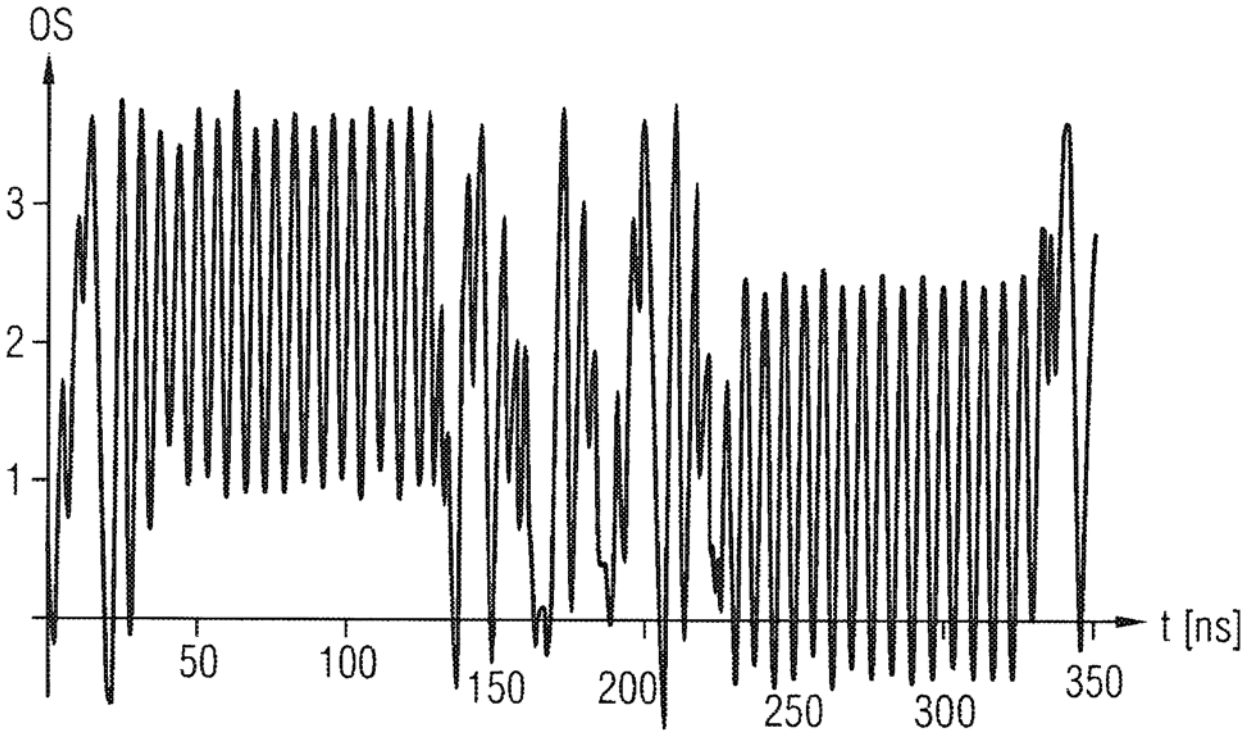


FIG 6

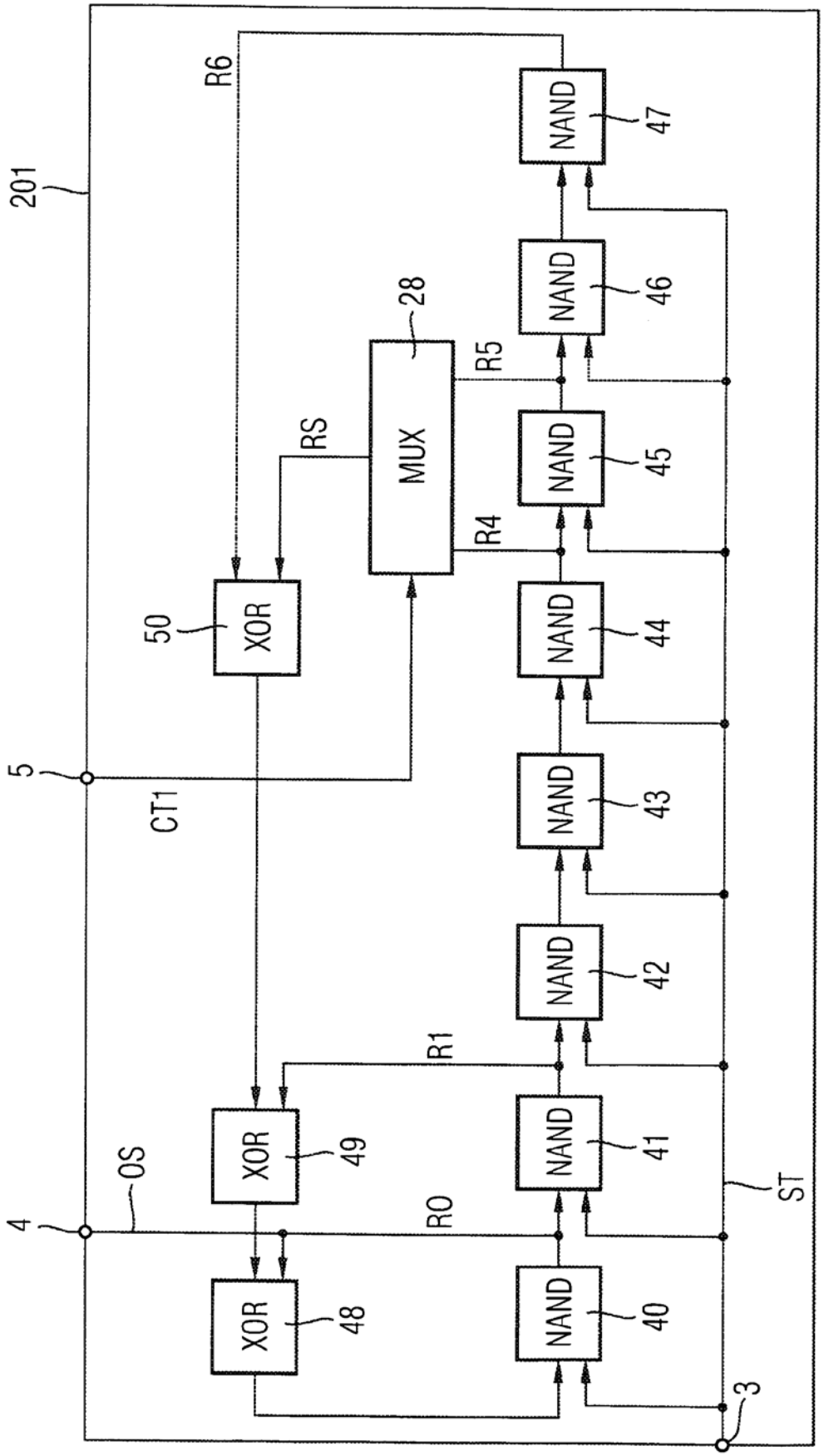
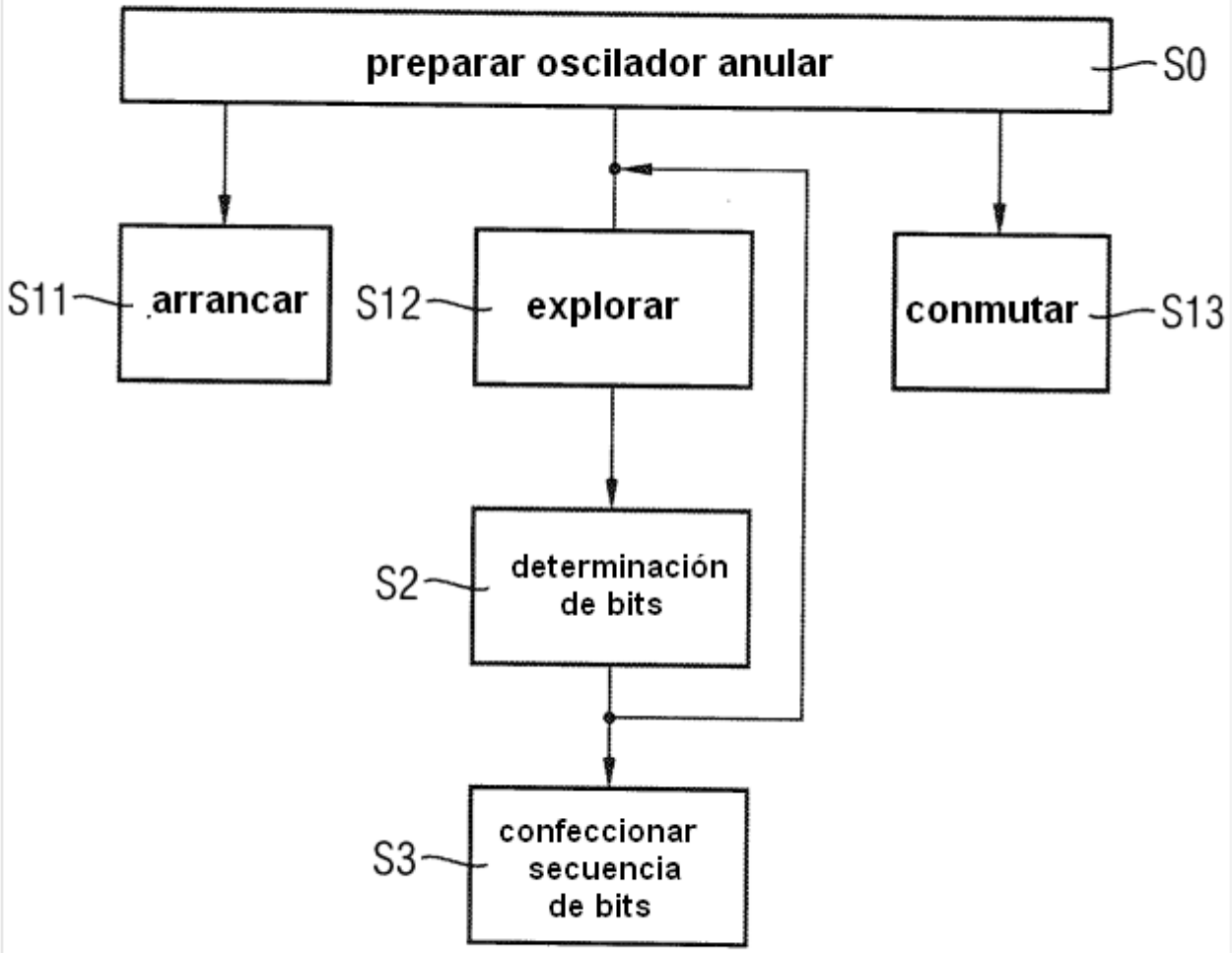

201
R6
NAND
47
NAND
46
28
R5
MUX
RS
NAND
45
R4
50
XOR
NAND
44
5
CT1
NAND
43
NAND
42
R1
OS
XOR
49
NAND
41
4
RO
ST
XOR
48
NAND
40
3

FIG 7


preparar oscilador anular
S0
S11
arrancar
S12
explorar
conmutar
S13
S2
determinación de bits
S3
confeccionar secuencia de bits