(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 326 718**

(21) Número de solicitud: 200702299

(51) Int. Cl.:

H03K 3/84 (2006.01)

G06F 7/58 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación: **17.08.2007**

(43) Fecha de publicación de la solicitud: **16.10.2009**

(43) Fecha de publicación del folleto de la solicitud: **16.10.2009**

(71) Solicitante/s: **Universidad del País Vasco-Euskal Herriko Unibertsitatea**
Barrio Sarriena, s/n
48940 Leioa, Vizcaya, ES

(72) Inventor/es: **Bidarte Peraita, Unai;**
Astarloa Cuellar, Armando;
Lázaro Arrotegui, Jesús y
Zuloaga Izaguirre, Aitzol

(74) Agente: **Carpintero López, Francisco**

(54) Título: **Generador de números realmente aleatorios.**

(57) Resumen:
Generador de números realmente aleatorios.
Generador de números aleatorios, que comprende un primer circuito para compensación digital de retardo (CCDR1), un segundo circuito para compensación digital de retardo (CCDR2), un primer flip-flop (DFF1), un segundo flip-flop (DFF2) y un tercer flip-flop (DFF3). Adicionalmente el generador comprende un circuito de control y enganche.
Dicho generador consigue un estado estacionario de generación de números aleatorios logrando un cierto desfase entre una primera señal de reloj (CLK) y una segunda señal de reloj (clk_des), de tal modo que el segundo flip-flop (DFF2) trabaje en un estado de metaestabilidad.

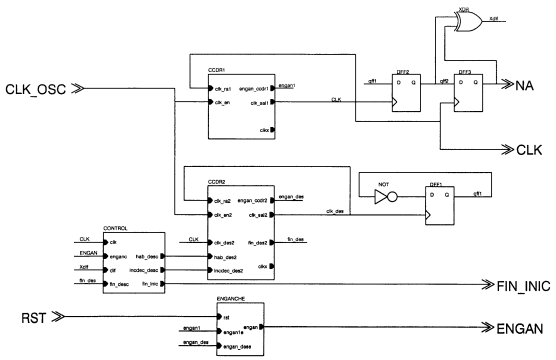

FIG. 1

ES 2 326 718 A1

DESCRIPCIÓN

Generador de números realmente aleatorios.

Campo de la invención

La presente invención pertenece al campo de la electrónica digital, más concretamente al de los generadores de números aleatorios.

Antecedentes de la invención

Cuando una aplicación requiere números aleatorios se pueden emplear secuencias de números aleatorios existentes o generar nuevas secuencias. El primer caso consiste en emplear secuencias aleatorias disponibles en bases de datos, lo cual tiene la ventaja de emplear datos cuyas características estadísticas han sido previamente analizadas, pero, por el contrario, existe un grave problema de seguridad. Por este motivo, lo más habitual es generar los números aleatorios en tiempo real en un generador que reúna los requisitos impuestos por la aplicación. Requisitos habituales para las secuencias generadas son: distribución uniforme, autocorrelación tendente a cero, varianza determinada, período largo, velocidad de generación determinada, etc.

La mayor parte de los generadores de números aleatorios son en realidad generadores de números pseudoaleatorios, es decir, son secuencias de números generadas de manera determinística. Las secuencias parecen aleatorias, pero se calculan mediante la aplicación de un algoritmo a un número inicial o semilla. Siempre que se parta de una misma semilla la secuencia generada será exactamente la misma. Su mayor ventaja es que permiten la generación a alta velocidad, sólo requieren una semilla inicial y se pueden reproducir exactamente. Existen multitud de estos generadores probados y descritos en detalle actualmente y se pueden destacar, entre otros, los siguientes métodos: generadores de congruencia lineal, generadores de desplazamiento de bits, generadores de Fibonacci y de Galois, generadores no lineales, etc.

Aunque los generadores de números pseudoaleatorios pueden generar secuencias aleatorias con buenas características estadísticas a alta velocidad, no son adecuados para aplicaciones en las que prime la seguridad. Tal es el caso de las secuencias aleatorias para criptografía, en las que debe ser imposible calcular el siguiente número de una secuencia conocidos todos los anteriores, es decir la secuencia ha de ser realmente aleatoria. Un generador de números aleatorios con unas características estadísticas y de seguridad adecuadas para aplicaciones tan exigentes como pueden ser las de criptografía, ha de emplear como circuito fundamental no un generador de números pseudoaleatorios sino un generador de números realmente aleatorios. Los generadores de números realmente aleatorios se basan en el muestreo de variables estocásticas presentes en procesos físicos, tales como la desintegración radiactiva, el lanzamiento de un dado, el tiempo transcurrido entre dos pulsaciones de teclado o ratón de un usuario, fenómenos meteorológicos, etc.

Cuando la secuencia aleatoria fundamental se genera a alta velocidad suele presentar parámetros estadísticos que no se ajustan a los deseados, como por ejemplo distinta probabilidad de aparición de los valores 0 y 1, o correlación en los bits cercanos en el tiempo. Esto es consecuencia de las características intrínsecas de los procesos físicos que originan las secuencias aleatorias. Por este motivo normalmente un circuito adicional realiza un post-procesamiento de la secuencia aleatoria fundamental obtenida en el generador de números realmente aleatorios para eliminar características estadísticas indeseadas y conseguir una secuencia aleatoria válida para la aplicación. Otro objetivo del post-procesamiento consiste en minimizar el efecto que cambios ambientales en parámetros como la temperatura puedan tener en la secuencia aleatoria.

Existen multitud de propuestas de probada eficacia para implementar lo que se han denominado circuitos postprocesadores (unas basadas en técnicas lineales como el método de von Neyman, las funciones de hash o los registros de desplazamiento con realimentación lineal y otras basadas en técnicas no lineales para mejorar la seguridad) pero, por el contrario, la generación de secuencias realmente aleatorias en base a circuitos digitales implementables en tecnología FPGA (Field Programmable Gate Array) o ASIC (Application Specific Integrated Circuit) continúa siendo un reto.

Por razones prácticas, los fenómenos físicos más adecuados para los generadores de números realmente aleatorios son aquellos integrables en circuitos electrónicos de estado sólido, ya que las aplicaciones que hacen uso de los números aleatorios se implementan casi en su totalidad en circuitos integrados. Dos métodos convencionales son el ruido térmico de resistencias o uniones PN y los osciladores controlados por tensión, pero requieren circuitos analógicos. Dado que la gran mayoría de los circuitos electrónicos empleados hoy día para tareas de procesamiento y control son digitales, resultan mucho más interesantes los generadores de números realmente aleatorios implementables en su totalidad en tecnología digital.

Descripción de la invención

La invención se refiere a un generador de números aleatorios.

En un primer aspecto de la invención, dicho generador comprende un primer circuito para compensación digital de retardo, un segundo circuito para compensación digital de retardo, un primer flip-flop, un segundo flip-flop y un tercer flip-flop.

El primer circuito para compensación digital de retardo y el segundo circuito para compensación digital de retardo están conectados en un primer puerto de entrada a una señal de un oscilador.

El primer circuito para compensación digital de retardo tiene como salida de su primer puerto de salida una primera señal de reloj, dicha primera señal de reloj realimenta el primer circuito para compensación digital de retardo en un segundo puerto de entrada.

El segundo circuito para compensación digital de retardo tiene como salida de su primer puerto de salida una segunda señal de reloj, dicha segunda señal de reloj realimenta el segundo circuito para compensación digital de retardo en un segundo puerto de entrada.

El primer flip-flop tiene como señal de reloj la segunda señal de reloj y usa la señal de salida de dicho primer flip-flop invertida como entrada del primer flip-flop.

El segundo flip-flop tiene como señal de reloj la primera señal de reloj y usa la señal de salida del primer flip-flop como señal de entrada.

El tercer flip-flop tiene como señal de reloj la primera señal de reloj y usa la señal de salida del segundo flip-flop como señal de entrada, obteniendo como señal de salida del tercer flip-flop una señal aleatoria.

El segundo circuito para compensación digital de retardo adicionalmente podrá comprender un tercer puerto de entrada, un cuarto puerto de entrada y un quinto puerto de entrada.

Adicionalmente, el generador de números aleatorios podrá comprender un circuito de control con un primer puerto de entrada, un segundo puerto de entrada, un tercer puerto de entrada, un cuarto puerto de entrada, un primer puerto de salida, un segundo puerto de salida y un tercer puerto de salida.

El primer puerto de salida del circuito de control está conectado con el cuarto puerto de entrada del segundo circuito para compensación digital de retardo, el segundo puerto de salida del circuito de control con el quinto puerto de entrada del segundo circuito para compensación digital de retardo, y el primer puerto de entrada del circuito de control estando conectado con la primera señal de reloj.

Adicionalmente, el generador de números aleatorios podrá comprender un circuito de enganche con un primer puerto de entrada, un segundo puerto de entrada, un tercer puerto de entrada y un puerto de salida.

En dicho circuito de enganche, la entrada al primer puerto de entrada es una señal de reset. El segundo puerto de entrada está conectado al segundo puerto de salida del primer circuito para compensación digital de retardo, el tercer puerto de entrada al segundo puerto de salida del segundo circuito para compensación digital de retardo y el puerto se salida al segundo puerto de entrada del circuito de control.

El circuito de enganche podrá estar configurado de tal modo que su puerto de salida proporciona una señal de enganche cuando la señal de reset pasa a estado inactivo, y las señales de los segundos puertos de salida del primer y segundo circuito para compensación digital de retardo se activan.

El segundo circuito para compensación digital de retardo podrá comprender una línea de retardo programable, un ajuste dinámico de desfase y una lógica de estado.

Dicha línea de retardo programable comprende una pluralidad de puertas de retardo individuales. Como señal de entrada tiene la señal del primer puerto de entrada y como señal de salida la señal del primer puerto de salida, dicha salida realimenta la línea de retardo programable en el segundo puerto de entrada.

El ajuste dinámico de desfase cuenta como entradas la señal del tercer puerto de entrada, la señal del cuarto puerto de entrada y la señal del quinto puerto de entrada, y como señal de salida la señal de un tercer puerto de salida.

La lógica de estado transmite su señal de salida a través del segundo puerto de salida.

Por su parte, el primer circuito para compensación digital de retardo podrá comprender una línea de retardo programable y una lógica de estado, tal y como han sido descritas anteriormente.

El primer y segundo circuito para compensación digital de retardo podrán ser idénticos en una realización práctica, sin embargo, el primer circuito para compensación digital de retardo no utilizará el ajuste dinámico de desfase.

El generador de números aleatorios puede comprender adicionalmente una puerta XOR, cuyas señales de entrada son la señal de salida del segundo flip-flop y la señal de salida del tercer flip-flop. La señal de salida de dicha puerta XOR es la señal de entrada del tercer puerto de entrada del circuito de control.

La lógica interna del circuito de control podrá comprender un primer contador configurado para determinar el número máximo de ciclos a evaluar la señal de salida de la puerta XOR. Es decir, el contador tendrá un valor prefijado

y esperará encontrar un 1 a la salida de dicha puerta XOR en un número máximo de ciclos, siendo el valor máximo el valor prefijado. Si estamos fuera de la ventana metaestable nunca encontrará el 1. Por el contrario, si estamos en dentro de la ventana metaestable, en algún momento llegará el 1. El valor máximo prefijado limita la espera a un número de ciclos. Este valor depende de la tecnología y el azar. Una posible forma de usar el contador es iniciarlo al valor prefijado e ir decrementando en una unidad cada ciclo de reloj. Si antes de llegar a cero detectamos un 1 en la puerta XOR, estamos en la zona metaestable. Si llegamos hasta cero y aún no se ha detectado un 1 en la puerta XOR podemos decir que estamos fuera de la zona metaestable. Adicionalmente, podrá contar con un segundo contador configurado para memorizar la situación de desfase actual, en base al número de solicitudes de incremento y decremento de fase, un registro configurado para memorizar la amplitud de una ventana y un comparador del valor del segundo contador y de un desfase definido dentro de dicha ventana.

En un segundo aspecto de la invención, ésta se refiere a un procedimiento para generar números aleatorios a la salida de un tercer flip-flop, dicho tercer flip-flop teniendo como señal de entrada la señal de salida de un segundo flip-flop que comprende las siguientes etapas:

- una etapa de generación de una primera señal de reloj y una segunda señal de reloj, ambas señales de reloj en fase,

- una etapa de incremento de la fase de la segunda señal de reloj hasta lograr la metaestabilidad en un segundo flip-flop,

- una etapa de incremento de la fase de la segunda señal de reloj hasta lograr abandonar el estado de metaestabilidad en un segundo flip-flop,

- una etapa de decremento de la fase de la segunda señal de reloj hasta una fase entre la fase de logro del estado de metaestabilidad y la fase de abandono del estado de metaestabilidad, dicho margen para la fase de la segunda señal de reloj se denomina ventana metaestable,

- una fase estacionaria de obtención de números aleatorios en la salida del tercer flip-flop.

El desfase de trabajo, preferentemente, podrá ser determinado de tal modo que sea la semisuma del primer valor de desfase y del segundo valor de desfase.

Una vez alcanzado el desfase de trabajo, se podrá producir la activación de la señal del tercer puerto de salida de un circuito de control siendo la señal de salida del tercer flip-flop aleatoria a partir de dicha activación.

El generador de números aleatorios y el método de generación de números aleatorios descritos tienen las siguientes ventajas frente a los conocidos en el estado de la técnica:

- Trabaja a muy alta velocidad porque, debido a que trabaja en régimen de metaestabilidad continuo, se obtiene un bit realmente aleatorio cada periodo de reloj. En tecnología FPGA hasta 300 Megabits por segundo aproximadamente.

- Requiere pocos recursos para su implementación.

- Es fácilmente implementable ya que actualmente se dispone de circuitos para compensación digital de retardo específicos, por lo que no se requieren consignas especiales de posicionamiento y rutado de circuitos.

- El comportamiento deseado queda asegurado porque el circuito se ajusta en cada encendido, lo cual permite emplear este diseño en equipos que se vayan a industrializar en serie.

- Se ha comprobado que un generador de números aleatorios compuesto del generador objeto de esta solicitud de patente y un sencillo circuito de postprocesamiento basado en un registro de desplazamiento con realimentación lineal, proporciona secuencias de números aleatorios que superan los 16 tests propuestos por el National Institute of Standards and Technology (NIST). Estas pruebas son un referente aceptado a nivel mundial para evaluar posibles desviaciones en secuencias binarias aleatorias. Esta prueba valida la posibilidad de utilizar el circuito propuesto para aplicaciones de criptografía.

Descripción de los dibujos

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

La figura 1 muestra un esquema del generador de números aleatorios propuesto en esta patente. Incluye todos los bloques principales que lo forman, así como la señalización fundamental entre los mismos.

La figura 2 muestra un diagrama de tiempos con las dos señales de reloj generadas en los dos circuitos para compensación digital de retardo, así como la señal salida del primer flip-flop. Indica también todos los tiempos involucrados en la definición de la ventana metaestable.

La figura 3 muestra el diagrama de bloques de un circuito para compensación digital de retardo genérico.

Realización preferente de la invención

A continuación, con referencia a las figuras, se describe un modo de realización preferente del circuito y procedimiento generador de números aleatorios que constituye el objeto de esta invención.

Dada la señal periódica y cuadrada de entrada (CLK_OSC) de un oscilador externo, un circuito genera una señal de salida (NA) continuamente aleatoria y sincronizada con una primera señal de reloj (CLK) que se emplea como señal de reloj interna del circuito integrado y está compensada dinámicamente para estar en fase con la señal de un oscilador externo (CLK_OSC). La frecuencia de la primera señal de reloj (CLK) puede ser la misma que la señal de un oscilador externo (CLK_OSC) o un múltiplo de la misma. La señal de salida del circuito (NA) continuamente aleatoria se puede introducir en un registro de desplazamiento con entrada serie y salida paralelo para formar números aleatorios del número de bits requerido por la aplicación.

La figura 1 muestra un diagrama de bloques del generador de números aleatorios propuesto. A continuación se describe el funcionamiento del generador.

El primer circuito para compensación digital de retardo (CCDR1) y el segundo circuito para compensación digital de retardo (CCDR2) son elementos fundamentales para la definición del generador. Se basan en líneas de retardo programable con una unidad de control que ajusta la fase de la señal en unos primeros puertos de salida (clk_sal1, clk_sal2) del primer circuito para compensación digital de retardo (CCDR1) y del segundo circuito para compensación digital de retardo (CCDR2) con respecto a las respectivas señales de los primeros puertos de entrada (clk_en1, clk_en2), para lo cual requiere realimentar la salida hacia la entrada, en unos segundos puertos de entrada (clk_ra1, clk_ra2). La frecuencia de salida puede ser la misma o un múltiplo de la de la entrada. El primer circuito para compensación digital de retardo (CCDR1) ajusta dinámicamente la señal de reloj de su primer puerto de salida (clk_sal1) para que esté en fase con la señal del oscilador (CLK_OSC). Mediante la activación de la señal del segundo puerto de salida (engan_ccdr1) del primer circuito para compensación digital de retardo (CCDR1) se indica que ha conseguido el enganche de fase. En ese momento la señal del primer puerto de salida (clk_sal1) está exactamente en fase con la señal del primer puerto de entrada (clk_en1) y se distribuye dentro del circuito integrado a través de un buffer especial para distribución de señales de reloj.

El segundo circuito para compensación digital de retardo (CCDR2) realiza una tarea similar pero en este caso, en lugar de estar en fase, permite el ajuste digital de la fase de la señal del primer puerto de salida (clk_sal2) con respecto a la señal del primer puerto de entrada (clk_en2). El ajuste digital lo realiza el circuito de control (CONTROL) con la siguiente señalización: cada vez que se produce un flanco activo en la segunda señal de reloj (clk_des), siempre que esté activa la señal del cuarto puerto de entrada (hab_des2) se produce, según sea el estado de la señal del quinto puerto de entrada (incdec_des2), la petición de un incremento o decremento de una unidad en la fase de la salida con respecto a la entrada. El primer circuito para compensación digital de retardo (CCDR1) y el segundo circuito para compensación digital de retardo (CCDR2) disponen de una línea de retardo compuesta por un número discreto de retardadores, y la unidad de desfase es una división entera del período de la señal del primer puerto de entrada (clk_en2). Una vez que el segundo circuito para compensación digital de retardo (CCDR2) ha realizado la variación de fase solicitada, lo comunica al circuito de control (CONTROL) a través del quinto puerto de salida (fin_des2).

De esta forma se distribuyen mediante buffers dedicados de reloj una primera señal del reloj (CLK) y una segunda señal de reloj (clk_des) de la misma frecuencia y con un desfase constante e independiente de la deriva del oscilador, ya que los circuitos de compensación son capaces de compensar dinámicamente esta deriva. La primera señal de reloj (CLK) se puede emplear en todos los bloques del circuito integrado como señal de reloj.

El generador emplea tres flip-flops tipo D: un primer flip-flop (DFF1) que usa como señal de reloj la segunda señal de reloj (clk_des) y un segundo flip-flop (DFF2) y un tercer flip-flop (DFF3) con la señal de reloj de la primera señal de reloj (CLK). El primer flip-flop (DFF1) realimenta su salida invertida hacia su entrada y su salida no invertida hacia el segundo flip-flop (DFF2). El tercer flip-flop (DFF3) recibe la salida del segundo flip-flop (DFF2) a su entrada. El circuito de control (CONTROL) ajusta el desfase de la segunda señal de reloj (clk_des), obtenida en el segundo puerto de salida (clk_sal2) del segundo circuito para compensación digital de retardo (CCDR2) de forma que el segundo flip-flop (DFF2) trabaje en régimen de metaestabilidad en el punto medio dentro del margen metaestable posible. Siempre que hay un incumplimiento de los tiempos de establecimiento (setup) o mantenimiento (hold) la salida del flip-flop entra en un estado transitorio simétricamente balanceado que se denomina estado metaestable.

La figura 2 explica bajo qué condiciones el segundo flip-flop (DFF2) trabaja en régimen metaestable. Este flip-flop tiene como señal de reloj la primera señal de reloj (CLK) y como entrada de datos la salida del primer flip-flop (DFF1), por lo que el comportamiento será metaestable en su salida cuando la señal de salida del primer flip-flop (DFF1) cambie de valor en la ventana temporal (Ventana Metaestable VM en la figura 2) que va desde un tiempo de establecimiento (tes) antes del flanco activo de la primera señal de reloj (CLK) hasta un tiempo de mantenimiento

(tma) posterior a dicho flanco activo. La salida del primer flip-flop (DFF1) cambia de valor en todos los ciclos de reloj y lo hace siempre un tiempo de retardo (tr) después de que se produzca el flanco activo de la segunda señal de reloj (clk_des). Dado un tiempo de desfase (td) entre la primera señal de reloj (CLK) y la segunda señal de reloj (clk_des), el segundo flip-flop (DFF2) trabaja en régimen metaestable cuando se cumple que:

$$tr\text{-}tma < td < tr+tes,$$

siendo tr el retardo de la señal de salida del primer flip-flop (DFF1) con respecto del flanco activo de la segunda señal del reloj (clk_des), td el desfase de la segunda señal de reloj (clk_des) con respecto a la primera señal de reloj (CLK) y tes y tma los tiempos de establecimiento y de mantenimiento, respectivamente, de los flip-flops empleados. No es necesario conocer el tiempo de retardo (tr), que depende de las líneas de rutado internas, ya que el generador ajusta el tiempo de desfase entre la primera y segunda señal de reloj (td) para trabajar en el punto deseado. Por este motivo no son necesarias consignas de rutado en la descripción del circuito.

Dado que la anchura de esta ventana es tes+tma, la unidad de desfase (Ft) de la señal del segundo puerto de salida (clk_sal2) del segundo circuito para compensación digital de retardo (CCDR2) ha de ser inferior a este valor para poder ajustar el punto metaestable con total seguridad.

A continuación se resume el proceso transitorio desde la inicialización hasta conseguir un régimen continuo y estable de bits aleatorios en la salida del tercer flip-flop (NA):

- Detectada en la señal de reset (RST), tanto el primer circuito para compensación de retardo (CCDR1) como el segundo circuito para compensación de retardo (CCDR2) ajustan el desfase de la primera señal de reloj (CLK) y la segunda señal de reloj (clk_des) con la señal de un oscilador externo (CLK_OSC). Una vez que acaba este proceso activan las salidas de sus segundos puertos de salida (engan ccdr1, engan_ccdr2) que son recibas en el segundo y tercer puerto del circuito de enganche (engan1e, engan_dese), lo que provoca, junto con la señal de reset (RST) recibida en el primer puerto de entrada (clk)del circuito de enganche, que el circuito de enganche (ENGANCHE) active la señal de su puerto de salida (engan). Dicha señal del puerto de salida (engan) del circuito de enganche (ENGANCHE) inicializa todos los circuitos, incluido el circuito de control (CONTROL). A partir de este momento la primera señal de reloj (CLK) y la segunda señal de reloj (clk_des) son estables y se pueden emplear en los circuitos secuenciales. Inicialmente, tanto la primera señal de reloj (CLK) como la segunda señal de reloj (clk_des) son señales de reloj en fase con la señal del oscilador (CLK_OSC). A continuación el circuito de control (CONTROL) aumenta el desfase en la segunda señal de reloj (clk_des) hasta localizar el comienzo de la zona metaestable (F1). Cada vez que aumenta el desfase en una unidad evalúa la salida de una puerta XOR conectada a las salidas del segundo flip-flop (DFF2) y del tercer flip-flop (DFF3), ya que ésta toma valor lógico 1 si dos valores consecutivos difieren, lo cual indica estado metaestable en el segundo flip-flop (DFF2).

- Una vez localizado el punto de comienzo de la zona metaestable (F1) el circuito de control (CONTROL) sigue aumentando el desfase hasta salir de la zona metaestable y memoriza la fase de dicho punto (F2), controlando también la salida de la puerta XOR.

- Cuando se alcanza el final de la zona metaestable el circuito de control (CONTROL) inicia un proceso de disminución del desfase. Este proceso concluye cuando queda fijado el punto o fase de trabajo (Ft) en mitad de dicha zona, que es el que proporciona mayor margen ante posibles desajustes.

- Cuando finaliza el ajuste el circuito de control (CONTROL) activa la señal de su tercer puerto de salida (fin_inic), lo cual indica que se puede emplear la señal de salida del tercer flip-flop (NA) como secuencia aleatoria.

Respecto a la razón por la cual el estado de metaestabilidad se detecta en la puerta XOR, cabe decir lo siguiente.

Las transiciones de la señal de salida del primer flip-flop (DFF1) se pueden dar dentro o fuera de la ventana metaestable (VM), pero, mientras no se modifique el desfase en el segundo circuito para compensación digital de retardo (CCDR2) mediante una nueva petición de incremento o decremento, esta condición se mantiene, es decir, las transiciones de la señal de salida del primer flip-flop (dff1) siempre se dan o dentro o fuera de la ventana metaestable (VM), porque el primer y segundo circuito para compensación digital de retardo (CCDR1, CCDR2) mantienen los desfases constantes.

La señal de salida del primer flip-flop (DFF1), que es la señal de entrada del segundo flip-flop (DFF2), cambia su valor una vez por periodo, por lo que, si las transiciones de dicha señal (dff1) se dan fuera de la ventana metaestable (VM), cada vez que llegue un nuevo flanco en el reloj (CLK) del segundo flip-flop (DFF2), el valor de la señal de entrada del segundo flip-flop (DFF2) es estable durante la ventana metaestable (VM) y en este tiempo vale 0 ó 1, por lo que el valor de salida del segundo flip-flop (DFF2) será dicho valor 0 ó 1 y será siempre el mismo valor en todos los periodos.

Por el contrario, si las transiciones de la señal de salida del primer flip-flop (DFF1) se dan dentro de la ventana metaestable (VM), cada vez que llegue un nuevo flanco en el reloj (CLK) del segundo flip-flop (DFF2), el valor de la señal de entrada del segundo flip-flop (DFF2) no es estable durante la ventana metaestable, por lo que el valor de salida del segundo flip-flop (dff2) es impredecible (aleatorio y simétricamente balanceado).

La salida de la puerta XOR es 1 únicamente si los valores de las dos señales a su entrada son diferentes (01 ó 10).

La puerta XOR tiene en sus entradas, en todo momento, los valores de salida del segundo y tercer flip-flops (DFF2, DFF3), es decir, la salida actual en el segundo flip-flop (DFF2) y la salida del mismo flip-flop (DFF2) en el periodo de reloj anterior.

Si estamos en la región de funcionamiento estable la salida del segundo flip-flop (dff2) tendrá el mismo valor indefinidamente (puede ser 0 ó 1, pero siempre el mismo). Por lo tanto la salida de la puerta XOR será siempre 0.

Por el contrario, si el segundo flip-flop (DFF2) está trabajando dentro de la ventana metaestable (VM), la salida de la puerta XOR será 1 en algún momento. El número de ciclos durante los cuales es necesario evaluar la salida de la puerta XOR es difícil de prever, ya que depende de la tecnología y del azar.

Las señales de reloj generadas en el primer circuito para compensación digital de retardo (CCDR1) y en el segundo circuito para compensación digital de retardo (CCDR2) tienen la relación de fase (Ft) descrita, pero su frecuencia puede ser la misma o un múltiplo de la frecuencia del oscilador, con lo que se puede ajustar la velocidad de generación de la secuencia aleatoria a las necesidades de la aplicación.

Dado que los circuitos de compensación de retardo se adaptan a la deriva del oscilador y el rutado interno de las señales de reloj en el chip se hace por líneas de distribución especiales sin desfase, después del régimen de ajuste transitorio, se consigue mantener el funcionamiento metaestable del flip-flop, por lo que todos los valores a su salida son impredecibles o aleatorios.

El generador de números aleatorios se puede implementar completamente tanto en tecnología FPGA como en tecnología ASIC. Los recursos necesarios para implementar el generador propuesto se encuentran disponibles en ambas tecnologías. Se requieren circuitos combinacionales y secuenciales básicos y dos circuitos para compensación digital de retardo. Aunque la funcionalidad de estos últimos se puede conseguir mediante circuitos digitales básicos, el generador ha sido concebido para lograr unos resultados óptimos cuando, para implementar los circuitos para compensación digital de retardo, se empleen circuitos para compensación digital de retardo específicos, es decir, cuando la tecnología empleada disponga de unidades de compensación digital de retardo construidas en silicio para ser usadas exclusivamente con ese fin, debido a que estos circuitos aseguran la precisión necesaria en el ajuste de fase. La figura 3 muestra el diagrama de bloques básico de cualquier circuito CCDR. A continuación se describe la funcionalidad y la señalización fundamental:

- Línea de Retardo Programable (LRP): es el circuito principal y se basa en un conjunto discreto de puertas de retardo individuales. Dispone de una unidad de control que ajusta el retardo de la señal del primer puerto de salida (clk_sal2) con respecto a la de referencia en la señal del primer puerto de entrada (clk_en2). Para conseguirlo requiere la realimentación de la salida, que se distribuye a través de un árbol de distribución de reloj, hacia el segundo puerto de entrada (clk_ra2). La unidad de retardo en cada puerta individual puede ser constante o, lo que es mas habitual, una proporción del período de la señal del primer puerto de entrada (clk_en2). En este caso la unidad de desfase es menor cuanto menor es el período del oscilador, ya que la línea de retardo programable se divide en un número fijo de etapas de retardo que suman en conjunto un período. Dado que la ventana de funcionamiento metaestable es constante para una tecnología dada, a mayor frecuencia el número de unidades de retardo incluidas en esta ventana es mayor, por lo que el ajuste para funcionamiento en el punto medio es más preciso. Se ha comprobado que para la tecnología actual se consigue un funcionamiento estable para frecuencias superiores a 50 MHz.

- Ajuste Dinámico de Desfase (ADD): modifica el desfase de la salida con respecto a la entrada. Recibe peticiones a través de una interfaz compuesta de una segunda señal de reloj (clk_des) con una entrada a través del tercer puerto de entrada (clk_des2), una línea de selección de incremento o decremento de desfase a través del quinto puerto de entrada (incdec_des2) y una línea de habilitación a través de un cuarto puerto de entrada (hab_des2). El circuito permite ajustar el desfase con pasos unitarios, siendo la resolución mayor cuanto mayor sea el número de pasos. Dispone de un puerto de salida (fin_des2) cuya señal indica la finalización del proceso de ajuste de desfase.

- Síntesis de Frecuencia (SF): realiza la síntesis de frecuencia mediante la multiplicación y/o división de la frecuencia de entrada. Empleando este recurso se puede variar la frecuencia de generación de bits aleatorios en un amplio rango. La tecnología FPGA permite un rango de frecuencias entre 50 MHz y 300 MHz aproximadamente. Esta capacidad permite usar como reloj de salida la señal del primer puerto de salida (clk_sal2), de igual frecuencia que la señal del primer puerto de entrada (clk_en2), o la señal del cuarto puerto de salida (clkx), cuya frecuencia es múltiplo de la señal del primer puerto de entrada (clk_en2) y se obtiene mediante multiplicación y/o división de la misma.

- Lógica de Estado (LE): tras la inicialización del sistema, el circuito de control de la línea de Retardo Programable (LRP) ajusta, mediante un lazo realimentado, el desfase de salida con respecto al de entrada. El circuito lógica de estado activa una señal en el segundo puerto de salida (engan_ccdr2) cuando, tras un periodo transitorio inicial, finaliza este proceso de ajuste y se alcanza el régimen estable.

El circuito de enganche (ENGANCHE) se puede implementar como un sencillo circuito combinacional que activa la salida de su puerto de salida (engan) cuando, tras la inicialización, la señal de reset (RST) pasa a estado inactivo y la señal del segundo puerto de salida (engan_ccdr1, engan_ccdr2) del primer y segundo circuito para compensación digital de retardo (CCDR1, CCDR2) se activan. Todos los bloques del circuito integrado han de emplear la señal puerto de salida (engan) para iniciarse, ya que hasta la activación de la misma los relojes distribuidos en el chip, no son estables.

Además de los dos circuitos para compensación digital de retardo, el circuito de enganche (ENGANCHE), los buffers de entrada de señal y de distribución de reloj, los tres flip-flops (DFF1, DFF2, DFF3) y una puerta lógica XOR, solo se requiere una unidad de control para el ajuste inicial del punto de trabajo. La funcionalidad del circuito de control (CONTROL) se puede implementar en base a una máquina de estados finitos con los siguientes circuitos de proceso: un primer contador que determine el número de ciclos a evaluar la señal de salida de la puerta XOR (xdif) para determinar el régimen de funcionamiento del segundo flip-flop (DFF2); un segundo contador como puntero de desfase para memorizar la situación de desfase en función del número de solicitudes de incremento y decremento realizadas una vez detectado el inicio de la zona metaestable; un registro para memorizar el número de ciclos de la ventana metaestable y un comparador de los valores del segundo contador y de la mitad del resultado del registro para determinar cuando se alcanza el centro de la ventana metaestable.

Dado que los circuitos para compensación digital de retardo son dependientes de la tecnología, se puede reutilizar una descripción VHDL o Verilog genérica siempre que se sustituyan los circuitos para compensación digital de retardo por los que correspondan en cada tecnología.

A la vista de esta descripción y juego de figuras, el experto en la materia podrá entender que la invención ha sido descrita según una realización preferente de la misma, pero que múltiples variaciones pueden ser introducidas en dicha realización preferente, sin salir del objeto de la invención tal y como ha sido reivindicada.

REIVINDICACIONES

1. Generador de números aleatorios, que comprende

un primer circuito para compensación digital de retardo (CCDR1), un segundo circuito para compensación digital de retardo (CCDR2), un primer flip-flop (DFF1), un segundo flip-flop (DFF2) y un tercer flip-flop (DFF3),

estando conectado el primer circuito para compensación digital de retardo (CCDR1) en un primer puerto de entrada (clk_en1) y el segundo circuito para compensación digital de retardo (CCDR2) en un primer puerto de entrada (clk_en2) a una señal de un oscilador (CLK_OSC),

el primer circuito para compensación digital de retardo (CCDR1) tiene como salida de su primer puerto de salida (clk_sal1) una primera señal de reloj (CLK), dicha primera señal de reloj (CLK) realimenta el primer circuito para compensación digital de retardo (CCDR1) en un segundo puerto de entrada (clk_ra1),

el segundo circuito para compensación digital de retardo (CCDR2) tiene como salida de su primer puerto de salida (clk_sal2) una segunda señal de reloj (clk_des), dicha segunda señal de reloj (clk_des) realimenta el segundo circuito para compensación digital de retardo (CCDR2) en un segundo puerto de entrada (clk_ra2),

el primer flip-flop (DFF1) tiene como señal de reloj la segunda señal de reloj (clk_des) y usa la señal de salida (dff1) de dicho primer flip-flop (DFF1) invertida como entrada del primer flip-flop (DFF1),

el segundo flip-flop (DFF2) tiene como señal de reloj la primera señal de reloj (CLK) y usa la señal de salida del primer flip-flop (dff1) como señal de entrada,

el tercer flip-flop (DFF3) tiene como señal de reloj la primera señal de reloj (CLK) y usa la señal de salida del segundo flip-flop (dff2) como señal de entrada, obteniendo como señal de salida (NA) del tercer flip-flop (DFF3) una señal aleatoria.

2. Generador de números aleatorios según la reivindicación 1, **caracterizado** por que el segundo circuito para compensación digital de retardo (CCDR2) adicionalmente comprende un tercer puerto de entrada (clk_des2), un cuarto puerto de entrada (hab_des2) y un quinto puerto de entrada (indec_des2).

3. Generador de números aleatorios según la reivindicación 2, **caracterizado** por que adicionalmente comprende un circuito de control (CONTROL) con un primer puerto de entrada (clk), un segundo puerto de entrada (enganc), un tercer puerto de entrada (dif), un cuarto puerto de entrada (fin_desc), y un primer puerto de salida (hab_desc), un segundo puerto de salida (incdec_desc) y un tercer puerto de salida (fin_inic),

estando conectado el primer puerto de salida (hab_desc) del circuito de control (CONTROL) con el cuarto puerto de entrada (hab_des2) del segundo circuito para compensación digital de retardo (CCDR2), el segundo puerto de salida (incdec_desc) del circuito de control (CONTROL) con el quinto puerto de entrada (indec_des2) del segundo circuito para compensación digital de retardo (CCDR2), el primer puerto de entrada (cik) del circuito de control (CONTROL) estando conectado con la primera señal de reloj (CLK).

4. Generador de números aleatorios según la reivindicación 3, **caracterizado** por que adicionalmente comprende un circuito de enganche (ENGANCHE) con un primer puerto de entrada (rst), un segundo puerto de entrada (engan1e), un tercer puerto de entrada (engan_dese) y un puerto de salida (engan),

siendo la entrada al primer puerto de entrada (rst) una señal de reset (RST), estando conectado el segundo puerto de entrada (engan1e) al segundo puerto de salida (engan_ccdr1) del primer circuito para compensación digital de retardo (CCDR1), el tercer puerto de entrada (engan_dese) al segundo puerto de salida (engan_ccdr2) del segundo circuito para compensación digital de retardo (CCDR2) y el primer puerto se salida (engan) al segundo puerto de entrada (enganc) del circuito de control (CONTROL).

5. Generador de números aleatorios según la reivindicación 4, **caracterizado** por que el puerto de salida (engan) del circuito de enganche (ENGANCHE) activa una señal de enganche (ENGAN) cuando la señal de reset (RST) pasa a estado inactivo, y las señales de los segundos puertos de salida (engan_ccdr1, engan_ccdr2) del primer circuito para compensación digital de retardo (CCDR1) y del segundo circuito para compensación digital de retardo (CCDR2) se activan.

6. Generador de números aleatorios según la reivindicación 1, **caracterizado** por que el primer circuito para compensación digital de retardo (CCDR1) comprende una línea de retardo programable (LRP) y una lógica de estado (LE),

la línea de retardo programable (LRP) comprende una pluralidad de puertas de retardo individuales, dicha línea de retardo programable (LRP) tiene como señal de entrada la señal del primer puerto de entrada (clk_en1) y como señal de salida la señal del primer puerto de salida (clk_sal1), dicha señal de salida realimenta la línea de retardo programable (LRP) en el segundo puerto de entrada (clk_ra1),

la lógica de estado (LE) transmite su señal de salida a través del segundo puerto de salida (engan_ccdr1).

7. Generador de números aleatorios según la reivindicación 1, **caracterizado** por que el segundo circuito para compensación digital de retardo (CCDR2) comprende una línea de retardo programable (LRP), un ajuste dinámico de desfase (ADD), y una lógica de estado (LE),

la línea de retardo programable (LRP) comprende una pluralidad de puertas de retardo individuales, dicha línea de retardo programable (LRP) tiene como señal de entrada la señal del primer puerto de entrada (clk_en2) y como señal de salida la señal del primer puerto de salida (clk_sal2), dicha señal de salida realimenta la línea de retardo programable (LRP) en el segundo puerto de entrada (clk_ra2),

el ajuste dinámico de desfase (ADD) cuenta como entradas la señal del tercer puerto de entrada (clk_des2), la señal del cuarto puerto de entrada (hab_des2) y la señal del quinto puerto de entrada (indec_des2), y como señal del salida la señal de un tercer puerto de salida (fin_des2),

la lógica de estado (LE) transmite su señal de salida a través del segundo puerto de salida (engan_ccdr2).

8. Generador de números aleatorios según la reivindicación 1, **caracterizado** por que la señal de salida del segundo flip-flop (dff2) y la señal de salida del tercer flip-flop (NA) son señales de entrada de una puerta XOR, siendo la señal de salida de dicha puerta XOR (xdif) la señal de entrada del tercer puerto de entrada (dif) del circuito de control (CONTROL).

9. Generador de números aleatorios según las reivindicaciones 3 u 8, **caracterizado** por que el circuito de control (CONTROL) comprende un primer contador configurado para determinar el número máximo de ciclos a evaluar la señal de salida de la puerta XOR (xdif), un segundo contador configurado para memorizar la situación de desfase actual, en base al número de solicitudes de incremento y decremento de fase, un registro configurado para memorizar la amplitud de una ventana (VM) y un comparador del valor del segundo contador y de un desfase definido dentro de dicha ventana (VM).

10. Procedimiento para generar números aleatorios a la salida de un tercer flip-flop (NA), dicho tercer flip-flop (DFF3) teniendo como señal de entrada la señal de salida de un segundo flip-flop (dff2), **caracterizado** por que comprende las siguientes etapas:

- una etapa de generación de una primera señal de reloj (CLK) y una segunda señal de reloj (clk_des) en fase,
- una etapa de incremento de la fase (F1) de la segunda señal de reloj (clk_des) hasta lograr la metaestabilidad en el segundo flip-flop (DFF2),
- un etapa de incremento de la fase (F2) de la segunda señal de reloj (clk_des) hasta lograr abandonar el estado de metaestabilidad en el segundo flip-flop (DFF2),
- una etapa de decremento de la fase de la segunda señal de reloj (clk_des) hasta una fase (Ft) entre la fase (F1) de logro del estado de metaestabilidad y la fase (F2) de abandono del estado de metaestabilidad,
- una fase estacionaria de obtención de números aleatorios en la salida del tercer flip-flop (NA).

11. Procedimiento según la reivindicación 10, **caracterizado** por que el desfase de trabajo (Ft) es la semisuma del primer valor de desfase (F1) y del segundo valor de desfase (F2).

12. Procedimiento según cualquiera de las reivindicaciones 10-11, **caracterizado** por que una vez alcanzado el desfase de trabajo (Ft) se produce la activación de la señal del tercer puerto de salida (fin_inic) de un circuito de control (CONTROL) siendo la señal de salida del tercer flip-flop (NA) aleatoria a partir de dicha activación.

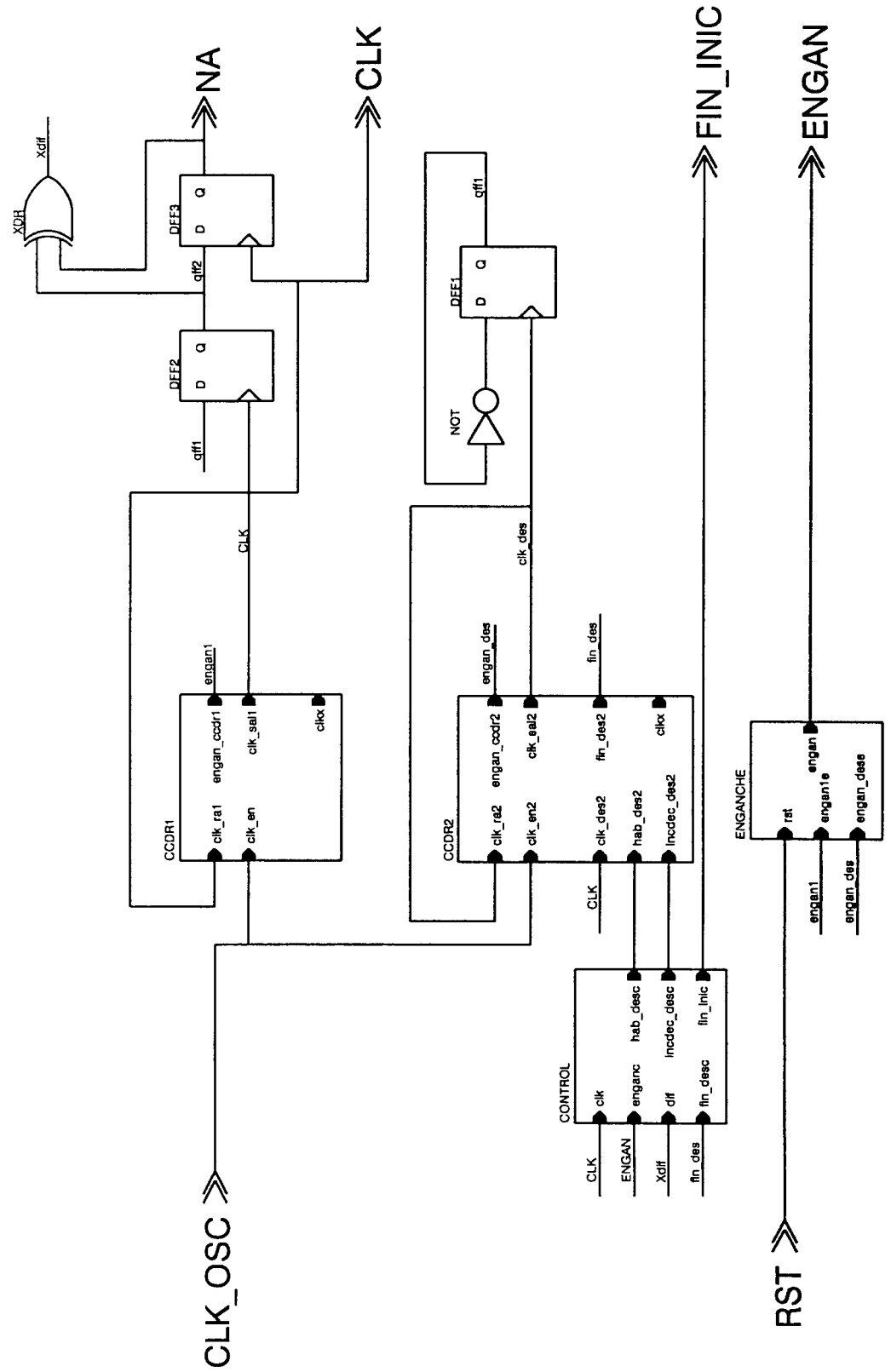
CLK_OSC
RST
NA
CLK
FIN_INIC
ENGAN
XDR
Xdif
DFF3
DFF2
DFF1
NOT
qff1
qff2
CCDR1
clk_ra1
clk_en
engan_ccdr1
clk_sal1
clkx
engan1
CLK
CCDR2
clk_ra2
clk_en2
engan_ccdr2
clk_sal2
clk_des2
hab_des2
incdec_des2
fin_des2
engan_des
clk_des
fin_des
CONTROL
clk
enganc
dif
fin_desc
hab_desc
incdec_desc
fin_inic
ENGAN
Xdif
fin_des
ENGANCHE
rst
engan1e
engan
engan_dese
engan1
engan_des

FIG. 1

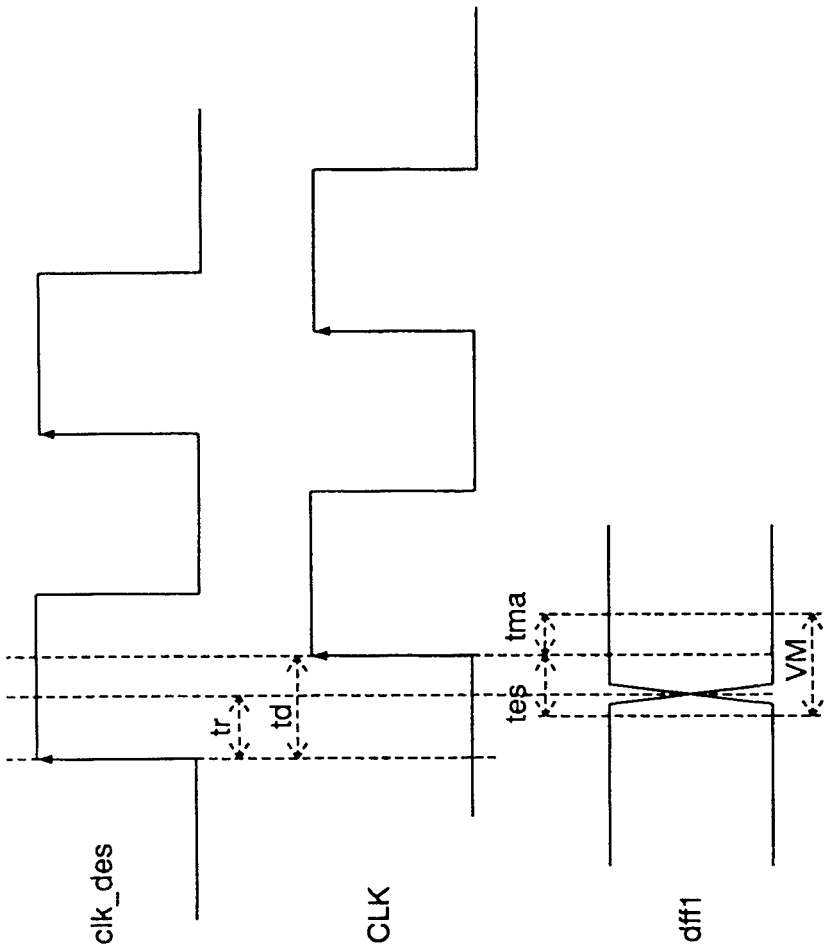

FIG. 2

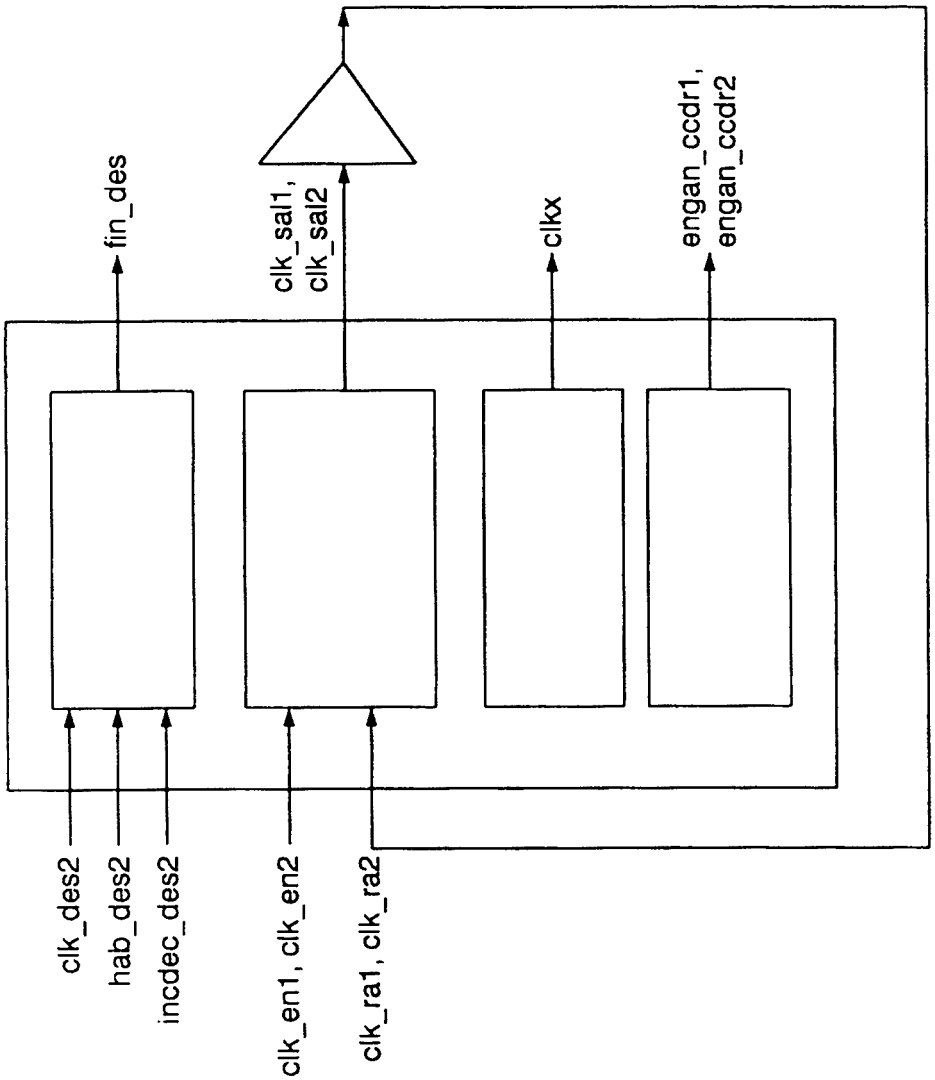
fin_des
clk_sal1,
clk_sal2
clkx
engan_ccdr1,
engan_ccdr2
clk_des2
hab_des2
incdec_des2
clk_en1, clk_en2
clk_ra1, clk_ra2

FIG. 3

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 326 718

(21) Nº de solicitud: 200702299

(22) Fecha de presentación de la solicitud: **17.08.2007**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** ***H03K 3/84*** (2006.01)
G06F 7/58 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
X	EP 1188109 A2 (KONINKL PHILIPS ELECTRONICS NV) 20.03.2002, página 3, línea 15 - página 4, línea 12;página 5, línea 5 - página 9, línea 9; figuras 1-6.	1-12
X	EP 1367715 A1 (FDK CORP) 03.12.2003, párrafos [0014-0067]; párrafos [0097-0174]; figuras 1-19.	1-7,9-12
A	US 2005004961 A1 (HARS et al.) 06.01.2005, párrafos [0017-0053]; figuras 1-3.	1-12

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
23.09.2009	J. Herrando Calvo	1/5

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H03K, G06F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC

OPINIÓN ESCRITA

Nº de solicitud: 200702299

Fecha de Realización de la Opinión Escrita: 23.09.2009

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-12	**SÍ**
	Reivindicaciones		**NO**
Actividad inventiva	Reivindicaciones		**SÍ**
(Art. 8.1 LP 11/1986)	Reivindicaciones	1-12	**NO**

Se considera que la solicitud cumple con el requisito de **aplicación industrial.** Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión:

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como ha sido publicada.

1. Documentos considerados:

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	EP 1188109 A2	20-03-2002
D02	EP 1367715 A1	03-12-2003
D03	US 2005004961 A1	06-01-2005

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

El documento D01 se considera el más próximo del estado de la técnica al objeto de la invención, el cual afecta a la actividad inventiva de todas las reivindicaciones tal y como se explica a continuación.

Reivindicación R01

El documento D01 divulga un aparato para generar números aleatorios basado en la metaestabilidad de flip-flops. Dicho generador de números aleatorios comprende medios para retardar o desfasar las señales de entrada a los flip-flops y violar así intencionadamente el tiempo de hold y/o el tiempo de setup provocando el estado de metaestabilidad (página 3, líneas 15-20; página 5, líneas 5-31; figura 2A) a su salida.

Los circuito de compensación de retardo CCDR1 y CCDR2 utilizados para desfasar las señales de entrada al flip-flop DFF2 de la invención son un equivalente a los retardos (215,220) del documento D01 utilizados para retardar las señales del flip-flop (210) de salida (considerando el flip-flop DFF1 como parte del circuito de compensación CCDR2). Además, el documento D01 incluye un sistema para sincronizar (235, figura 2B) la salida metestable asíncrona con el reloj del sistema (página 3, líneas 21-24; páginas 5, línea 32 - página 6, línea 12), similar a la función realizada por flip-flop DFF3 de la invención.

El mismo planteamiento y conclusión es aplicable para el documento D02 (párrafos 0014-0067 y párrafo 0127, figuras 1-6).

Por tanto, el objeto en la reivindicación R01 no difiere de la técnica conocida descrita en el documento D01 en ninguna forma esencial y sólo comprende un modo de realización del estado de la técnica existente. Por tanto, no se puede considerar que implique actividad inventiva (Artículo 8.1 LP).

Reivindicaciones R02-R09

Tanto los puertos de entrada/salida como la interconexión de los mismos descritos en la reivindicaciones R02-R09 se consideran que son opciones normales de diseño y suponen un modo de realización alternativo con las mismas ventajas que los modos de realización divulgados en los documentos D01 (página 5, línea 5 - página 9, línea 9) y D02 (párrafos 0097-0174) para resolver el mismo problema técnico planteado. Por tanto, no se puede considerar que implique actividad inventiva (Artículo 8.1 LP).

Por otro lado, el sistema de control reivindicado por R3 que permite el ajuste del retardo o desfase entre las señales de entrada para obtener la señal metaestable a la salida, ya se encuentra divulgado por el documento D01 (página 8, líneas 13-21) proporcionando el mismo efecto técnico que el de la presente solicitud. Igualmente, el documento D02 (párrafos 0014 y 0104) divulga un generador de números aleatorios con sistema de ajuste del retardo.

La invención de la reivindicación R8 consiste en la utilización de una puerta XOR para detectar el estado de metaestabilidad, sin embargo el documento D01 también comprende una puerta XOR para detectar dicho estado (página 3, líneas 25-27; página 6, líneas 13-32) comparando la salida y entrada del flip-flop de salida.

La utilización de contadores en el sistema de control para almacenar, incrementar o decrementar el desfase actual de las señales es una técnica muy conocida y por lo tanto, obvia para un experto en la materia tal y como se muestra en el documento citado D02 (111,112,113; párrafos 0016-0021 y párrafos 0102-0107).

En conclusión, no se puede considerar que las reivindicaciones R02-R09 impliquen actividad inventiva (Artículo 8.1 LP) según lo expuesto anteriormente.

Hoja adicional

Reivindicación R10

El procedimiento definido en las reivindicación R10 no difiere de la técnica conocida descrita en los documentos D01 (página 5, línea 5 - página 9, línea 9) y D02 (párrafos 0097-0174) en ninguna forma esencial ya que comprenden las mismas etapas para generar números aleatorios basados en la metaestabilidad de flip-flops:

- Etapa de generación de señales desfasadas: desfasar las señales de entrada al flip-flop y violar así intencionadamente el tiempo de hold y/o el tiempo de setup provocando el estado de metaestabilidad.

- Etapas de incremento/decremento de fase para fijar el punto de trabajo: Mientras que en la presente invención, se fijan las fases F1 y F2 como las fases de entrada y salida del estado de metestabilidad del flip flop y se fija el punto de trabajo en algún punto intermedio entre F1 y F2, en el documento D01 (página 4, líneas 6-9; página 8, líneas 13-21, figura 5) ajusta dicho punto de trabajo para provocar la metaestabilidad en la salida con más frecuencia y en D02 (párrafos 0040-0041 y párrafos 0103-105) se ajusta el punto de trabajo para conseguir un ratio de 0 y 1 uniforme a la salida. Por consiguiente, se considera que la etapas para fijar el punto de trabajo son unas de las varias posibilidades evidentes que un experto en la materia seleccionaría según las circunstancias.

- Etapa estacionaria: Una vez fijado el punto de trabajo, obtener números aleatorios a la salida del flip-flop.

Por lo tanto, se considera que la invención según la reivindicación R10 no se considera que implique actividad inventiva.

Reivindicaciones R11-R12

Según la reivindicación R11, la elección del desfase de trabajo Ft como la semisuma de los desfases F1 y F2 es simplemente una de varias posibilidades evidentes que un experto en la materia seleccionaría según las circunstancias; por ejemplo, en el documento D01 (página 4, líneas 6-9; página 8, líneas 13-21, figura 5) se ajusta el valor del desfase para provocar la metaestabilidad en la salida con más frecuencia mientras que el documento D02 (párrafos 0040-0041 y párrafos 0103-105) se ajusta dicho retardo para conseguir un ratio de 0 y 1 uniforme a la salida.

La activación de un puerto de salida una vez alcanzado el punto de trabajo Ft reivindicado en R12, se considera una característica obvia para un experto en la materia.

Por lo tanto, se considera que la invención según las reivindicaciones R11-R12 no se considera que implique actividad inventiva.