(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 703 983**

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.05.2015 PCT/IB2015/054077**

(87) Fecha y número de publicación internacional: **04.02.2016 WO16016741**

(96) Fecha de presentación y número de la solicitud europea: **29.05.2015 E 15734727 (9)**

(97) Fecha y número de publicación de la concesión europea: **03.10.2018 EP 3175354**

(54) Título: **Generador de números aleatorios verdaderos**

(30) Prioridad:

30.07.2014 IT VI20140200

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2019

(73) Titular/es:

TRENTINO SVILUPPO S.P.A. (100.0%)
Via Fortunato Zeni, 8
38068 Rovereto, (TN), IT

(72) Inventor/es:

PAVESI, LORENZO;
BETTOTTI, PAOLO;
CAZZANELLI, MASSIMO;
GASPARINI, LEONARDO;
MASSARI, NICOLA;
PUCKER, GEORG;
RIMOLDI, ANNA;
SALA, MASSIMILIANO y
TOMASI, ALESSANDRO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Generador de números aleatorios verdaderos

La presente invención se refiere a un generador de números aleatorios (RNG) en particular a un generador de números aleatorios verdaderos (TRNG), del tipo perfeccionado.

Se sabe que los generadores de números aleatorios son actualmente utilizados en varias aplicaciones que varían desde el campo de la ciencia al de los cripto-diagramas.

En el primer caso, un ejemplo típico es el de la ciencia computacional, que requiere la generación de un cierto número de estados aleatorios iniciales que sirven como una descripción del estado inicial de la simulación.

El tipo de aplicación generalmente requiere que las configuraciones iniciales no estén correlacionadas estrictamente entre sí, pero que puedan ser reproducidas de una manera determinística para hacer posible verificar, por ejemplo, el efecto de variaciones sobre los códigos que llevan a cabo las simulaciones. Por esta razón, estas secuencias son definidas más correctamente como números pseudo-aleatorios (PRN), debido a que son definidas mediante algoritmos complejos que comienzan a partir de un valor inicial. En otras palabras, dado un número aleatorio inicial, que en la jerga técnica es denominado "semilla", una fórmula, incluso si es muy compleja, reproducirá de manera constante la misma secuencia de números aleatorios. Los generadores correspondientes son definidos como generadores de números pseudo-aleatorios (PRNG).

Por el contrario, en el segundo caso, es decir, en el caso de utilizar números aleatorios en técnicas de cripto-diagramas para la ejecución, por ejemplo, de operaciones bancarias, este enfoque es débil, ya que es necesario asegurar la impredicibilidad total de las secuencias generadas, de tal modo que se mantenga una seguridad de información muy sensible. En este caso, el enfoque más seguro puede ser conseguido mediante la generación de números aleatorios obtenidos a partir de un proceso de generación que es realmente aleatorio y no permite que la secuencia generada sea predicha de ninguna forma. Estos generadores, de hecho, son conocidos como generadores de números aleatorios verdaderos (TRNG). En particular, los mecanismos cuánticos, como por ejemplo la generación de fotones por una fuente de luz, están entre los métodos más investigados para obtener dichas secuencias de números aleatorios verdaderos y están basados en la indeterminación del evento medido que es inherente a las propiedades del propio sistema cuántico.

Desde el punto de vista de la teoría de información, el nivel de impredicibilidad de los números aleatorios generados mediante ambas de dichas dos técnicas puede ser expresado por medio del parámetro definido como "entropía", que de hecho es conocido como la medida de la incertidumbre o información en una variable aleatoria. Además, es importante subrayar que el National Institute of Standards and Technology (NIST) (Instituto Nacional de Normas y Tecnología) con su directiva NIST SP800-22 especifica aproximadamente quince ensayos estadísticos que hacen posible determinar si un generador dado de números aleatorios tienen un nivel suficiente de entropía o no.

Como ya se ha mencionado, el uso de generadores de números pseudo-aleatorios para propósitos de cripto-diagramas es arriesgado, no solamente debido a que ciertos algoritmos tienen debilidades que potencialmente son reveladas sólo algún tiempo después de su introducción, sino también debido a que si un sujeto malintencionado recuperase la semilla a partir de la cual se generan todas las secuencias aleatorias, todas las salidas sucesivas basadas en la misma semilla podrían ser predichas con absoluta certeza.

Una solución basada en fenómenos físicos y en particular en fenómenos cuánticos particulares es por ello muy preferible, dada la impredicibilidad intrínseca de estos eventos, incluso para sujetos que tienen un conocimiento perfecto de los algoritmos utilizados y que tienen una elevada capacidad de cálculo a su disposición. Sin embargo, aunque los algoritmos para la generación de números pseudo-aleatorios pueden ser seleccionados para crear secuencias que tienen algunas propiedades estadísticas determinadas con absoluta certeza debido, de hecho, a su naturaleza determinística, los números aleatorios obtenidos comenzando a partir de fenómenos físicos están sujetos a limitaciones prácticas debido, por ejemplo, a variaciones en la calidad de fabricación del instrumento, a fluctuaciones en la alimentación de corriente, a factores medioambientales tales como campos externos y cambios súbitos de temperatura. En general, estas desviaciones del caso ideal determinan una desviación de una distribución estadística uniforme e independiente de los eventos que pueden ser medidos en un espacio de muestreo. Consecuentemente es posible observar un nivel inferior de entropía también en dichos generadores de números aleatorios verdaderos.

Para evitar lo anterior, dichos generadores de números aleatorios verdaderos necesitan una etapa adicional, llamada una operación de "post-procesamiento", realizada aguas abajo de la extracción de la secuencia de códigos aleatorios que comienza a partir del fenómeno físico específico. Esta etapa post-procesamiento, de hecho, hace posible mejorar la uniformidad de distribución de probabilidad de la secuencia de códigos aleatorios. Sin embargo, como desventaja, dicha etapa de post-procesamiento afecta a la denominada "tasa de bit" que puede ser asegurada por el generador.

Es también conocido, como ya se ha mencionado anteriormente, que uno de los fenómenos físicos que son más explotados para la generación de los números aleatorios es la fotónica cuántica. Por esta razón, dichos generadores que pertenecen a la macro-categoría de generadores TRNG están también indicados más específicamente por el acrónimo QRNG (Quantum Random Number Generator) (“Generador Cuántico de Números Aleatorios”). En estos generadores, de hecho, una fuente de luz atenuada genera pocos fotones (bajo valor del flujo λ de fotones detectados) que son

adquiridos por uno o más detectores de fotones individuales, cada uno de los cuales es conocido por el acrónimo SPAD (Single Photon Avalanche Diode) (“Diodo de Avalancha de Un solo Fotón”). Además, el sistema está provisto de circuitos electrónicos específicos situados aguas abajo de dichos SPAD, usualmente uno o más TDC (Time to Digital Converter) (“Convertidor de Tiempo a Digital”) capaz de extraer una secuencia aleatoria de bits desde cada uno de dichos SPAD. Más precisamente, en estos generadores los fotones obedecen a un proceso de Poisson, que significa que los eventos adquiridos son independientes entre sí y que la probabilidad de contar n fotones dentro de una ventana de observación T_w sigue la distribución de Poisson:

$$P(x = n) = \frac{e^{-\lambda T_w} (\lambda T_w)^n}{n!}$$

donde λ indica, de hecho, el flujo de fotones detectados.

El flujo λ de fotones detectados, las características de los detectores SPAD y los modos de extracción de bit determinan el rendimiento final del generador.

Habiéndose indicado lo anterior, hay disponibles en el mercado diferentes tipos de generadores de números aleatorios basados en el concepto QRNG. Estos generadores, en particular, cubren una amplia variedad de aplicaciones, que varían desde dispositivos portátiles USB que ofrecen justo unos pocos centenares de kbits a grandes sistemas electrónicos capaces de garantizar una tasa de bits de centenares de Mbits. En la bibliografía, además, se han propuesto diferentes estructuras y arquitecturas lógicas para determinar las secuencias de números aleatorios verdaderos comenzando desde un fenómeno físico, en particular a partir de la detección de fotones. La mayor parte de ellos detectan el "tiempo de llegada" o el número de fotones incidente sobre la superficie sensible del generador/generadores SPAD.

En particular, en lo que se refiere a la técnica basada en el así llamado tiempo de llegada, se ha hecho una proposición de acuerdo con la cual el tiempo que transcurre entre el momento en el que un fotón incide sobre un SPAD individual y el momento en el que el fotón sucesivos incide sobre el mismo SPAD debería ser medido. Estas mediciones son ordenadas sucesivamente dentro de porciones de tiempo adyacentes con la misma duración en la que la ventana de observación T_w de cada SPAD está subdividida. Basándose en la porción de tiempo dentro de la cual cae dicha medición, se genera y extrae una secuencia aleatoria correspondiente de bits.

Sin embargo, aunque esta técnica hace posible obtener una elevada tasa de bits, tiene una predisposición considerable debido al hecho de que, como ya se ha explicado, la fuente de fotones obedece a dicho proceso de Poisson.

De acuerdo con la técnica conocida, para superar el inconveniente anteriormente mencionado debería actuarse directamente sobre la fuente de fotones, comprobando apropiadamente el flujo de fotones generado por la misma fuente de fotones. Esta operación, en particular, incluye la etapa de variar la corriente de polarización de la fuente de fotones de tal modo que haga su distribución estadística a lo largo del tiempo tan uniforme como sea posible.

Sin embargo, como desventaja, de acuerdo con este enfoque, necesitan ser introducidos en el generador circuitos electrónicos especiales capaces de variar la corriente de polarización de la fuente de fotones, como se ha descrito anteriormente, lo que aumenta la complejidad y el tamaño del propio generador.

La presente invención pretende superar los inconvenientes mencionados anteriormente. En particular, la invención tiene el propósito de proporcionar un generador de números aleatorios verdaderos que haga posible garantizar un elevado nivel de entropía de tal modo que cumpla al menos los ensayos estadísticos del NIST.

Es otro objeto de la invención proporcionar un generador de números aleatorios verdaderos que haga posible obtener una elevada tasa de bits en la generación de secuencias de bits aleatorias.

Es otro objeto de la invención proporcionar un generador de números aleatorios verdaderos cuya estructura sea más compacta, menos compleja y requiera menos consumo de energía comparado con los generadores de números aleatorios de la técnica anterior.

De nuevo es otro objeto de la invención proporcionar un generador de números aleatorios verdaderos con un elevado nivel de seguridad contra cualquier falsificación de sus componentes internos.

Es aún otro, aunque no menos objeto de la invención proporcionar un generador de números aleatorios verdaderos que sea más económico que los generadores de la técnica conocida.

NIE YOU-QI ET AL: “ Practical and fast quantum random number generation based on photon arrival time relative to external reference”, APPLIED PHYSICS LETTERS, AMERCIAN INSTITUTE OF PHYSICS, USA, vol. 104, np. 5, 3 de febrero de 2014 (2014-02-03), XP012181569, ISSN: 0003-6951, DOI: 10.1063/1.4863224 describe un generador de números aleatorios de acuerdo con el preámbulo de la reivindicación 1. Los objetos mencionados anteriormente son conseguidos por el generador de números aleatorios verdaderos que tiene las características descritas en la reivindicación principal.

En particular, el generador de números aleatorios verdaderos de la invención, que comprende una fuente de fotones con un flujo λ de fotones detectados y medios de muestreo electrónico con ventanas T_w, de observación está caracterizado por que dicha fuente de fotones y dichos medios de muestreo electrónicos están configurados de tal manera que el producto $\lambda*T_w$ es menor o igual a 0,01.

Otras características del generador de números aleatorios verdaderos de la invención están descritas en las reivindicaciones dependientes.

En particular, el hecho de que los componentes que constituyen el generador de números aleatorios verdaderos de la invención están hechos de manera que son integrados en un único sustrato de silicio, como se ha explicado en la reivindicación 5 dependiente, hace ventajosamente posible obtener un generador que es más compacto y está sujeto menos a falsificación que los generadores de la técnica anterior.

Dichos objetos, junto con las ventajas que se describirán aquí a continuación, son resaltados en la descripción de una realización preferida de la invención que es proporcionada a modo de ejemplo no limitativo con referencia a los dibujos adjuntos, en los que:

- La fig. 1a muestra una vista esquemática de la arquitectura del generador de números aleatorios de la presente invención;

- La fig. 1b muestra una vista axonométrica esquemática de la agrupación de detectores del generador de números aleatorios de la invención;

- La fig. 2 muestra una ventana de observación con duración T_w subdividida en r porciones de tiempo que tienen la misma duración;

- La fig. 3 muestra primeros diagramas relativos a la distribución de probabilidad de diferentes valores del producto $\lambda*T_w$, en particular para diferentes valores de λ;

- La fig. 4 muestra segundos diagramas relativos a la distribución de probabilidad para diferentes valores del producto $\lambda*T_w$, en particular para diferentes valores de T_w.

El generador de números aleatorios (RNG) que es el objeto de la invención, en particular el generador de números aleatorios verdaderos (TRNG) de la invención, está representado esquemáticamente en la fig. 1a, donde está indicado por 1.

Como puede observarse en la fig. 1a, el generador 1 de números aleatorios de la invención comprende una fuente 2 de fotones que tiene un flujo de fotones detectados igual a λ.

De acuerdo con la realización preferida de la invención, el generador 1 de números aleatorios comprende además, como se ha mostrado en la fig. 1b, una agrupación 3 de detectores 311 de fotones del tipo SPAD. En particular, como ya se ha mencionado anteriormente, un único detector SPAD 311 es capaz de recoger y suministrar como salida la información relativa a la incidencia de un único fotón sobre su superficie sensible y posiblemente el tiempo de llegada de dicho único fotón con una ventana de observación con una duración preestablecida de T_w. Entre dos ventanas de observación T_w sucesivas, el detector SPAD 311 sufre una etapa de procesamiento durante la cual se restauran las condiciones iniciales, llamada tiempo muerto T_{dead} en jerga técnica, durante el cual el mismo SPAD 311 no puede detectar ningún fotón.

El generador 1 de números aleatorios de la invención, como se ha mostrado esquemáticamente en la fig. 1a, comprende también medios 4 de muestreo electrónicos conectados operativamente a dicha agrupación 3 de detectores SPAD 311.

Dichos medios 4 de muestreo electrónico están configurados para detectar el tiempo t de llegada de un fotón incidente sobre cada uno de los detectores SPAD 311 que pertenecen a la agrupación de detectores SPAD 3, para cada una de las ventanas de observación T_w. Además, los mismos medios 4 de muestreo electrónico están configurados de tal modo que convierten cada tiempo t de llegada detectado en una secuencia binaria con una longitud igual a $n = \log_2 r$, donde r representa el número de porciones de tiempo que tienen la misma duración en la que cada ventana de observación con duración T_w está subdividida previamente, como se ha mostrado esquemáticamente en la fig. 2.

El valor asumido por dicha secuencia binaria depende de la porción de tiempo específica dentro de la cual cae dicho tiempo t de llegada detectado.

De acuerdo con la invención, la fuente 2 de fotones y los medios 4 de muestreo electrónico están configurados de tal modo que el producto $\lambda*T_w$ entre el flujo λ de fotones detectados y la duración T_w de cada ventana de observación es menor o igual a 0,01.

Como se ha mostrado aquí más adelante, dichas características hacen posible ventajosamente obtener una distribución de probabilidad de los tiempos de llegada de los fotones que es esencialmente lineal y sustancialmente uniforme. Consecuentemente, dicha relación entre dichas dos cantidades λ y T_w hace posible aumentar el nivel de entropía del generador 1 de números aleatorios de la invención.

En particular, se ha mostrado que, preferible, pero no necesariamente, en el caso donde los instrumentos utilizados no son la solución ideal, se obtiene una mayor uniformidad de la distribución de probabilidad el tiempo de llegada de los fotones, y por ello un mayor nivel de entropía del generador 1 de la invención, con un valor de dicho producto λ^*T_w menor o igual a 0,001.

Dichos valores han sido determinados por medio de análisis teóricos, simulaciones de Monte Carlo y mediciones empíricas, que han hecho posible restablecer que el generador 1 de números aleatorios de la invención, configurado como se ha descrito anteriormente, tiene un nivel de entropía que es al menos suficiente para pasar los ensayos estadísticos del NIST.

En particular, el análisis realizado estaba basado en dos suposiciones. La primera se refiere al hecho de que en un proceso de Poisson, como uno al que los fotones generados por la fuente 2 de luz obedecen, la diferencia entre cualquier tiempo aleatorio y el evento sucesivo sigue una distribución exponencial del tipo $1 – e^{-\lambda t}$, donde λ es el número de eventos detectados. La segunda suposición es que la medición más fiable de la desviación desde una distribución estadística uniforme, en el caso en el que la ventana T_w de observación esta subdividida en una pluralidad de dichas porciones r de tiempo, se obtiene por medio de la denominada distancia de variación total (TVD).

En mayor detalle, el valor de dicha distancia de variación total es igual a:

$$\mathrm{TVD}(P, Q) = \|P - Q\| = \frac{1}{2}\sum_{\omega\in\Omega}|P(\omega) - Q(\omega)|$$

donde P y Q son dos medidas de probabilidad definidas en el espacio de muestreo Ω de eventos ω mensurables.

Habiéndose explicado lo anterior, puede ser fácilmente mostrado que subdividiendo dicha distribución exponencial en dicho número r de porciones de tiempo que tienen la misma duración, si la primera porción de tiempo comprende el intervalo t_i, entonces la $m^{ésima}$ porción de tiempo r representará el intervalo de tiempo $t \in [(m-1)t_i, mt_i]$y y comprenderá una densidad de probabilidad igual a:

$$p(m) = \varepsilon(mt_i; \lambda) – \varepsilon((m-1)t_i; \lambda)$$

$$= e^{-(m-1)\lambda t_i}(1 – e^{-\lambda t_i})$$

donde $\varepsilon(t; \lambda)$ es la función de distribución acumulativa de una variable aleatoria exponencial con parámetro de tasa λ en tiempo t.

La fig. 3 muestra los resultados gráficos obtenidos a través de la simulación, respectivamente, de la distribución de probabilidad exponencial y de la densidad de probabilidad para diferentes valores de λ, con un número de porciones r de tiempo igual a 10 y con una ventana de observación T_w con valor unitario.

Puede comprenderse a partir de la ecuación y antes de la totalidad de dichos diagramas que cuando el valor del flujo λ de fotones detectados disminuye, la densidad de probabilidad tiende a enderezarse.

Además, el valor de la TVD en dichas condiciones, es proporcional al recuento de fotones. En particular, una TVD ≈ 0,01, considerada aceptable, es obtenida con el producto $\lambda T_w = 1/100$.

La fig. 4 muestra otra representación gráfica de la distribución de la densidad de probabilidad, en este caso manteniendo el flujo λ de fotones detectados constante, por ejemplo a 10^6 recuentos/s y variando la duración T_w de la ventana de observación. En particular, en el primer diagrama a la izquierda se ha seleccionado la ventana de observación T_w de modo que es igual a 0,1 ns, en el segundo diagrama T_w = 1 ns mientras que en el último diagrama a la derecha T > 10 ns. Es evidente que con T_w = 0,1 ns la distribución es esencialmente uniforme, con T_w = 1 ns la distribución es sustancialmente lineal, mientras con T > 10 ns la distribución no es ni uniforme ni lineal, con una reducción consecuente del nivel de entropía del sistema. También en este caso, como es evidente, el mejor resultado es obtenido cuando el producto λT_w es igual a $10^6 *(0{,}1 *10^{-9}) = 0{,}01$.

De este modo, se ha mostrado que, de acuerdo con la invención, configurando el producto λ^*T_w entre el flujo λ de fotones detectados y la duración T_w de la ventana de observación del generador 1 de modo que sea igual o menor que 0,01 se obtiene una distribución sustancialmente uniforme y, por ello, el generador 1 tiene un nivel de entropía elevado.

Volviendo a la arquitectura del generador 1 de números aleatorios, de acuerdo con la realización preferida de la invención dicha fuente 2 de fotones y la agrupación 3 de detectores SPAD 311 están hechos de tal modo que están integrados en un único sustrato 5 de silicio.

En mayor detalle, la fuente 2 de fotones y la agrupación 3 de detectores SPAD 311 están hechos en dicho sustrato 5 de silicio mediante la técnica de micro-fabricación de circuitos integrados CMOS.

Ventajosamente, dicha integración permite que el generador 1 de números aleatorios de la invención sea construido de tal modo que sea más compacto y estructuralmente menos complejo que los generadores de tipo conocido.

En particular, de acuerdo con la realización preferida de la invención, la fuente 2 de fotones es un dispositivo LED 21. Por

esta razón, dicho dispositivo LED 21 integrado es denominado Si-LED 21.

No puede ser excluido, sin embargo, que en diferentes realizaciones de la invención dicha fuente 2 de fotones puede ser un dispositivo LED del tipo discreto instalado sobre una placa de soporte que pertenece al generador 1 de números aleatorios de la invención o la misma fuente 2 de fotones puede ser de un tipo diferente de un dispositivo LED. De acuerdo con la realización preferida de la invención, la agrupación 3 de detectores SPAD 311 está subdividida en grupos 31 de detectores SPAD 311, comprendiendo cada grupo 31 un número predefinido de detectores SPAD 311.

Cada uno de dichos grupos 31 de detectores SPAD 311 es gestionado independientemente de los restantes grupos 31 por medios 4 de muestreo electrónicos especiales mencionados anteriormente.

Dicha gestión independiente de los distintos grupos 31 de detectores SPAD 311 hace posible ventajosamente hacer paralela la extracción de las secuencias binarias aleatorias a partir del generador 1 de números aleatorios, aumentando así la tasa de bits del último.

No puede excluirse sin embargo, que en diferentes realizaciones de la invención dicha agrupación 3 de detectores SPAD 311 no esté subdividida en grupos 31 de detectores SPAD 311, sino que sea controlada por medios 4 de muestreo electrónico comunes. Además, no puede excluirse que en una realización alternativa de la invención dicho generador 1 puede comprender un único detector SPAD 311. Con relación al acoplamiento entre dicho Si-LED 21 y la agrupación 3 de detectores SPAD 311 esto es preferible, pero no necesariamente, hecho de una manera directa. Dicho acoplamiento directo hace ventajosamente posible maximizar el flujo incidente de fotones sobre las superficies sensibles de la agrupación 3 de detectores SPAD 311. Además, hace posible evitar cualquier posible polarización de la distribución estadística que pueda ocurrir en diferentes arquitecturas utilizando un divisor del flujo de fotones si dicho divisor no está correctamente equilibrado. En la práctica, el acoplamiento directo hace más fácil controlar el instrumento y hace posible evitar desviaciones significativas de las condiciones operativas iniciales debido a derivas. Finalmente, aun ventajosamente, dicho acoplamiento directo hace posible simplificar la arquitectura del generador 1 de números aleatorios de la invención, ya que no hay necesidad de fabricar un circuito óptico integrado entre dichos dos componentes.

No puede excluirse, sin embargo, que en diferentes realizaciones de la invención el acoplamiento entre el Si-LED 21 y la agrupación 3 de detectores SPAD 311 pueda ser obtenido de una manera indirecta, a través de la interposición de guías de onda adecuadas.

Como ya se ha mencionado anteriormente, de acuerdo con la realización preferida de la invención cada grupo 31 de detectores SPAD 311 está conectado operativamente con sus propios medios 4 de muestreo electrónico. En particular, dichos medios 4 de muestreo electrónico, asociados con un grupo 31 específico de detectores SPAD 311, están configurados para detectar el tiempo t de llegada de un fotón incidente sobre cada SPAD 311 y también para identificar sobre qué detector SPAD 311 incide dicho fotón en el tiempo t de llegada. Esta característica, gracias a la cual es posible identificar el detector SPAD 311 específico sobre el que incide el fotón, hace posible ventajosamente conocer la distribución de cada elemento que pertenece al grupo de SPAD 31, incluso si se utilizan medios 4 de muestreo electrónico.

Por ello, el uso de medios 4 de muestreo electrónico que son compartidos por un grupo 31 de detectores SPAD 311 y al mismo tiempo son capaces de determinar sobre cuál de dichos detectores 311 está incidiendo un fotón en un tiempo t de llegada dado, hace posible mantener un elevado nivel de entropía de todo el generador 1 de números aleatorios de la invención y al mismo tiempo reducir el tamaño del último.

No puede excluirse, sin embargo, que en realizaciones alternativas de la invención dichos medios 4 de muestreo electrónico sean compartidos por la agrupación 3 completa de detectores SPAD 311 o que cada detector SPAD 311 esté provisto de sus propios medios 4 de muestreo electrónico.

Además, de acuerdo con la realización preferida de la invención, cada uno de dichos medios 4 de muestreo electrónico comprende un dispositivo TDC (Convertidor de Tiempo a Digital) 41.

Finalmente, siempre de acuerdo con la realización preferida de la invención, dichos medios 4 de muestreo electrónico están hechos de tal modo que están integrados en dicho sustrato 5 de silicio.

Preferible pero no necesariamente, el generador 1 de números aleatorios de la invención comprende además medios 6 de post-procesamiento electrónicos configurados para recibir las secuencias binarias extraídas desde dichos medios 4 de muestreo electrónico como una salida, estando dichos medios de muestreo electrónicos a su vez asociados con cada uno de dichos grupos 31 de detectores SPAD 311.

Además, dichos medios 6 de post-procesamiento electrónicos están configurados para procesar dichas secuencias binarias de tal modo que lleven a cabo un denominado ciclo de "blanqueador". El término "blanqueador" indica una operación de extracción de correlación capaz de transformar secuencias de códigos binarios aleatorios posiblemente limitados por una matriz M de covarianza en nuevas secuencias de códigos binarios aleatorios cuya covarianza es la matriz de identidad. En otras palabras, dichas nuevas secuencias de códigos binarios aleatorios no están correlacionadas y todas tienen un valor de varianza igual a 1. Consecuentemente, para mayor ventaja, dicha etapa de

post-procesamiento adicional hace posible aumentar además el nivel de entropía del mismo generador 1 de números aleatorios de la invención.

A modo de ejemplo, dichos medios 6 de post-procesamiento electrónicos están configurados para procesar las secuencias binarias recibidas como una entrada mediante el algoritmo de Von Neumann.

No puede excluirse, sin embargo, que en diferentes realizaciones de la invención dichos medios 6 de post-procesamiento electrónicos pueden estar configurados para procesar dichas secuencias binarias a través de un algoritmo de función hash, un algoritmo de cifra de bloque, o multiplicaciones por una matriz creada específicamente para este propósito, siempre que sean capaces de aumentar adicionalmente la entropía del generador 1 de números aleatorios de la invención por bit de salida.

De acuerdo con lo anterior, por ello, el generador 1 de números aleatorios de la invención consigue la totalidad de los objetos establecidos.

En particular, consigue el objeto de proporcionar un generador de números aleatorios verdaderos que hace posible asegurar un elevado nivel de entropía, de tal manera que cumpla al menos los ensayos estadísticos del NIST.

Además, la invención consigue también el objeto de proporcionar un generador de números aleatorios verdaderos que hace posible obtener una elevada tasa de bits en la generación de secuencias de bit aleatorias.

La invención también consigue el objeto de proporcionar un generador de números aleatorios verdaderos que tiene una estructura más compacta y menos compleja y requiere menos consumo de energía comparado con los generadores de números aleatorios de la técnica anterior.

La invención, consigue además el objeto de proporcionar un generador de números aleatorios verdaderos que tiene un elevado nivel de seguridad contra cualquier falsificación con sus componentes internos.

Finalmente, la invención también consigue el objeto de proporcionar un generador de números aleatorios verdaderos que sea más económico que los generadores de la técnica anterior.

REIVINDICACIONES

1. Un generador (1) de números aleatorios del tipo que comprende:

- una fuente (2) de fotones;

- uno o más detectores de fotones del tipo SPAD (311) configurados de tal modo que detecten un flujo de fotones igual a λ, siendo generados dichos fotones por dicha fuente (2) de fotones;

- medios (4) de muestreo electrónico configurados de tal modo que detecten el tiempo t de llegada de un fotón incidente en cada uno de dichos detectores SPAD (311) de fotones para cada una de las ventanas de observación con una duración T_w,

estando dichos medios (4) de muestreo electrónico configurados además de tal modo que convierten dicho tiempo t de llegada en una secuencia binaria con una longitud igual a $n = \log_2 r$, siendo r el número de porciones de tiempo que tienen la misma duración en la que cada una de dichas ventanas de observación con duración T_w es subdividida, asumiendo dicha secuencia binaria un valor que depende de la porción de tiempo específica dentro de la cual cae dicho tiempo t de llegada,

caracterizado por que dicha fuente (2) de fotones y dicho medios (4) de muestreo electrónico están configurados de tal manera que el producto $\lambda * T_w$ entre el flujo λ de fotones detectados y la duración T_w de cada ventana de observación es menor o igual a 0,01.

2. Un generador (1) de números aleatorios según la reivindicación 1, caracterizado por que dicha fuente (2) de fotones y dichos medios (4) de muestreo electrónico están configurados de tal modo que el producto $\lambda * T_w$ entre el flujo λ de fotones detectados y la duración T_w de cada ventana de observación es menor o igual a 0,001.

3. Un generador (1) de números aleatorios según cualquiera de las reivindicaciones precedentes, caracterizado por que comprende una agrupación (3) de detectores SPAD (311) de fotones subdividida en varios grupos (31), estando cada uno de dichos grupos (31) conectado operativamente a sus propios medios (4) de muestreo electrónicos configurados de tal modo que identifiquen el detector SPAD (311) sobre el que ha sido detectado un fotón en un intervalo t de llegada específico, independientemente de los medios (4) de muestreo electrónicos asociados con otros grupos (31) de detectores SPAD (311).

4. Un generador (1) de números aleatorios según cualquiera de las reivindicaciones precedentes, caracterizado por que dichos medios (4) de muestreo electrónicos comprenden uno o más TDC (Convertidor de Tiempo a Digital) (41).

5. Un generador (1) de números aleatorios según cualquiera de las reivindicaciones precedentes, caracterizada por que dicha fuente (2) de fotones y dichos uno o más detectores SPAD (311) de fotones están hechos de modo que están integrados en un único sustrato (5) de silicio.

6. Un generador (1) de números aleatorios según la reivindicación 5, caracterizado por que dicha fuente (2) de fotones y dichos uno o más detectores SPAD (311) de fotones están hechos sobre dicho sustrato (5) de silicio mediante la técnica de micro-fabricación de circuitos integrados CMOS.

7. Un generador (1) de números aleatorios según cualquiera de las reivindicaciones precedentes, caracterizado por que dicha fuente (2) de fotones es un componente (21) de Si-LED hecho sobre dicho sustrato (4) de silicio.

8. Un generador (1) de números aleatorios según cualquiera de las reivindicaciones precedentes, caracterizado por que comprende medios (6) de post-procesamiento electrónicos configurados de modo que reciben dichas secuencias binarias extraídas por dichos medios (4) de muestreo electrónicos como entrada y para procesar dichas secuencias de binarias de tal modo que aumenten el valor de entropía por bit de salida de dicho generador (1).

9. Un generador (1) de números aleatorios según la reivindicación 8, caracterizado por que dichos medios (6) de post-procesamiento electrónicos están configurados de modo que procesen dichas secuencias binarias mediante un algoritmo de Von Neumann.

10. Un generador (1) de números aleatorios según la reivindicación 8, caracterizado por que dichos medios (6) de post-procesamiento electrónicos están configurados de modo que procesen dichas secuencias ordinarias a través de un algoritmo de función hash.

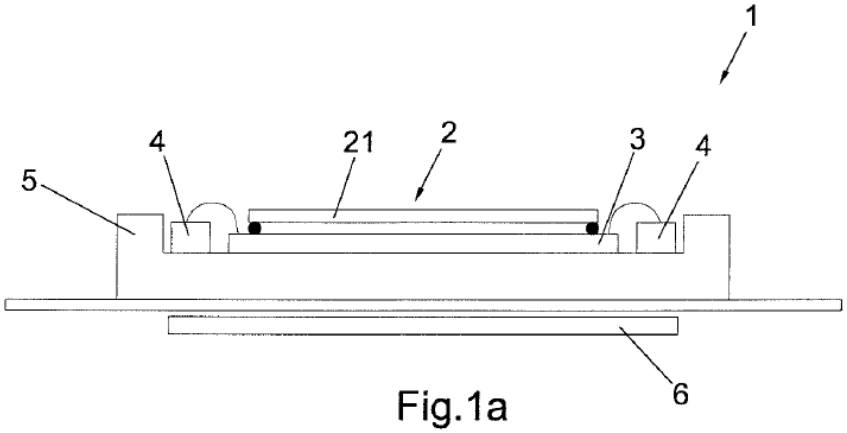

Fig.1a

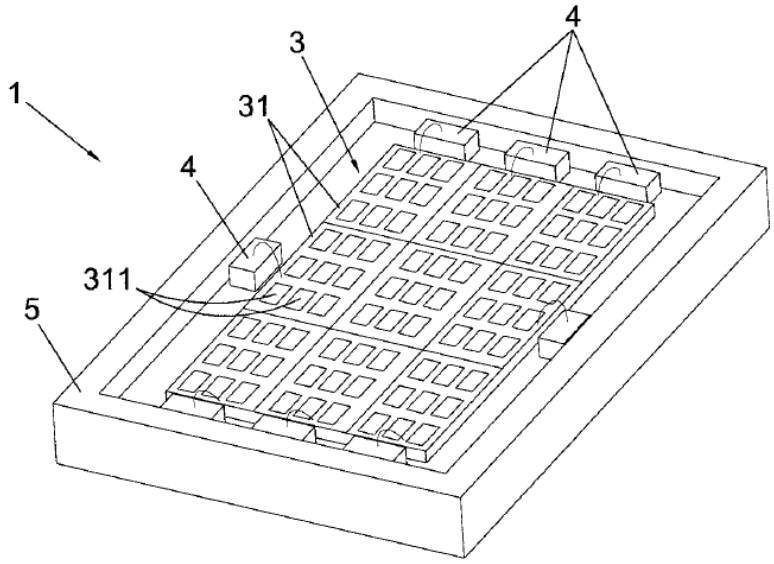

Fig.1b

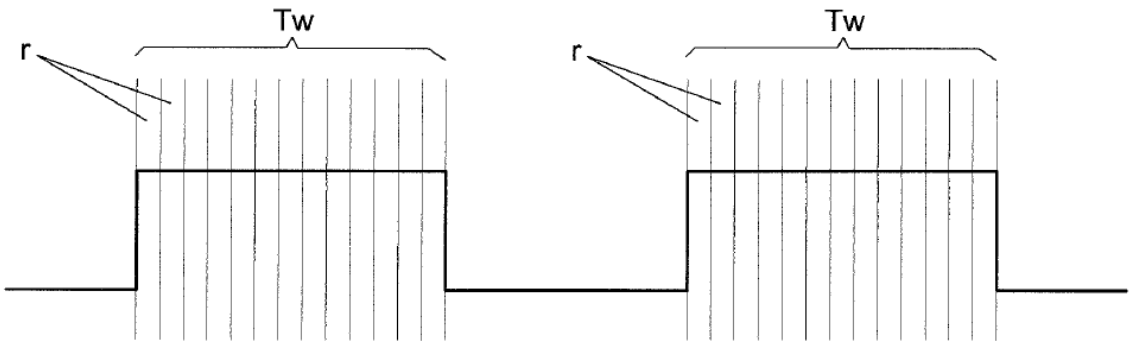

Fig.2

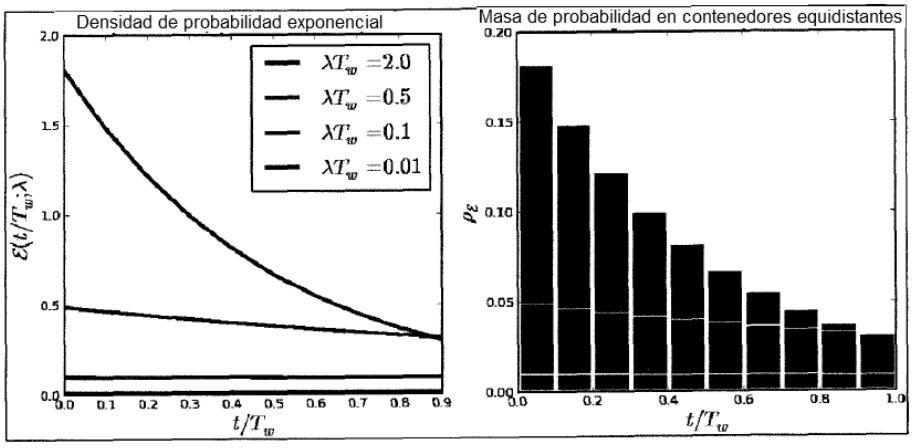
Densidad de probabilidad exponencial
$\lambda T_w = 2.0$
$\lambda T_w = 0.5$
$\lambda T_w = 0.1$
$\lambda T_w = 0.01$
$\mathcal{E}(t/T_w;\lambda)$
t/T_w
Masa de probabilidad en contenedores equidistantes
$\rho_\mathcal{E}$
t/T_w

Fig.3

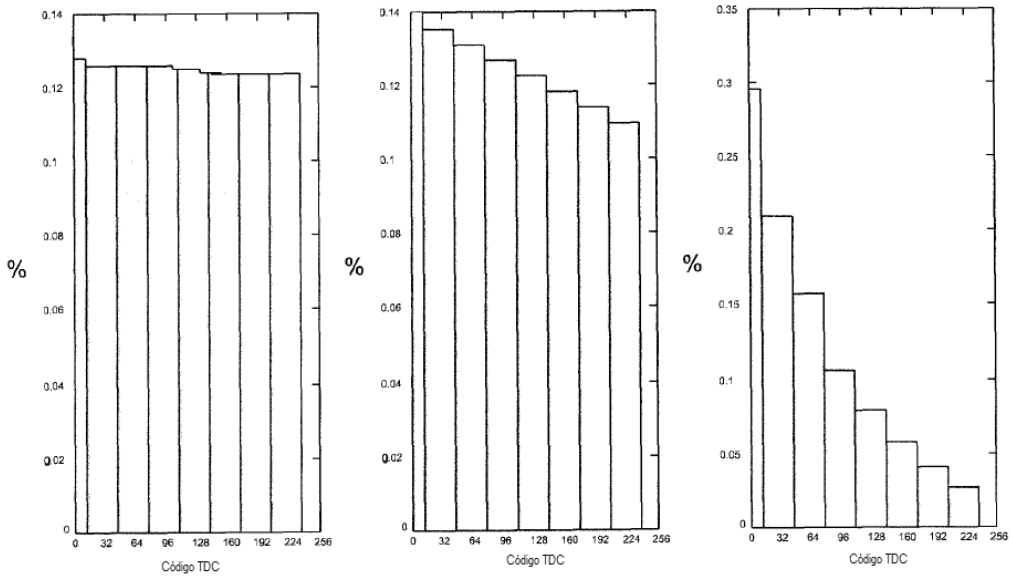
%
Código TDC
%
Código TDC
%
Código TDC

Fig.4