(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 861 512**

(21) Número de solicitud: 202030271

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN B2

(22) Fecha de presentación:

03.04.2020

(43) Fecha de publicación de la solicitud:

06.10.2021

Fecha de concesión:

22.12.2022

(45) Fecha de publicación de la concesión:

30.12.2022

(73) Titular/es:

UNIVERSIDAD DE VIGO (100.0%)
Campus Lagoas- Marcosende s/n
36310 VIGO (Pontevedra) ES

(72) Inventor/es:

DÍAZ OTERO, Francisco Javier

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

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

(57) Resumen:
Generador cuántico de números aleatorios.
Un dispositivo QRNG que comprende integrados en un PIC fabricado en tecnología de InP que es un chip (100),:
- un láser (L1) de ganancia conmutada, monomodo, con capacidad de alcanzar un nivel de ruido cuántico entre pulsos ópticos para obtener una aleatoriedad de fase entre los pulsos ópticos;
- dos interferómetros MZI (I1, I2) conectados en serie, donde un primer interferómetro MZI (I1) es simétrico y está configurado para recibir la señal de salida de la fuente láser y equilibrar la potencia de la señal a la entrada al segundo interferómetro MZI (I2), que es asimétrico y está configurado para convertir variaciones de fase aleatorias entre pulsos ópticos consecutivos en variaciones de amplitude;: y
- un fotodetector (10) a la salida del segundo interferómetro MZI (I2) para detectar dichas variaciones de amplitudes convirtiéndolas en señales eléctricas para entregar en una de las salidas del PIC.

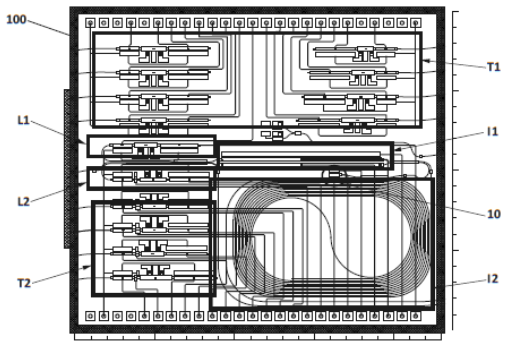

FIG. 4

ES 2 861 512 B2

DESCRIPCIÓN

Generador cuántico de números aleatorios

OBJETO DE LA INVENCIÓN

La presente invención está relacionada con la industria dedicada a la fabricación de circuitos ópticos integrados o circuitos integrados fotónicos (PIC: Photonic Integrated Circuit, en inglés).

La presente invención se refiere a generadores de números aleatorios cuánticos (QRNG: "Quantum random number generator", en inglés) y, más particularmente, a un dispositivo QRNG integrado en un circuito fotónico integrado.

ANTECEDENTES DE LA INVENCIÓN

La aleatoriedad es un tema muy multidisciplinario que abarca desde matemáticas, ingeniería, informática, filosofía hasta física.

Hay diferentes tipos de generadores de números aleatorios y sus propiedades se indican a continuación:

- Generador de números pseudo-aleatorios (PRNG: "Pseudorandom number generator", en inglés): Generación de números aparentemente aleatorios mediante un algoritmo. La secuencia obtenida es difícil de diferenciar de una secuencia puramente aleatoria, pero su orden está completamente predefinido. Sus principales ventajas son la facilidad y velocidad para generar grandes cantidades de números.

- Generador de números aleatorios reales (TRNG: "True random number generator", en inglés), donde a su vez se distinguen dos tipos:

    - Generador de números aleatorios físicos ("Physical random number generator", en inglés): Generación de números aleatorios basado en mediciones de parámetros con comportamiento caótico de sistemas clásicos. Las secuencias obtenidas suelen considerarse aleatorias, pero a un nivel más fundamental son de carácter determinista. Bien implementados, ofrecen mayor impredictabilidad e irreproducibilidad que los PRNG, pero los números son más difíciles y lentos de generar.

- Generador de números aleatorios cuánticos (QRNG: “Quantum random number generator”, en inglés): Generación de números aleatorios mediante el uso de la incertidumbre inherente a la física cuántica. Permiten la obtención de secuencias procedentes de procesos puramente aleatorios, pero las medidas están superpuestas a componentes de carácter clásico. La tasa de generación varía en función del tipo de QRNG que se utilice.

Considerando esos tipos de generadores de números aleatorios y sus propiedades, no resulta sorprendente la afirmación de que los generadores cuánticos de números aleatorios son el futuro de la ciberseguridad.

Los primeros generadores de números aleatorios se basaban en procesos físicos inherentes a mecanismos químicos o atómicos. Posteriormente se basaron en mecanismos electrónicos. A medida que los requisitos exigidos de aleatoriedad fueron creciendo, estos números aleatorios no fueron lo suficientemente fuertes para el uso al que iban destinados, ya que se basaban en la información sobre el estado interno de un algoritmo que describía un proceso físico ya fuera químico, atómico o electrónico. Es por eso que a mediados de los años 90 se optó por métodos basados en mecanismos aleatorios basados en procesos cuánticos y, por tanto, impresos en la propia naturaleza física, para obtener este tipo de números.

Fundamentalmente, se han experimentado distintas soluciones para obtener números aleatorios basadas en la naturaleza cuántica de la luz, obteniendo así los llamados QRNG ópticos, Los generadores de números aleatorios cuánticos (QRNG) son dispositivos físicos aleatorios basados en sistemas cuánticos de muestreo con parámetros observables macroscópicamente que varían aleatoriamente de manera dinámica, como por ejemplo la fase o intensidad de un láser o un amplificador óptico. Por ejemplo, hay dispositivos QRNG que se fundamentan en la velocidad del ruido de fase del láser de onda continua (CW: “Continuous Wave”, en inglés), de las fluctuaciones de vacío, del tiempo de llegada de los fotones o en el uso de Emisiones Espontáneas Amplificadas (ASE: “Amplified Spontaneous Emission”, en inglés).

Los esquemas basados en la generación y medida del ruido de fase poseen numerosas ventajas respecto al resto de esquemas citados anteriormente, independientemente de la aplicación a la que se destinen debido a que:

- Utilizan componentes estándar de aplicación comercial
- Son rápidos, presentan una mayor tasa de generación de números aleatorios

- Son robustos frente a las fluctuaciones de amplitud y de fase.

Diversos autores, en publicaciones recientes, muestran el funcionamiento de detectores homodinos en experimentos de laboratorio que pueden discretizarse para uso comercial. Todos estos casos han sido desarrollados en componentes discretos (componentes de laboratorio o componentes comerciales) y no integrados en un único elemento.

Recientemente, diversos autores han desarrollado en laboratorio varios QRNG que utilizan circuitos integrados fotónicos (PIC). Dependiendo de la tecnología de fabricación empleada existen diversos dispositivos QRNG:

- En una primera implementación que combina dos láseres, un acoplador óptico y dos fotodetectores, se han podido generar números aleatorios en régimen de gigahercios (GHz).
- En otra implementación que utiliza plasmones de superficie (no fabricable de manera estándar), se han producido QRNG a velocidades de megahercios (MHz).
- Otras demostraciones basadas en la fotónica de silicio han producido QRNG a tasas de GHz recurriendo a interferómetros Mach-Zehnder en el chip.

Por otro lado, existen diversos documentos de patentes relacionados con métodos de generación de dichos números aleatorios:

US9218160 describe un procedimiento para la generación de números aleatorios a través del ruido de fase de una cavidad laser, donde el procedimiento comprende operar un láser en monomodo y alto ancho de banda de modulación mediante un generador de pulsos eléctricos, transformar los pulsos ópticos de fase aleatoria producidos anteriormente en pulsos ópticos con amplitud aleatoria y detectar las señales de amplitud aleatoria resultantes mediante un fotodiodo rápido. Los números así producidos son verdaderamente aleatorios.

US2017/0115960 describe un procedimiento basado en una cavidad laser multimodo con la modulación periódica de una ganancia neta, donde el procedimiento comprende operar un láser multimodo en una cavidad láser con modulación periódica de una ganancia neta y detectar el patrón de intensidad aleatorio producido por el latido intermodal que ocurre dentro de la cavidad láser. Los números producidos son verdaderamente aleatorios y además se requiere un número mínimo de elementos para operar el sistema.

El problema técnico objetivo que se presenta es proveer un generador de números aleatorios cuánticos (QRNG) que pueda fabricarse a bajo coste y por volumen.

DESCRIPCIÓN DE LA INVENCIÓN

La presente invención sirve para solucionar el problema mencionado anteriormente, mediante la provisión en un circuito fotónico integrado monolítico de fosfuro de indio (InP) de un dispositivo para la generación de números aleatorios (QRNG) basada en la combinación de ruido de fase producido en una cavidad laser e interferometría.

Un aspecto de la invención se refiere a un dispositivo generador de números aleatorios cuánticos (QRNG) que comprende los siguientes componentes integrados dentro de un circuito integrado fotónico o PIC (chip), fabricado en tecnología de InP:

- una fuente de luz que comprende un (primer) láser de ganancia conmutada integrado, en el extremo inicial del generador QRNG, que es monomodo y está configurado para alcanzar un nivel de ruido cuántico entre pulsos ópticos para obtener una aleatoriedad de fase entre los pulsos ópticos;
- dos interferómetros Mach-Zehnder, MZI conectados en serie, donde un primer interferómetro MZI es simétrico y está configurado para recibir la señal de salida de la fuente de luz y equilibrar la potencia de la señal a la entrada a un segundo interferómetro MZI, y donde el segundo interferómetro MZI es asimétrico y está configurado para convertir variaciones de fase aleatorias entre pulsos ópticos consecutivos en variaciones de amplitudes; y
- un solo fotodetector integrado en el extremo final del generador QRNG y que está configurado para detectar las variaciones de amplitudes de los pulsos ópticos a la salida del segundo interferómetro MZI, convirtiendo las variaciones en señales eléctricas para entregar en una de las salidas del circuito PIC.

En una realización preferida, la fuente de luz integrada en el circuito PIC puede comprende un segundo láser de ganancia conmutada, cuya señal de salida se une a la señal de salida del primer láser. Ambos láseres conectados como posibles fuentes de ruido de fase permiten tener multiplexación frecuencial y duplicar la tasa de bits aleatorios generada. En una posible realización, el ruido de fase generado se produce utilizando una cavidad Fabry-Perot con reflectores distribuidos de Bragg, DBR.

Las ventajas de la presente invención frente al estado de la técnica anterior y en relación a los dispositivos integrados existentes actualmente son fundamentalmente:

- Permite un alto grado de repetibilidad, estandarización y fiabilidad en el proceso de fabricación de los QRNGs integrados en el PIC, de forma que pueden fabricarse a bajo coste y por volumen. El dispositivo generador de números aleatorios propuesto se fabrica en tecnología de fosfuro de indio (InP) en una plataforma monolítica integrada comercial, que presenta las ventajas mencionadas. La tecnología de InP permite integrar todos los dispositivos activos y pasivos en un único chip, manteniendo además la polarización.
- El dispositivo integrado propuesto constituye un generador de números aleatorios (QRNG) basado en el ruido de fase producido en una cavidad laser que es además autónomo y autocontenido. Es decir, en un mismo circuito integrado (chip) se han introducido tanto los dispositivos activos (láseres y fotodetectores), como los dispositivos pasivos (guías de onda e interferómetros Mach-Zehnder) necesarios para el correcto funcionamiento del generador. Esta característica también diferencia a este chip y a todos los fabricados en InP, de aquellos fabricados en silicio (Si).
- Respecto a otros QRNG fabricados en tecnologías monolíticas integradas de InP, esta invención requiere únicamente un solo láser como dispositivo activo, en vez de dos láseres, disminuyendo así la posibilidad de fallo de operación y proporcionando mayor facilidad de control del punto de funcionamiento de un único laser. Además, el dispositivo QRNG de la invención necesita un único dispositivo fotodetector y no dos, como otros QRNG existentes, ya que no utiliza una detección homodina para extraer números aleatorios. El uso de dos fotodetectores, además de incrementar la posibilidad de fallo en el dispositivo, implica una correcta caracterización de ambos elementos (que deben ser lo más idénticos posible) y la extracción de los pulsos en la misma zona plana del espectro de ambos fotodetectores. Por consiguiente, el post-procesado de los pulsos de salida del fotodetector, que en la presente invención es solo uno, es más sencillo que el post-procesado de los QRNG con dos fotodetectores.
- El chip en el que está contenido este dispositivo tiene entradas y salidas eléctricas y todos los componentes requeridos incorporados, Por lo tanto, desde los pines o pads eléctricos hacia afuera, se puede operar y cablear como un chip electrónico normal, a pesar de utilizar fotónica en el interior.

- La huella total del dispositivo en el chip es la menor de los QRNGs integrados de InP, 9mm2.
- El dispositivo opera en el régimen de GHz. En una realización preferida, la tasa de bits generada se sitúa en 1.8Gbps
- El dispositivo es sintonizable dentro de su rango libre espectral, lo que permite el ajuste de la tasa de bits generada sintonizando de manera adecuada el interferómetro Mach-Zehnder asimétrico utilizado para convertir el ruido de fase aleatorio en amplitudes aleatorias.
- El dispositivo tiene, además, un segundo interferómetro Mach-Zehnder simétrico, que permite el ajuste de potencia de los pulsos que recorren ambas ramas del interferómetro asimétrico y, por tanto, una colisión con el máximo nivel de extinción posible.
- El dispositivo tiene capacidad de multiplexación frecuencial, mediante el uso de dos láseres conectados como posibles fuentes de ruido de fase que, cuando operan ambas ligeramente fuera de sintonía en frecuencia, consiguen duplicar la tasa de bits aleatorios generada, al duplicar los bits en canales paralelos de frecuencia. El ruido de fase generado se produce, en una realización preferida, a través de un láser DBR, con la capacidad de proporcionar alta potencia óptica de salida, alta eficiencia óptica y un ancho de línea reducido.

BREVE DESCRIPCIÓN DE LAS FIGURAS

A continuación, se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

FIGURA 1.- Muestra un diagrama de bloques de la arquitectura del dispositivo integrado QRNG, según una realización preferente de la invención.

FIGURA 2.- Muestra un diagrama de bloques del primer láser en correspondencia con su integración en el dispositivo integrado QRNG.

FIGURA 3.- Muestra un diagrama de bloques del segundo láser en correspondencia con su integración en el dispositivo integrado QRNG.

FIGURA 4.- Muestra un chip con el dispositivo integrado QRNG y distintas estructuras de prueba del dispositivo.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Se propone un dispositivo integrado para la generación de números aleatorios, QRNG, que se basa en un procedimiento para la generación de ruido de fase de un láser, seguido de una interferometría, realizado en un proceso genérico de integración fotónica monolítica de fosfuro de indio, InP.

El procedimiento mencionado está basado en que a la salida de un láser se tiene una fase aleatoria de origen cuántico que se puede usar para producir bits aleatorios. Dentro de la cavidad de un láser semiconductor monomodo, la emisión espontánea causa fluctuaciones en el campo de salida. Este ruido de fase, también conocido como difusión de fase, proviene de una combinación de diferentes efectos cuánticos. Aunque la medición directa de la fase de una señal óptica no es tecnológicamente factible, un interferómetro asimétrico o no balanceado Mach-Zehnder, MZI, puede traducir las diferencias de fase en variaciones de amplitud.

En dicho MZI asimétrico o no balanceado, una de las ramas introduce un retraso τ con respecto a la otra rama. Asumiendo una variación de amplitud variable o lenta en cada rama, la salida tiene una media de nivel constante y la amplitud en los puertos de salida del interferómetro puede ser medida con detectores ópticos estándar de alta velocidad. Si el retraso introducido está muy por encima del tiempo de coherencia del láser, $\tau \gg \tau_{coh}$, la diferencia de fase $\Delta\phi(t)$ es una variable aleatoria gaussiana con una media que tiende a 0. En ese caso, si se muestrea la amplitud del detector con una diferencia de tiempo entre las muestras tal que $\Delta t \gg \tau + \tau_{coh}$, las amplitudes resultantes son independientes. Estas amplitudes son las variables aleatorias que usa el dispositivo integrado QRNG que se propone.

Para el funcionamiento de este QRNG se requiere al menos un láser de ganancia conmutada (“gain switching”, en inglés) que produce pulsos periódicos que se propagan a través de un interferómetro Mach-Zehnder, MZI, y un fotodetector que convierte los pulsos de luz en señales eléctricas. Las amplitudes obtenidas son aleatorias y su tasa de transmisión está en el rango de los GHz.

En la Figura 1 se muestran los componentes del dispositivo integrado QRNG, según una posible realización:

- dos láseres de ganancia conmutada integrados (L1, L2);
- dos interferómetros Mach-Zehnder, MZI (I1, I2) conectados en serie; y
- un fotodetector integrado (10) que al final del circuito convierte la luz en una señal eléctrica.

El primer interferómetro MZI (I1), que es simétrico, equilibra la potencia de la entrada a los brazos del segundo interferómetro MZI (I2) para obtener a su salida una relación de extinción máxima; mientras que el segundo interferómetro MZI (I2), que es asimétrico convierte las variaciones de fase aleatorias entre los pulsos ópticos consecutivos en variaciones de amplitudes, retardando en su brazo asimétrico exactamente un periodo de bit, que el fotodetector (10) detecta.

Además, la existencia de dos fuentes láser (L1, L2) conectadas permite un rango de multiplexación dentro del dominio de la frecuencia, pudiendo duplicar la tasa de generación de bits aleatorios. Los dos láseres (L1, L2) son esencialmente monomodo con capacidad de alcanzar un nivel de ruido cuántico entre pulsos. La condición de monomodo es necesaria para una interferencia eficiente entre los pulsos en el segundo interferómetro MZI (I2), mientras que la condición de alcanzar un nivel de ruido cuántico entre pulsos es necesaria para obtener una aleatoriedad de fase entre los pulsos. Además, ambos láseres (L1, L2) utilizan una cavidad Fabry-Perot con reflectores distribuidos de Bragg, DBR, que funcionan como espejos que proporcionan alta potencia óptica de salida, alta eficiencia óptica y un ancho de línea reducido.

Opcionalmente, el dispositivo integrado QRNG comprende unos acopladores de interferencia multimodo (11, 12, 13) que pueden ser acopladores (11) MMI 3x3 o acopladores (12, 13) MMI 2x2. Los acopladores de interferencia multimodo (11, 12, 13) o acopladores MMI, (MMI: “MultiMode Interference”, en inglés) se utilizan para unir señales de manera coherente dentro de la misma guía de onda. En concreto, el acoplador (11) MMI 3x3 permite unir las señales procedentes de ambos láseres (L1, L2) en ganancia conmutada y, además, dejar abierta la opción a que la señal óptica provenga de una fuente de luz externa. Asimismo, la salida del acoplador (11) MMI 3x3 puede disponer de un componente con salida óptica al exterior del chip para tener así una perfecta monitorización de la fuente láser y garantizar el correcto funcionamiento del QRNG.

El primer interferómetro MZI (I1) o modulador Mach-Zehnder simétrico, con dos brazos EOPM ("Electro Optic Phase Modulation", en inglés)" o ramas de modulación de fase electroóptica (14, 15), equilibra la potencia de la entrada a los brazos del segundo interferómetro MZI (I2) para obtener a su salida una relación de extinción máxima. La longitud de las ramas de modulación de fase electroóptica (14, 15) de este primer interferómetro MZI (I1) que permiten el correcto funcionamiento del dispositivo es de 2mm, en una realización preferida. El desplazamiento de fase en la rama superior (14) necesario para esta relación de extinción se obtiene a -5,66V.

El segundo interferómetro MZI (I2) convierte las variaciones de fase aleatorias entre los pulsos ópticos consecutivos en variaciones de amplitud, retardando exactamente un periodo de bit entre pulsos consecutivos, que posteriormente el fotodetector (10) detecta. El brazo asimétrico de este segundo interferómetro MZI (I2) tiene una longitud de 65,4mm, en una realización preferida. A la salida del segundo interferómetro MZI (I2) se obtienen pulsos aleatorios con un voltaje de pico medio de 40.4mV y un periodo de 797,47ps. Estos pulsos se envían al fotodetector (10), que en una realización preferida es un fotodetector de 100um, con un ancho de banda de 10GHz y corriente de oscuridad de 50nA a -5V. La corriente eléctrica fotodetectada se post-procesa fuera de línea de operación del QRNG ("offline") para la extracción definitiva de bits aleatorios.

En la Figura 2 se muestra la estructura del primer láser (L1) o laser superior, porque se sitúa encima del segundo láser (L2) o láser inferior en el circuito integrado. El primer láser (L1) tiene dos reflectores distribuidos de Bragg, DBR, donde un primer DBR (21) se conecta a un segundo DBR (23) a través de un amplificador SOA (SOA: "Semiconductor optical amplifier", en inglés) o amplificador óptico de semiconductor (22). Las características del primer láser (L1) para el correcto funcionamiento del dispositivo QRNG, según una realización preferida, son:

- Longitud cavidad con ganancia: 340 μm
- Longitud del primer DBR (21): 250 μm
- Longitud del segundo DBR (23): 500 μm
- Rejilla de difracción ("Pitch gratings"): 237,5 μm

En la Figura 3 se muestra la estructura del segundo láser (L2) que también tiene dos reflectores distribuidos de Bragg, DBR, donde un primer DBR (31) se conecta a un segundo DBR (34) a través de un amplificador óptico de semiconductor (33) antes del cual se usa un absorbente

saturable (32). Las características del segundo láser (L2) para el correcto funcionamiento del dispositivo QRNG, según una realización preferida, son:

- Longitud cavidad con ganancia: 340 µm
- Longitud del primer DBR (31): 250 µm
- Longitud del segundo DBR (34): 500 µm
- Rejilla de difracción (“Pitch gratings”): 237,5 µm
- Longitud absorbente saturable (32): 30 µm

A la salida de los láseres (L1, L2) se proporciona una potencia de 21dBm a 1.245GHz en radiofrecuencia, funcionando en ganancia conmutada, con una corriente de modulación del láser de 19mA.

El dispositivo QRNG descrito está inmerso dentro de un chip en el que además pueden integrarse distintas estructuras de test o prueba (T1, T2) para diferentes configuraciones de láseres DBR del dispositivo, tal y como se refleja en la Figura 4. En una realización preferida, el dispositivo se integra en un chip de 4x4,6 mm como un circuito integrado fotónico, PIC, diseñado específicamente para ser fabricado en tecnología de InP, en un proceso genérico de integración monolítica disponible a través de rondas de fabricación multiproyecto. Dicho PIC tiene hacia el exterior únicamente entradas y salidas eléctricas, siendo por tanto autocontenido y autónomo en su funcionamiento óptico. El dispositivo QRNG integrado dentro del chip de 4x4,6 mm^2, mide 4x2,1 mm^2, ocupando solo una huella del 50% de la superficie total del chip. Así, la huella (“footprint”, en inglés) del dispositivo QRNG dentro de este chip es de 9 mm^2, siendo la menor de los QRNG integrados en InP.

Además, existe una característica opcional de este dispositivo QRNG, que consiste en la posibilidad de inyectar externamente una fuente de luz alternativa a los láseres integrados, con objeto de permitir el correcto funcionamiento del dispositivo aun en el caso de fallo de los dispositivos activos integrados en este PIC.

REIVINDICACIONES

1. Un generador de números aleatorios cuánticos, QRNG, **caracterizado por que** comprende integrados dentro de un chip (100), que es un circuito integrado fotónico, PIC, fabricado en tecnología de InP con entradas y salidas eléctricas, los siguientes componentes conectados de un extremo inicial a un extremo final del generador QRNG:

   - una fuente de luz que comprende un primer láser (L1) de ganancia conmutada integrado en el extremo inicial del generador QRNG, donde el primer láser (L1) es monomodo con capacidad de alcanzar un nivel de ruido cuántico entre pulsos ópticos para obtener una aleatoriedad de fase entre los pulsos ópticos;
   - dos interferómetros Mach-Zehnder, MZI (I1, I2) conectados en serie, donde un primer interferómetro MZI (I1) es simétrico y está configurado para recibir la señal de salida de la fuente de luz y equilibrar la potencia de la señal a la entrada a un segundo interferómetro MZI (I2), y donde el segundo interferómetro MZI (I2) es asimétrico y está configurado para convertir variaciones de fase aleatorias entre pulsos ópticos consecutivos en variaciones de amplitudes; y
   - un único fotodetector (10) integrado en el extremo final del generador QRNG y que está configurado para detectar las variaciones de amplitudes de los pulsos ópticos a la salida del segundo interferómetro MZI (I2) convirtiendo las variaciones en señales eléctricas para entregar en una de las salidas del circuito PIC.

2. El generador QRNG de acuerdo con la reivindicación 1, **caracterizado por que** la fuente de luz integrada en el circuito PIC además comprende un segundo láser (L2) de ganancia conmutada integrado en el extremo inicial del generador QRNG y cuya señal de salida se une a la señal de salida del primer láser (L1), donde ambos láseres (L1, L2) utilizan una cavidad Fabry-Perot con reflectores distribuidos de Bragg, DBR.

3. El generador QRNG de acuerdo con la reivindicación 2, **caracterizado por que** los dos láseres (L1, L2) están configurados para operar fuera de sintonía en frecuencia.

4. El generador QRNG de acuerdo con cualquiera de las reivindicaciones 2-3, **caracterizado por que** además comprende un acoplador de interferencia multimodo, MMI, que es un acoplador (11) MMI 3x3 que une las señales de salida de los dos láseres (L1, L2) en la señal de salida de la fuente de luz enviada al primer

interferómetro MZI (I1).

5. El generador QRNG de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** además comprende una entrada para inyectar una fuente de luz externa, en el caso de fallo de la fuente de luz láser integrada en el circuito PIC.

6. El generador QRNG de acuerdo con las reivindicaciones 4 y 5, **caracterizado por que** el acoplador (11) MMI 3x3 dispone de entrada a la fuente de luz integrada en el circuito PIC y de entrada a la fuente de luz externa.

7. El generador QRNG de acuerdo con cualquiera de las reivindicaciones 4-6, **caracterizado por que** el acoplador (11) MMI 3x3 dispone de una salida óptica al exterior para monitorizar la fuente de luz integrada en el circuito PIC.

8. El generador QRNG de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** el chip tiene unas dimensiones de 4 milímetros de largo por 4,6 milímetros de ancho.

9. El generador QRNG de acuerdo con la reivindicación 1, **caracterizado por que** tiene una huella dentro del chip que es de 9 mm^2.

10. El generador QRNG de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** además comprende unos acopladores de interferencia multimodo, MMI, que son dos acopladores (12, 13) MMI 2x2, donde un primer acoplador (12) MMI 2x2 se conecta entre el primer interferómetro MZI (I1) y el segundo interferómetro MZI (I2), y un segundo acoplador (13) MMI 2x2 se conecta entre el segundo interferómetro MZI (I2) y el fotodetector (10).

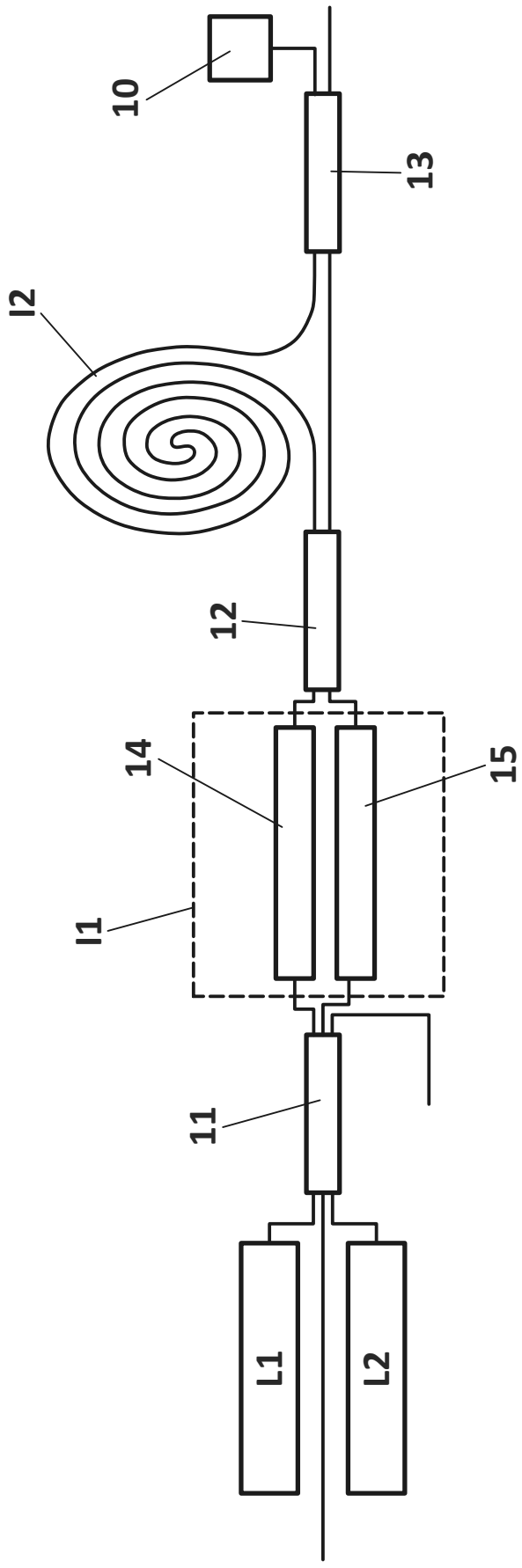

FIG. 1

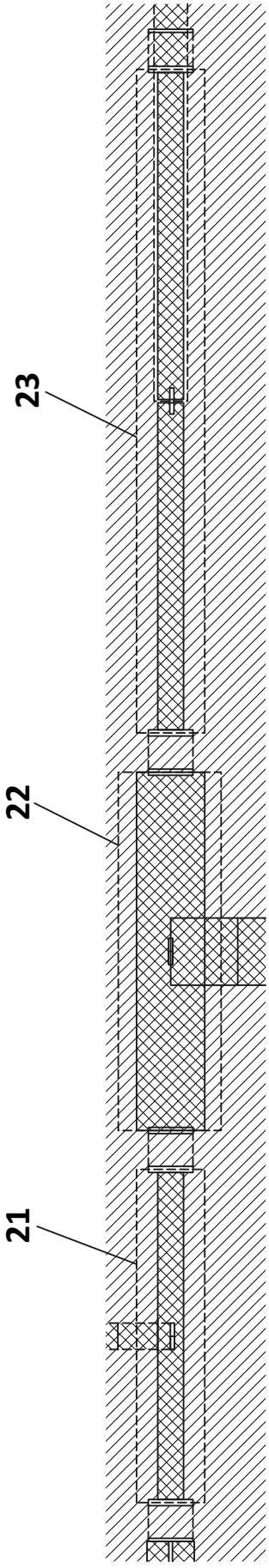

FIG. 2

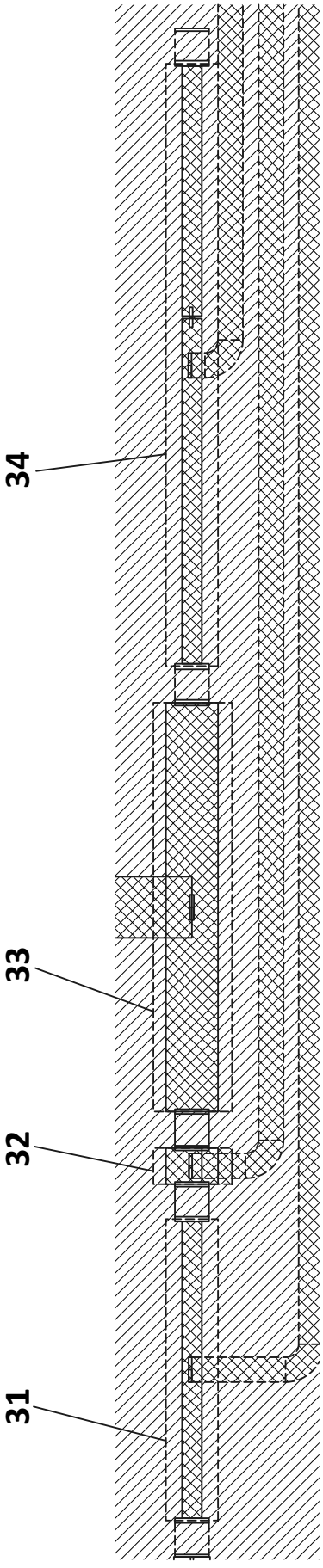

FIG. 3

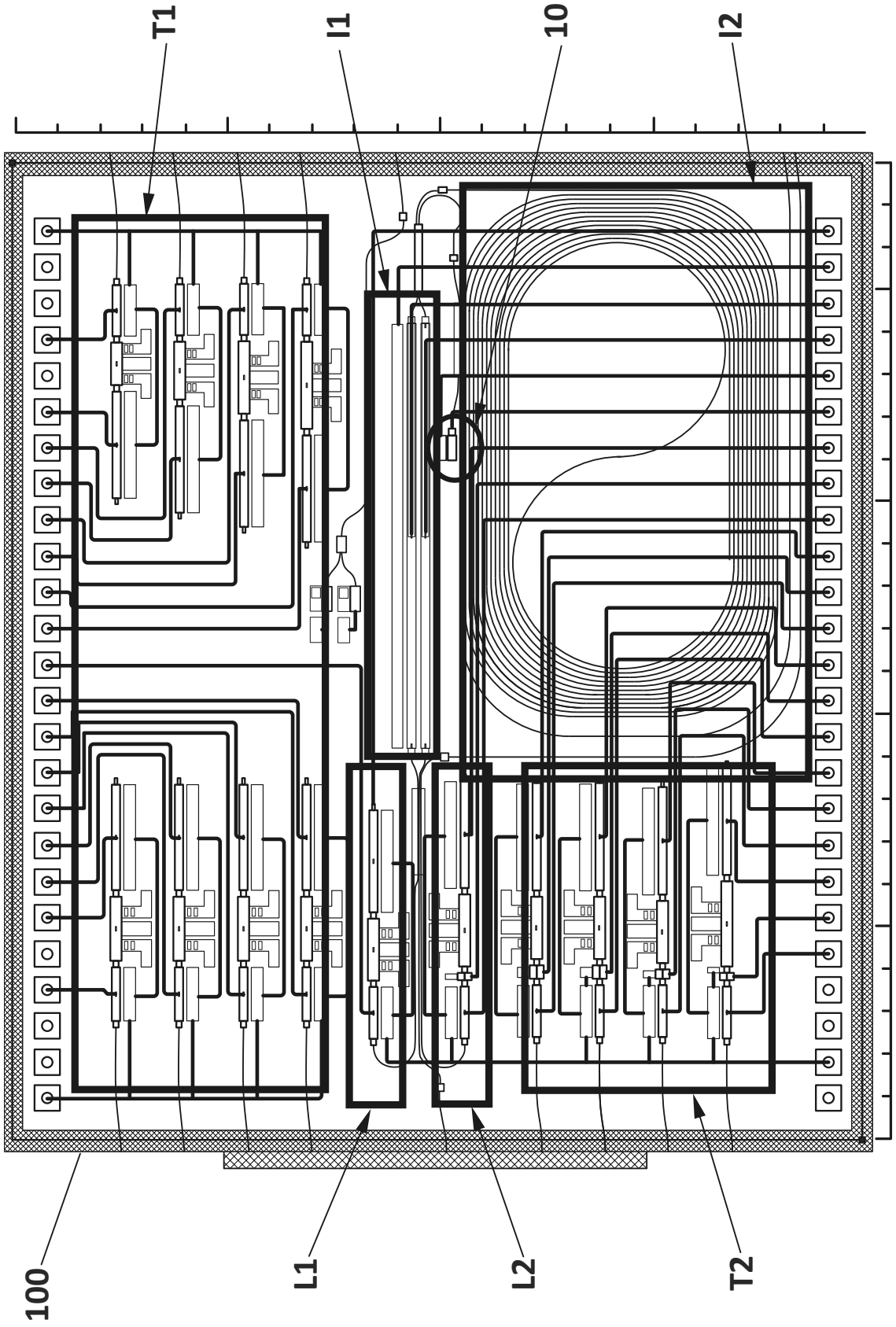

FIG. 4