FUENTES DE CADENA ALEATORIA DE BITS USANDO FUENTES DÉBILES

Campo técnico de la invención

El presente concepto inventivo se refiere a dispositivos de seguridad y, más particularmente, a generadores de números aleatorios utilizados por ejemplo en dispositivos de seguridad.

Descripción del estado de la técnica

A medida que se han desarrollado tecnologías basadas en la información y la comunicación, el cifrado y el descifrado de información se han convertido en importantes formas de proteger la confidencialidad de la información. Los números aleatorios se utilizan en diversas aplicaciones, incluyendo, entre otras, la generación de claves secretas para los sistemas de seguridad.

En el estado de la técnica se encuentran diversas formas de implementar generadores de números aleatorios. Generalmente, un generador aleatorio verdadero como se define en US 9335972 B2 produce un número que es impredecible, basándose en un fenómeno físico como el ruido térmico y está compuesto de tres partes principales. Para la primera parte se necesita una fuente de entropía física que proporciona la imprevisibilidad que lo diferencia de los generadores pseudo-aleatorios. Para la segunda parte, es necesario convertir el fenómeno físico en un dato digital mediante una etapa de digitalización. Y en la tercera parte, idealmente los datos extraídos de un generador de números aleatorios deberán contener igual número de valores lógicos de “uno” y “cero”, además de no tener patrones de datos que puedan considerarse periódicos o repetitivos. Sin embargo esto no ocurre, y es considerado un sesgo o polarización que es asociado a la naturaleza de las fuentes de entropía. Este fenómeno se ve aumentado debido a la sensibilidad a variaciones ambientales y de fabricación, haciendo necesario hacer un post-procesamiento a los datos digitalizados de tal forma que se reduzca el sesgo asociado a la fuente de entropía. Aunque el resultado de los generadores aleatorios verdaderos que se usan actualmente sigue teniendo una polarización, se denominan generadores verdaderos si los resultados de las pruebas propuestas por estándares cumplen con ciertas propiedades de entropía. A estos generadores aleatorios verdaderos que cumplen propiedades de entropía de acuerdo a los estándares como por ejemplo, el estándar NIST (*National Institute of Standards and Technology*), los denominaremos generadores de entropía débiles o fuentes débiles.

Con el objetivo de superar las limitaciones de las fuentes de entropía, se han propuesto alternativas donde se observa una fuerte tendencia al uso de circuitos en el dominio digital más que en el analógico dado su inherente robustez a variaciones de voltaje, temperatura y de proceso de fabricación. Sin embargo, la fuente de entropía siempre tiene un sesgo

asociado haciendo necesario el uso de complejos sistemas de calibración y además el uso de pos-procesamiento para garantizar que los datos de salida cumplan con las pruebas estadísticas que proporcionan agencias de estándares como el, NIST (*National Institute of Standards and Technology*). Estas pruebas estadísticas permiten identificar si una secuencia puede ser considera lo suficientemente aleatoria para ser usada en aplicaciones de criptografía o en general de seguridad informática.

La manera de implementar generadores de números aleatorios es similar en el estado del arte, construyendo sistemas donde los resultados siempre están limitados principalmente por la polarización y susceptibilidad a variaciones de las fuentes de entropía. Se considera que todas las fuentes de entropía que se pueden construir físicamente son fuentes de entropía débiles, ya que su entropía es limitada y su distribución nunca a llegar ser uniforme como la de una fuente ideal. Sin embargo, esta ha sido hasta la fecha, la forma tradicional de aproximarse a la construcción de generadores de verdaderos números aleatorios, es decir, que no son predecibles a cierto grado de acuerdo a los resultados de las pruebas propuestas por NIST.

Se ha demostrado matemáticamente que el uso de una única fuente débil nunca puede generar una buena aproximación a un número con una distribución uniforme en su estadística. El trabajo de (Chattopadhyay, 2016) menciona que la estadística de una secuencia generada a partir de una fuente de entropía débil difiere considerablemente de una distribución uniforme (que es lo que se esperaría si fuera aleatoria), y estudia la posibilidad de construir un generador empleando dos fuentes de entropía. Los autores prueban que teórica y matemáticamente es posible a partir de dos fuentes débiles obtener un generador de números aleatorios con distribución cercana a la uniforme. Sin embargo, no se describe ni divulga ninguna metodología, proceso o aparato para la realización e implementación a nivel de circuito.

En la literatura se encuentra que una alternativa al uso de verdaderos generadores de números aleatorios son los generadores pseudo-aleatorios. Los generadores pseudo-aleatorios hacen uso de una semilla para generar secuencias de números pseudo-aleatorios de mayor longitud. Una semilla se puede definir con un número corto uniforme aleatorio. En la referencia US8019802B2 proponen un generador pseudo-aleatorio y usan múltiples fuentes de entropía para generar las semillas del mismo. La desventaja de los generadores pseudo-aleatorios es la dependencia absoluta de la semilla, si la semilla se conoce toda secuencia de números generados puede predecirse.

En el estado de la técnica también se encuentra la referencia US9569176B2 donde se plantea el uso de diferentes fuentes de entropía para generar diferentes niveles de confidencialidad. Los números generados a partir de fuentes de entropía que se asumen están disponibles en un sistema operativo o en el *hardware* de un computador, son clasificados con base en la

entropía de cada fuente. La utilización de cada uno queda limitada entonces por un sistema que asigna pesos según su nivel de entropía, dándole mayor prioridad de uso a los que tienen mayor entropía o la misma prioridad en caso de que coincidan. Es decir que directamente no están extrayendo entropía de una fuente a partir de otra, sino que aprovechan la generación de las fuentes disponibles y combinan su uso. Como se indica, es un generador pseudo-aleatorio y su uso está limitado por el hecho de que es necesario tener disponibles un sistema operativo o sistema de cómputo completo donde se encuentren las fuentes de entropía necesarias, además que no se aprovecha en su totalidad la entropía de cada fuente.

En el caso del documento US9405510B2, se propone el uso de dos osciladores de anillo como fuente de entropía, en donde uno de ellos usa un interruptor que permite cambiar su operación modo de oscilación a modo meta-estable. Además, utiliza una unidad para combinar la entropía de los dos osciladores de anillo. En este caso la desventaja es que el uso del interruptor hace que la implementación no se pueda construir completamente con compuertas digitales aumentado su complejidad y usa una única fuente de entropía.

Al usar únicamente compuertas digitales para implementar un circuito como un generador de números aleatorios, se logra reducir la complejidad de su construcción y reproducción, además, de mantener un consumo de recursos tanto en área como en consumo de potencia reducidos. La propuesta de US 9335972 B2 se enfoca en la generación de números aleatorios empleando únicamente compuertas digitales, lo que permite describir el circuito en un lenguaje de descripción de hardware y ser sintetizado como se hace en una FPGA, reduciendo tiempos de implementación. La fuente de entropía en este caso se basa en el concepto de colapso de un oscilador de anillo *multimode*, que se inicia operando en un primer modo y luego su frecuencia colapsa a la natural en un tiempo que es aleatorio y usado para generar el respectivo número. Sin embargo, usa una única fuente de entropía por lo que se limita la estadística de los datos de salida.

Así las cosas no se encuentra en el estado del arte un documento que describa la implementación de un generador de números aleatorios con distribución cercana a la uniforme que parta de dos fuentes de entropías con algún tipo de sesgo y obtenga una fuente de alta aleatoriedad y de alta resistencia a ataques.

Breve descripción de la invención

La presente invención corresponde a un generador de números aleatorios que comprende: una unidad determinística de muestreo (3) con una primera entrada, una segunda entrada y una salida, una primera fuente de entropía (1a) conectada a la primera entrada de la unidad determinística de muestreo (3), una segunda fuente de entropía (2a) conectada a la segunda entrada de la unidad determinística de muestreo (3), una unidad determinística de posprocesamiento (4) conectada a la salida de la unidad determinística de muestreo (3).

Para el entendimiento de la presente invención, se entenderá como unidad determinística aquella función que su salida es totalmente predecible si se conocen sus entradas y un ejemplo de la realización de una unidad determinística es un comparador digital; y una función de posprocesamiento como por ejemplo una función que tiene como entrada un número aleatorio y extrae parte de ese número aleatorio para obtener un número que tiene una distribución más cercana a la uniforme tal como la función de voto por mayoría, donde su salida depende si la cantidad de unos es mayor o menor a la cantidad de ceros en un dato digital.

En una modalidad de la invención la fuente de entropía (1a) puede ser implementada empleando osciladores de anillo o la metaestabilidad de un latch.

En una modalidad de la invención la fuente de entropía (2a) puede ser implementada empleando osciladores de anillo o la metaestabilidad de un latch.

En otra modalidad de la invención la fuente de entropía (1a) y la segunda fuente de entropía (2a) son intercambiables.

Breve descripción de las figuras

La FIG. 1 corresponde al diagrama de bloques de la presente invención.

La FIG. 2 corresponde al diagrama de una fuente de entropía que está conformada por la conexión de compuertas NAND que son multiplexadas para calibrar el punto de metaestabilidad.

La FIG. 3 corresponde al diagrama de una fuente de entropía empleando osciladores de anillo de una modalidad del invento donde se tiene un oscilador conectado a un generador pseudo aleatorio como reloj de un flip-flop y el otro oscilador de anillo como entrada de datos al flip-flop.

La FIG. 4 corresponde al diagrama de una fuente de entropía empleando osciladores de anillo conectados a contadores, que a su vez están conectados a un comparador digital para seleccionar la salida de los contadores por medio de un multiplexor, que a su vez está conectado a un detector que determina cuando un flip-flop captura el número generado.

La FIG. 5 corresponde al diagrama de una fuente de entropía que está conformada por un primer oscilador de anillo conectado a un detector que inicia la oscilación de un segundo oscilador de anillo. Ambos osciladores están conectados a contadores donde la salida final del contador es la suma de los dos y el segundo detector da la orden de captura al flip-flop.

La FIG. 6 corresponde al esquema de circuito de una modalidad de la presente invención que

emplea dos fuentes de entropía que pueden ser seleccionadas por medio de un multiplexor de un grupo de fuentes de entropía. Las salidas de los multiplexores están conectadas a una unidad que realiza el muestreo y el posprocesamiento.

La FIG. 7 corresponde al esquema de circuito de una modalidad de la presente invención que emplea dos fuentes de entropía que pueden ser seleccionadas por medio de un multiplexor de forma pseudoaleatoria.

La FIG. 8 corresponde al esquema de circuito de una modalidad de la presente invención que emplea dos fuentes de entropía que pueden ser seleccionadas por medio de un multiplexor de forma pseudoaleatoria y que a su vez son conectadas a una unidad de muestreo implementada por medio de un flip-flop donde el reloj es determinado por un generador pseudo aleatorio que emplea como semilla una de las fuentes de entropía.

La FIG. 9 corresponde al esquema de circuito de una modalidad de la presente invención que emplea un oscilador de anillo conectado a un limitador de tensión para reducir la amplitud a la entrada de un flip-flop al nivel de sensibilidad y un segundo oscilador de anillo conectado a un generador pseudo aleatorio donde su salida se emplea como reloj del flip-flop.

Descripción detallada

La presente invención se refiere a un generador de números aleatorios empleando dos fuentes de entropía independientes. Para el entendimiento de la presente invención el término independiente se refiere a que cualquier evento de generación en alguna de las fuentes no tiene relación con la otra. El concepto de emplear dos fuentes de entropía es necesario para generar números aleatorios que pasen pruebas estadísticas pertenecientes a los estándares internacionales.

La presente invención propone emplear esquemas de pseudo muestreo. Los esquemas de pseudo muestreo permiten muestrear una fuente de entropía empleando una segunda fuente pero con algoritmos de baja complejidad fácilmente implementados a nivel de circuito. La implementación de las fuentes de entropía es en el dominio digital y se proponen esquemas de procesamiento que permiten muestrear/pseudo-muestrear una primera fuente por medio de una segunda fuente que se emplea como semilla. Finalmente, se aplica un pos-procesamiento para obtener el dato de salida.

Para el entendimiento de la presente invención cuando se habla de fuentes de entropía se refiere a fuente de entropía débil.

Haciendo referencia a la FIG. 1, el esquema divulgado en la presente invención exhibe un generador de números aleatorios que comprende: una unidad determinística de muestreo (3)

con una primera entrada, una segunda entrada y una salida; una primera fuente de entropía (1a) conectada a la primera entrada de la unidad determinística de muestreo(3); una segunda fuente de entropía (2a) conectada a la segunda entrada de la unidad determinística de muestreo (3); una unidad determinística de posprocesamiento (4) conectada a la salida la unidad determinística de muestreo(3).

Haciendo referencia a la FIG. 1, la presente invención en un ejemplo, presenta una primera fuente de entropía (1a) y segunda fuente de entropía (2a) corresponde a una segunda fuente de entropía (2a) en el dominio digital. Estas fuentes en principio pueden ser cualquier tipo de fuente que proporcione un dato digital y que sean independientes entre sí. La segunda fuente de entropía (2a) se emplea como semilla para que la unidad determinística de muestreo (3) genere un número que luego es posprocesado por la unidad determinística de posprocesamiento (4) para generar el dato de salida.

En una modalidad de la invención la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) son fuentes en el dominio digital. En otra modalidad de la invención la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) se implementan en el dominio analógico.

En referencia a la FIG. 1, en una modalidad del generador de número aleatorios por ejemplo, la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende una unidad de muestreo (3), la segunda fuente de entropía (2a) se conecta a la segunda entrada de la unidad de muestreo (3) y la salida del unidad de muestreo (3) se conecta a una unidad determinística de posprocesamiento (4).

Las fuentes de entropía débiles pueden ser implementadas como se muestran en las figuras de la FIG.2 a la FIG.4, como se describe a continuación:

Haciendo referencia a la FIG. 2, en un ejemplo el esquema divulgado en la presente invención la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) que comprende: un primer conjunto de compuertas NAND (14a) conectado a la entrada de un segundo multiplexor (11b); la salida del segundo multiplexor (11b) se conecta la entrada de un segundo conjunto de compuertas NAND (14b) cuyas salidas se conectan a la entrada de un primer multiplexor (11a); la salida del primer multiplexor (11a) se conecta con la entrada del primer conjunto de compuertas NAND; donde el primer conjunto de compuertas NAND (14a) se forman desde una compuerta NAND (14a) hasta un número (n) de compuertas NAND (14a), siendo (n) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b) y el segundo conjunto de compuertas NAND (14b) se forman desde una compuerta NAND (14b) hasta un número (m) de compuertas NAND (14b), siendo (m) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta el primer multiplexor (11a).

Haciendo referencia a la FIG. 2 se tiene una forma alternativa de obtener una fuente de entropía empleando compuertas NAND conectadas en antiparalelo para lograr una condición metaestable. Las compuertas NAND funcionan como un inversor cuando una de sus entradas se conecta a un uno lógico y si se conecta a un cero lógico la salida siempre será uno por lo que se puede decir que está deshabilitada. En conclusión, la compuerta NAND se puede emplear como un inversor donde una de sus entradas es un habilitador que determina cuando actúa como inversor. Este habilitador corresponde al reloj del generador que determina cuando se genera el bit aleatorio en el momento en que las compuertas actúan como inversor, y luego las salidas de las compuertas se establecen en uno lógico para preparar la próxima condición metaestable. Para reducir los efectos del desacoplamiento entre las compuertas dado que se necesitan que sean iguales idealmente para que sea aleatoria la decisión, se utilizan compuertas en paralelo para calibrar el punto de mestaestabilidad, empleando un multiplexor para determinar la compuerta que se ajusta mejor. Se considera calibrado cuando el número de unos 1s y ceros 0s lógicos generados por el *latch* es cercano al 50%. Para generar un número mayor de bits, se utilizan varios de estos elementos en paralelo que generan datos al tiempo. El número de bits dependerá de las necesidades del usuario, por lo tanto el número de elementos en paralelo también.

Haciendo referencia a la FIG. 3, el esquema divulgado en la presente invención muestra la fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) conectada a un flip-flop (8), una segunda fuente de entropía interna (18b) conectada a un primer generador de bits pseudo aleatorio (*Pseudo Random Bit Stream* por sus siglas en inglés, PRBS) en adelante PRBS (7a) que se conecta al flip-flop (8).

Haciendo referencia a la FIG. 3, un oscilador de anillo denotado como una segunda fuente de entropía interna (18b) se conecta a un primer PRBS (7a) que puede ser en un ejemplo, un registro de desplazamiento con realimentación (*Linear Feedback Shift Register*, por sus siglas en inglés LFSR). El primer PRBS (7a) emplea la segunda fuente de entropía interna (18b) como semilla para generar una secuencia serial que se conecta al flip-flop (8) como reloj. Una primera fuente de entropía interna (18a) se conecta como entrada de datos al flip-flop (8) de forma tal que se realiza un muestreo del mismo obteniendo un número aleatorio listo para ser usado en el esquema propuesto como una de las fuentes de entropía.

En una realización de la presente invención, la primera fuente de entropía interna (18a) y la segunda fuente de entropía interna (18b) se seleccionan del grupo de fuentes de entropía conformado por osciladores de anillo, *latches* metaestables, ruido térmico amplificado de una resistencia y circuitos de tiempo de captura y ruptura del óxido de un transistor bajo una tensión de estrés.

Opcionalmente, la primera fuente de entropía interna (18a) y la segunda fuente de entropía interna (18b) se comprenden por una fuente de entropía que emplea compuertas NAND

conectadas en antiparalelo como se describió anteriormente.

Haciendo referencia a la FIG. 4, el esquema divulgado en la presente invención muestra la fuente de entropía (1a) o una segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) conectada a la entrada de un primer contador (9a), una segunda fuente de entropía interna (18b) conectada a un segundo contador (9b); la salida del primer contador (9a) conectada a una de las dos entradas de un comparador digital (10) y a una entrada de un primer multiplexor (11a), la salida del segundo contador (9b) conectada a una de las entradas de un comparador digital (10) y a una entrada del primer multiplexor (11a); la salida del comparador digital (10) conectada al primer multiplexor (11a) cuya salida a su vez está conectada a un medidor de cambio de frecuencia (12a) y a un flip-flop (13).

En una modalidad el generador de números aleatorios de la presente invención, en un ejemplo, la primera fuente de entropía interna (18a) y la segunda fuente de entropía interna (18b) son osciladores de anillo y el medidor de cambio de frecuencia (12a) es un detector de colapso.

En una modalidad de la presente invención, por ejemplo, la primera fuente de entropía interna (18a) o la segunda fuente de entropía interna (18b) comprende: un primer conjunto de compuertas NAND (14a) conectado a la entrada de un segundo multiplexor (11b); la salida del segundo multiplexor (11b) está conectada a la entrada de un segundo conjunto de compuertas NAND (14b) cuyas salidas están conectadas a la entrada de un primer multiplexor (11a); la salida del primer multiplexor (11a) está conectada con la entrada del primer conjunto de compuertas NAND; donde el primer conjunto de compuertas NAND(14a) se forman desde una compuerta NAND (14a) hasta un número (n) de compuertas NAND (14a), siendo (n) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b) y el segundo conjunto de compuertas NAND (14b) se forman desde una compuerta NAND (14b) hasta un número (m) de compuertas NAND (14b), siendo (m) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta el primer multiplexor (11a).

Haciendo referencia a la FIG. 4 se tiene una primera fuente de entropía (1a) y una segunda fuente de entropía (2a) conectados a una señal de inicio que controla cuando se da inicio a la generación del número aleatorio. A su vez la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) están conectadas a un primer contador (9a) y un segundo contador (9b) respectivamente; el primer contador (9a) y el segundo contador (9b) están conectados a un comparador digital (10) y a un primer multiplexor (11a). El comparador digital (10) se encarga de determinar si el primer contador (9a) es más lento que el segundo contador (9b) o viceversa y da la señal al primer multiplexor (11a) para seleccionar entre el primer contador (9a) y el segundo contador (9b), siendo esta selección de forma aleatoria por que no se puede determinar cuál de los dos contadores (primer contador (9a) y segundo contador (9b)) irá más

lento; el primer multiplexor (11a) se conecta a un primer detector de colapso (12a) que se encarga de darle la orden al flip-flop (13) de capturar el número que viene del primer multiplexor (11a).

Haciendo referencia a la FIG. 5, el esquema divulgado en la presente invención muestra la fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) cuya salida está conectada a un primer medidor de cambio de frecuencia (12a) y a una de las entradas de un primer contador (9a); el primer medidor de cambio de frecuencia (12a) se conecta a su vez a una segunda fuente de entropía interna (18b) y su salida está conectada a una segunda entrada del primer contador (9a) y a un segundo medidor de cambio de frecuencia (12b) que se conecta al CLK de un flip-flop (13), y la salida del primer contador (9a) está conectada a un flip-flop (13).

Haciendo referencia a la FIG. 5 una variación del esquema de la FIG. 4 es conectar en cascada una primera fuente de entropía (1a) y una segunda fuente de entropía (2a). Una señal de inicio que es una señal que va de cero a uno lógico inicia la generación donde el tiempo de generación a partir de la primera fuente de entropía (1a) es indeterminado; un primer detector de colapso (12a) se conecta al conectado a la primera fuente de entropía (1a) y da la señal de inicio a la segunda fuente de entropía (2a) al determinar que la primera fuente de entropía (1a) ha terminado; la segunda fuente de entropía (2a) se conecta a un segundo detector de colapso (12b) que determina cuanto termina la generación de la segunda fuente de entropía (2a); un primer contador (9a) se conecta a la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) donde la cuenta total es la suma de la primera fuente de entropía (1a) y la segunda fuente de entropía (2a), el segundo detector de colapso (12b) da la orden de capturar el número de salida al flip-flop (13).

En consecuencia, diversas realizaciones de la presente descripción se dirigen a un dispositivo para la generación de números aleatorios en forma de cadena aleatoria de bits aleatorios o secuencias de bits aleatorios empleando las fuentes de entropía ya mencionadas, las cuales pueden ser seleccionadas en pares como se explica a continuación.

Otra alternativa para la generación de en fuentes de entropía es empleando el pseudo muestreo de la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) se pueden apreciar de la FIG. 6 a la FIG. 9.

Haciendo referencia a la FIG. 6, el esquema divulgado en la presente invención muestra un primer conjunto de fuentes de entropía conectado a la entrada de un primer multiplexor (11a); el primer multiplexor (11a) está conectado a una unidad determinística de muestreo y posprocesamiento (15); un segundo conjunto de fuentes de entropía conectado a un segundo multiplexor (11b); la salida del segundo multiplexor (11b) está conectada con la unidad determinística de muestreo y posprocesamiento (15); donde el primer conjunto de fuentes de

entropía va desde una primera fuente (19a) a un número (o) de fuentes de entropía (19a), siendo (o) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un primer multiplexor (11a) y el segundo conjunto de fuentes de entropía va desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b).

Haciendo referencia a la FIG. 6 puede observarse la estructura general del generador de números aleatorios empleando un primer conjunto de fuentes de entropía y un segundo conjunto de fuentes de entropía. El generador de números aleatorios comprende un primer conjunto de fuentes de entropía que va desde una primera fuente de entropía (19a) a un número (o) de fuentes de entropía (19a), siendo (o) un número natural mayor que cero y un segundo conjunto de fuentes de entropía que va desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un numero natural mayor que cero. Estas fuentes de entropía están organizadas en dos grupos de los cuales están conectados cada uno mediante un primer multiplexor (11a) y un segundo multiplexor (11b), donde se selecciona la salida de una fuente de cada conjunto. Esto permite posteriormente emplear una unidad determinística que muestrea la primera fuente de entropía (19a) del conjunto de fuentes de entropía empleando como semilla la segunda fuente de entropía (19b). En ésta función también se considera incluida la etapa de pos-procesamiento que se aplica luego del muestreo, empleando, por ejemplo, la función de mayoría. Cabe resaltar el grupo de fuentes de entropía no tiene un orden específico, es decir se puede seleccionar de cualquier conjunto la primera fuente de entropía (1a) y del restante, la segunda fuente de entropía (2a).

Haciendo referencia a la FIG. 7, el esquema divulgado en la presente invención muestra que la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) son arreglos de fuente de entropía y comprende: un primer conjunto de fuentes de entropía conectado a la entrada de un primer multiplexor (11a), una tercera fuente de entropía (3a) conectada a un primer PRBS (7a) y cuya salida está conectada al primer multiplexor (11a); la salida del primer multiplexor (11a) está conectada a una de las entradas de la unidad determinística de muestreo y posprocesamiento (15); un segundo conjunto de fuentes de entropía conectado a la entrada de un segundo multiplexor (11b), una cuarta fuente de entropía (3b) conectada a un segundo PRBS (7b) y cuya salida conecta a la unidad determinística de muestreo y posprocesamiento (15), la salida del segundo multiplexor (11b) conectada a una de las entradas de la unidad determinística de muestreo y posprocesamiento (15); donde el primer conjunto de fuentes de entropía va desde una primera fuente (19a) a un número (o) de fuentes de entropía (19a), siendo (o) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un primer multiplexor (11a) y el segundo conjunto de fuentes de entropía va desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b).

Haciendo referencia a la FIG. 7 en un ejemplo de otra modalidad de la invención, manteniendo la misma estructura se seleccionan la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) de forma pseudo aleatoria. El generador comprende un primer conjunto de fuentes de entropía que va desde una primera fuente de entropía (19a) a un número (o) de fuentes de entropía (18a), siendo (o) un número natural mayor que cero y un segundo conjunto de fuentes de entropía que va desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (2a), siendo (p) un numero natural mayor que cero. Para la selección de una de las fuentes de entropía del primer conjunto de fuentes de entropía se utiliza una tercera fuente de entropía (3a) la cual sirve de semilla para un primer PRBS (7a); la salida del primer PRBS (7a) se emplea para seleccionar por medio de un primer multiplexor (11a) la fuente de entropía a utilizar del primer conjunto de fuentes de entropía; para la selección de una de las fuentes de entropía del segundo conjunto de fuentes de entropía se utiliza una cuarta fuente de entropía (3b) la cual sirve de semilla para un segundo PRBS (7b); la salida del segundo PRBS (7b) se utiliza para seleccionar por medio de un segundo multiplexor (11b) la fuente de entropía a utilizar del segundo conjunto de fuentes de entropía; la salida del primer multiplexor (11a) y la salida del segundo multiplexor (11b) se conectan a la unidad determinística de muestreo y posprocesamiento (15); la salida de la unidad determinística de muestreo y posprocesamiento (15) es el número aleatorio.

Haciendo referencia a la FIG. 8 en una modalidad de la invención la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) son arreglos de fuente de entropía y comprende: un primer conjunto de fuentes de entropía se forma desde una primera fuente de entropía (19a) a un número (o) de fuentes de entropía (1a), siendo (o) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta a un primer multiplexor (11a), la salida de cada fuente de entropía (19a) conectada a cada una de las entradas del primer multiplexor (11a), una tercera fuente de entropía (3a) conectada a un primer PRBS (7a) y cuya salida está conectada al primer multiplexor (11a), la salida del primer multiplexor (11a) está conectada a un flip-flop (16); un segundo conjunto de fuentes de entropía (19b) se forma desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b), la salida de cada fuente de entropía (19b) está conectada a cada una de las entradas del segundo multiplexor (11b), una cuarta fuente de entropía (3b) está conectada a un segundo PRBS (7b) y cuya salida está conectada al segundo multiplexor (11b), la salida del segundo multiplexor (11b) está conectada a un tercer PRBS (7c) y su salida conectada a un flip-flop (16).

Haciendo referencia a la FIG. 8 se muestra en un ejemplo como se implementa una función de muestreo empleando dos fuentes de entropía. Se muestra en la FIG. 8 el esquema de selección pseudoaleatorio de las fuentes de entropía. Luego una de las fuentes seleccionadas sirve como semilla para un generador pseudo aleatorio donde su salida serial es usada como el reloj de un muestreador que puede ser implementado como un flip-flop o registro. La

fuente restante es usada como la entrada de datos del muestreador por lo que a la salida se obtiene una versión muestreada de la fuente.

Haciendo referencia a la FIG. 9, el esquema divulgado en la presente invención muestra la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) que conecta a un primer PRBS (7a) que conecta a un limitador (17) que a su vez está conecto a un flip-flop (16), una segunda fuente de entropía interna (18b) está conectada a un segundo PRBS (7b) cuya señal de salida está conectada a un flip-flop (16).

Para el entendimiento de la presente invención, se entenderá que CLK corresponde a una señal de reloj.

Haciendo referencia a la FIG. 9 corresponde en un ejemplo a una alternativa de realizar muestreo a una fuente aleatoria con una primera fuente de entropía (1a) y una segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) conectada a un primer PRBS (7a) y una segunda fuente de entropía interna (18b) conectada a un segundo PRBS (7b). La salida del segundo PRBS (7b) se utiliza como el reloj de una unidad de muestreo determinístico (16). La primera fuente de entropía (1a) está conectada a un primer PRBS (7a) que se utiliza como dato de entrada a un limitador de tensión (17), este limitador de tensión (17) se encarga de reducir la amplitud del dato de entrada a un limitador de tensión (17) de tal forma que sean percibidos por el muestreador. Como resultado, la salida del muestreador va estar dominado por el ruido a la salida del limitador de tensión (17). El limitador de tensión (17) puede ser implementado como un filtro paso-bajo de frecuencia de corte 10 veces menor a la frecuencia de oscilación de entrada de tal forma que la salida se vea reducida en amplitud.

En una modalidad de la presente invención la unidad de muestreo determinístico (16) es un flip-flop.

Se debe entender que la presente invención no se halla limitada a las modalidades descritas e ilustradas, pues como será evidente para una persona versada en el arte, existen variaciones y modificaciones posibles que no se apartan del espíritu de la invención, esta descripción es solamente ilustrativa, y se pueden hacer cambios en detalle, especialmente en cuestiones de estructura y arreglos de las partes dentro de los principios de la presente divulgación a toda la extensión indicada por el amplio significado general de los términos en el que las reivindicaciones anexas se expresan.

Glosario

Entropía: mide la incertidumbre de una fuente de información, experimento o señal aleatoria.

Fuentes de entropía débil: toda fuente de entropía implementada físicamente es considerada una fuente débil, esto se debe a que ninguna posee una distribución uniforme que sería el caso ideal.

Fuentes de entropía en el dominio digital: fuente de entropía que es implementada físicamente por medio de compuertas digitales que pueden ser implementadas por medio de flujo digital, es decir, que pueden ser completamente sintetizadas.

Semilla: una semilla se puede definir con un número corto uniforme aleatorio.

Dominio digital: dominio en el que se opera con señales lógicas.

Dominio Analógico: dominio en el que se opera con señales de naturaleza analógica.

Ruido inherente: fluctuación aleatoria de una señal eléctrica presente en todos los dispositivas electrónicas que puede ser ruido térmico o ruido *flicker*.

Metaestabilidad: propiedad que exhibe un sistema con varios estados de equilibrio, cuando permanece en un estado de equilibrio débilmente estable durante un considerable período de tiempo.

Función determinística: las funciones deterministas devuelven siempre el mismo resultado cada vez que se invocan con un conjunto específico de valores de entrada.

Función de mayoría: es una función cuya salida corresponde al símbolo de entrada de mayor frecuencia o mayor ocurrencia.

Pseudo muestreo: es la operación de extracción de un número aleatorio basado en secuencias pseudo aleatorias.

Fuente de entropía interna: se entiende una fuente de entropía interna como una fuente de entropía al interior de un circuito que compone una fuente de entropía compuesta.

Detector de colapso: circuito que permite identificar el instante en el cuál un oscilador de anillo cambia de un modo de oscilación a otro.

Medidor de cambio de frecuencia: circuito que permite capturar el instante de tiempo en el que cambia la frecuencia de una señal.

Unidad determinística de muestreo: circuito que permite seleccionar de una cadena de números aleatorios, aquellos números con distribución estadística cercana a la uniforme.

Unidad determinística de posprocesamiento: circuito que permite reducir el sesgo de una cadena de datos aleatoria.