(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 433**

(51) Int. CI.:

G06F 7/58 (2006.01)
G09C 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.03.2018 E 18161523 (8)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2019 EP 3511819**

(54) Título: **Procedimiento y sistema de generación de bits cuánticos aleatorios**

(30) Prioridad:

15.01.2018 US 201862617444 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.06.2020

(73) Titular/es:

QUANTUM NUMBERS CORP. (100.0%)
201-3755 E. Boul. Matte
Brossard, Québec J4Y 2P4, CA

(72) Inventor/es:

REULET, BERTRAND y
PHANEUF, JEAN-CHARLES

(74) Agente/Representante:

GARCÍA GONZÁLEZ, Sergio

DESCRIPCIÓN

Procedimiento y sistema de generación de bits cuánticos aleatorios.

Campo

Las mejoras, en general, se refiere al campo de la generación de bits aleatorios mediante el uso de la tunelización cuántica de cargas.

Antecedentes

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

La expresión "aleatorio" se usa de una manera relativamente liberal en el campo de los generadores de bits aleatorios debido a que se conoce típicamente que los flujos de bits que se producen tienen un cierto nivel determinístico (es decir, no son puramente aleatorios). Se han desarrollado varios enfoques para evaluar la calidad de la aleatoriedad en muestras de bits aleatorios, tal como el conjunto de pruebas estadísticas para generadores de bits aleatorios desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).

Las características que se buscan de los generadores de bits aleatorios incluyen la calidad de la aleatoriedad, la capacidad de producir bits aleatorios a una tasa relativamente alta, precios, huella, etc. Por lo tanto, queda margen de mejora para proporcionar un dispositivo adecuado de producción de generación de bits aleatorios.

Sumario

Las fuentes de ruido cuántico presentan características que son inherentemente aleatorias y, por lo tanto, pueden aprovecharse para la generación de bits aleatorios que tienen un alto nivel de calidad de aleatoriedad. Por ejemplo, las muestras de bits se pueden generar sobre la base de una corriente de cargas (electrones cargados negativamente y/o agujeros cargados positivamente) que se tunelizan aleatoriamente a través de una barrera de tunelización cuántica. La barrera de tunelización cuántica puede tener la forma de un aislante eléctrico intercalado entre los conductores, por ejemplo. La corriente de cargas tunelizadas tiene un nivel instantáneo que varía aleatoriamente debido a la naturaleza aleatoria inherente de la tunelización cuántica y, por lo tanto, forma un ruido eléctrico de bajo nivel. Como se puede entender, el ruido eléctrico de bajo nivel se filtra, amplifica y digitaliza típicamente en muestras de bits en bruto a partir de las cuales se pueden determinar luego las muestras de bits de aleatoriedad satisfactoria.

Puede ser necesario procesar la señal proveniente de una barrera de tunelización cuántica, tal como por ejemplo a través de la amplificación, para poder proporcionar una señal en bruto que puede usarse para la generación de bits aleatorios. El procesamiento puede ser de naturaleza parcial o totalmente determinista, y puede generar ruido externo que se enreda intrínsecamente con el ruido cuántico de la señal en bruto, y que reduce la calidad de la aleatoriedad de las muestras de bits en bruto resultantes. En consecuencia, incluso cuando se utiliza un proceso verdaderamente cuántico tal como la tunelización cuántica como fuente de generación de muestras de bits en bruto, la calidad de la aleatoriedad puede ser menos que perfecta y puede verse obstaculizada durante el procesamiento.

En la presente memoria se describe un procedimiento que puede aliviar al menos algunos de los inconvenientes asociados con el procesamiento de la señal en bruto derivada de una barrera de tunelización cuántica. Esto se puede hacer mediante la extracción de muestras de bits de mayor calidad de aleatoriedad de tales muestras de bits en bruto mediante el uso de datos de calibración que comprenden un valor de contribución cuántica de la barrera de tunelización cuántica y un valor de contribución externa debido al menos a los amplificadores.

La invención se define por las reivindicaciones independientes. Las realizaciones preferentes se exponen en las reivindicaciones dependientes.

En un aspecto, se proporciona un procedimiento para generar una muestra de bits aleatorios mediante el uso de una barrera de tunelización cuántica que comprende un aislante intercalado entre dos conductores, el procedimiento que comprende: generar una corriente de cargas de túnel a partir del primero de los dos conductores a un segundo de los dos conductores y a través del aislante, la corriente de las cargas tunelizadas que tiene un nivel instantáneo que varía aleatoriamente debido a las fluctuaciones de tunelización cuántica y que forma una señal en bruto; a partir de dicha señal en bruto, obtener una muestra de bits en bruto que tiene un primer número de bits n, el primer número de bits n que es un entero; extraer la aleatoriedad de la muestra de bits en bruto en la muestra de bits aleatorios, la muestra de bits aleatorios que tiene un segundo número de bits m que es más pequeño que el primer número de bits n, dicha extracción se basa en los datos de calibración que comprenden al menos un valor de contribución cuántica de dichas fluctuaciones de tunelización cuántica en dicha muestra de bits en bruto; y un valor de contribución externa en dicha muestra de bits en bruto.

En un aspecto, se proporciona un sistema para generar una muestra de bits aleatorios, el sistema que comprende: un circuito de barrera de tunelización cuántica que tiene una barrera de tunelización cuántica que incorpora un aislante intercalado entre dos conductores, una corriente de cargas que se tuneliza desde el primero de los dos conductores a un segundo de los dos conductores y a través del aislante, la corriente de las cargas tunelizadas que tiene un nivel instantáneo que varía aleatoriamente debido a las fluctuaciones de tunelización cuántica y que forma una señal en bruto; un monitor configurado para recibir dicha señal en bruto y, a partir de dicha señal en bruto, obtener una muestra de bits en bruto que tiene un primer número de bits n, el primer número de bits n que es un número entero; y un extractor de aleatoriedad configurado para extraer la aleatoriedad de la muestra de bits en bruto en la muestra de bits aleatorios, la muestra de bits aleatorios que tiene un segundo número de bits m que es más pequeño que el primer número de bits n, dicha extracción que se basa en los datos de calibración que comprenden al menos un valor de contribución cuántica de dichas fluctuaciones de tunelización cuántica en dicha muestra de bits en bruto; y un valor de contribución externa en dicha muestra de bits en bruto.

El procedimiento puede realizarse mediante componentes electrónicos relativamente simples y, por lo tanto, estar fácilmente disponible en una placa común. Además, la calibración y la elección de componentes electrónicos también pueden permitir producir tales muestras de bits aleatorios a una velocidad satisfactoria, mediante el uso de componentes electrónicos sorprendentemente simples. Además, se proporciona un generador de bits aleatorios que comprende una placa o una placa de circuito impreso (PCB) que tiene una o más barreras de tunelización cuántica montadas sobre la misma, y adaptadas para conectarse a una fuente de polarización (fuente de cargas) que puede incorporarse o bien directamente sobre 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 bits aleatorios puede, en teoría, permitir una generación y adquisición muy rápida de muestras de bits aleatorios.

Se debe entender que la expresión "ordenador" como se usa en la presente memoria no debe interpretarse de manera limitante. Se usa más bien en un sentido amplio para referirse generalmente a la combinación de alguna forma de una o más unidades de procesamiento y alguna forma de sistema de memoria accesible por la(s) unidad(es) de procesamiento. De manera similar, la expresión "controlador", como se usa en la presente memoria, no debe interpretarse de manera limitante, sino más bien en un sentido general de un dispositivo, o de un sistema que tiene más de un dispositivo, que realiza la(s) función(es) de controlar uno o más dispositivo tal como un dispositivo electrónico o un actuador, por ejemplo.

Se debe entender que las diversas funciones de un ordenador o de un controlador pueden realizarse mediante hardware o mediante una combinación de hardware y software. Por ejemplo, el hardware puede incluir puertas lógicas incluidas como parte de un chip de silicio del procesador. El software puede estar en forma de datos, tales como instrucciones legibles por ordenador almacenadas en el sistema de memoria. Con respecto a un ordenador, un controlador, una unidad de procesamiento o un chip del procesador, la expresión "configurado para" se refiere a la presencia de hardware o una combinación de hardware y software que es operable para realizar las funciones asociadas.

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.

Descripción de las figuras

En las figuras,

La Figura 1 es una vista esquemática de un ejemplo de un generador de bits aleatorios que comprende un generador de bits en bruto y un extractor de aleatoriedad, de acuerdo con una realización;

La Figura 2 es una vista esquemática de un ejemplo del generador de bits en bruto de la Figura 1;

La Figura 3 es un gráfico que muestra la probabilidad de obtener muestras de bits en bruto dadas del generador de bits en bruto de la Figura 2;

La Figura 4 es una vista esquemática de un ejemplo del extractor de aleatoriedad de la Figura 1;

La Figura 5 es un gráfico que muestra una variación de muestras de bits en bruto obtenidas del generador de bits en bruto de la Figura 2;

La Figura 6 es una vista esquemática de un ejemplo del extractor de aleatoriedad de la Figura 4 mostrado que genera una alerta cuando la diferencia entre los datos de calibración anteriores y los datos de calibración posteriores está por encima de un valor de tolerancia dado;

La Figura 7 es una vista esquemática de un ejemplo del extractor de aleatoriedad de la Figura 4 mediante el uso de una muestra de bits semilla que se sustituye iterativamente con muestras de bits aleatorios recibidas del extractor de aleatoriedad;

La Figura 8 es una vista en elevación frontal de un ejemplo de un dispositivo electrónico que incorpora el generador de bits aleatorios de la Figura 1;

La Figura 9 es una vista esquemática de un ejemplo de un circuito de barrera de tunelización cuántica de la Figura 2;

La Figura 10A es una vista esquemática de otro ejemplo de un generador de bits en bruto, con dos circuitos de barrera de tunelización cuántica;

La Figura 10B es un circuito eléctrico del generador de bits en bruto de la Figura 10A; y

La Figura 10C es una vista oblicua de las barreras de tunelización cuántica del generador de bits en bruto de la Figura 10A.

Descripción detallada

La Figura 1 muestra un ejemplo de generador de bits aleatorios. Como se representa, el generador de bits aleatorios tiene un generador de bits en bruto que incorpora una barrera de tunelización cuántica y un extractor de aleatoriedad. Como se describirá en detalle a continuación con referencia a la Figura 9, el generador de bits en bruto tiene un circuito de barrera de tunelización cuántica que incorpora una barrera de tunelización cuántica que tiene un aislante intercalado entre dos conductores.

Volviendo ahora a la Figura 2, el circuito de barrera de tunelización cuántica se configura para proporcionar una señal en bruto resultante de una corriente de cargas que se tuneliza desde el primero de los dos conductores al segundo de los dos conductores y a través del aislante. Como la señal en bruto es una señal analógica, la corriente de las cargas tunelizadas tiene un nivel instantáneo que varía aleatoriamente debido a las fluctuaciones de tunelización cuántica.

Como se muestra, el generador de bits en bruto tiene un monitor, que se configura para recibir, directa o indirectamente, la señal en bruto de la barrera de tunelización cuántica. Por ejemplo, la señal en bruto puede recibirse directamente de la barrera de tunelización cuántica. Sin embargo, en algunas otras realizaciones, tal como en la realización ilustrada, la señal en bruto proporcionada por el circuito de barrera de tunelización cuántica se amplifica convenientemente mediante el uso de al menos un amplificador para proporcionar una señal en bruto amplificada de un nivel satisfactorio. En este caso, la señal en bruto se recibe indirectamente desde la barrera de tunelización cuántica a través del al menos un amplificador.

El monitor también se configura para proporcionar una o más muestras digitales de bits en bruto de la señal en bruto. En la realización ilustrada, el monitor proporciona las muestras de bits en bruto de la señal en bruto amplificada recibida desde el amplificador. Cada muestra de bits en bruto tiene un primer número de bits n, en el que el primer número de bits n es un número entero. Como se describirá a continuación, el monitor puede proporcionarse en forma de muestra. Sin embargo, el probador es opcional ya que se pueden usar otras alternativas de monitor para convertir la señal en bruto en la muestra de bits en bruto.

En algunas realizaciones, el monitor se proporciona en forma de un probador que se configura para tomar muestras del nivel instantáneo de la señal en bruto y atribuir un valor al nivel instantáneo de la corriente de cargas que se tuneliza a través de la barrera de tunelización cuántica. En algunas realizaciones, la muestra de bits en bruto puede corresponder al valor del nivel instantáneo de la corriente. Por ejemplo, en un momento de tiempo dado, el probador puede tomar muestras de la señal en bruto para tener un valor de 5 de un valor máximo de 2^4-1 = 15, y luego proporcionar la muestra de bits en bruto 0101, cuando el primer número de bits n es 4.

En algunas realizaciones, el probador puede tomar muestras del nivel instantáneo de la señal en bruto en diferentes momentos en el tiempo para proporcionar muestras de bits de origen correspondientes cada una al valor del nivel instantáneo de la corriente. Sin embargo, en estas realizaciones, puede usarse un concatenador para concatenar las muestras de bits de origen entre sí en la muestra de bits en bruto. Por ejemplo, en un primer momento en el tiempo, el probador puede tomar muestras de la señal en bruto para tener un valor de 1 de 2^2 - 1 = 3, y luego proporcionar una primera muestra de bit de origen de 01. Luego, en un segundo momento en el tiempo, el probador puede tomar muestras de la señal en bruto para tener un valor de 2 de 2^2 - 1 = 3, y luego proporcionar una segunda muestra de bits de origen de 10. En este ejemplo, el concatenador puede concatenar la primera muestra de bits de origen y la segunda muestra de bits de origen entre sí para proporcionar la muestra de bits en bruto 0110 o 1001. En tales realizaciones, el primer número de bits n corresponde a un número de bits de origen de cada una de las muestras de bit de origen multiplicado por el número de muestras de bit de origen concatenados entre sí. Como se puede entender, el concatenador puede ser opcional, ya que el monitor puede configurarse para convertir la señal en bruto directamente en la muestra de bits en bruto. Se considera que la concatenación de muestras de bits de origen entre sí puede no ser necesaria en las realizaciones donde las sucesivas muestras de bits de origen no están correlacionadas entre sí.

Como puede entenderse, la señal en bruto proporcionada por el circuito de barrera de tunelización cuántica puede considerarse cuántica y, por lo tanto, no determinista. Sin embargo, no es el caso para la señal en bruto amplificada o cualquier forma de señal en bruto procesada. De hecho, en esta realización, la amplificación realizada por el amplificador agrega una contribución externa, no cuántica y determinista a la señal. El monitor también puede agregar alguna contribución externa (por ejemplo, un probador) u otros componentes eléctricos del generador de bits en bruto. Por lo tanto, la señal en bruto tiene una contribución cuántica y una contribución externa, y también las muestras de bits en bruto. Como puede entenderse, al tener una contribución externa que es determinista, los bits aleatorios que provienen directamente de una señal en bruto pueden ser deducibles y/o controlarse por un adversario de terceros, lo que puede hacer que tales bits aleatorios sean menos confiables para algunas aplicaciones tales como aplicaciones de criptografía.

La Figura 3 muestra un ejemplo de distribución de probabilidad de las muestras de bits en bruto obtenidas del generador de bits en bruto. En este ejemplo específico, el primer número de bits n corresponde a 3 por simplicidad. Por ejemplo,

cuando el valor instantáneo de la señal en bruto varía entre 0 y 5 mA cuando el probador lo prueba, la muestra de bits en bruto generada es 100; cuando el valor instantáneo de la señal en bruto varía entre 5 y 10 mA cuando el probador lo prueba, la muestra de bits en bruto generada es 101, y etcétera. Como se muestra, la probabilidad de obtener la muestra de bits en bruto 100 es mayor que la probabilidad de obtener la muestra de bits en bruto 101, y etcétera. La distribución de probabilidad ilustrada se caracteriza por una desviación estándar σ y una varianza σ^2.
Los inventores afirman que la varianza σ^2 de las muestras de bits en bruto generadas por el generador de bits en bruto pueden darse por una relación equivalente a la siguiente relación:

$$\sigma^2 = A\left(S_J + S_{ext}\right), \qquad (1)$$

en la que A denota una ganancia efectiva del generador de bits en bruto, S_J denota un valor de contribución cuántica de las fluctuaciones de tunelización cuántica en la muestra de bits en bruto, y S_{ext} denota un valor de contribución externa de al menos la amplificación en la muestra de bits en bruto. En este ejemplo, la ganancia efectiva A del generador de bits en bruto puede incluir ganancias e impedancias de amplificadores, así como también el ancho de banda de detección. Más específicamente, la ganancia efectiva A puede darse por la relación $A = R^2G^2\Delta f$, donde R denota una resistencia de la barrera de tunelización cuántica, G denota la ganancia efectiva del amplificador y Δf denota el ancho de banda de la señal en bruto monitoreada. En algunas otras realizaciones, la ganancia efectiva G del amplificador puede deducirse de las especificaciones del amplificador utilizado. En las realizaciones alternativas, la ganancia efectiva G del amplificador puede determinarse mediante la amplificación de una señal dada que tiene una amplitud conocida, y mediante la comparación de la amplitud de la señal amplificada con la amplitud conocida de la señal dada. De cualquier otra manera, cuando el amplificador está ausente, la ganancia efectiva G del amplificador corresponde a la unidad, y la ganancia efectiva A del generador de bits en bruto se da por $A = R^2\Delta f$.

En el siguiente ejemplo, el valor de contribución cuántica S_J es una densidad espectral de la señal en bruto obtenida del circuito de barrera de tunelización cuántica, mientras que el valor de contribución externa S_{ext} es una densidad espectral de la contribución externa debido al menos a la amplificación proporcionada por el amplificador.

Sin embargo, puede apreciarse que el valor de contribución cuántica puede proporcionarse en forma de un valor de potencia resultante de la integración de la densidad espectral de la señal en bruto sobre un ancho de banda de frecuencia dado en algunas otras realizaciones. De manera similar, en estas realizaciones, el valor de contribución externa puede proporcionarse en forma de un valor de potencia resultante de la integración de la densidad espectral de la contribución externa integrada sobre un ancho de banda de frecuencia dado.

Con referencia ahora a la Figura 4, el extractor de aleatoriedad se configura para extraer la aleatoriedad de las muestras de bits en bruto en muestras de bits aleatorios que tienen un segundo número de bits m. Como se entenderá a partir de la descripción más abajo, el segundo número de bits m es más pequeño que el primer número de bits n. En consecuencia, por lo tanto, los bits se pierden en el proceso de extracción.

Tal extracción de la aleatoriedad se basa en datos de calibración que comprenden al menos el valor de contribución cuántica S_J y el valor de la contribución externa S_{ext}.

En algunas realizaciones, los datos de calibración, por ejemplo, el valor de contribución cuántica S_J y el valor de la contribución externa S_{ext}, se han determinado previamente y se almacenan en el sistema de memoria del extractor de aleatoriedad. Por ejemplo, los datos de calibración pueden haberse determinado durante la fabricación del generador de bits aleatorios y luego almacenarse en el sistema de memoria. En este caso, el generador de bits aleatorios puede producir resultados satisfactorios cuando el generador de bits aleatorios se utiliza dentro de ciertos límites, por ejemplo, algunos límites de temperatura predefinidos.

En algunas otras realizaciones, los datos de calibración, por ejemplo, el valor de contribución cuántica S_J y el valor de la contribución externa S_{ext}, se puede determinar sobre la marcha a partir de datos de varianza $\sigma^2(V)$ que indican cómo la varianza σ^2 de la(s) muestra(s) de bits en bruto obtenida de la barrera de tunelización cuántica varía en función de la tensión V al que se opera la barrera de tunelización cuántica.

Un ejemplo de datos de varianza $\sigma^2(V)$ se muestra en la Figura 5 por conveniencia.

Nuevamente, los datos de varianza $\sigma^2(V)$ de la barrera de tunelización cuántica puede determinarse durante la fabricación del generador de bits aleatorios y luego almacenarse en el sistema de memoria, para obtener resultados satisfactorios siempre que el generador de bits aleatorios se utilice dentro de ciertos límites.

Sin embargo, los datos de la varianza $\sigma^2(V)$ no necesitan determinarse previamente. De hecho, en algunas realizaciones, los datos de varianza $\sigma^2(V)$ se pueden determinar al variar la tensión a la que se opera la barrera de tunelización cuántica mientras se mide la varianza de la muestra o muestras de bits en bruto.

En cualquier caso, el valor de contribución cuántica S_J puede darse por una ecuación equivalente a la siguiente ecuación:

$$S_j = \frac{2eV}{R} \cdot \cot\left(\frac{eV}{2k_BT}\right), \qquad (2a)$$

en la que e denota la carga de electrones, V denota una tensión a la que se opera la barrera de tunelización cuántica, k_B denota la constante de Boltzmann, y T denota una temperatura a la cual se opera la barrera de tunelización cuántica, como se presenta por Spietz, Lafe y otros. "Primary electronic thermometry using the shot noise of a tunnel junction." Science 300.5627 (2003).

La ecuación (2a) puede ser válida para frecuencias f de manera que $hf \ll k_BT$ en el que h denota la constante de Planck. En la práctica a temperatura ambiente, la ecuación (2a) puede ser válida para frecuencias $f \ll 6$ THz. Trabajar a frecuencias de 10 GHz puede agregar una corrección exponencialmente pequeña.

Como se puede entender, la ecuación (1) no es una ecuación lineal. En consecuencia, uno podría medir la varianza $\sigma^2(V)$ al menos tres valores de tensión para deducir el valor de contribución externa $S_{ext,}$ la temperatura T y la ganancia efectiva A del generador de bits en bruto. Por ejemplo, uno puede usar el procedimiento de mínimos cuadrados ordinarios para determinar una ecuación para la varianza $\sigma^2(V)$ de las muestras de bits en bruto, a partir de las cuales el valor de contribución externa $S_{ext,}$ la temperatura T y la ganancia efectiva A se pueden deducir. En la práctica, uno puede seleccionar dos valores de tensión mayores que k_BT/e en cuyo caso la varianza $\sigma^2(V)$ de las muestras de bits en bruto pueden ser lineales en función de la tensión V: la pendiente de la relación lineal puede dar la ganancia efectiva A mientras que la intersección en y produce la contribución externa $S_{ext.}$ Entonces, uno puede deducir la temperatura T a partir de la evaluación de la relación lineal a una tensión nula.

Como se muestra en la Figura 5, basado en las ecuaciones (1) y (2a) anteriores, el valor de contribución externa S_{ext} se puede determinar a partir de los datos de varianza $\sigma^2(V)$ de la(s) muestra(s) de bits en bruto en algunas otras realizaciones. Más específicamente, en algunas realizaciones, la varianza $\sigma^2(0)$ de la(s) muestra(s) de bits en bruto cuando la tensión V es nula puede darse por una relación equivalente a la siguiente relación:

$$\sigma^2(0) = A\left(S_{ext} + \frac{4k_BT}{R}\right). \qquad (3)$$

Adicional o alternativamente, la varianza $\sigma^2(V_i)$ de las muestras de bits en bruto cuando la tensión V_i es mayor que un umbral de tensión dado $V_{umbral} < V_i$ puede darse por una relación equivalente a la siguiente relación:

$$\sigma^2(V_i) = A\left(S_{ext} + \frac{2eV_i}{R}\right). \qquad (4)$$

En este ejemplo, dados los datos de varianza $\sigma^2(V)$ de las muestras de bits en bruto y las ecuaciones (2a), (3) y (4), los datos de calibración, por ejemplo, el valor de contribución cuántica S_J y el valor de la contribución externa $S_{ext,}$ pueden determinarse, ya que el valor de contribución externa S_{ext} se sabe que no varía en función de la tensión a la que se opera la barrera de tunelización cuántica. Véase Thibault, Karl y otros. "Pauli-heisenberg oscillations in electron quantum transport." Physical review letters 114.23 (2015), por ejemplo.

En consecuencia, al conocer la contribución relativa de cada uno de los valores de contribución cuántica S_J y el valor de la contribución externa S_{ext} uno con relación al otro, se puede determinar qué cantidad de muestras de bits en bruto se pueden asociar a la contribución cuántica y qué cantidad de muestras de bits en bruto se pueden asociar a la contribución externa.

En el ejemplo descrito anteriormente, la barrera de tunelización cuántica se opera en un régimen lineal, que permite que pueda utilizarse la Ley de Ohm ($V = RI$). En consecuencia, la relación V/I y la derivada dV/dI sería constante y produciría la resistencia R. Sin embargo, en algunas otras realizaciones, la barrera de tunelización cuántica puede no operarse en un régimen lineal, sino en un régimen no lineal, en cuyo caso la relación V/I y la derivada dV/dI no son constantes. En este contexto, siempre que el transporte de cargas a través de la barrera de tunelización cuántica se produzca a través de la tunelización cuántica, el valor de contribución cuántica S_j se da por:

$$S_j = 2eI \cdot \cot\left(\frac{eV}{2k_BT}\right), \qquad (2b)$$

en la que I denota la corriente a través de la barrera de tunelización cuántica. En este contexto, la varianza $\sigma^2(0)$ de las muestras de bits en bruto cuando la tensión V es nula se relaciona $R = \frac{V}{I} = dV/dI$ con para I cerca de cero, y la varianza $\sigma^2(V_I)$ de las muestras de bits en bruto cuando la tensión V_i es mayor que un umbral de tensión dado $V_{umbral} < V_i$ puede darse por una relación equivalente a la siguiente relación: $\sigma^2(V_i) = 2eI$. Como se puede entender, las no linealidades de la barrera de tunelización cuántica pueden provenir de la altura de la barrera potencial de la barrera de tunelización cuántica que no es infinita y/o la densidad de estados en los contactos eléctricos que dependen de la energía, por ejemplo.

Un procedimiento para determinar cuántos bits de las muestras de bits en bruto se deben a la contribución cuántica consiste en determinar una entropía mínima $H_{\infty,Q}$ de la contribución cuántica. De acuerdo con una definición, la entropía mínima $H_{\infty,Q}$ puede darse por una relación equivalente a la siguiente relación:

$$H_{\infty,Q} = -\log_2 p_{\text{máx, }Q}, \quad (5)$$

en la que $p_{máx,\ Q}$ denota la mayor de las probabilidades de obtener uno u otro de los valores del nivel instantáneo de la señal en bruto que solo tiene la contribución cuántica. Sin embargo, se determina que la varianza de la muestra de bits en bruto

σ^2 se refiere a una varianza de la σ_Q^2 contribución cuántica por una relación equivalente a la siguiente relación:

$$\sigma_Q^2 = \frac{\gamma}{1+\gamma}\sigma^2, \quad (6)$$

en la que γ denota una relación entre el valor de contribución cuántica y el valor de contribución externa. Por ejemplo, la relación γ puede darse por:

$$\gamma = \frac{S_J}{S_{ext}}. \quad (7)$$

Sabiendo que una entropía mínima H_∞ de las muestras de bits en bruto pueden darse por una relación equivalente a la siguiente relación:

$$H_\infty = -\log_2 p_{\text{máx}}, \quad (8)$$

en la que $p_{máx}$ es la mayor de las probabilidades de obtener una de las otras muestras de bits en bruto. Por ejemplo, con referencia a la Figura 3, $p_{máx}$ sería la probabilidad de obtener un número de bits en bruto de 011 (o 100). En la práctica, la señal en bruto procesada puede ser indistinguible a partir de una curva gaussiana. En este caso, si $I_{máx}$ denota el valor máximo del monitor (por ejemplo, probador), dos enteros consecutivos corresponden a dos corrientes separadas por

$\Delta I = \frac{2 \cdot \text{máx}}{2^n - 1}$, donde n es el primer número de bits y la mayor de las probabilidades $p_{máx}$ y $p_{máx,\ Q}$ se dan por relaciones

equivalentes a las siguientes relaciones:

$$p_{\text{máx}} \cong = \frac{\Delta I}{\sigma\sqrt{2\pi}}, \quad (9)$$

$$p_{\text{máx},Q} \cong = \frac{\Delta I}{\sigma_Q\sqrt{2\pi}}, \quad (10)$$

En consecuencia, mediante el uso de las ecuaciones (5), (6), (8) y (10), uno puede obtener:

$$H_{\infty,Q} = H_\infty - \frac{1}{2}\log_2\frac{1+\gamma}{\gamma}, \quad (11)$$

Como la entropía mínima H_∞ de las muestras de bits en bruto y la relación γ se puede determinar como se describe anteriormente, la entropía mínima $H_{\infty,Q}$ de la contribución cuántica también se puede determinar. La entropía mínima $H_{\infty,Q}$ de la contribución cuántica puede usarse para determinar cuántos bits de las muestras de bits en bruto se deben a la contribución cuántica y, por lo tanto, puede usarse como una entrada al extractor de aleatoriedad.

Por ejemplo, en una realización dada, para n = 14 bits e $I_{máx} = 3\sigma$, uno puede obtener una entropía mínima H_∞ para los datos en bruto de 12,7 bits por muestra de bits en bruto. Para un amplificador con ruido de tensión de 1,4 nV por raíz Hz, el valor de contribución externa S_{ext} se puede determinar que es $2 \times 10^{-18} V^2/Hz$. Para una barrera de tunelización cuántica que tiene una resistencia R = 50 ohmios operados a una tensión V = 0,4 V, el valor de contribución cuántica S_J se puede determinar que es $2eVR = 6{,}4 \times 10^{-18} V^2/Hz$, lo que daría una relación γ de 3,2. En este caso, la entropía mínima $H_{\infty,Q}$ puede darse por 12,5 bits por muestra de bits en bruto. En este caso, puede usarse un factor de seguridad de 0,3 bits por muestra de bits en bruto, lo que daría como resultado la extracción de la aleatoriedad de las muestras de bits en bruto para mantener 12,2 bits por muestra de bits en bruto de inicialmente 14 bits. En tal realización, si el primer número de bits n de la muestra de bit en bruto es 14, el segundo número de bits m se puede poner a 12. Al hacerlo, se pueden perder 0,2 bits por muestra de bits en bruto que generalmente están asociados a una calidad de aleatoriedad satisfactoria.

Dado que el rendimiento de los generadores de bits aleatorios es importante en algunas aplicaciones, perder estos 0,2 bits por muestra de bits en bruto puede ser inconveniente. Para evitar esto, puede ser conveniente usar un

concatenador. En tales realizaciones, el monitor se configura para proporcionar muestras de bits de origen que tienen un número de bits de origen de 14, y que se determina que, en base a la entropía mínima $H_{\infty,Q}$ de las fluctuaciones de tunelización cuántica, se deben mantener 12,2 bits por muestra de bits de origen, el concatenador se puede utilizar para concatenar varias muestras de bits de origen entre sí para minimizar esa pérdida. Por ejemplo, el número de muestras de bits de origen que se concatenan entre sí puede corresponder al número que, cuando se multiplica por el número de bits por muestra de bits en bruto a mantener, produce un número entero. Por ejemplo, en este ejemplo específico, si el número de bits por muestra de bits en bruto a mantener es de 12,2 bits, multiplicar 12,2 bits por 5, 10 o cualquier múltiplo de 5 producirá un número entero. En consecuencia, puede preferirse que cualquier muestra de bits en bruto sea el resultado de la concatenación de 5, 10 o cualquier múltiplo de 5 muestras de bits de origen, para evitar la pérdida de bits asociada a una calidad de aleatoriedad satisfactoria.

La extracción de aleatoriedad se puede realizar mediante el uso de una pluralidad de algoritmos diferentes. Los ejemplos de tales algoritmos pueden incluir el procedimiento de bits menos significativo, las funciones hash no universales, el extractor de Trevisan y/o las funciones hash universales tal como la función Toeplitz-hash. En algunas realizaciones, el extractor de Trevisan y las funciones hash universales pueden preferirse ya que se consideran información demostrable teóricamente. Véase Mansour, Yishay, Noam Nisan y Prasoon Tiwari. The computational complexity of universal hashing." Theoretical Computer Science 107.1 (1993); Ma, Xiongfeng y otros. "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction." Physical Review A 87.6 (2013; y Xu, Feihu y otros "Ultrafast quantum random number generation based on quantum phase fluctuations." Optics express 20.11 (2012). Se conoce en el documento de la técnica US2015071432 "PHYSICALLY UNCLONABLE FUNCTION BASED ON RESISTIVITY OF MAGNETORESISTIVE RANDOM-ACCESS MEMORY MAGNETIC TUNNEL JUNCTIONS" Una característica se refiere al menos a una función físicamente inconclusa basada en una matriz de celdas de memoria de acceso aleatorio magnetorresistivo (MRAM). Un desafío al conjunto de celdas MRAM puede identificar algunas de las celdas que se utilizarán para la función físicamente inclonable. Cada celda MRAM puede incluir una pluralidad de uniones de túnel magnético (MTJ), donde los MTJ pueden exhibir resistencias distintas debido a variaciones de producción o fabricación. Se puede obtener una respuesta al desafío para cada celda mediante el uso de la(s) resistencia(s) de una o ambas MTJ para que una celda obtenga un valor que sirva como respuesta para esa celda. Las respuestas para una pluralidad de celdas se pueden mapear al menos parcialmente para proporcionar un identificador único para la matriz. Las respuestas generadas a partir de la matriz de celdas pueden servir como una función físicamente inclonable que se puede utilizar para identificar únicamente un dispositivo electrónico. Los documentos XP011594687 "Straintronics-Based True Random Number Generator for High-Speed and Energy-Limited Applications" XP011594713 "Spin-Transfer Torque Devices for Logic and Memory: Prospects and Perspectives" y el documento WO2009064375 "SYSTEMS AND METHODS EMPLOYING UNIQUE DEVICE FOR GENERATING RANDOM SIGNALS AND METERING AND ADDRESSING, E.G., UNUSUAL DEVIATIONS IN SAID RANDOM SIGNALS", se utiliza un dispositivo de hardware para producir una señal de ruido analógica, para convertir la señal de ruido analógica en una secuencia aleatoria verdadera de señales, y para monitorear la verdadera secuencia aleatoria de señales en busca de anomalías. Las anomalías se evalúan en relación con uno o más eventos u ocurrencias basadas en el tiempo.

Un ejemplo de un extractor de aleatoriedad implica el uso de un procedimiento Toeplitz-hash. En esta realización, se construye una matriz aleatoria de Toeplitz *T* de m × *n. Cada muestra de bits en bruto de n bits se multiplica por la matriz aleatoria T* para dar muestras de bits aleatorios de *m* bits En este caso, *m* está dada por la entropía mínima $H_{\infty,Q}$ de la contribución cuántica menos cualquier factor de seguridad eventual y, por supuesto, el segundo número de bits *m* es menor que la entropía mínima H_{∞} de las muestras de bits en bruto de *n* bits En este proceso de extracción, *n* - *m* bits se descartan.

Por ejemplo, consideremos que 100 muestras de bits de origen de 14 bits se concatenan entre sí para formar un número de bits en bruto que tiene un primer número de bits correspondiente a 1.400. La entropía mínima H_{∞} de las muestras de bits de origen pueden ser 12,7 bits por muestra de bits de origen. La entropía mínima $H_{\infty,Q}$ de la señal cuántica puede ser de 12,5 bits por muestra de bits en bruto. Tomando un factor de seguridad de 0,3 bit por muestra de bit en bruto, se pueden mantener 12,2 bits de los 14 bits iniciales. Así, en este ejemplo, el segundo número de bits m corresponde a 1.200. Como se puede observar, el número de muestras de bits de origen, es decir, 100, que se concatenan entre sí para formar el número de bits en bruto, cuando se multiplica por el número de bits a mantener, es decir, 12,2 en este ejemplo, produce un número entero y, por lo tanto, evita la pérdida de bits asociados a una calidad satisfactoria de aleatoriedad El primer número de bits n y el factor de seguridad se pueden elegir en dependencia de la velocidad de bits por segundo necesaria y del nivel de seguridad requerido. La matriz aleatoria *T* puede generarse mediante el uso de una semilla de bits aleatorios *n* + *m* - 1 de bits aleatorios, que pueden tomarse de la muestra de bits en bruto manteniendo, por ejemplo, el bit menos significativo de cada muestra de bits en bruto durante un corto período de tiempo. Se puede reiniciar tantas veces como se desee, un ejemplo del cual se describe a continuación con referencia a la Figura 7.

Se contempla que una barrera de tunelización cuántica típica tenga un ancho de banda de aproximadamente 600 MHz. Para evitar una correlación indeseable entre sucesivas muestras de bits en bruto, el muestreo generalmente se puede realizar a una velocidad de muestreo de 1.200 MS/s, si se utiliza un filtro antisolapamiento satisfactorio. Por ejemplo, si la velocidad de muestreo es de 800 MS/s y un primer número de bits de 14 bits, esto puede generar una velocidad de generación de muestras de bits en bruto de 11,2 Gb/s, por lo que una velocidad de generación de muestras de bits

aleatorios es de 9,6 Gb/s. En un prototipo, se usó satisfactoriamente una velocidad de muestreo de 125 MS/s, que produjo una velocidad de generación de muestras de bits en bruto de 1,75 Gb/s. Una característica limitante en tal realización es generalmente la velocidad a la que las muestras de bits aleatorios pueden transferirse al dispositivo electrónico.

Se contempla que un amplificador no solo agrega fluctuaciones de tensión $e(t)$ a la tensión V_{ent} medidas, también puede agregar una corriente fluctuante $i(t)$ en lo que esté conectado a su entrada, de manera que la tensión medida V_{sal} a su salida, puede darse por:

$$V_{\text{sal}} = G(V_{\text{ent}} + e + Ri),$$

en la que G denota la ganancia efectiva del amplificador y R denota la resistencia diferencial $R = dV/dI$ de la barrera de tunelización cuántica. Como consecuencia, el amplificador puede contribuir al ruido de tensión medido por $< e^2 > + R < ei > + R^2 < I^2 >$. El primer término $< e^2 >$ representa el ruido de tensión del amplificador, el tercer término $R^2 < I^2 >$ representa el ruido actual del amplificador en la resistencia de la unión, y el segundo término $R < ei >$ implica correlaciones entre los ruidos de corriente y tensión (y usualmente es insignificante). Esta cantidad depende de la corriente de polarización en la unión si R lo hace. Esto se puede tener en cuenta al ajustar el ruido total frente a la tensión/corriente de polarización. En consecuencia, usar un amplificador con bajo ruido de corriente y/o una unión con baja resistencia suficiente para que el tercer término $R^2 < I^2 >$ sea insignificante en comparación con el primer término $< e^2 >$ puede reducir los efectos no deseados generalmente asociados al ruido actual del amplificador.

La Figura 6 es una vista esquemática del extractor de aleatoriedad. En esta realización, el extractor de aleatoriedad recibe datos de calibración anteriores y datos de calibración posteriores, compara los datos de calibración anteriores y los datos de calibración posteriores entre sí, y luego genera una alerta cuando los datos de calibración anteriores difieren de los datos de calibración posteriores en más de un valor de tolerancia. Más específicamente, los datos de calibración anteriores se han determinado en un primer momento en el tiempo t_1 mientras que los datos de calibración posteriores se han determinado en un segundo momento en el tiempo t_2, que es posterior al primer momento en el tiempo t_1. En consecuencia, la alerta generada de esta manera puede proporcionar un diagnóstico en cuanto a si las muestras de bits aleatorios generadas son confiables.

Por ejemplo, en una realización, los datos de calibración anteriores pueden haberse determinado proporcionados en forma

de datos de varianza anteriores $\sigma_{t1}^2(V)$ determinados durante la fabricación del generador de bits aleatorios y almacenados en el sistema de memoria. En esta realización, los datos de calibración posteriores pueden proporcionarse

en forma de datos de varianza posteriores $\sigma_{t2}^2(V)$ determinados en tiempo real o en tiempo real al variar la

tensión a la que se opera la barrera de tunelización cuántica mientras se mide la σ_{t2}^2. varianza

Como se puede entender, si existe una diferencia significativa entre los datos de varianza $\sigma_{t1}^2(V)$ anteriores y los

datos de varianza posteriores $\sigma_{t2}^2(V)$, puede ser indicativo de que el generador de bits aleatorios se usa fuera de

algunos límites predefinidos, tales como fuera de un intervalo de temperatura predefinido. Además, tal diferencia también puede ser indicativa de que el generador de bits aleatorios que se modifica/altera por un adversario de terceros, en cuyo caso la alerta generada de esta manera podría justificar tal alerta.

Como se puede entender, el extractor de aleatoriedad se puede configurar para que tal diagnóstico se repita o bien a una frecuencia dada o bajo demanda.

Ahora, haciendo referencia a la Figura 7, se contempla que la extracción de aleatoriedad puede involucrar una semilla de bits aleatorios. Por ejemplo, en esta realización, la extracción puede requerir una matriz aleatoria, que se genera mediante el uso de la semilla de bits aleatorios antes de extraer realmente la aleatoriedad de las muestras de bits en bruto. Por ejemplo, las muestras de bits en bruto se pueden multiplicar por la matriz aleatoria para proporcionar las muestras de bits aleatorios durante la extracción. Aunque la muestra inicial de bits semilla puede tener solo una pseudoaleatoriedad, el bit aleatorio resultante puede ser de aleatoriedad satisfactoria debido a los bits de intercambio y/o eliminación durante la extracción. Sin embargo, en esta realización, el extractor de aleatoriedad genera una muestra de bits aleatorios mediante la multiplicación de la muestra de bits en bruto a la denominada matriz pseudoaleatoria, después de lo cual la semilla de bits aleatorios utilizada para generar la matriz aleatoria puede sustituirse por la muestra de bits aleatorios generada de esta manera. En este caso, la matriz aleatoria que puede ser pseudoaleatoria en primer lugar puede convertirse rápidamente en una matriz aleatoria, lo que puede generar muestras de bits aleatorios de mayor aleatoriedad.

La Figura 8 muestra un ejemplo de un dispositivo electrónico que incorpora el generador de bits aleatorios. Más específicamente, el dispositivo electrónico tiene un alojamiento dentro del cual se monta el generador de bits aleatorios. Como se puede entender, el dispositivo electrónico puede ser un teléfono inteligente, una tableta, tarjetas electrónicas de crédito o débito, un ordenador portátil, un televisor y similares, en dependencia de la aplicación. Además, en algunas realizaciones, el dispositivo electrónico puede proporcionarse en forma de un ordenador, un servidor y similares a los que se puede acceder a través de una red tal como Internet a través de conexiones cableadas y/o inalámbricas.

Como se muestra en esta realización, el dispositivo electrónico tiene una unidad de procesamiento y un sistema de memoria que están separados y acoplados comunicativamente (por ejemplo, comunicación por cable y/o inalámbrica) al generador de bits aleatorios. En algunas otras realizaciones, la unidad de procesamiento y el sistema de memoria del dispositivo electrónico pueden actuar como extractor de aleatoriedad, en cuyo caso el generador de bits en bruto está acoplado comunicativamente a la unidad de procesamiento y/o al sistema de memoria del dispositivo electrónico.

La Figura 9 muestra un ejemplo de un generador de bits en bruto. El generador de bits en bruto generalmente comprende una placa (no se muestra) sobre la cual se monta el circuito de barrera de tunelización cuántica. Como se muestra, el circuito de barrera de tunelización cuántica del generador de bits en bruto puede incluir la barrera de tunelización cuántica, condensador(es), inductor(es) y resistencia(s). Se proporciona una fuente de polarización para variar la tensión a la que se opera la barrera de tunelización cuántica. En este ejemplo, la señal en bruto proveniente del circuito de barrera de tunelización cuántica se amplifica mediante el uso de un amplificador. Se obtiene un flujo de muestras de bits en bruto mediante el uso del monitor, proporcionado en este ejemplo en forma de un probador que prueba la señal en bruto amplificada proveniente del amplificador. Como se puede entender, el circuito de barrera de tunelización cuántica, la fuente de polarización, el amplificador y el monitor se pueden montar 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 se puede proporcionar 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 las capas conductoras que actúan como conductores. Se hace notar que las capas conductoras pueden fabricarse de un material metálico o de un material semiconductor, por ejemplo, mientras que la capa aislante puede fabricarse de cualquier material que inhiba satisfactoriamente la conducción libre de electrones (o agujeros) a través de la reflexión clásica. La capa aislante tiene dos caras opuestas exteriores cada una en contacto con una correspondiente de las dos capas conductoras y las dos capas conductoras pueden conectarse a un primer terminal y un segundo terminal de una fuente de polarización. Puede apreciarse que la fuente de polarización puede montarse sobre la placa y conectarse de manera fija a las capas conductoras de la barrera de tunelización cuántica o proporcionarse por separado a la misma.

En esta realización, la fuente de polarización puede usarse para realizar una etapa de variación de la tensión a la que se opera la barrera de tunelización cuántica. El amplificador se puede adaptar para realizar una etapa de amplificación de la señal en bruto proporcionada por el circuito de barrera de tunelización cuántica. El probador se puede adaptar para realizar una etapa de muestreo de la señal en bruto y el filtro se puede adaptar para realizar la etapa de filtrado de la señal en bruto. El filtro se puede conectar a la barrera de tunelización cuántica, que, a su vez, se conecta al amplificador y luego al probador. Cuando está operativamente conectado uno a los otros, el generador de bits en bruto puede monitorear la señal en bruto para obtener una muestra de bits en bruto. Además, la fuente de polarización puede fijar la diferencia de potencial aplicada a la barrera de tunelización cuántica. La fuente de polarización también se puede variar para permitir la medición a bordo de la varianza $\sigma(V)$ de las muestras de bits en bruto.

La Figura 10A muestra otro ejemplo de un generador de bits en bruto, de acuerdo con otra realización. Como puede apreciarse, para reducir el efecto de la contribución externa, puede usarse ventajosamente un circuito diferencial que tiene dos circuitos de barrera de tunelización cuántica en algunas realizaciones. Como se muestra, el generador de bits en bruto tiene un amplificador diferencial que se configura para amplificar la diferencia entre la primera y segunda señal en bruto proporcionadas respectivamente por el primer circuito de barrera de tunelización cuántica y el segundo circuito de barrera de tunelización cuántica. Más específicamente, en este ejemplo, la primera y segunda barreras de tunelización cuántica se polarizan por una fuente de polarización común. En esta realización, la fuente de polarización se usa para aplicar una corriente o tensión de CC al primer y segundo circuito de barrera de tunelización cuántica. Se pueden incluir filtros de paso alto en cada circuito de barrera de tunelización cuántica para eliminar componentes de baja frecuencia en la primera y segunda señales en bruto en esta realización. De hecho, los filtros de paso alto se utilizan para separar la CC de las fluctuaciones en frecuencia finita, que son la señal en bruto que se pretende aislar y detectar. Aún en este ejemplo, se proporciona un monitor analógico a digital para monitorear la salida del amplificador diferencial y proporcionar las muestras de bits en bruto. La contribución externa común puede suprimirse mediante el uso de tal configuración.

Un circuito eléctrico de tal generador de bits en bruto se muestra en la Figura 10B. Como se muestra, la fuente de polarización genera la tensión V_0 usada para polarizar el primer y segundo circuito de barrera de tunelización cuántica. Las resistencias R se usan para limitar la corriente de cargas tunelizadas generadas por la primera y segunda barrera de tunelización cuántica. Los inductores y/o condensadores separan el componente de CC de las fluctuaciones de CA

de las señales en bruto. En este ejemplo, los condensadores actúan como filtros de paso alto. En esta realización, el posible ruido en la tensión V_0 al final no tiene influencia en la medición ya que las dos ramas del generador de bits en bruto son simétricas entre sí. Por lo tanto, pueden cancelarse a sí mismas.

La Figura 10C muestra una imagen de un par de barreras de tunelización cuántica del generador de bits en bruto de la Figura 10A. Como se muestra, el par de barreras de tunelización cuántica se puede fabricar mediante el uso de un contacto común mediante el uso de técnicas de fotolitografía. En el ejemplo ilustrado, una primera capa de aluminio (de aproximadamente 200 nm de grosor) se deposita sobre un sustrato para hacer el GND de contacto común que se conecta a la tierra del circuito. La primera capa se oxida mediante el uso de oxígeno puro para formar una barrera de tunelización cuántica de aproximadamente 1 nm de grosor. Se deposita una segunda capa de aluminio (aproximadamente 300 nm de grosor) para hacer el contacto C1 y el contacto C2. Cada uno de los contactos 1 y 2 se superpone a la primera capa, y la superposición define las barreras de tunelización cuántica J1 y J2.

Como se puede entender, los ejemplos descritos anteriormente e ilustrados están destinados a ser solo ejemplares. En algunas realizaciones, el monitor puede configurarse para identificar cruzamientos del nivel instantáneo de la corriente a través de un valor dado a medida que varía el nivel instantáneo de la corriente y para determinar un período de tiempo transcurrido entre dos cruzamientos sucesivos. En estas realizaciones, se atribuye un valor al período de tiempo transcurrido y forma la muestra de bits en bruto. Por ejemplo, el monitor puede identificar que el nivel instantáneo de la corriente cruza un valor cero en un primer momento en el tiempo y luego cruza el valor cero en un segundo momento en el tiempo. En consecuencia, el valor atribuido a la muestra de bits en bruto será la diferencia entre el primer momento en el tiempo y el segundo momento en el tiempo, o viceversa. De manera similar que cuando se usa un probador, se pueden obtener muestras de bits de origen a partir de la identificación de los pasos del valor instantáneo en el valor dado y la determinación de los períodos de tiempo transcurridos entre dos pasos sucesivos del nivel instantáneo de la corriente en el valor dado. En estas realizaciones, también puede usarse un concatenador para concatenar las muestras de bits de origen entre sí para proporcionar la muestra de bits en bruto. El alcance se indica por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento para generar una muestra de bits aleatorios mediante el uso de una barrera de tunelización cuántica que comprende un aislante intercalado entre dos conductores, el procedimiento comprende:
   generar una corriente de cargas que tuneliza desde un primero de dos conductores a un segundo de dos conductores y a través del aislante, la corriente de las cargas tunelizadas que tiene un nivel instantáneo que varía aleatoriamente debido a las fluctuaciones de tunelización cuántica y que forma una señal en bruto; dicho procedimiento que se **caracteriza porque** comprende además a partir de dicha señal en bruto, obtener una muestra de bits en bruto que tiene un primer número de bits n, el primer número de bits n que es un número entero, en el que la muestra de bits en bruto tiene una contribución cuántica debido a dichas fluctuaciones de tunelización cuántica y una contribución de ruido externo agregado a la contribución cuántica, siendo la contribución del ruido externo externa al aislante intercalado entre dos conductores;
   extraer la aleatoriedad de la muestra de bits en bruto en la muestra de bits aleatorios, teniendo la muestra de bits aleatorios un segundo número de bits m que es más pequeño que el primer número de bits n, dicha extracción se basa en los datos de calibración que comprenden al menos
      un valor de contribución cuántica de dicha contribución cuántica de dicha muestra de bits en bruto; y
      un valor de contribución externa de dicha contribución de ruido externo de dicha muestra de bits en bruto.

2. El procedimiento de la reivindicación 1, en el que dicho segundo número de bits m se basa en un número de bits a mantener por muestra de bit en bruto, el segundo número de bits m que se determina en base a una entropía mínima de dichas fluctuaciones de tunelización cuántica, dependiendo dicha entropía mínima de dicha fluctuaciones cuánticas de dicho valor de contribución cuántica y dicho valor de contribución externa.

3. El procedimiento de la reivindicación 1, en el que dicha extracción comprende determinar dichos datos de calibración a partir de los datos de varianza indicativos de una varianza de muestras de bits en bruto obtenidas de dicha barrera de tunelización cuántica como función de una tensión a la cual se opera la barrera de tunelización cuántica.

4. El procedimiento de la reivindicación 3 en el que dichos datos de varianza se dan por una relación equivalente a la siguiente relación:

$$\sigma^2 = A\left(S_J + S_{ext}\right),$$

   en la que σ^2 denota dichos datos de varianza, A denota una ganancia efectiva de dicha obtención, S_J denota dicho valor de contribución cuántica de las fluctuaciones de tunelización cuántica en la muestra de bits en bruto, y S_{ext} denota un valor de contribución externa en la muestra de bits en bruto.

5. El procedimiento de la reivindicación 4 en el que dicho valor de contribución cuántica S_J se da por una relación equivalente a la siguiente relación:

$$S_j = \frac{2eV}{R} \cdot \cot\left(\frac{eV}{2k_BT}\right),$$

   en la que e denota la carga de electrones, R denota una resistencia de la barrera de tunelización cuántica, V denota una tensión a la que se opera la barrera de tunelización cuántica, k_B denota la constante de Boltzmann, y T denota una temperatura a la cual se opera la barrera de tunelización cuántica.

6. El procedimiento de la reivindicación 4 en el que dicho valor de contribución externa S_{ext} se determina al menos a partir de uno de un valor de dichos datos de varianza σ^2 a una tensión nula dada por una relación equivalente a la siguiente relación:

$$\sigma^2(0) = A\left(S_{ext} + \frac{4k_BT}{R}\right),$$

   y un valor de dichos datos de varianza σ^2 a una tensión V_i que es mayor que un umbral de tensión dado V_{umbral} puede darse por una relación equivalente a la siguiente relación:

$$\sigma^2(V_i) = A\left(S_{ext} + \frac{2eV_i}{R}\right);$$

   en la que e denota la carga de electrones, R denota una resistencia de la barrera de tunelización cuántica, V_i denota una tensión a la que se opera la barrera de tunelización cuántica, k_B denota la constante de Boltzmann, y T denota una temperatura a la cual se opera la barrera de tunelización cuántica.

7. El procedimiento de la reivindicación 3, que comprende además determinar dichos datos de varianza al variar la tensión a la que se opera la barrera de tunelización cuántica y medir una variación de la muestra de bits en bruto a medida que se hace variar dicha tensión.

8. El procedimiento de la reivindicación 1, en el que dicha extracción comprende:
comparar datos de calibración anteriores indicativos de los datos de calibración en un momento anterior en el tiempo con datos de calibración posteriores indicativos de la calibración en un momento posterior en el tiempo, y
generar una alerta cuando los datos de calibración anteriores difieren de los datos de calibración posteriores en más de un valor de tolerancia.

9. El procedimiento de la reivindicación 8, en el que dicha comparación comprende
determinar los datos de calibración actuales a partir de los datos de varianza actuales obtenidos al variar una tensión al cual se opera la barrera de tunelización cuántica mientras se mide una varianza de la muestra de bits en bruto, dichos datos de calibración actuales corresponden a dichos datos de calibración posteriores.

10. El procedimiento de la reivindicación 1, en el que dicha obtención incluye obtener una pluralidad de muestras de bits de origen y concatenar la pluralidad de muestras de bits de origen en la muestra de bits en bruto.

11. El procedimiento de la reivindicación 10, que comprende además determinar un número de bits a mantener por muestra de bits de origen en base a una entropía mínima de dichas fluctuaciones de tunelización cuántica, la muestra de bits en bruto que incluye un número dado de muestras de bits de origen concatenados, dicho número dado que se determina de manera que, cuando se multiplica por dicho número de bits a mantener, produce un número entero.

12. El procedimiento de la reivindicación 1 en el que dicha extracción incluye multiplicar la muestra de bits en bruto a una matriz aleatoria generada mediante el uso de una muestra de bits semilla inicial para obtener dicha muestra de bits aleatorios.

13. El procedimiento de la reivindicación 12, en el que dicha muestra de bits en bruto es una primera muestra de bits en bruto y dicha muestra de bits aleatorios es una primera muestra de bits aleatorios, el procedimiento comprende además repetir dicha obtención para obtener una segunda muestra de bits en bruto, generar otra matriz aleatoria mediante el uso de al menos parte de dicha primera muestra de bits aleatorios como la muestra de bits semilla inicial, y repetir dicha extracción en la segunda muestra de bits en bruto mediante el uso de dicha otra matriz aleatoria.

14. El procedimiento de la reivindicación 1, que comprende además repetir dicha obtención para obtener una pluralidad de muestras de bits en bruto sucesivas y repetir dicha extracción en cada una de dichas muestras de bits en bruto sucesivas lo que produce de esta manera una corriente de bits aleatorios.

15. El procedimiento de la reivindicación 1, en el que dicha obtención incluye el muestreo de la señal en bruto, que incluye atribuir un valor al nivel instantáneo de la corriente, dicha obtención incluye obtener una muestra de bits de origen de dicha atribución, la muestra de bits de origen corresponde al valor del nivel instantáneo de la corriente, que comprende además repetir dicho muestreo para obtener una pluralidad de muestras de bits de origen, y concatenar la pluralidad de muestras de bits de origen en la muestra de bits en bruto.

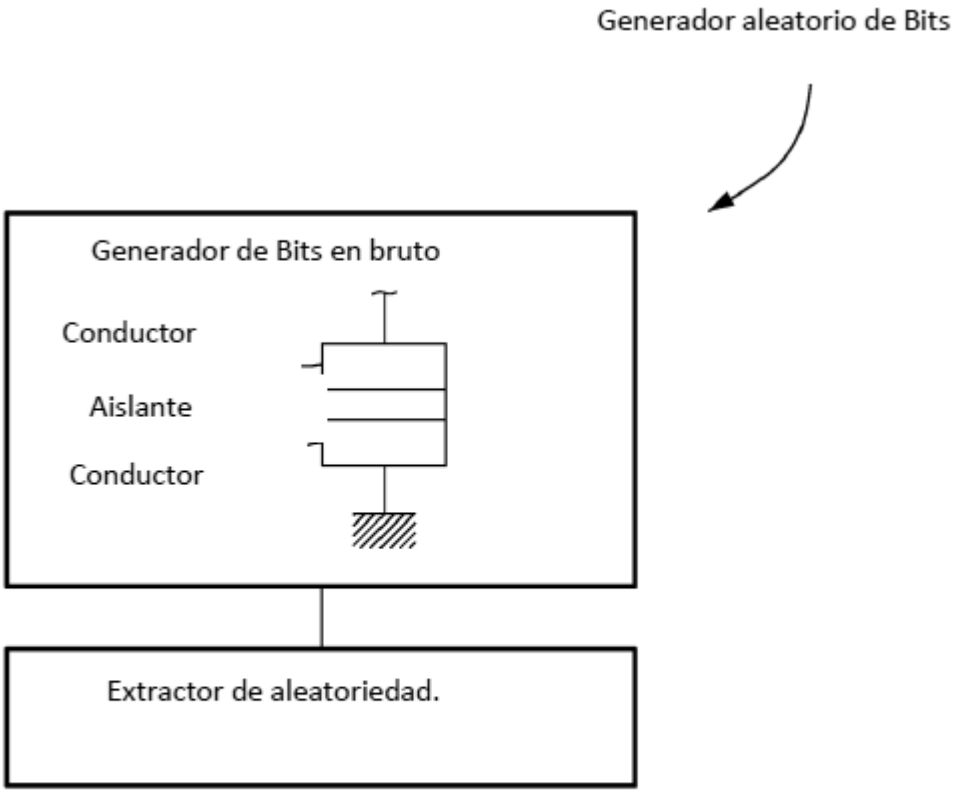
Generador aleatorio de Bits
Generador de Bits en bruto
Conductor
Aislante
Conductor
Extractor de aleatoriedad.

FIGURA 1

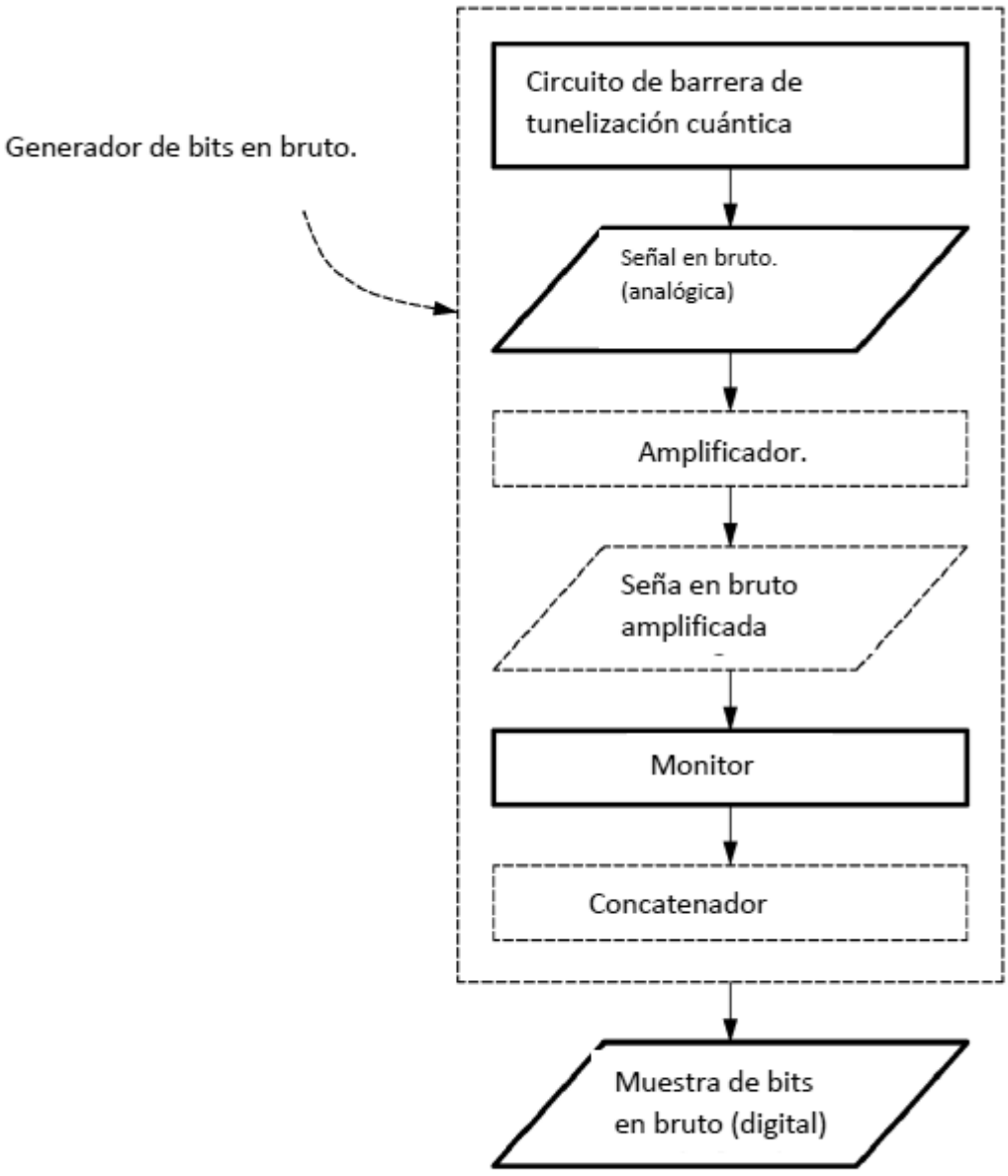
Generador de bits en bruto.
Circuito de barrera de tunelización cuántica
Señal en bruto. (analógica)
Amplificador.
Seña en bruto amplificada
Monitor
Concatenador
Muestra de bits en bruto (digital)

FIGURA 2

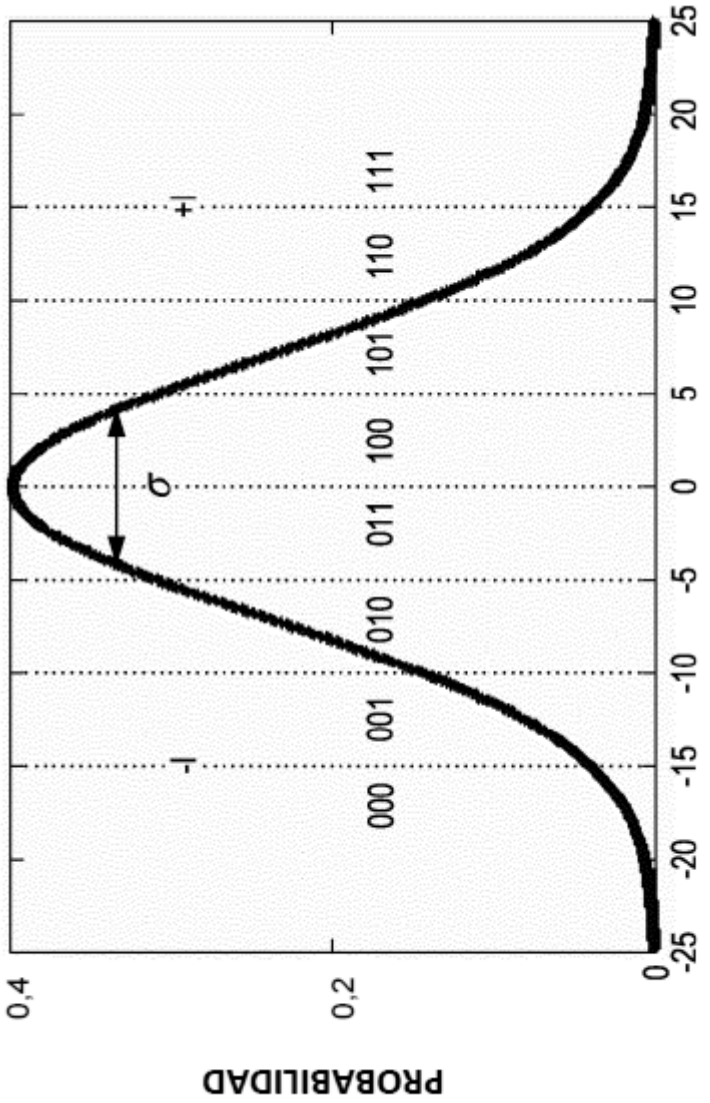
PROBABILIDAD
0,4
0,2
0
-25
-20
-15
-10
-5
0
5
10
15
20
25
CORRIENTE I DE LAS CARGAS TUNELIZADAS [mA]
-I
+I
σ
000
001
010
011
100
101
110
111

FIGURA 3

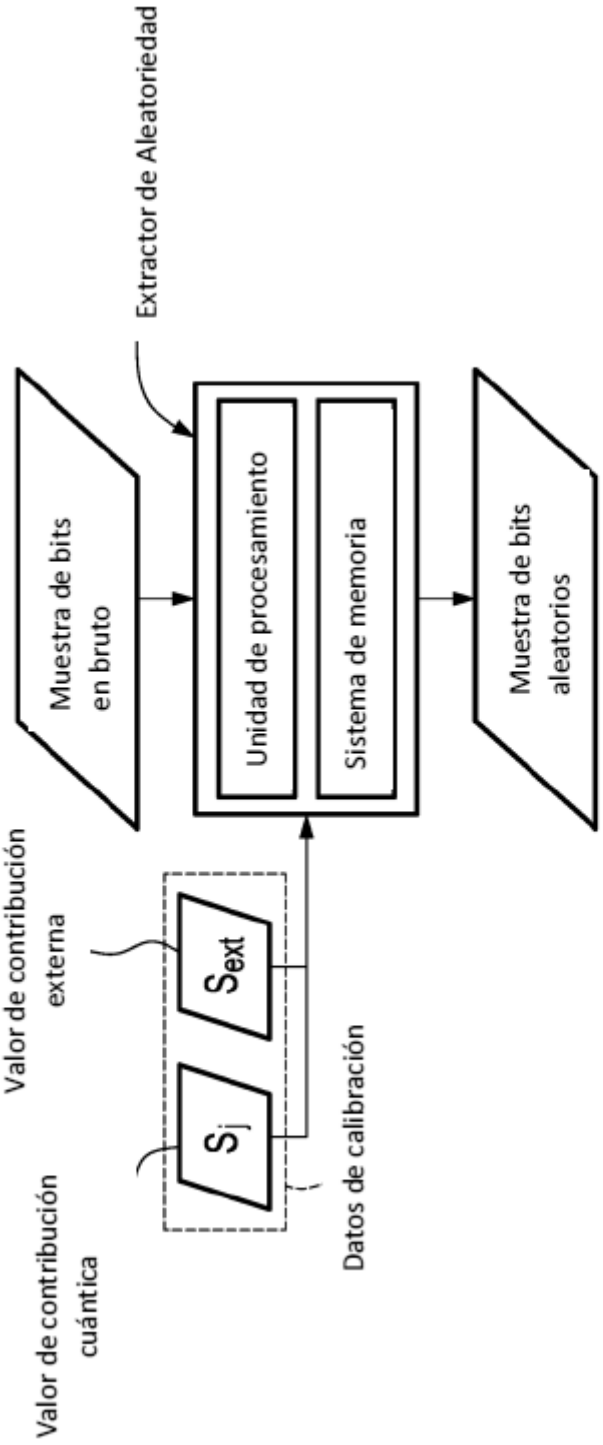
Extractor de Aleatoriedad
Muestra de bits en bruto
Unidad de procesamiento
Sistema de memoria
Muestra de bits aleatorios
Valor de contribución externa
Valor de contribución cuántica
Sext
Sj
Datos de calibración

FIGURA 4

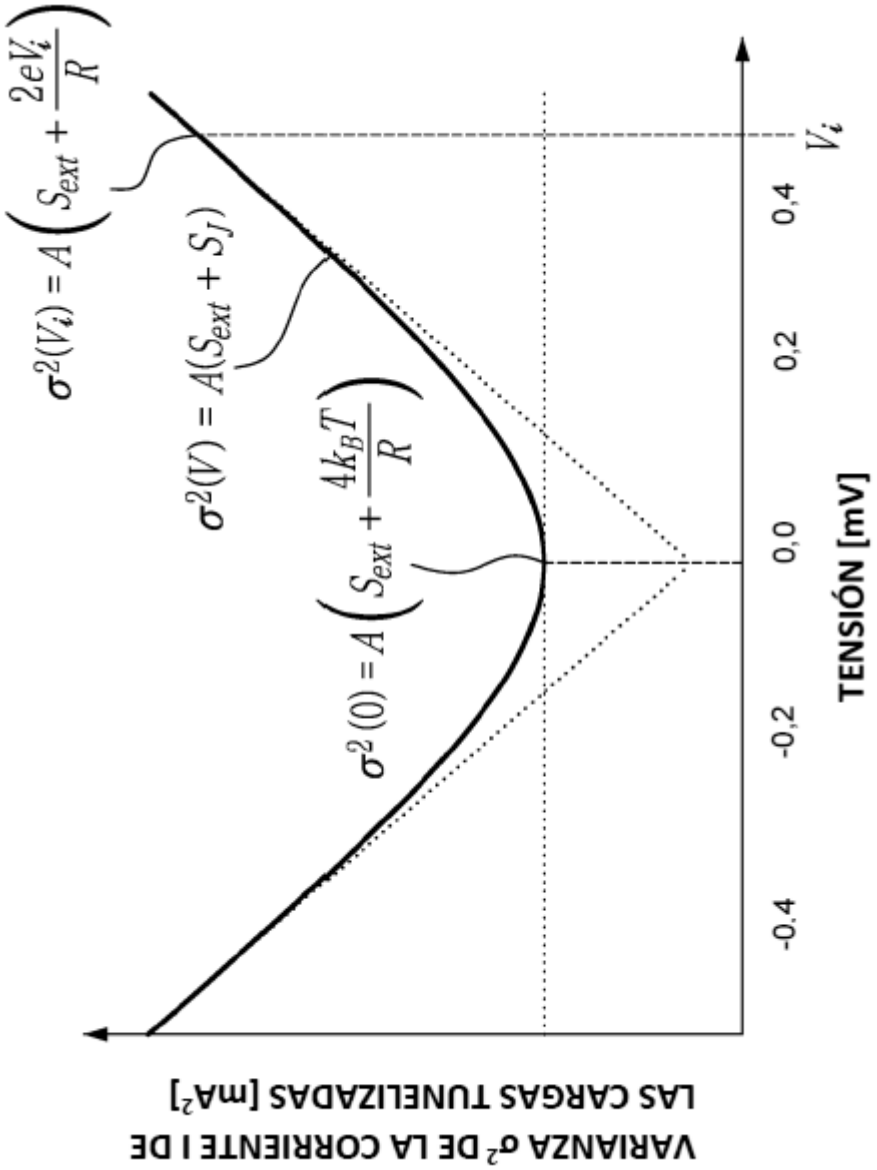
$\sigma^2(V_i) = A\left(S_{ext} + \frac{2eV_i}{R}\right)$
$\sigma^2(V) = A(S_{ext} + S_J)$
$\sigma^2(0) = A\left(S_{ext} + \frac{4k_BT}{R}\right)$
V_i
0,4
0,2
0,0
-0,2
-0.4
TENSIÓN [mV]
VARIANZA σ^2 DE LA CORRIENTE I DE LAS CARGAS TUNELIZADAS [mA^2]

FIGURA 5

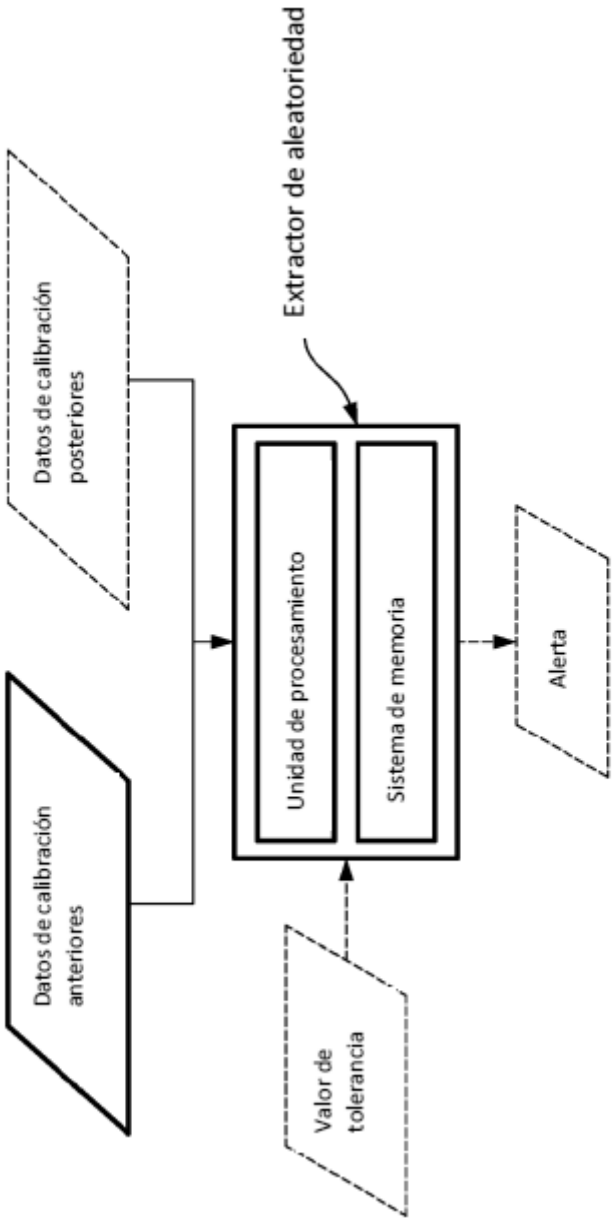
Extractor de aleatoriedad
Datos de calibración posteriores
Datos de calibración anteriores
Unidad de procesamiento
Sistema de memoria
Alerta
Valor de tolerancia

FIGURA 6

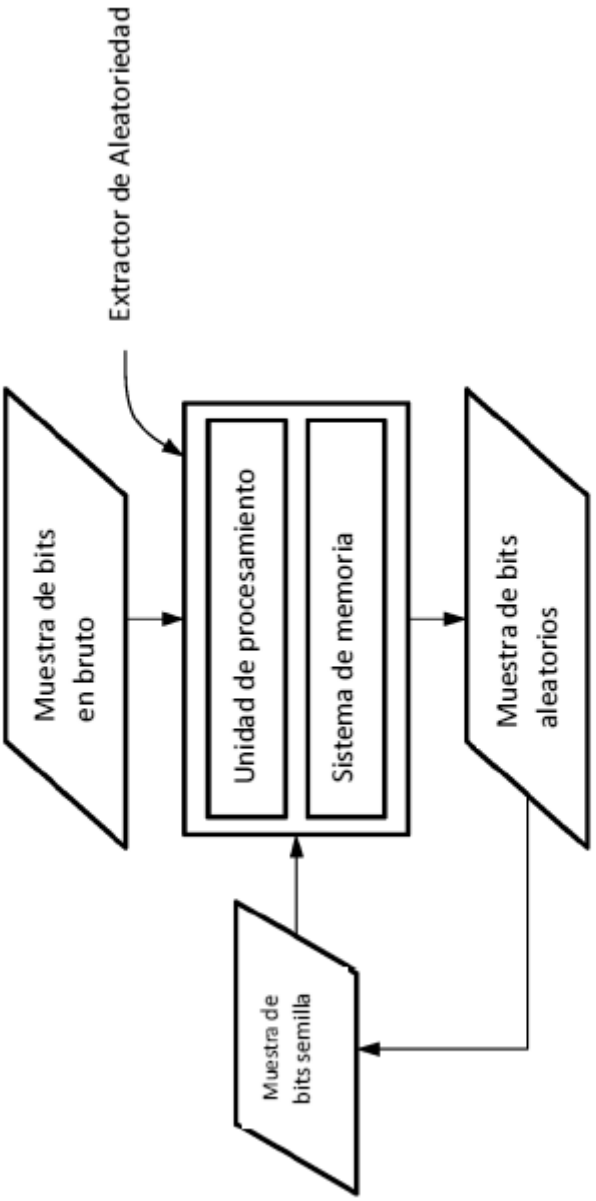
Extractor de Aleatoriedad
Muestra de bits en bruto
Unidad de procesamiento
Sistema de memoria
Muestra de bits aleatorios
Muestra de bits semilla

FIGURA 7

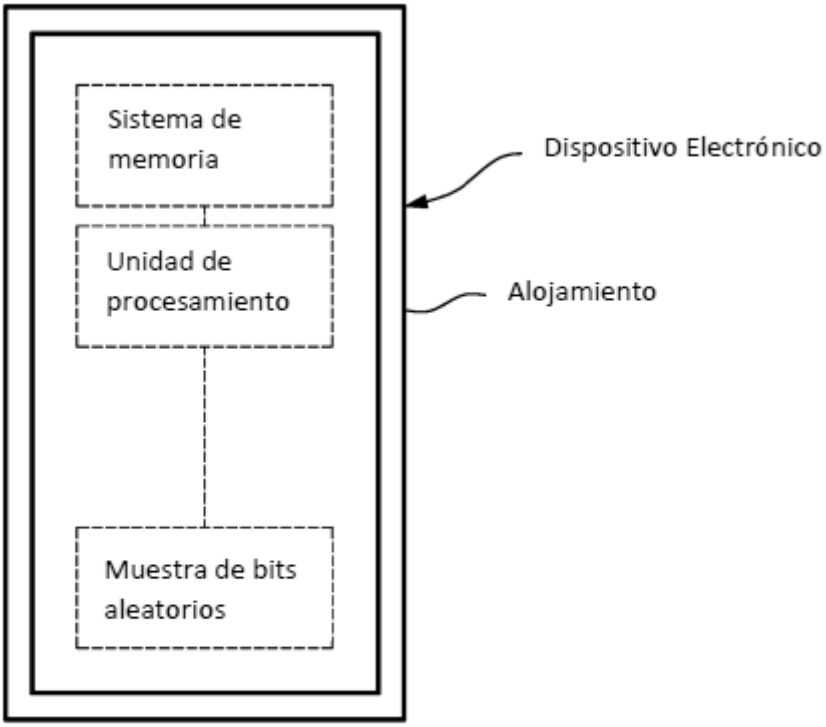
Sistema de memoria
Unidad de procesamiento
Muestra de bits aleatorios
Dispositivo Electrónico
Alojamiento

FIGURA 8

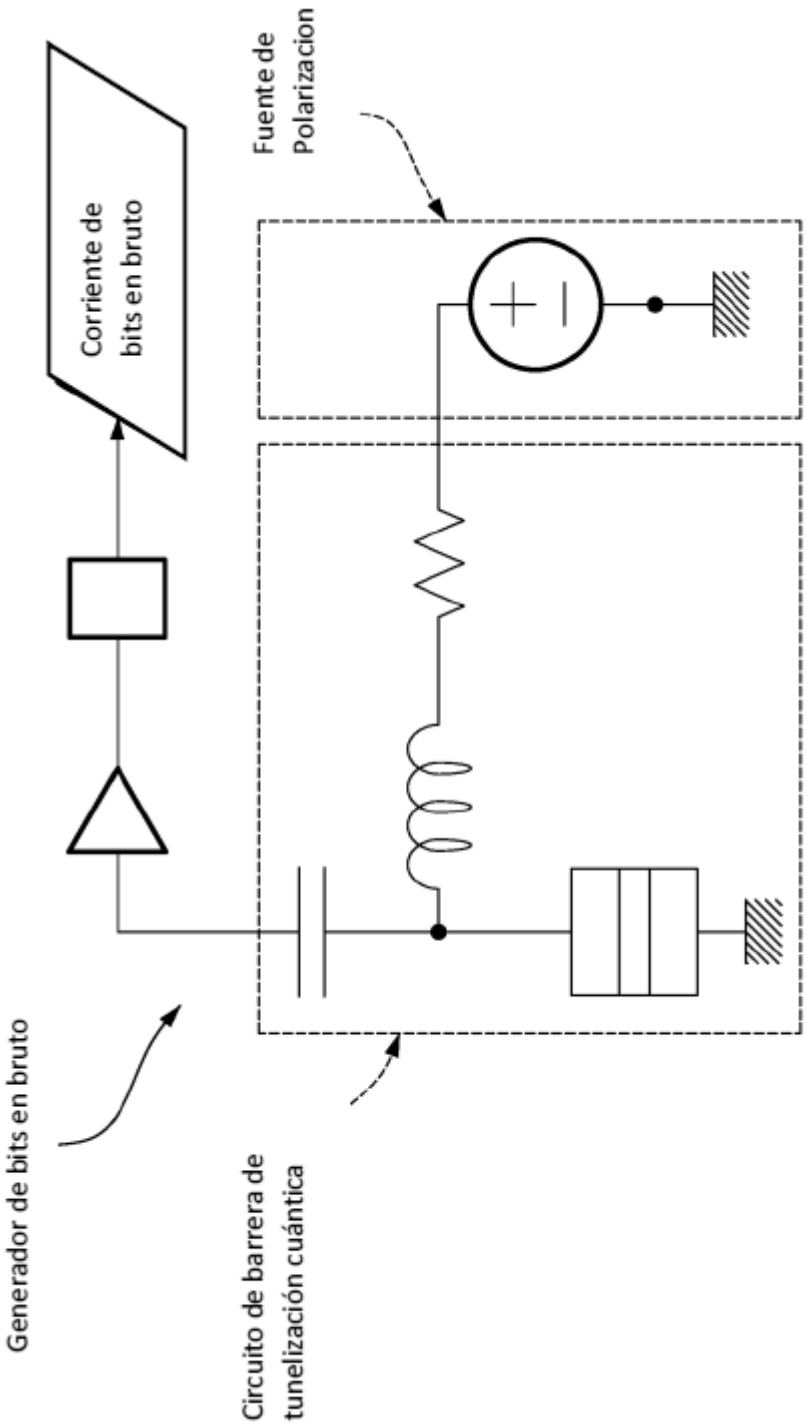
Fuente de Polarizacion
Corriente de bits en bruto
Generador de bits en bruto
Circuito de barrera de tunelización cuántica

FIGURA 9

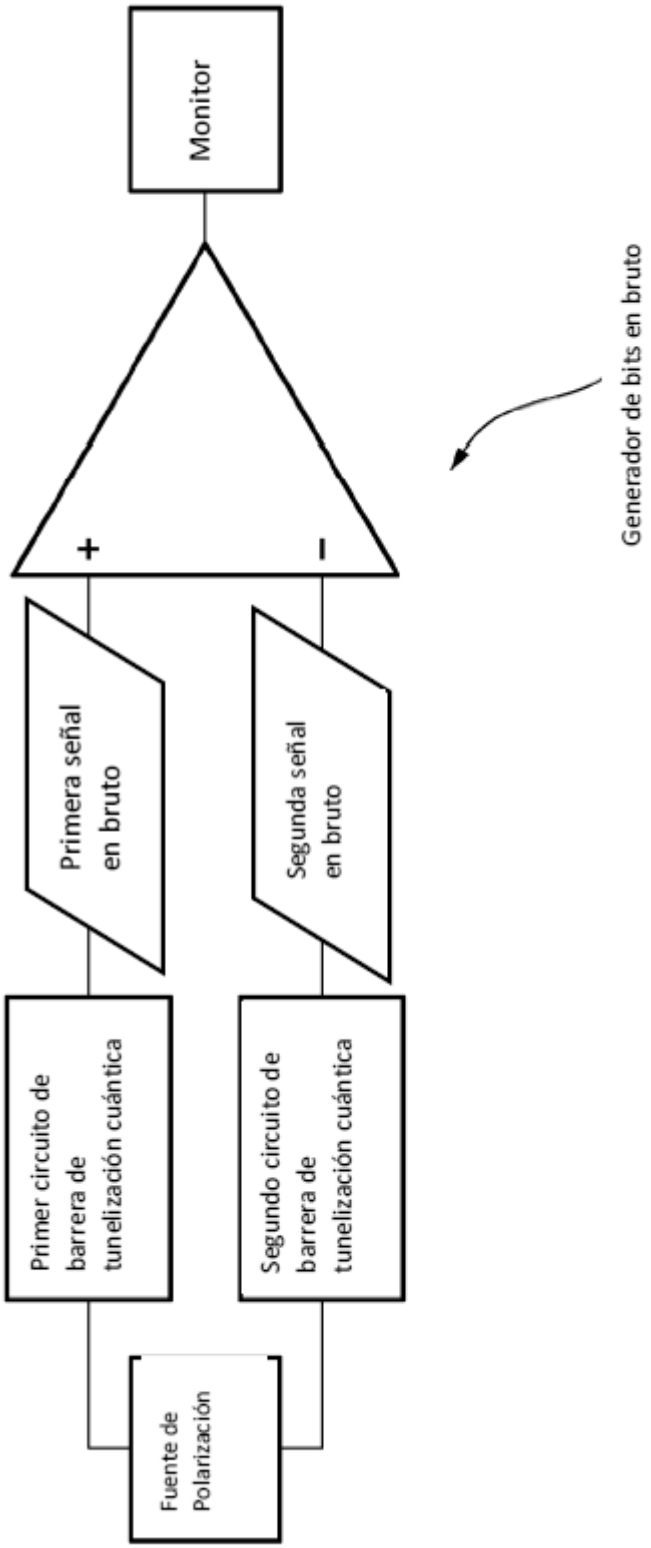
Monitor
Generador de bits en bruto
+
-
Primera señal en bruto
Segunda señal en bruto
Primer circuito de barrera de tunelización cuántica
Segundo circuito de barrera de tunelización cuántica
Fuente de Polarización

FIGURA 10A

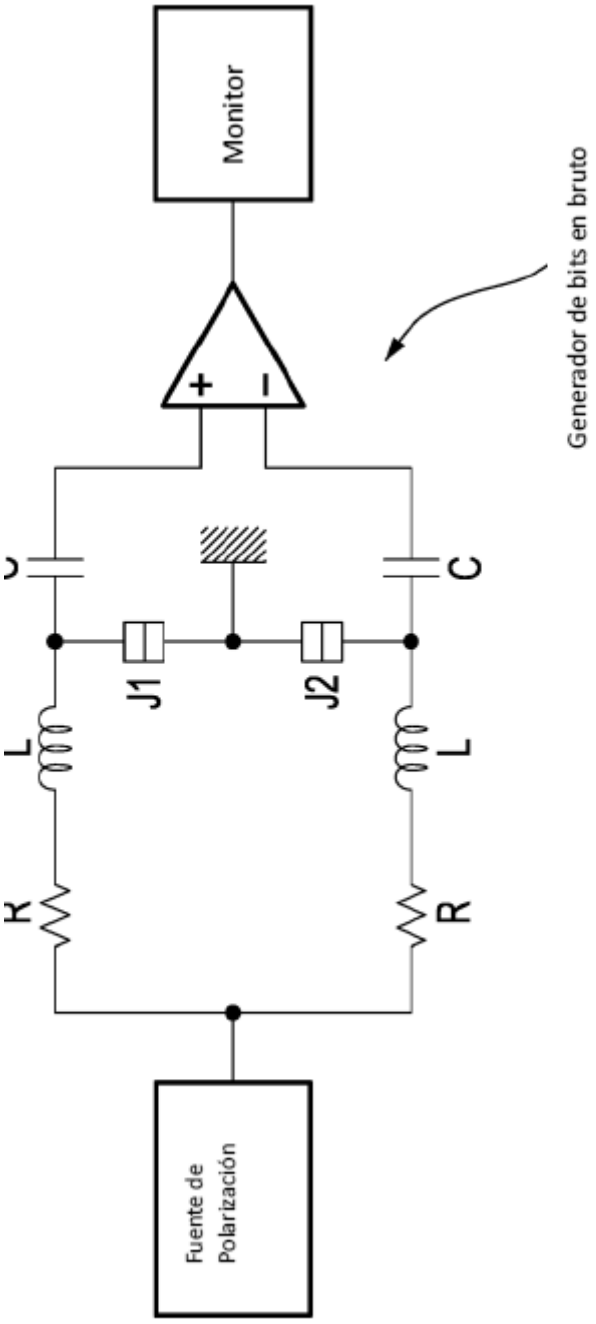
Monitor
Generador de bits en bruto
+
−
C
J1
J2
L
L
R
R
Fuente de Polarización

FIGURA 10B

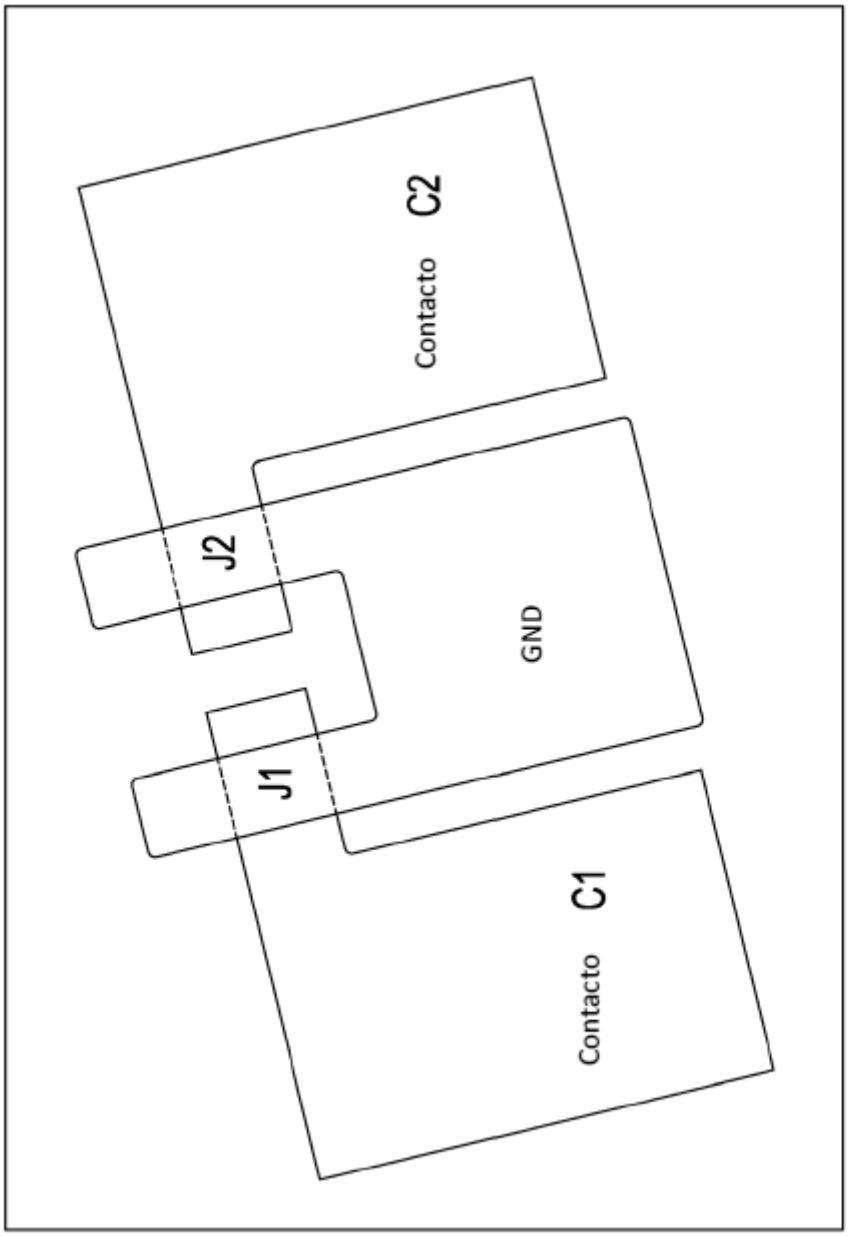

FIGURA 10C