(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 791 890**

(51) Int. CI.:

G07C 15/00 (2006.01)
B82Y 10/00 (2011.01)
G06F 7/58 (2006.01)
G06N 99/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.05.2015 PCT/CA2015/050408**

(87) Fecha y número de publicación internacional: **12.11.2015 WO15168798**

(96) Fecha de presentación y número de la solicitud europea: **08.05.2015 E 15789278 (7)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2020 EP 3140818**

(54) Título: **Método para generar números aleatorios y generador de número aleatorio asociado**

(30) Prioridad:

09.05.2014 US 201461990751 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.11.2020

(73) Titular/es:

QUANTUM NUMBERS CORP. (100.0%)
1000, rue Sherbrooke Ouest Bureau 2700
Montréal, Québec H3A 3G4, CA

(72) Inventor/es:

REULET, BERTRAND

(74) Agente/Representante:

VIDAL GONZÁLEZ, Maria Ester

DESCRIPCIÓN

Método para generar números aleatorios y generador de número aleatorio asociado

Campo

Las mejoras generalmente se relacionan con el campo de la generación de números aleatorios.

Antecedentes

Los números aleatorios han encontrado aplicaciones valiosas en muchos campos, como la criptografía, los juegos de azar, el cálculo científico y/o los estudios estadísticos. En estas aplicaciones, la aleatoriedad de los números aleatorios generados es de gran importancia ya que su previsibilidad puede conducir a una comunicación insegura, a trampas y/o resultados científicos poco confiables, por ejemplo.

Las características que se buscan de los generadores de números aleatorios incluyen la capacidad de producir números aleatorios a una tasa relativamente alta mientras se usan dispositivos que son relativamente accesibles en términos de precios, volumen, etc.

Para satisfacer estas necesidades, los métodos usados anteriormente se basaban típicamente en algoritmos pseudoaleatorios y/o propiedades físicas pseudoaleatorias de los materiales. Si bien los números aleatorios generados por tales métodos pueden parecer completamente aleatorios a primera vista (incluso pueden pasar el conjunto de pruebas estadísticas para generadores de números aleatorios del Instituto Nacional de Estándares y Tecnología (NIST)), tales generadores pseudoaleatorios a menudo se basan en aproximaciones deterministas y, por lo tanto, pueden tener una falla que puede permitir predecir los resultados si finalmente se descubre la falla.

Así quedaba margen de mejora para proporcionar un dispositivo adecuado para producir la generación de números aleatorios.

El documento US 2013/0110895 A1 divulga un generador de ruido aleatorio que usa un transistor de efecto de campo.

Resumen

Contrariamente a la mecánica clásica, la mecánica cuántica presenta características inherentemente aleatorias. Se proporciona aquí un método por el cual la naturaleza inherentemente aleatoria de la mecánica cuántica puede aprovecharse para la generación de números aleatorios.

Más específicamente, se proporciona un método para generar números aleatorios que involucran cargas (electrones cargados negativamente o agujeros cargados positivamente) que hacen túneles al azar a través de una barrera de tunelización cuántica. Las cargas tunelizadas pueden generar un ruido eléctrico aleatorio de bajo nivel que puede filtrarse, amplificarse y muestrearse para obtener números aleatorios de una fuente cuántica. El método puede realizarse mediante componentes electrónicos relativamente simples y, por lo tanto, estar fácilmente disponible en una placa común.

Las cargas son repelidas por la barrera por el mecanismo de la reflexión clásica. Sin embargo, debido al efecto de tunelización cuántica, algunas cargas atraviesan la barrera y, por lo tanto, logran pasar de uno de los conductores al otro. Este efecto de tunelización cuántica es intrínsecamente aleatorio y, por lo tanto, se utiliza para producir números aleatorios. Al medir con precisión este efecto de tunelización cuántica a través de la diferencia de potencial (por ejemplo, polarización), barrera, amplificación, filtración, etc., la señal de número aleatorio derivada del efecto de tunelización cuántica puede aprovecharse satisfactoriamente y asociar a números aleatorios verdaderos. Además, la medición y la elección de componentes electrónicos también pueden permitir producir tales números aleatorios a una velocidad satisfactoria, al usar componentes electrónicos sorprendentemente simples. La barrera de tunelización cuántica puede tener la forma de un aislante eléctrico intercalado entre conductores, por ejemplo.

De ahora en adelante, las cargas que pueden atravesar la barrera de tunelización cuántica y generar el ruido eléctrico aleatorio (denominado aquí señal aleatoria) pueden hacerlo de una manera verdaderamente aleatoria, sabiendo que la tunelización cuántica es un proceso cuántico verdaderamente aleatorio exento de elementos complejos pero deterministas.

Además, se proporciona un generador de números aleatorios que comprende una placa o una placa de circuito impreso (PCB) que tiene una barrera de tunelización cuántica montada sobre la misma y adaptada para conectarse a una fuente de voltaje (fuente de cargas) que puede incorporarse directamente en la placa o proporcionarse por separado. Dado que la tunelización cuántica puede involucrar una gran cantidad de cargas tunelizadas que pueden atravesar la barrera de tunelización cuántica a una velocidad alta, un generador de números aleatorios puede, en teoría, permitir una generación y adquisición muy rápida de números aleatorios.

De acuerdo con un aspecto, se proporciona un método para generar al menos un número aleatorio, el método comprende

los pasos de: cargas de tunelización cuántica de un conductor a otro conductor a través de una barrera de tunelización cuántica; recibir una señal aleatoria derivada de la tunelización cuántica de las cargas; asociar la señal aleatoria a un número aleatorio; y generar una señal indicativa del número aleatorio.

De acuerdo con otro aspecto, se proporciona un generador de números aleatorios que comprende: una placa; una barrera de tunelización cuántica montada en la placa entre dos conductores y que permite a las cargas hacer un túnel aleatorio de uno de los conductores al otro para generar una señal aleatoria; un amplificador montado en la placa, con el amplificador conectado a uno de los dos conductores para amplificar la señal aleatoria; un dispositivo de muestreo montado en la placa y conectado al amplificador para asociar, en tiempo real, la señal aleatoria a al menos un número aleatorio.

De acuerdo con un aspecto, se proporciona un método para generar al menos un número aleatorio, el método comprende los pasos de: aplicar una diferencia de potencial a través de dos capas conductoras separadas por al menos una capa aislante entre ellas, la diferencia de potencial provoca la tunelización cuántica aleatoria de cargas a través del al menos un aislante, que genera así una señal aleatoria; y asociar la señal aleatoria a un número aleatorio.

De acuerdo con otro aspecto, se proporciona un generador de números aleatorios que comprende: una placa; una barrera de tunelización cuántica montada en la placa y que tiene al menos dos capas conductoras y al menos una capa aislante entre ellas, la al menos una capa aislante tiene dos caras opuestas exteriores cada una en contacto con una correspondiente de las dos capas conductoras, las dos capas conductoras pueden conectarse a un primer terminal y un segundo terminal de una fuente de voltaje, la barrera de tunelización cuántica permite que las cargas hagan un túnel al azar para generar una señal aleatoria cuando se opera la fuente de voltaje; un amplificador montado en la placa, el amplificador conectado a cualquiera de las dos capas conductoras para amplificar la señal aleatoria; un dispositivo de muestreo montado en la placa y conectado al amplificador para asociar en tiempo real la señal aleatoria a al menos un número aleatorio.

Muchas características adicionales y combinaciones de las mismas con respecto a las mejoras presentes aparecerán para los expertos en la técnica después de una lectura de la divulgación instantánea. La invención se define por las reivindicaciones adjuntas.

Descripción de las figuras

En las figuras,

La Figura 1 es un diagrama de flujo asociado con la generación de números aleatorios;

La Figura 2 es una vista esquemática que ilustra un ejemplo de una reflexión clásica de un electrón contra una capa aislante y un ejemplo de tunelización cuántica de un electrón a través de una capa aislante;

La Figura 3 muestra un ejemplo de un mapeo de números aleatorios de acuerdo con una modalidad de la presente invención;

La Figura 4 es un circuito eléctrico asociado con un ejemplo de un generador de números aleatorios;

Las Figuras 5A a 5C muestran vistas esquemáticas de una barrera de tunelización cuántica que tiene al menos una capa aislante;

La Figura 6 muestra una vista esquemática de un ejemplo de una barrera de tunelización cuántica;

La Figura 7 muestra una vista esquemática de los pasos de un ejemplo de un proceso de fotolitografía para fabricar una barrera de tunelización cuántica.

Descripción detallada

La Figura 1 es un diagrama de flujo asociado con un método para generar números aleatorios basado en el principio de la tunelización cuántica aleatoria de cargas (electrones o agujeros) a través de una barrera de tunelización cuántica. Como se discutirá con más detalle a continuación con referencia a la Figura 2, la barrera de tunelización cuántica puede tener la forma de un espacio entre dos conductores, a través del cual las cargas pueden reflejarse por reflexión clásica o pasar por tunelización cuántica. La señal aleatoria derivada del túnel aleatorio de cargas a través de la barrera de tunelización cuántica es recibida (detectada, monitoreada), y la señal aleatoria puede asociarse a un número aleatorio por una computadora o por componentes electrónicos basados en una amplitud en tiempo real de la señal, por nombrar ejemplos. El proceso puede repetirse un número satisfactorio de veces, a una velocidad satisfactoria.

La tunelización cuántica aleatorio puede ser asistido opcionalmente por una diferencia de potencial aplicada a través de la barrera de tunelización cuántica. La barrera de tunelización cuántica puede seleccionarse de manera que cause la reflexión clásica de las cargas, mientras se permite que las cargas hagan un túnel al azar a través de los procesos cuánticos. La barrera de tunelización cuántica puede proporcionarse en forma de una o más capas aislantes superpuestas

como se detallará a continuación con referencia a las Figuras 5A, 5B, 5C, en cuyo caso los conductores pueden incluir capas conductoras aplicadas a la una o más capas aislantes, por ejemplo. A medida que se realiza el paso de aplicar la diferencia de potencial, la diferencia de potencial puede evitar que se realicen cargas desde una capa conductora a la otra debido a una barrera potencial inherente formada por al menos una capa aislante. Además, la capa aislante de la barrera de tunelización cuántica puede aprovecharse para la tunelización aleatoria de cargas a través de la barrera de tunelización cuántica. El método comprende además un paso de generar una señal aleatoria basada en las cargas tunelizadas aleatoriamente.

De hecho, a medida que las cargas se tunelizan de una capa conductora a la otra, una corriente o flujo de cargas tunelizadas pasa a través de la capa aislante de la barrera de tunelización cuántica. Estas cargas tunelizadas aleatoriamente generan así la señal aleatoria que puede procesarse en un paso de asociar la señal aleatoria recibida en un momento dado a un número digital aleatorio.

Como se ilustra en la Figura 2, la barrera de tunelización cuántica tiene al menos una capa aislante que actúa como reflector de las cargas entrantes. Por lo tanto, las cargas que pasan a través de la al menos una capa aislante lo han hecho al cruzar aleatoriamente la barrera potencial mediante una tunelización cuántica.

Además, el método puede incluir una etapa de polarización de la diferencia de potencial para fijar la diferencia de potencial aplicada en las dos capas conductoras. Además, los componentes de la señal aleatoria que tienen frecuencias inferiores a 0,1 MHz y superiores a 6000 MHz pueden filtrarse de la señal aleatoria, y limpiar así la señal aleatoria de cualquier ruido que pueda deberse a otros componentes eléctricos conectados a las capas conductoras. De hecho, la señal aleatoria puede limpiarse de una porción de corriente continua (CC) y de frecuencias más altas.

Dado que la señal aleatoria generada por las cargas tunelizadas generalmente es apenas medible, el método para generar números aleatorios puede incluir un paso de amplificación de la señal aleatoria. El uso de la señal aleatoria puede limitarse a los componentes de la señal aleatoria que tienen frecuencias entre 0,1 MHz y 1000 MHz, según sea adecuado para abordar componentes de ruido potencialmente no deseados. En otras palabras, los componentes de la señal aleatoria que tienen una porción de corriente continua (CC) y frecuencias más altas no se amplifican, por ejemplo.

Puede apreciarse que el paso de asociar la señal aleatoria a un número digital aleatorio puede incluir un paso al que se hace referencia aquí como muestreo de la señal aleatoria. De hecho, el paso de muestreo puede asociar un nivel instantáneo (en tiempo real) de la señal aleatoria a un número digital particular. Una vez que el número digital particular se asocia al nivel instantáneo de la señal aleatoria, puede discriminarse el bit más significativo y conservar solo los bits menos significativos, esto tiene el efecto de generar una distribución uniforme del número digital aleatorio obtenido a partir de él. Por ejemplo, si el paso de muestreo digitaliza la señal aleatoria a un número digital de 8 bits, pueden discriminarse los cuatro bits más significativos y utilizar los cuatro bits menos significativos.

Además, se observa que, dado que la tunelización cuántica puede implicar una gran cantidad de cargas tunelizadas que pueden atravesar la barrera de tunelización cuántica a una velocidad alta, el paso de generar una señal aleatoria puede permitir una variación muy rápida de la señal aleatoria que, a su vez, permite una velocidad de adquisición rápida de los números digitales aleatorios. Por ejemplo, el muestreo de la señal aleatoria a una velocidad de muestreo superior a 400 000 kbits/s, preferiblemente superior a 1 000 Mbits/s y más preferiblemente superior a 8 Gbits/s está habilitado. Sin embargo, se observa que puede conectarse más de un generador de números aleatorios en paralelo para aumentar el número total de números aleatorios generados. Por ejemplo, al conectar en paralelo dos generadores de números aleatorios, cada uno con una tasa de generación de 8 Gbits/s (1 GB/s), puede lograrse una tasa de generación total de 16 Gbits/s (2 GB/s), y así sucesivamente.

La Figura 4 muestra un circuito eléctrico 10 asociado con un ejemplo de un generador de números aleatorios. El generador de números aleatorios generalmente comprende una placa (no se muestra) en la que está montado el circuito eléctrico 10. El circuito eléctrico 10 del generador de números aleatorios puede incluir la barrera de tunelización cuántica 12, un dispositivo de polarización 20, un amplificador 16, un dispositivo de muestreo 18 y un filtro 14 que pueden montarse en la placa. Por ejemplo, la placa puede ser una placa de circuito impreso (PCB) que soporta mecánicamente los componentes y conecta eléctricamente los componentes entre sí a través de pistas conductoras grabadas en láminas de cobre laminadas sobre un sustrato no conductor.

Como se mencionó anteriormente, la barrera de tunelización cuántica puede proporcionarse en forma de un componente de tunelización cuántica que tiene una barrera de tunelización cuántica en forma de una o más capas aislantes intercaladas entre capas conductoras que actúan como conductores. Se observa que las capas conductoras pueden estar hechas de un material metálico o de un material semiconductor, por ejemplo, mientras que la capa aislante puede estar hecha de cualquier material que inhiba satisfactoriamente la conducción libre de electrones (o agujeros) a través de la reflexión clásica. De hecho, cualquier material que pueda proporcionar una barrera de energía que se pueda atravesar tunelización cuántica puede usarse en la barrera de tunelización cuántica. En consecuencia, las dos capas conductoras pueden estar hechas de material semiconductor, mientras que la capa aislante puede estar hecha de un aislante. En este ejemplo, el aislante puede tener un intervalo de banda que obliga a las cargas (electrones o agujeros) a pasar a través de la tunelización cuántica, y en donde las dos capas conductoras pueden doparse en n o doparse en p. La capa aislante tiene dos caras opuestas exteriores cada una en contacto con una de las dos capas conductoras correspondientes y las

dos capas conductoras pueden ser conectables a un primer terminal y un segundo terminal de una fuente de voltaje. Puede apreciarse que la fuente de voltaje puede estar montada en la placa y conectada de manera fija a las capas conductoras de la barrera de tunelización cuántica o proporcionarse por separado a la misma.

En esta modalidad, el dispositivo de polarización 20 puede usarse para realizar un paso de polarización, el amplificador 16 puede adaptarse para realizar un paso de amplificación de la señal aleatoria, el dispositivo de muestreo 18 puede adaptarse para realizar un paso de muestreo de la señal aleatoria y el filtro 14 puede adaptarse para realizar el paso de filtrar la señal aleatoria. El filtro puede conectarse a la barrera de tunelización cuántica, que, a su vez, se conecta al amplificador y luego al dispositivo de muestreo. Cuando está operativamente conectado uno a los otros, el circuito eléctrico puede muestrear instantáneamente la señal aleatoria para obtener un número aleatorio. Además, el dispositivo de polarización puede corregir la diferencia de potencial aplicada a la barrera de tunelización cuántica. En consecuencia, la polarización del dispositivo de polarización puede ajustarse para abarcar cualquier ruido que pueda incorporarse, en el circuito eléctrico, por el amplificador o el dispositivo de muestreo, por ejemplo.

Las Figuras 5A a 5C muestran tres ejemplos de la barrera de tunelización cuántica. En estos ejemplos, puede verse que pueden usarse una o más capas aislantes. Más específicamente, la Figura 5A muestra una capa aislante que tiene un primer grosor d_1, mientras que la Figura 5B muestra una barrera de tunelización cuántica que tiene dos capas aislantes, que tienen respectivamente un primer grosor d_1 y un segundo grosor d_2. Además, y de manera ejemplar, la Figura 5C muestra una barrera de tunelización cuántica que tiene tres capas aislantes, que tienen respectivamente un primer espesor d_1, un segundo espesor d_2 y un tercer espesor d_3. Aunque solo se han proporcionado tres ejemplos, la barrera de tunelización cuántica también puede tener más de tres capas aislantes. El material de las capas aislantes puede variar y pueden usarse diferentes materiales de una capa sucesiva a otra. Típicamente, las capas sucesivas pueden tener un efecto aditivo en términos del nivel del efecto barrera, permitiendo alcanzar un nivel deseado con una pluralidad de capas si se desea.

La Figura 6 muestra una vista superior esquemática de una barrera de tunelización cuántica de acuerdo con la presente invención. En este ejemplo, las capas conductoras de la barrera de tunelización cuántica están grabadas de un material metálico como el aluminio y están laminadas sobre un sustrato no conductor como el dióxido de silicio. La barrera de tunelización cuántica se ilustra con una línea roja y tiene una región superpuesta de aproximadamente 10 μm^2 que tiene dimensiones de 1 µm por 10 µm, por ejemplo. Aún en este ejemplo, la capa de aislante está comprendida entre las dos capas conductoras, donde se observa que las cargas pueden viajar desde la capa conductora superior a través de la capa conductora inferior mediante tunelización cuántica. La capa aislante puede estar hecha de óxido de aluminio (Al_2O_3). Se puede ver que el grosor de la capa aislante es de 1 nm, por ejemplo, y puede tener una resistencia de aproximadamente 50 ohmios. Se sabe que la resistencia de la barrera de tunelización cuántica puede depender del área superpuesta.

Aunque el método de fabricación de la barrera de tunelización cuántica puede variar, se proporcionará ahora un ejemplo de método de fabricación basado en una técnica de fotolitografía conocida como puente Dolan con fines ilustrativos con referencia a la Figura 7. En este ejemplo, un sistema de fotolitografía como un SF-100 Xpress se usó simultáneamente con resinas denominadas LOR30B y S1813. De hecho, el método de fabricación puede incluir un paso de limpiar un sustrato de impurezas (a), un paso de aplicar una capa de resina LOR30B sobre el sustrato limpio, aplicar una capa de resina S1813 sobre la capa de resina LOS30B (b). Luego, puede realizarse un paso adicional de exposición, a la luz UV, de la resina S1813 en todas partes excepto en un segmento (que puede formar un puente Dolan) (c). Luego, puede realizarse un paso de eliminación química de la capa de resina S1813 que se expuso con luz UV, así como un paso de eliminación química de la capa de LOR30B para dejar el segmento de la capa S1813 (denominado puente Dolan) intacto (d). Posteriormente, puede evaporarse una primera capa conductora sobre el sustrato al usar el puente Dolan como máscara para que la primera capa conductora se deposite sobre el sustrato y sobresalga de un lado del puente Dolan, y debajo de la misma, hasta que la última lo permita (e). Luego, puede evaporarse una capa aislante de óxido de aluminio sobre la primera capa conductora (f). Puede evaporarse una segunda capa conductora sobre la capa aislante, y usar el otro lado del puente Dolan, y a continuación, en la medida en que lo permita, formar una región superpuesta donde la capa aislante se intercala entre las dos capas conductoras. Finalmente, el puente Dolan puede quitarse para descubrir un componente de tunelización cuántica completo.

Además, un experto en la materia puede apreciar que al proporcionar un dispositivo de tunelización cuántica montado directamente en una placa, puede dar lugar a un dispositivo que tenga un bajo costo y cuyo proceso de fabricación se pueda implementar en instalaciones especializadas como fabs, por ejemplo.

Aunque una persona experta en la técnica puede saber qué componentes de hardware pueden usarse en el generador de números aleatorios. En una modalidad, por ejemplo, la barrera de tunelización cuántica puede exhibir una resistencia de 54 ohmios. El dispositivo de polarización puede ser una T de polarización Mini-Circuits ZFBT-6GW+. El dispositivo de muestreo puede ser una placa de adquisición de datos de 8 bits con una frecuencia de muestreo de 3 billones de muestras por segundo y fabricada por Ultraview™. Como se mencionó anteriormente, la frecuencia de muestreo puede limitarse para limitar una correlación entre niveles consecutivos de señal aleatoria. Por ejemplo, la frecuencia de muestreo puede limitarse a mil millones de muestras por segundo. Además, amplificar la señal aleatoria en 52 dB fue suficiente para el generador de números aleatorios. Los amplificadores pueden incorporar dos amplificadores Mini-Circuits ZFL-1000LN+ junto con atenuadores Mini-Circuits BW-S3W2+ para sintonizar el nivel de amplificación de la señal aleatoria. Con tal modalidad, el generador de números aleatorios puede generar hasta 4 billones de bits por segundo (4 Gbits/s), que es

mucho más rápido que el competidor más cercano, el generador de números aleatorios GRANG de LETech, que logra 0,4 Gbits/s.

Se observa además que cuando la polarización es 0 V (es decir, en ausencia de un dispositivo de polarización), el ruido es térmico y las cargas pueden pasar a través de la barrera de tunelización cuántica a través de la tunelización cuántica. Tal ruido térmico puede usarse directamente como la fuente de la señal aleatoria, aunque en la modalidad presentada anteriormente, se prefirió usar la tunelización cuántica efectuado generado por la aplicación de una diferencia de potencial a través de la barrera. En el caso de que la energía eV sea mayor que kT, en donde e es la carga eléctrica, V es la polarización, k es la constante de Boltzmann y T es la temperatura absoluta en grados Kelvin, por ejemplo, V > 25 mV, el ruido puede convertirse en un ruido de disparo que es proporcional a V, es decir, mayor es V, mayor es la señal aleatoria generada. En esta situación, la contribución de los otros componentes eléctricos del circuito eléctrico puede ser insignificante. Sin embargo, puede preferirse polarizar V. Por ejemplo, la barrera de tunelización cuántica puede colapsar si supera un umbral de colapso, lo que puede motivar la polarización. En el ejemplo descrito e ilustrado, el uso adecuado de la barrera de tunelización cuántica se logró a V = 0,25 V.

Además, se observa que el dispositivo de muestreo puede proporcionarse en forma de un comparador digital que tiene un número de entrada que es la señal aleatoria y otro número de entrada que es cero. Cuando la señal aleatoria es positiva, el comparador digital está adaptado para proporcionar un 1 binario, de lo contrario, proporciona un 0 binario. En dicha configuración, pueden usarse algoritmos conocidos para evitar una polarización del valor cero del otro número de entrada. En consecuencia, el comparador digital puede usarse para obtener una serie de 1 y 0 binarios sucesivos y aleatorios que pueden usarse para proporcionar números aleatorios. Como puede apreciar una persona experta en la técnica, el amplificador y el dispositivo de muestreo podrían limitarse a frecuencias en el orden de los kHz para limitar el costo del generador de números aleatorios. Además, el dispositivo de polarización puede integrarse directamente en el amplificador. Tal dispositivo de polarización podría polarizar la diferencia de potencial y también amplificar la diferencia de potencial polarizada en el mismo componente eléctrico. Se observa además que la polarización de la diferencia de potencial puede usarse siempre que no interfiera con el amplificador. Aunque aquí se presenta el uso de un dispositivo de muestreo o un comparador digital para convertir el ruido aleatorio en números aleatorios, una persona experta en la técnica también podría implementar otras técnicas.

Se observa además que el generador de números aleatorios puede montarse en un dispositivo de bus serie universal (USB) que puede proporcionar un dispositivo portátil que alcanza velocidades de hasta 480 Mb/s con USB 2.0 e incluso más con USB 3.0. Alternativamente, el generador de números aleatorios puede montarse en un dispositivo de interconexión de componentes periféricos (PCI) y alcanzar hasta 1 Gb/s hasta 17 Gb/s. Además, el generador de números aleatorios puede implementarse directamente desde una placa base del fabricante de equipos originales (OEM).

Aumentar la diferencia de potencial puede aumentar la señal. Alternativamente, calentar la unión puede aumentar el ruido cuántico y, por lo tanto, también la señal.

Como puede entenderse, los ejemplos descritos anteriormente e ilustrados están destinados a ser solo ejemplares. El alcance está indicado por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para generar al menos un número aleatorio, el método comprende los pasos de: generar una corriente de tunelización de cargas desde un primero de dos conductores a un segundo de dos conductores a través de un aislante, la corriente de las cargas tunelizadas tiene un nivel instantáneo que varía aleatoriamente debido a la tunelización cuántica y forma una señal aleatoria, en donde cada uno de los dos conductores está configurado para poder ser conectado a un terminal correspondiente de una fuente de voltaje; asociar el nivel instantáneo de la señal aleatoria a un número aleatorio; y generar una señal indicativa del número aleatorio.

2. El método de la reivindicación 1, que comprende además generar la tunelización cuántica de cargas al aplicar una diferencia de potencial a través de los dos conductores, y en donde durante dicha aplicación de una diferencia de potencial, dicho aislante provoca la reflexión clásica de las cargas impulsadas contra este por la diferencia de potencial.

3. El método de la reivindicación 1, que comprende además amplificar el nivel instantáneo de la señal aleatoria antes de dicha asociación.

4. El método de la reivindicación 3, en donde dicha amplificación se aplica únicamente a componentes del nivel instantáneo de la señal aleatoria dentro de un ancho de banda de frecuencia de 0,1 MHz a 1000 MHz.

5. El método de la reivindicación 1, en donde dicha asociación comprende además muestrear el nivel instantáneo de la señal aleatoria.

6. El método de la reivindicación 5, en donde dicho muestreo comprende además determinar el número aleatorio basado en uno o más de los bits menos significativos de una pluralidad de bits de la señal aleatoria muestreada.

7. El método de la reivindicación 5, en donde dicho muestreo se realiza a una velocidad superior a mil millones de muestreos por segundo.

8. El método de la reivindicación 1, en donde los dos conductores tienen forma de capas conductoras que intercalan el aislante.

9. Un generador de números aleatorios que comprende:

   una barrera de tunelización cuántica (12) que tiene un aislante que tiene dos caras opuestas exteriores cada una en contacto con un conductor correspondiente de los dos conductores y que permite que las cargas hagan un túnel aleatorio desde uno de los conductores al otro conductor a través del aislante para formar una corriente de cargas tunelizadas que pasan a través del aislante, la corriente de cargas tunelizadas tiene un nivel instantáneo que varía aleatoriamente debido a la tunelización cuántica y forma una señal aleatoria, en donde cada uno de los conductores está configurado para poder ser conectado a un terminal correspondiente de una fuente de voltaje;
   un amplificador (16) conectado a uno de los dos conductores para amplificar la señal aleatoria;
   un dispositivo de muestreo (18) conectado al amplificador para asociar, en tiempo real, el nivel instantáneo de la señal aleatoria amplificada a al menos un número aleatorio.

10. El generador de números aleatorios de la reivindicación 9 en donde los dos conductores están forma de capas conductoras que intercalan el aislante.

11. El generador de números aleatorios de la reivindicación 9, en donde la fuente de voltaje conectada a los dos conductores y que funciona para generar una diferencia de potencial provoca que las cargas se canalicen aleatoriamente desde uno de los conductores al otro conductor a través del aislante para formar la corriente de cargas tunelizadas.

12. El generador de números aleatorios de la reivindicación 11, en donde la barrera de tunelización cuántica (12) evita que las cargas de la fuente de voltaje pasen a través de la reflexión clásica.

13. El generador de números aleatorios de la reivindicación 10, en donde al menos una de las dos capas conductoras está fabricada de un material metálico.

14. El generador de números aleatorios de la reivindicación 10, en donde al menos una de las dos capas conductoras está fabricada de un material semiconductor.

15. El generador de números aleatorios de la reivindicación 9, que comprende además una placa proporcionada en forma de una placa de circuito impreso (PCB) que soporta mecánicamente la barrera de tunelización cuántica (12), los conductores, el amplificador (16) y el dispositivo de muestreo (18), que tienen pistas conductoras grabadas a partir de láminas de cobre laminadas sobre un sustrato no conductor y que conecta eléctricamente los

componentes entre sí.

16. El generador de números aleatorios de la reivindicación 9, en donde el dispositivo de muestreo (18) es una placa de adquisición de datos que tiene una frecuencia de muestreo de 3 billones de muestreos por segundo.

17. El generador de números aleatorios de la reivindicación 9, en donde el amplificador (16) amplifica la señal aleatoria con más de 50 dB.

18. El generador de números aleatorios de la reivindicación 9, en donde el amplificador (16) tiene un paso de banda de amplificación de 0,1 MHz a 1000 MHz.

19. El generador de números aleatorios de la reivindicación 11 que comprende además un dispositivo de polarización (20) entre la barrera de tunelización cuántica (12) y el amplificador (16), el dispositivo de polarización (20) para polarizar la fuente de voltaje y fijar la diferencia de potencial aplicada en la barrera de tunelización cuántica (12); y un filtro (14) montado en la placa, entre la barrera de tunelización cuántica (12) y el amplificador (16).

20. El generador de números aleatorios de la reivindicación 9 conectado en paralelo con al menos otro generador de números aleatorios.

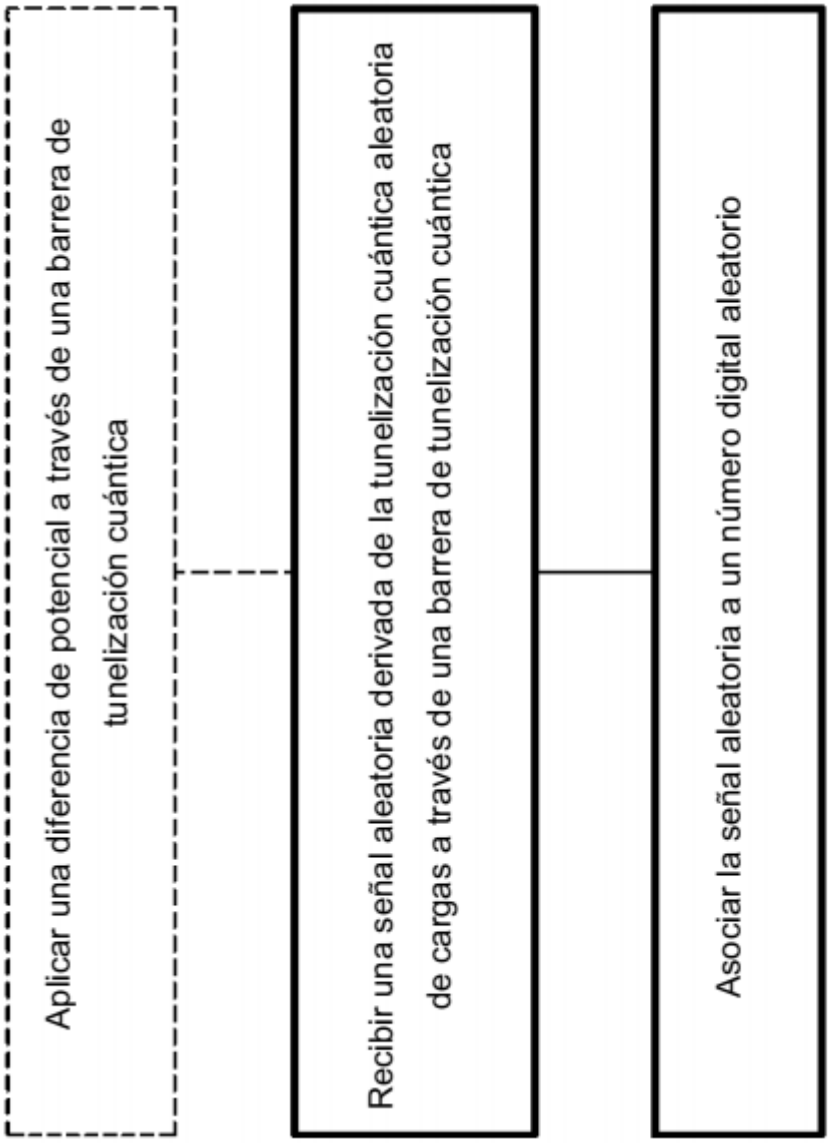
Aplicar una diferencia de potencial a través de una barrera de tunelización cuántica
Recibir una señal aleatoria derivada de la tunelización cuántica aleatoria de cargas a través de una barrera de tunelización cuántica
Asociar la señal aleatoria a un número digital aleatorio

Figura 1

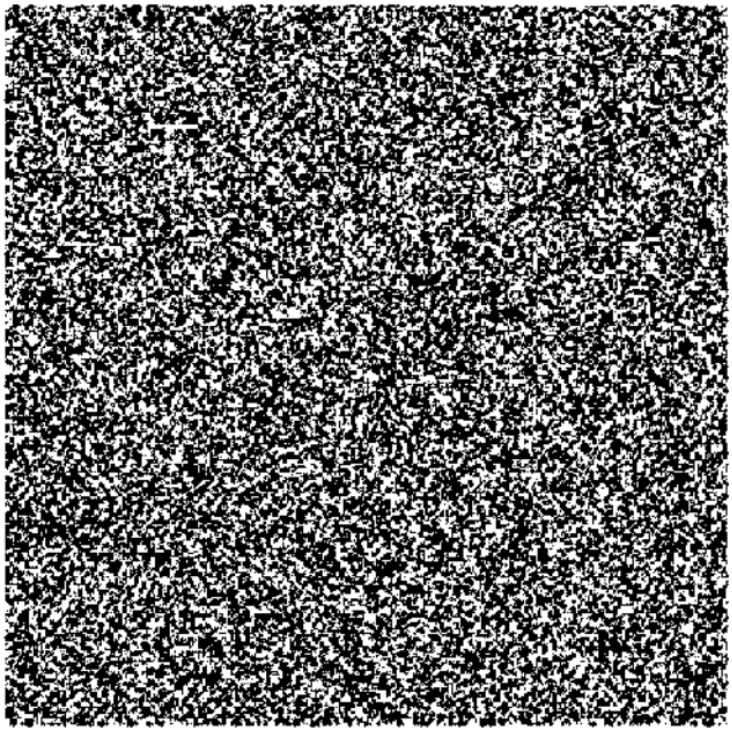

Figura 3

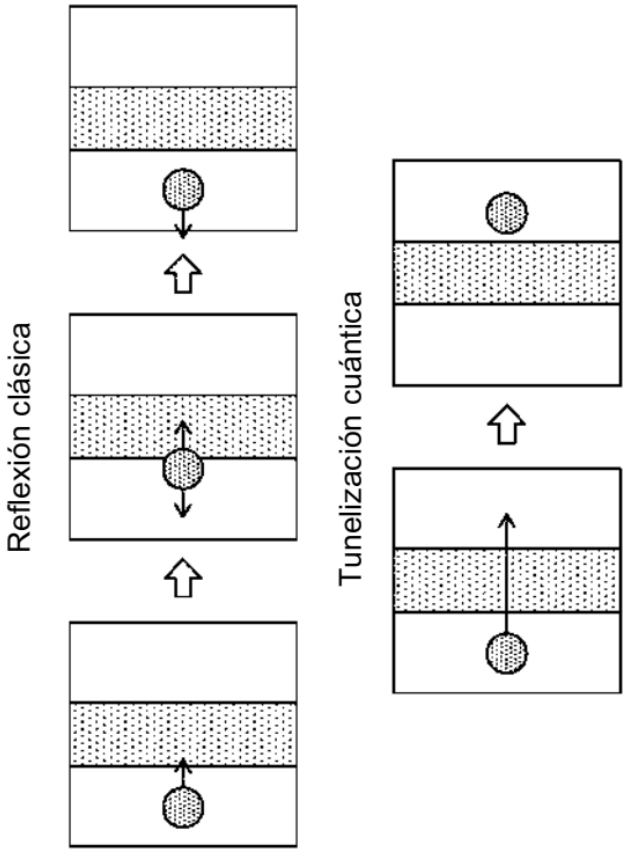

Figura 2

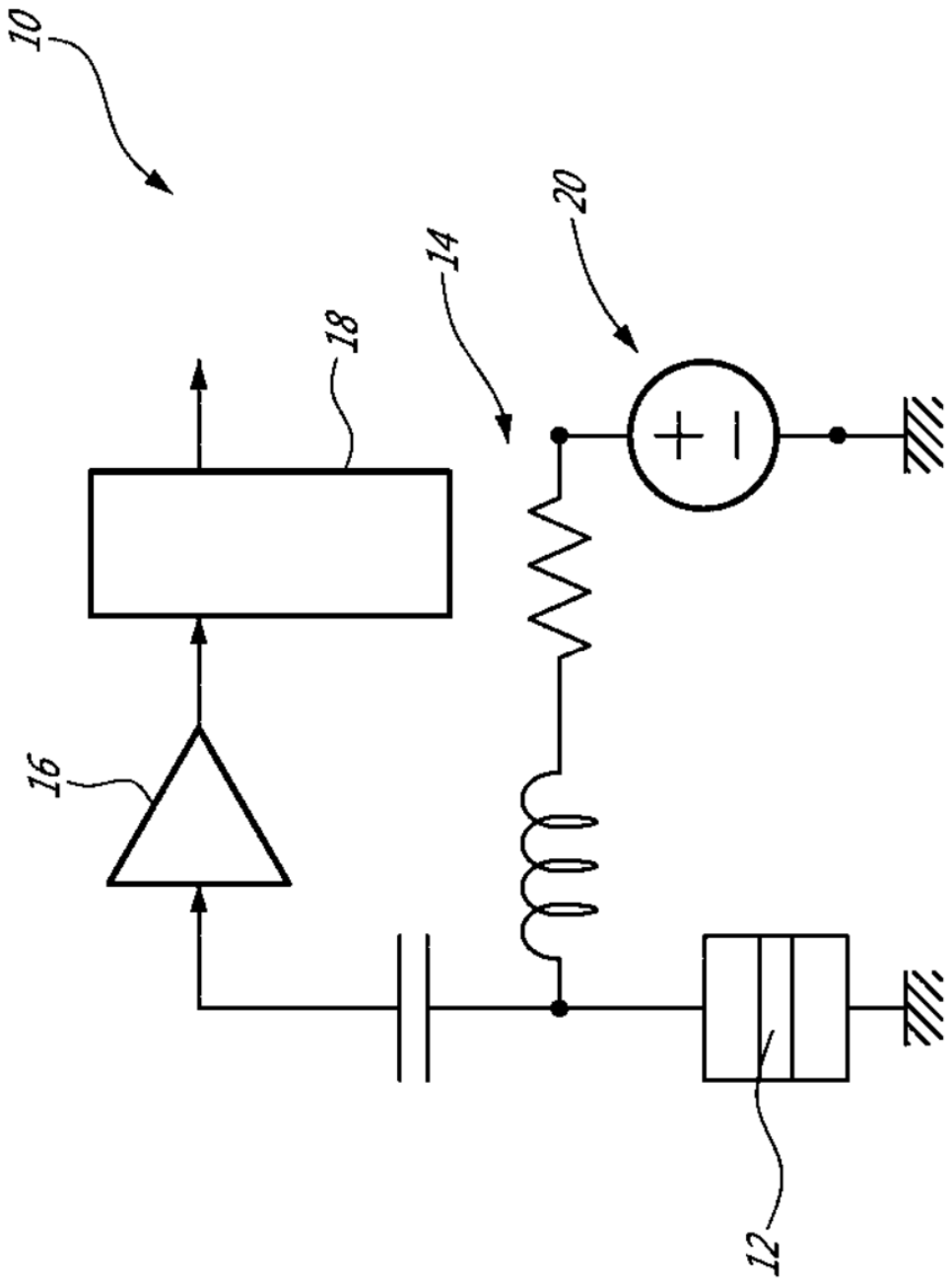

Figura 4

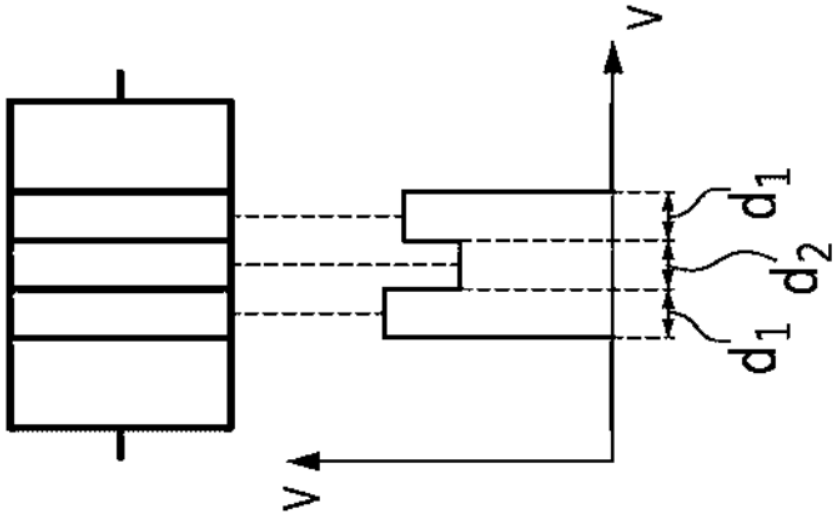

Figura 5C

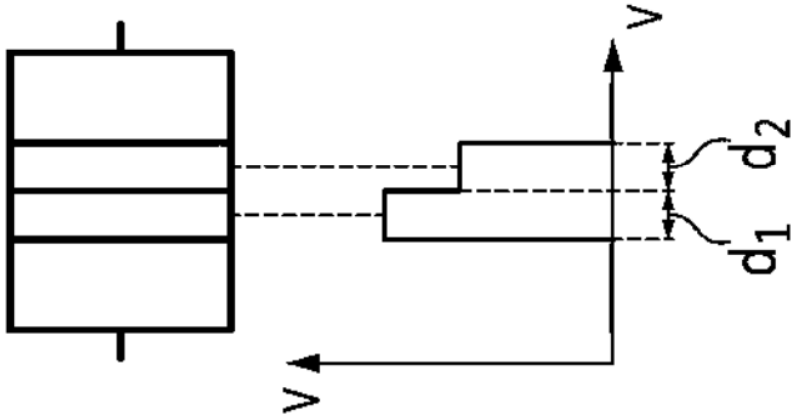

Figura 5B

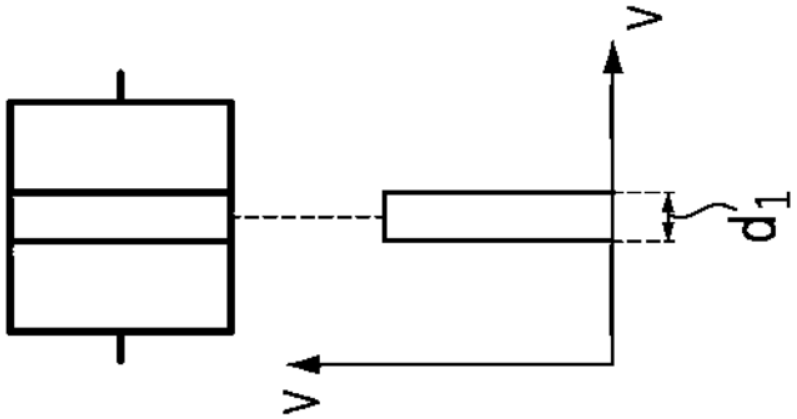

Figura 5A

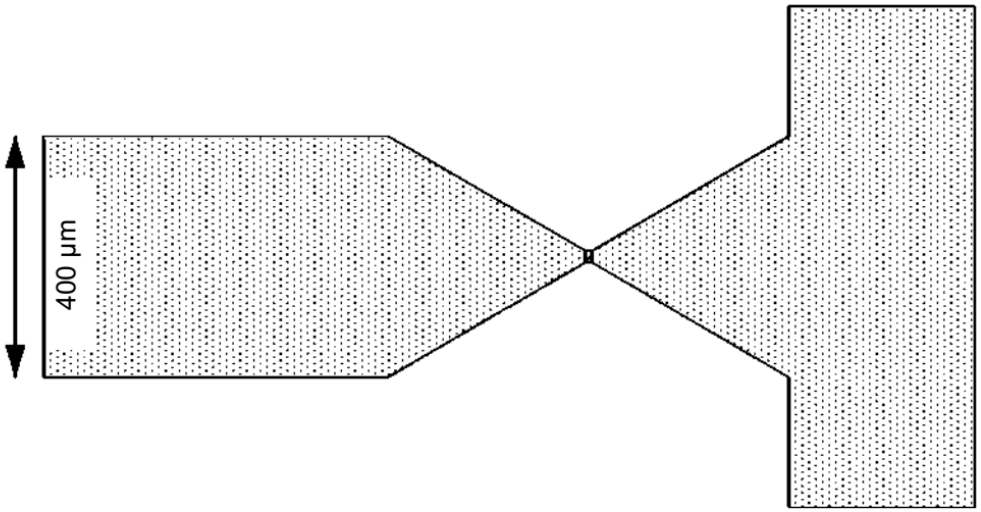

Figura 6

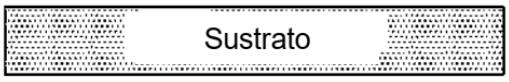

Figura 7A

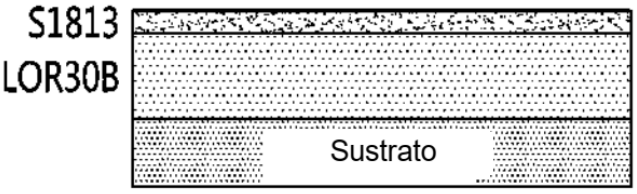

Figura 7B

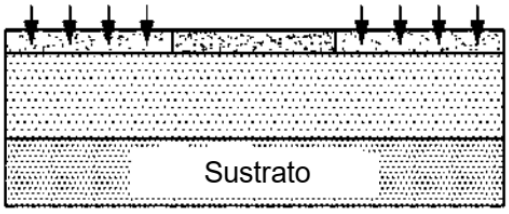

Figura 7C

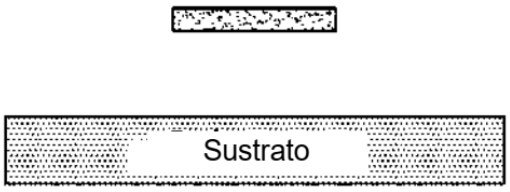

Figura 7D

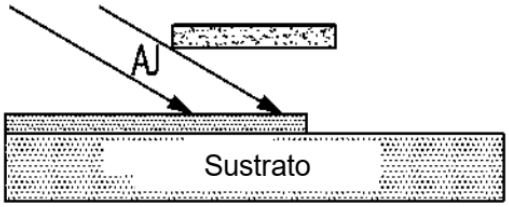

Figura 7E

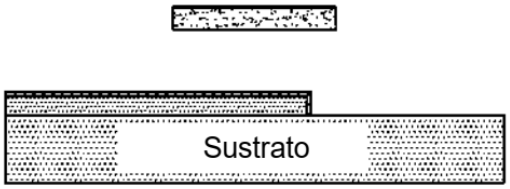

Figura 7F

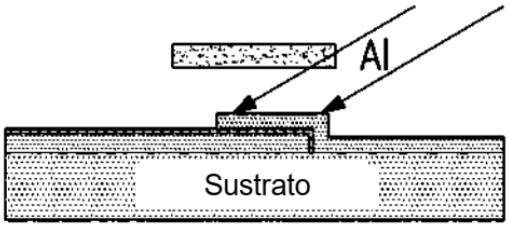

Figura 7G

Figura 7H