(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 707**

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.09.2014 PCT/EP2014/069756**

(87) Fecha y número de publicación internacional: **07.05.2015 WO15062780**

(96) Fecha de presentación y número de la solicitud europea: **17.09.2014 E 14772301 (9)**

(97) Fecha y número de publicación de la concesión europea: **02.08.2017 EP 3028140**

(54) Título: **Diseño de un circuito adecuado para generar bits aleatorios y circuito para generar bits aleatorios**

(30) Prioridad:

31.10.2013 DE 102013222218

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.11.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

BÖFFGEN, PASCALE y
DICHTL, MARKUS

(74) Agente/Representante:

LOZANO GANDIA, José

DISEÑO DE UN CIRCUITO ADECUADO PARA GENERAR BITS ALEATORIOS Y CIRCUITO PARA GENERAR BITS ALEATORIOS

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un equipo para diseñar un circuito adecuado para generar bits aleatorios y a un circuito para generar bits aleatorios. Se genera por ejemplo una secuencia de bits aleatorios, que se utiliza como número binario aleatorio. El procedimiento propuesto y el equipo, así como el circuito, sirven por ejemplo para implementar generadores de números aleatorios.

En aplicaciones relevantes para la seguridad, por ejemplo en procedimientos de autentificación asimétricos, son necesarias secuencias de bits aleatorios como números binarios aleatorios. Al respecto se desea, en particular en aplicaciones móviles, una inversión en hardware lo más reducida posible. Las medidas conocidas para generar números aleatorios utilizan fuentes aleatorias analógicas.

Como fuentes aleatorias analógicas se amplifican y digitalizan fuentes de ruidos, como por ejemplo el ruido de diodos Zener. Al respecto se unen la técnica de conexión digital con la analógica.

Además se utilizan osciladores en anillo y sus variantes como generadores de números aleatorios. En osciladores en anillo, que están constituidos por un número impar de inversores conectados uno tras otro, resulta por ejemplo una jitter (fluctuación de fase) aleatoria debido a tiempos de propagación oscilantes de las señales a través de los inversores. Esta jitter, es decir, una oscilación irregular en el tiempo cuando se modifica el estado de las señales enviadas a través de los inversores, puede acumularse cuando hay varias pasadas a través del circuito del oscilador en anillo, con lo que en definitiva resulta una señal analógica aleatoria.

La entidad solicitante conoce un llamado oscilador en anillo multipista. En consecuencia, se propone un equipo para generar bits aleatorios que incluye: varios equipos de representación, estando preparado el equipo de representación correspondiente para representar una cantidad n predeterminada de señales de entrada con ayuda de una representación combinatoria en una cantidad p predeterminada de señales de salida. Al respecto están concatenados los equipos de representación entre sí y está configurado al menos un bucle de realimentación**.** El bucle de realimentación está configurado en particular tal que una variación del estado de al menos una señal de salida de un equipo de representación elegido se lleva como una variación del estado de al menos una señal de entrada a otro equipo de representación.

Con preferencia no es el otro equipo de representación ningún equipo de representación directamente contiguo.

Al respecto existe en particular un bucle de realimentación cuando una variación de estado de al menos una señal de salida de realimentación de un determinado equipo de representación se lleva como una variación de estado de al menos una señal de entrada de otro equipo de representación tal que una o varias señales de salida del equipo de representación determinado se ve/n influida/s por la variación del estado de la señal de salida de realimentación.

Además está establecida al menos una representación combinatoria tal que una variación de estado de una señal de entrada del correspondiente equipo de representación en promedio se reproduce en más de una señal de salida del correspondiente equipo de representación.

La cantidad n de señales de entrada del correspondiente equipo de representación puede corresponderse con la cantidad p de señales de salida. No obstante, puede también pensarse en que n sea diferente de p, es decir, que con ayuda del correspondiente equipo de representación se reproduzcan los estados de las señales de entrada en estados de señales de salida, siendo la cantidad de señales de salida menor o mayor que la cantidad de señales de entrada para el correspondiente equipo de representación.

Los equipos de representación pueden ser puertas lógicas o combinatorias, que en particular realizan una representación biyectiva de n señales de entrada en n señales de salida. Las señales de entrada oscilan entre niveles que pueden asociarse a estados lógicos, como bits 1 o high (alto) o bien 0 o low (bajo). Bajo una reproducción biyectiva se entiende una reproducción inequívoca entre los 2^n valores lógicos posibles de las señales de entrada y los 2^n valores lógicos de las señales de salida.

En este sentido resulta con ayuda de los equipos de representación, en unas formas de realización del equipo, un oscilador en anillo de n pistas. Los equipos de representación pueden denominarse también nodos o puertas. La correspondiente representación combinatoria está realizada en particular tal que en promedio cuando tiene lugar una variación del estado de una señal de entrada tiene lugar un cambio de estado en más de una señal de salida. Esto da lugar a que el correspondiente jitter de la señal de entrada se reproduzca en varias señales de salida y por lo tanto se amplifique. Un jitter que se presente una sola vez en una señal, se copia con ayuda de los equipos de representación o bien de las reproducciones combinatorias allí implementadas en varias pistas de salida, con lo que los componentes del jitter apenas pueden compensarse.

Se puede hablar en cuanto al equipo también de un circuito oscilador en anillo multipista. Frente a los osciladores en anillo clásicos de una sola pista, existe en particular la ventaja de que pueden tomarse valores de bits aleatorios con una mayor velocidad de datos. Por ejemplo puede derivarse una señal de bits aleatoria en una o varias de las rutas de datos que resultan en base a las n señales de entrada y/o salida.

Se puede decir que el equipo desarrolla "oscilaciones" o propaga cambios de señal en el circuito. Con preferencia depende al menos una de las señales de salida causalmente de sí misma, al realimentarse, realizándose la realimentación con ayuda de al menos una representación intercalada.

Para un tal oscilador en anillo multipista es especialmente ventajoso que no presente ningún punto fijo, ya que la existencia de un punto fijo puede dar lugar a que el anillo entre en un estado estacionario sin oscilaciones, con lo que ya no podrían generarse otros bits aleatorios.

Se conoce por el estado de la técnica la generación aleatoria de un circuito en anillo con una determinada longitud hasta que se encuentra un oscilador en anillo multipista sin un punto fijo.

El documento de patente US 8099449 B1 da a conocer un método para generar números aleatorios mediante una oscilación multiplicadora con un circuito multiplicador para recibir señales de entrada asíncronas, siendo una primera señal de entrada una señal de realimentación en base a una salida del multiplicador.

Partiendo de esta base, consiste el objetivo de la presente invención en proporcionar un procedimiento mejorado y un equipo para diseñar circuitos complejos y/o flexibles.

Este objetivo se logra de acuerdo con la invención mediante un procedimiento, un equipo y un circuito según las características indicadas en las reivindicaciones independientes. Otras variantes ventajosas de la invención se indican en las reivindicaciones dependientes.

Se propone un procedimiento para diseñar un circuito adecuado para generar bits aleatorios, en el que

- el circuito presenta un número m de equipos de representación;
- a cada uno de los equipos de representación se lleva un número n de bits de entrada, siendo n un valor mayor que 1;
- mediante cada uno de los equipos de representación se ejecuta mediante la correspondiente función una representación biyectiva de los n bits de entrada en n bits de salida, presentando las siguientes etapas:

  (a) elección de un equipo de representación j-ésimo desde el primer equipo de representación hasta el equipo de representación m-ésimo y prescripción de una función específica j-ésima a partir de un conjunto de representaciones biyectivas como función j-ésima, sucediendo que

- mediante una concatenación j-ésima de las j funciones al prescribir la función específica j-ésima como función j-ésima, se ejecuta una representación j-ésima sin puntos fijos;
- mediante la concatenación j-ésima, se aplican las j funciones en una secuencia ascendente, comenzando con la primera función;

  (b) elección de al menos un equipo de representación i-ésimo desde el primer equipo de representación hasta el equipo de representación m-ésimo, siendo i diferente de j y prescripción de una función específica i-ésima a partir de un conjunto de representaciones biyectivas como función i-ésima, sucediendo que

- mediante una concatenación i-ésima de las i funciones al prescribir la función específica i-ésima como función i-ésima, se ejecuta una representación i-ésima sin puntos fijos;
- mediante la concatenación i-ésima, se aplican las i funciones en una secuencia ascendente, comenzando con la primera función.

Por lo tanto discurren por ejemplo n señales a través de un circuito con forma anular con m equipos de representación, denominados también nodos. Cada nodo está formado por puertas lógicas. Cada nodo tiene n bits de input (entrada) y output (salida). Los nodos están elegidos tal que su representación de los n bits de input sobre los n bits de output significa una representación biyectiva o biyección, es decir, cuando los inputs asumen todos los 2^n valores posibles, asumen también los outputs todos los 2^n valores posibles, desde luego en general en otra secuencia.

El circuito es en particular un oscilador anular multipista. En particular origina una variación de estado de una señal de entrada del correspondiente equipo de representación en promedio una variación en más de una señal de salida.

Para asegurar que un tal circuito con forma anular – denominado abreviadamente anillo – oscila continuamente, no tiene que tener el circuito ningún punto fijo. Para describir con más exactitud las circunstancias del punto fijo, se separa el anillo en un punto cualquiera, pero que sea fijo, entre los nodos.

Entonces se tiene un circuito con n bits de input (entrada), que a través de m nodos, de los cuales cada uno ejecuta una representación biyectiva f_i para un índice i que tiene los valores 1 a m de n bits de entrada en n bits de salida, aporta tras el nodo m-ésimo n bits de output (salida).

En particular, resulta una m-ésima representación o representación global f_m' del anillo dividido mediante una concatenación m-ésima $f_m' = f_m \circ f_{m-1} \circ f_{m-2} \circ \ldots \circ f_2 \circ f_1$, leyéndose en la presente solicitud una concatenación de funciones de derecha a izquierda, es decir, se aplica primero f_1, a continuación f_2, etc. Aplicar significa aquí que la primera función f_1 se aplica a una primera tupla de entrada en el primer equipo de representación, que está formado por los n bits de entrada, es decir, la primera tupla de entrada se representa en una primera tupla de salida, según una norma de representación de la primera función. La segunda función se aplica en particular a la primera tupla de salida, que forma así una segunda tupla de entrada para el segundo equipo de representación. El segundo equipo de representación proporciona a continuación una segunda tupla de salida. Luego se aplica una tercera función, por ejemplo a la segunda tupla de salida, etc.

El anillo completo queda entonces exactamente libre de puntos fijos cuando para todas las posibles n tuplas x como primera tupla de entrada es $f_m'(x) \neq x$.

En texto, esto significa que para todas las posibles n tuplas x, la primera tupla de entrada no es igual a la tupla de salida m-ésima en el equipo de representación m-ésimo.

De acuerdo con la invención, se elige como función j-ésima del equipo de representación j-ésimo una función específica j-ésima de un conjunto de representaciones biyectivas, con lo que mediante una concatenación j-ésima de las j funciones se realiza una representación j-ésima libre de puntos fijos. Se buscan biyecciones de n a n bits como candidatos para la función j-ésima hasta que se encuentra una función j-ésima específica que cumple la condición de que la concatenación de todas las funciones precedentes en el anillo hasta la función j-ésima está libre de puntos fijos y la misma se utiliza como función j-ésima. Por ejemplo puede realizarse la búsqueda de la función j-ésima aleatoriamente.

A continuación se elige al menos un equipo de representación i-ésimo desde el primer hasta el m-ésimo equipo de representación, siendo i ≠ de j. A la función i-ésima se asocia una función específica i-ésima de entre un conjunto de representaciones biyectivas, con lo que mediante una concatenación i-ésima de las i funciones se realiza una representación i-ésima libre de puntos fijos.

También entonces se analizan biyecciones de n a n bits como candidatos para la función i-ésima, hasta que para todas las posibles n tuplas x la aplicación de la concatenación de la primera hasta la i-ésima función sobre la primera tupla de entrada aporta una tupla de salida i-ésima, que es distinta de la primera tupla de entrada. Por ejemplo puede realizarse la búsqueda de la función i-ésima aleatoriamente.

Se analiza entonces por lo tanto la representación de la primera tupla de entrada en la tupla de salida i-ésima, es decir, la concatenación i-ésima de la primera función hasta la función i-ésima en relación con la característica de libre de puntos fijos. Puede considerarse por lo tanto en particular una concatenación parcial dentro del circuito.

El procedimiento descrito hace posible un diseño eficiente de circuitos con forma anular de cualquier longitud y que pueden acortarse flexiblemente para generar bits aleatorios.

El circuito diseñado según el procedimiento descrito hace posible la conmutación flexible de la realimentación desde la salida del equipo de representación j-ésimo a la entrada del primer equipo de representación a una realimentación desde la salida del equipo de representación i-ésimo a la entrada del primer equipo de representación. Entonces se forman con ambas realimentaciones anillos libres de puntos fijos.

Según un perfeccionamiento, se elige basándose en el procedimiento de diseño antes descrito, cada uno de los m-1 equipos de representación a partir del primer equipo de representación hasta el equipo de representación m-ésimo y una función específica correspondiente se asocia a la correspondiente función, con lo que cada concatenación $fj' = fj \circ \ldots \circ f1$ para todos los j de 1 a m, inclusive 1 y m, significa una representación libre de puntos fijos de la primera tupla de entrada. Para la primera función f_1 es suficiente entonces elegir una función libre de puntos fijos, ya que para crear la primera tupla de salida no se utiliza ninguna concatenación. Con ello resulta una flexibilidad especialmente alta al acortar el circuito.

El circuito así diseñado hace posible la utilización de un oscilador anular u oscilador anular multipista con longitud flexible. Es posible diseñar, a partir del anillo libre de puntos fijos diseñado mediante el procedimiento descrito, sin necesidad de puertas adicionales, anillos libres de puntos fijos de longitud variable. Por ejemplo se obtiene, mediante realimentación de los bits de salida de un nodo i-ésimo

cualquiera de entre los m nodos a las entradas del primer nodo, anillos libres de puntos fijos de la longitud i, es decir, longitudes con valores de 1 a m.

Para un anillo elegido aleatoriamente con por ejemplo 100 nodos y en cada caso 4 bits de entrada y de salida, la probabilidad de obtener un anillo libre de puntos fijos, que también pueda acortarse hasta cualquier longitud, manteniendo con ello su característica de libre de puntos fijos, sólo es de aprox. $2{,}53 \times 10^{-43}$. Un tal procedimiento no sería realizable. Por el contrario se indica según el procedimiento descrito una solución iterativa eficiente.

El procedimiento iterativo descrito se utiliza sólo una vez en el diseño del anillo. Posteriores reestructuraciones que acortan el anillo, por ejemplo desde una longitud de j equipos de representación, encontrándose j entre 1 y m o pudiendo ser m, a i equipos de representación con i mayor o igual a 1 e inferior a j, no originan, ventajosamente, ningún nuevo coste para asegurar la existencia de un oscilador libre de puntos fijos.

Según una variante, se configura el circuito como oscilador de anillo multipista. Esto posibilita el diseño eficiente de un circuito libre de puntos fijos, en el que existe una gran cantidad n de bits de entrada por cada equipo de representación y debiendo ser posible una realimentación variable al primer equipo de representación, con lo que también el anillo acortado mediante la realimentación está libre de puntos fijos.

La invención se refiere además a un equipo para diseñar un circuito adecuado para generar bits aleatorios, en el que

- el circuito presenta un número m de equipos de representación;
- cada uno de los equipos de representación recibe un número n de bits de entrada, siendo n un valor mayor que 1;
- mediante cada uno de los equipos de representación puede ejecutarse mediante la correspondiente función una representación biyectiva de los n bits de entrada en n bits de salida, incluyendo:

  una unidad j-ésima

  para elegir un equipo de representación j-ésimo desde el primer equipo de representación hasta el equipo de representación m-ésimo y

  para prescribir una función específica j-ésima a partir de un conjunto de representaciones biyectivas como función j-ésima, sucediendo que

  mediante una concatenación j-ésima de las j funciones al prescribir la función específica j-ésima como función j-ésima, puede ejecutarse una representación j-ésima sin puntos fijos y

  mediante la concatenación j-ésima, pueden aplicarse las j funciones en una secuencia ascendente, comenzando con la primera función;

- una unidad i-ésima

  para elegir al menos otro equipo de representación i-ésimo desde el primer equipo de representación hasta el equipo de representación m-ésimo, siendo i diferente de j y

  para prescribir una función específica i-ésima de entre un conjunto de representaciones biyectivas como función i-ésima, sucediendo que

  mediante una concatenación i-ésima de las i funciones al prescribir la función específica i-ésima como función i-ésima, puede ejecutarse una representación i-ésima sin puntos fijos y

  mediante la concatenación i-ésima, pueden aplicarse las i funciones en una secuencia ascendente comenzando con la primera función.

Con ayuda del equipo propuesto se determina un circuito de utilización flexible. Pueden generarse sin coste adicional en cuanto a puertas dentro del circuito, mediante conmutación adecuada de las líneas de unión, anillos libres de puntos fijos de longitud variable. Con un anillo de la longitud m determinado con ayuda del equipo propuesto, se dispone de anillos flexibles también adecuados con longitudes inferiores.

La unidad j-ésima y la unidad i-ésima pueden estar implementadas en técnica de hardware y/o también en técnica de software. En una implementación en técnica de hardware puede estar configurada la correspondiente unidad como equipo o como parte de un equipo, por ejemplo como ordenador o como microprocesador. En una implementación en técnica de software puede estar configurada la correspondiente unidad como producto de programa de ordenador, como una función, como una rutina, como parte de un código de programa o como objeto que puede ejecutarse.

La invención se refiere además a un circuito para generar bits aleatorios, en el que

- el circuito presenta un número m de equipos de representación;
- cada uno de los equipos de representación recibe un número n de bits de entrada, siendo n un valor mayor que 1;
- mediante cada uno de los equipos de representación puede ejecutarse mediante la correspondiente función una representación biyectiva de los n bits de entrada en n bits de salida;

- puede elegirse un equipo de representación j-ésimo desde el primer equipo de representación hasta el equipo de representación m-ésimo y puede prescribirse como la función j-ésima una función específica j-ésima a partir de un conjunto de representaciones biyectivas, sucediendo que

  mediante una concatenación j-ésima de las j funciones al prescribir la función específica j-ésima como función j-ésima, puede ejecutarse una representación j-ésima sin puntos fijos y

  mediante la concatenación j-ésima, pueden aplicarse las j funciones en una secuencia ascendente, comenzando con la primera función;

- puede elegirse al menos otro equipo de representación i-ésimo desde el primer equipo de representación hasta el equipo de representación m-ésimo, siendo i diferente de j y puede prescribirse como función i-ésima una función específica i-ésima de entre un conjunto de representaciones biyectivas, sucediendo que

  mediante una concatenación i-ésima de las i funciones al prescribir la función específica i-ésima como función i-ésima, puede ejecutarse una representación i-ésima sin puntos fijos y

  mediante la concatenación i-ésima, pueden aplicarse las i funciones en una secuencia ascendente comenzando con la primera función.

El circuito propuesto o el anillo propuesto de la longitud m se puede acortar flexiblemente sin necesitar puertas adicionales. Puede conmutarse entre una realimentación desde la salida del equipo de representación j-ésima hasta la entrada del primer equipo de representación a una realimentación desde la salida del equipo de representación i-ésimo hasta la entrada del primer equipo de representación. Ambos anillos generados están libres de puntos fijos.

Puede ser en particular procedente mantener flexible la longitud del anillo, para poder influir sobre el consumo de corriente del anillo. Otra ventaja adicional de los anillos con longitud variable es que, puesto que los osciladores en anillo multipista muy cortos tienden a oscilaciones periódicas en vez de caóticas, con un anillo de acuerdo con la invención puede buscarse un anillo corto en el que se presentan oscilaciones caóticas sin modificar las funciones lógicas.

La invención se describirá a continuación más en detalle con un ejemplo de realización en base a una figura.

Se muestra en:

figura 1 una representación esquemática de un circuito según un ejemplo de realización de la invención.

En la figura se representa un circuito 10 con un número m, m = 4, de equipos de representación K_1, K_2, $K_3 = K_j$, $K_4 = K_i = K_m$.

A modo de ejemplo se genera un circuito de la longitud 4 y el mismo se cierra para formar un anillo. En la figura se representa un oscilador en anillo multipista con tres pistas (n = 3).

En el primer equipo de representación K_1 se elige una biyección aleatoria como primera función f_1, con lo que la primera representación está libre de puntos fijos. Con ello se ha encontrado una primera función específica g_1. En el segundo equipo de representación K_2 se elige una biyección como segunda función f_2, con lo que la segunda concatenación f_2' de la primera función f_1 y la segunda función f_2 está libre de puntos fijos. Con ello se ha encontrado una segunda función específica g_2. Igualmente se elige en el tercer equipo de representación K_3 una biyección como tercera función f_3, con lo que la tercera concatenación f_3' de la primera función f_1, segunda función f_2 y tercera función f_3 está libre de puntos fijos. Con ello se ha encontrado una tercera función específica g_3. Igualmente se elige en el cuarto equipo de representación K_4 una biyección como cuarta función f_4, con lo que la cuarta concatenación f_4' de la primera función f_1, segunda función f_2, tercera función f_3 y cuarta función f_4 está libre de puntos fijos. Con ello se ha encontrado una cuarta función específica g_4.

El siguiente fragmento VHDL muestra cómo está constituido un anillo de 4 pistas de la longitud 4 de Spartan-3 Look-Up-Tables (tablas de búsqueda), abreviadamente LUTs, para un chip Xilinx. Cada uno de los equipos de representación K_1, K_2, K_3, K_4 está compuesto por 4 LUTs, representando cada LUT los 4

bits de input (entrada) sobre un bit de output (salida). La representación en cada equipo de representación K_1, K_2, K_3, K_4 es una biyección del conjunto de todas las tuplas de 4 bits sobre el conjunto de todas las tuplas de 4 bits.

- LUT4: 4-input Look-Up Table with general output (tabla de búsqueda de 4 entradas con salida general)
- Spartan-3
- Xilinx HDL Libraries Guide (guía de librerias), version 12.2

LUT0inst:LUT4
mapeo genérico (generic map) (INIT ≥ x"c92e")
mapeo de puertos (port map)
(O ≥ salida (4), I0 ≥ salida (0), I1 ≥ salida
(1), I2 ≥ salida (2), I 3 ≥ salida (3));
LUT1inst:LUT4
mapeo genérico (INIT ≥ x"a8da")
mapeo de puertos
(O ≥ salida (5), I0 ≥ salida (0), I1 ≥ salida
(1), I2 ≥ salida (2), I 3 ≥ salida (3));
LUT2inst:LUT4
mapeo genérico (INIT ≥ x"b1a3")
mapeo de puertos
(O ≥ salida (6), I0 ≥ salida (0), I1 ≥ salida
(1), I2 ≥ salida (2), I 3 ≥ salida (3));
LUT3inst:LUT4
mapeo genérico (INIT ≥ x"44eb")
mapeo de puertos
(O≥salida (7), I0 ≥ salida (0), I1 ≥ salida
(1), I2 ≥ salida (2), I 3 ≥ salida (3));
LUT4inst:LUT4
mapeo genérico (INIT ≥ x"21b7")
mapeo de puertos
(O ≥ salida (8), I0 ≥ salida (4), I1 ≥ salida
(5), I2 ≥ salida (6), I 3 ≥ salida (7));
LUT5inst:LUT4
mapeo genérico (INIT ≥ x"7a23")
mapeo de puertos
(O ≥ salida (9), I0 ≥ salida (4), I1 ≥ salida
(5), I2 ≥ salida (6), I 3 ≥ salida (7));
LUT6inst:LUT4
mapeo genérico (INIT ≥ x"1d0f")
mapeo de puertos
(O ≥ salida (10), I0 ≥ salida (4), I1 ≥ salida
(5), I2 ≥ salida (6), I3 ≥ salida (7));
LUT7inst:LUT4
mapeo genérico (INIT ≥ x"cda2")
mapeo de puertos
(O ≥ salida (11), IO ≥ salida (4), I1 ≥ salida
(5), I2 ≥ salida (6), I3 ≥ salida(7));
LUT8inst:LUT4
mapeo genérico (INIT ≥ x"6d2c")
mapeo de puertos
(O ≥ salida (12), IO ≥ salida (8), I1 ≥ salida
(9), I2 ≥ salida (10), I3 ≥ salida (11));
LUT9inst:LUT4
mapeo genérico (INIT ≥ x"5f81")
mapeo de puertos
(O ≥ salida (13), I0 ≥ salida (8), I1 ≥ salida
(9), I2 ≥ salida (10) , I3 ≥ salida (11));
LUT10inst:LUT4
mapeo genérico
mapeo de puertos
(O ≥ salida (14), I0 ≥ salida (8), I1 ≥ salida
(9), I2 ≥ salida (10), I3 ≥ salida (11));
LUT11inst:LUT4
mapeo genérico (INIT ≥ x"7658")
mapeo de puertos
(O ≥ salida (15), I0 ≥ salida (8), I1 ≥ salida
(9), I2 ≥ salida (10) , I3 ≥ salida (11));

LUT12inst:LUT4
mapeo genérico (INIT ≥ x"1c5e")
mapeo de puertos
(O ≥ salida (16), I0 ≥ salida (12), I1 ≥ salida
(13), I2 ≥ salida (1 4), I3 ≥ salida (15));
LUT13inst:LUT4
mapeo genérico (INIT ≥ x"16e9")
mapeo de puertos
(O ≥ salida (17), I0 ≥ salida (12), I1 ≥ salida
(13), I2≥salida (1 4), I3≥salida (15));
LUT14inst:LUT4
mapeo genérico (INIT ≥ x"9353")
mapeo de puertos
(O ≥ salida (18), I0 ≥ salida (12), I1 ≥ salida
(13), I2 ≥ salida (14), I3 ≥ salida (15);
LUT15inst:LUT4
mapeo genérico (INIT ≥ x"bc31")
mapeo de puertos
(O ≥ salida (19), I0 ≥ salida (12), I1 ≥ salida
(13), I2 ≥ salida(14), I3 ≥ salida (15));

La función lógica de la LUT se adjunta entonces como parámetro hexadecimal en forma de una tabla de valores de 16 bits como el llamado parámetro INIT, por ejemplo INIT ≥ x"bc31" para la última LUT.

Con las siguientes 4 instrucciones puede transformarse el circuito 10 en un anillo libre de puntos fijos de la longitud 4 con el primer equipo de representación K1, el segundo equipo de representación K2, el tercer equipo de representación K3 y el cuarto equipo de representación K4:

salida (0) ≤ salida (16);
salida (1) ≤ salida (17);
salida (2) ≤ salida (18);
salida (3) ≤ salida (19);

Con las siguientes 4 asignaciones puede acortarse por ejemplo el circuito 10 en un anillo libre de puntos fijos de la longitud 2 con el primer equipo de representación K1 y el segundo equipo de representación K2:

salida (0) ≤ salida (8);
salida (1) ≤ salida (9);
salida (2) ≤ salida (10);
salida (3) ≤ salida(11);

Así es posible una conmutación flexible entre las longitudes 4 y 2.

Puesto que esta conmutación flexible es posible para cualesquiera longitudes y para cualesquiera acortamientos, puede por ejemplo reducirse el consumo de corriente claramente mediante la conmutación y con ello adaptarse a exigencias a formular a un generador de números aleatorios en función del campo de aplicación, sin que sea necesario un nuevo diseño del circuito 10.

REIVINDICACIONES

1. Procedimiento para diseñar un circuito (10) adecuado para generar bits aleatorios,
en el que
- el circuito (10) presenta un número m de equipos de representación (K_1, K_2,… K_j,… K_i,… K_m);
- a cada uno de los equipos de representación (K1, K2,… Kj,… Ki,… Km) se lleva un número n de bits de entrada, siendo n un valor mayor que 1;
- mediante cada uno de los equipos de representación (K_1, K_2,… K_j,… K_i,… K_m) se ejecuta mediante la correspondiente función (f_1, f_2,… f_j,…f_i,…, f_m) una representación biyectiva de los n bits de entrada en n bits de salida,

presentando las siguientes etapas:

(a) elección de un equipo de representación j-ésimo (K_j) desde el primer equipo de representación (K_1) hasta el equipo de representación m-ésimo (K_m) y prescripción de una función específica j-ésima (g_i) a partir de un conjunto de representaciones biyectivas como función j-ésima (f_j), sucediendo que

- mediante una concatenación j-ésima (f_j') de las j funciones (f_1,… f_j) al prescribir la función específica j-ésima (g_j) como función j-ésima (f_j), se ejecuta una representación j-ésima sin puntos fijos;
- mediante la concatenación j-ésima, se aplican las j funciones en una secuencia ascendente, comenzando con la primera función (f_1);

(b) elección de al menos un equipo de representación i-ésimo (K_i) desde el primer equipo de representación (K_1) hasta el equipo de representación m-ésimo (K_m), siendo i diferente de j y prescripción de una función específica i-ésima (g_i) a partir de un conjunto de representaciones biyectivas como función i-ésima (f_i), sucediendo que

- mediante una concatenación i-ésima (f_i') de las i funciones (f_1,… f_i) al prescribir la función específica i-ésima (g_i) como función i-ésima (f_i), se ejecuta una representación i-ésima sin puntos fijos;
- mediante la concatenación i-ésima, se aplican las i funciones en una secuencia ascendente comenzando con la primera función (f1).

2. Procedimiento de acuerdo con la reivindicación 1,
en el que
- se elige cada uno de los m equipos de representación de entre el primer equipo de representación (K1) hasta el equipo de representación m-ésimo (Km) y se prescribe según las etapas (a) o (b) una función específica correspondiente (g1, g2,… gj,…gi,…, gm) como la correspondiente función (f1, f2,… fj,…fi,…, fm).

3. Procedimiento de acuerdo con la reivindicación 1 ó 2,
en el que el circuito (10) se configura como oscilador en anillo multipista.

4. Equipo para diseñar un circuito (10) adecuado para generar bits aleatorios,
en el que
- el circuito (10) presenta un número m de equipos de representación (K1, K2,… Kj, … Ki, … Km);
- cada uno de los equipos de representación (K_1, K_2,… K_j,… K_i, … K_m) recibe un número n de bits de entrada, siendo n un valor mayor que 1;
- mediante cada uno de los equipos de representación (K_1, K_2,… K_j, … K_i, … K_m) puede ejecutarse mediante la correspondiente función (f_1, f_2, … f_j, …f_i,…, f_m) una representación biyectiva de los n bits de entrada en n bits de salida,

incluyendo:

- una unidad j-ésima

para elegir un equipo de representación j-ésimo (K_j) desde el primer equipo de representación (K_1) hasta el equipo de representación m-ésimo (K_m) y

para prescribir una función específica j-ésima (g_j) a partir de un conjunto de representaciones biyectivas como función j-ésima (f_j), sucediendo que

mediante una concatenación j-ésima (f_j') de las j funciones (f_1,… f_j) al prescribir la función específica j-ésima (g_j) como función j-ésima (f_j), puede ejecutarse una representación j-ésima sin puntos fijos y

mediante la concatenación j-ésima, pueden aplicarse las j funciones en una secuencia ascendente, comenzando con la primera función (f_1);

- una unidad i-ésima

para elegir al menos otro equipo de representación i-ésimo (K_i) de entre el primer equipo de representación (K_1) hasta el equipo de representación m-ésimo (K_m), siendo i diferente de j y

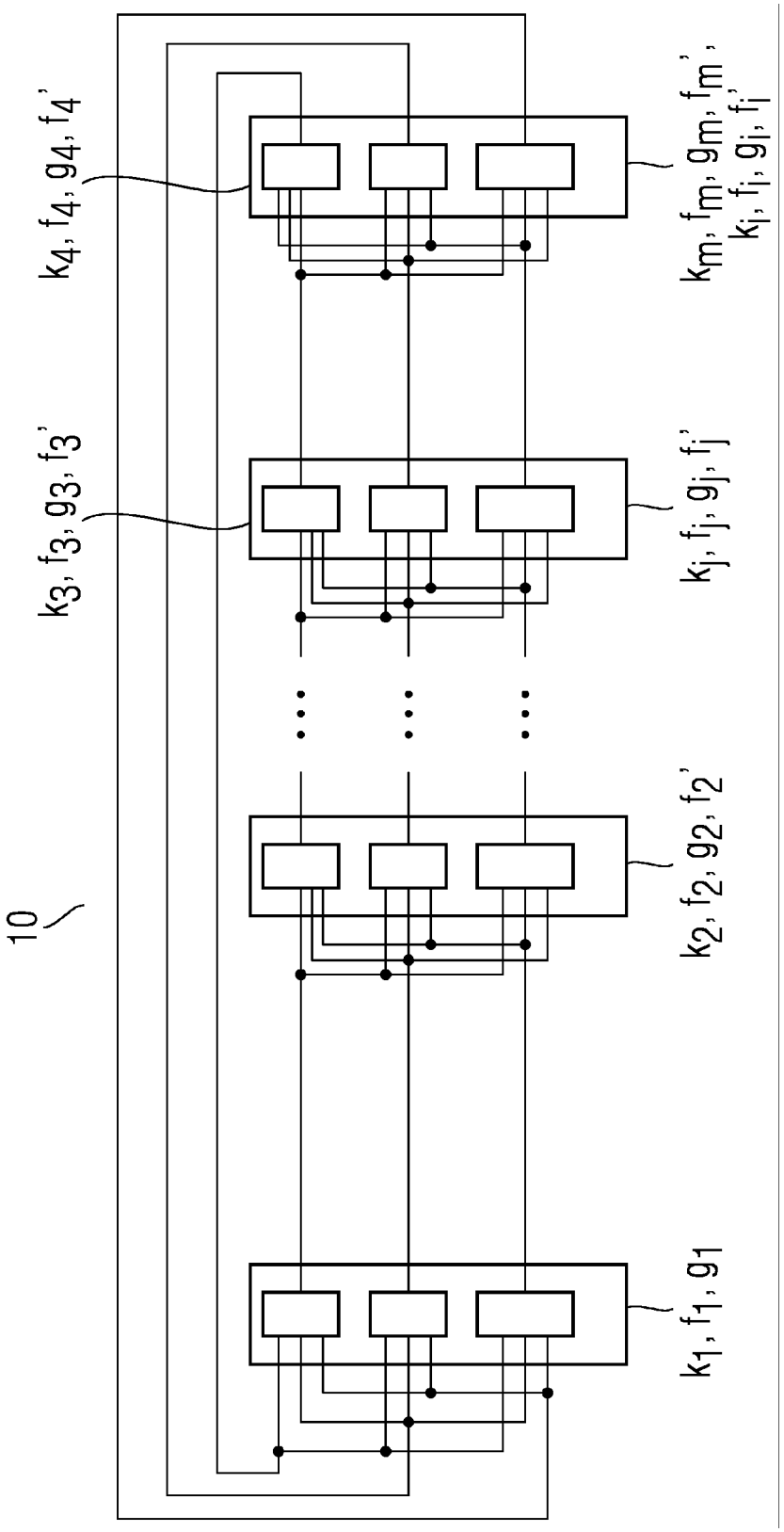
para prescribir una función específica i-ésima (g_i) de entre un conjunto de representaciones biyectivas como función i-ésima (f_i), sucediendo que

mediante una concatenación i-ésima (f_i') de las i funciones (f_1,… f_i) al prescribir la función específica i-ésima (g_i) como función i-ésima (f_i), puede ejecutarse una representación i-ésima sin puntos fijos y

mediante la concatenación i-ésima, pueden aplicarse las i funciones en una secuencia ascendente, comenzando con la primera función (f_1).

5. Circuito (10) para generar bits aleatorios,
en el que
- el circuito (10) presenta un número m de equipos de representación (K_1, K_2,… K_j, … K_i, … K_m);
- cada uno de los equipos de representación (K_1, K_2,… K_j, … K_i, … K_m) recibe un número n de bits de entrada, siendo n un valor mayor que 1;

caracterizado porque
- mediante cada uno de los equipos de representación (K1, K2,… Kj, … Ki, … Km) puede ejecutarse mediante la correspondiente función (f1, f2, … fj, …fi,…, fm) una representación biyectiva de los n bits de entrada en n bits de salida;
- puede elegirse un equipo de representación j-ésimo (Kj) desde el primer equipo de representación (K1) hasta el equipo de representación m-ésimo (Km) y puede prescribirse como la función j-ésima (fj) una función específica j-ésima (gj) a partir de un conjunto de representaciones biyectivas,
  sucediendo que
  mediante una concatenación j-ésima (fj') de las j funciones (f1,… fi) al prescribir la función específica j-ésima (gj) como función j-ésima (fj), puede ejecutarse una representación j-ésima sin puntos fijos y
  mediante la concatenación j-ésima pueden aplicarse las j funciones en una secuencia ascendente, comenzando con la primera función (f_1);
- puede elegirse al menos otro equipo de representación i-ésimo (K_i) desde el primer equipo de representación (K_1) hasta el equipo de representación m-ésimo (K_m), siendo i diferente de j y puede prescribirse como función i-ésima (f_i) una función específica i-ésima (g_i) de entre un conjunto de representaciones biyectivas, sucediendo que
  mediante una concatenación i-ésima (f_i') de las i funciones (f_1,… f_i) al prescribir la función específica i-ésima (g_i) como función i-ésima (f_i), puede ejecutarse una representación i-ésima sin puntos fijos y
  mediante la concatenación i-ésima, pueden aplicarse las i funciones en una secuencia ascendente. comenzando con la primera función (f_i).


10
k4, f4, g4, f4'
k3, f3, g3, f3'
k2, f2, g2, f2'
k1, f1, g1
km, fm, gm, fm',
ki, fi, gi, fi'
kj, fj, gj, fj'