(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 937 442**

(21) Número de solicitud: 202100100

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

28.09.2021

(43) Fecha de publicación de la solicitud:

28.03.2023

(71) Solicitantes:

UNIVERSIDADE DE VIGO (100.0%)
Campus Universitario de Vigo s/n
36310 Vigo (Pontevedra) ES

(72) Inventor/es:

DÍAZ OTERO, Francisco Javier y
ÁLVAREZ OUTERELO, David

(54) Título: **Transmisor de clave cuántica de variable continua**

(57) Resumen:
Un transmisor de clave cuántica de variable continua, que comprende integrados dentro de un chip (10) de InP:
- una fuente óptica integrada con un láser de retroalimentación distribuida (100);
- una doble salida: una salida óptica (199) y una salida eléctrica (162) para la transmisión óptica y eléctrica respectivamente de la clave cuántica;
- una etapa de modulación conectada a la salida de la fuente óptica que comprende un modulador de amplitud (110) implementado mediante un interferómetro de MachZehnder balanceado y un modulador de fase (120). conectados en serie entregando una señal modulada en una rama superior de la doble salida;
- un divisor de potencia regulable (N2) con al menos un divisor de potencia (151, 152) para desviar parle de la señal de potencia óptica a una rama inferior de la doble salida que actúa como piloto y se mezcla con la señal modulada;
- un detector homodino (189) para equilibrar la salida óptica (199).

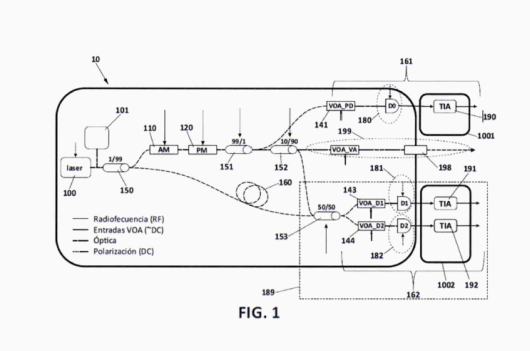

FIG. 1

ES 2 937 442 A1

DESCRIPCIÓN

Transmisor de clave cuántica de variable continua

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 dispositivos de distribución de clave cuántica (QKD: "Quantum Key Distribution", en inglés) y, más particularmente, a un transmisor QKD integrado en un circuito fotónico.

Antecedentes de la invención

La seguridad en las comunicaciones es un área tecnológica en constante evolución e innovación, desde la aparición de los primeros cifrados de sustitución mono alfabéticos empleados por los hebreos hasta los métodos actuales, como los que permiten hoy en día las comunicaciones inalámbricas seguras como el wifi. Todos estos sistemas tienen una parte común y bien diferenciada: la codificación de la información empleando una clave que tanto el emisor como el receptor conocen y la cual permite la codificación y la decodificación de la información por ambos integrantes. Esta clave o se conoce de antemano o ha de ser transmitida entre los integrantes de la comunicación al menos una vez para que éstos sean capaces de comunicarse.

La distribución de claves cuánticas (QKD: Quantum Key Distribution) se puede definir como un método de comunicación seguro implementando un protocolo criptográfico que involucra componentes de la mecánica cuántica. Permite a dos partes producir una clave secreta aleatoria compartida que solo ellos conocen, que luego se puede utilizar para cifrar y descifrar mensajes.

Hay diferentes tipos de transmisores de clave cuántica y sus propiedades se indican a continuación:

- Transmisor de distribución de claves cuánticas de variable continua (CVQKD: "Continuous Variable Quantum Key Distribution Transmitter", en inglés): La de la clave cuántica se hace codificando la información en ráfagas de baja potencia.

Cada símbolo a transmitir se cuantifica en una sucesión de entre 10 y 30 fotones, por lo que se manejan potencias de entorno a micro wattios.

- Transmisor de distribución de claves cuánticas de variable discreta (DVQKD: "Continuous Variable Quantum Key Distribution Transmitter", en inglés): La transmisión se realiza empleando fotones. La información se codifica empleando las propiedades cuánticas de los fotones, de tal forma que cada símbolo a transmitir se codifica en un fotón y en una de sus propiedades como, por ejemplo, su polarización

Considerando los tipos de transmisores de clave cuántica arriba descritos y sus propiedades, no resulta sorprendente la afirmación de que los transmisores de clave cuántica son el futuro de la ciberseguridad.

Actualmente existen diferentes sistemas comerciales de transmisores QKD, sin embargo, la mayoría de éstos emplean dispositivos discretos y de grandes dimensiones, al no estar el sistema

integrado en un bloque monolítico. Así, los sistemas de transmisores QKD existentes requieren de unas dimensiones relativamente grandes e imposibilita su integración cuando se necesitan dimensiones reducidas, como en el caso por ejemplo de satélites, dispositivos de comunicación portátiles o incluso en el internet de las cosas (IoT: "Internet of Things", en inglés).

El problema técnico objetivo que se presenta es proveer en un bloque monolítico un transmisor integrado para la distribución de la clave que permite una comunicación encriptada entre los interlocutores de una forma segura mediante fenómenos físicos cuánticos.

Descripción de la invención

La presente invención sirve para solucionar el problema mencionado anteriormente, mediante la provisión de un dispositivo codificador basado en la codificación de la información mediante el empleo de una modulación IQ de ráfagas de fotones super atenuadas (de en torno a 20 micro watts de potencia), integrando todos los componentes en un solo circuito fotónico monolítico de fosfuro de indio (InP).

Este dispositivo cuenta con un láser de retroalimentación distribuida o DFB ("Distributed Feedback Laser", en inglés) integrado en el propio chip, que proporciona una potencia óptica necesaria (preferentemente, en torno a unos 6 mili watts), lo que ahorra el tener que atenuar drásticamente la potencia como en el caso del uso de láseres externos. Esta potencia óptica se reparte en dos ramas: i) la potencia de la rama inferior actúa como piloto y se mezcla con la señal modulada justo antes de la salida óptica y ii) la potencia óptica en la rama superior se emplear para realizar la modulación IQ mediante un modulador de amplitud implementado con un interferómetro de Mach-Zehnder simétrico seguido de un modulador de fase óptico diseñado para una variación máxima de fase de 3 pi.

La fotónica integrada permite lograr dimensiones de milímetros y por el tipo de plataforma se consigue la integración de elementos complejos como los láseres y los fotodiodos receptores de luz en el mismo chip.

Una vez se ha codificado la información en la señal óptica, esta señal se envía fuera del chip mediante un convertidor de tamaño de punto o convertidor SSC ("Spot Size Converter", en inglés)

Un aspecto de la invención se refiere a un dispositivo transmisor de clave cuántica del tipo de variable continua que comprende, integrados dentro de un chip de fosfuro de indio (InP), los siguientes componentes:

- una fuente óptica integrada, que comprende un láser de retroalimentación distribuida, para entregar una señal de potencia óptica en una salida de la fuente óptica;

- una salida doble, con una rama superior de salida y una rama inferior de salida, donde la que doble salida consta de (i) una salida óptica y (ii) una salida eléctrica para la transmisión, óptica y eléctrica respectivamente, de la clave cuántica;

- una etapa de modulación, conectada a la salida de la fuente óptica, que comprende un modulador de amplitud implementado por un interferómetro de Mach-Zehnder balanceado y un modulador de fase, conectados en serie para entregar una señal modulada en la rama superior de la doble salida;

- uno más divisores de potencia para desviar a la rama inferior de la doble salida parte de la señal de potencia óptica que actúa como piloto, parte ue se mezcla (en la rama inferior) con la señal modulada procedente de la rama superior de la doble salida;

- un detector homodino para equilibrar la salida óptica.

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

- Integración en el propio chip de la fuente de luz: El láser DFB integrado en el chip proporciona la potencia óptica necesaria, lo cual es una de las principales ventajas a la hora de emplear la plataforma de fosfuro de indio (InP), ya que otras plataformas, como las de silicio, no permiten esta integración y necesitan de un láser externo que incrementa enormemente las dimensiones del dispositivo.

- El empleo de variable continua en vez de fotón único ("single photon", en inglés) simplifica enormemente el receptor, no siendo necesario el uso de receptores enfriados a muy baja temperatura para favorecer así la superconducción y disminuir el ruido del sistema. El modelo de variable continua emplea este ruido propio del sistema para la detección de la interceptación de la transmisión de la clave lo que le brinda de una capa más de seguridad.

- Este dispositivo se fabrica en tecnología de fosfuro de indio (InP) en una plataforma monolítica integrada comercial, repetible, estandarizada y de alta fiabilidad.

- 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.

- Salida óptica y eléctrica integradas: El dispositivo cuenta con una doble salida que pueden ser empleadas para la transmisión óptica o eléctrica de la clave.

- Integración de un receptor homodino: El diseño incluye un receptor homodino que puede ser empleado para la generación de número aleatorios.

- Todos los módulos electroópticos empleados en el chip son controlados por corriente, lo que permite mayores tasas de bit ("bit rate", en inglés) y una respuesta de ajuste mucho más rápida que otros dispositivos termo-ópticos.

- Simplicidad de diseño: La estructura básica empleada tanto para la construcción del modulador de amplitud como de los divisores de potencia ajustables es la misma. Esta estructura es un interferómetro de Mach-Zehnder balanceado a la cual solo se le cambia el último elemento (MMI).

- 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 como modulador de amplitud.

- El dispositivo opera en el régimen de megahercios (MHz) suficiente a la hora de la generación de claves.

- Dimensiones súper reducidas. Las dimensiones totales del dispositivo son, en una realización preferida, aproximadamente 2 x 12 mm, lo que le confiere una alta capacidad de integración.

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 de un dispositivo transmisor de clave cuántica integrado en un chip, según una realización preferente de la invención.

FIGURA 2.- Muestra un diagrama de bloques de la estructura del divisor de potencia variable incluido en el dispositivo integrado.

FIGURA 3.- Muestra un diagrama de bloques de la estructura del modulador de amplitud incluido en el dispositivo integrado.

FIGURA 4.- Muestra un chip con el dispositivo transmisor integrado y una parte de circuito de pruebas del dispositivo.

Realización preferente de la invención

Se propone un dispositivo que se encuentra integrado, mediante un proceso de integración fotónica monolítica de fosfuro de indio, InP, en un circuito fotónico o chip, con unas dimensiones preferentes de 2 mm x 12 mm, ocupando solo una huella del 95% de la superficie total del chip, correspondiendo el 5 % restante a un circuito de test. El dispositivo propuesto, incluyendo tanto los componentes opcionales como aquellos indispensables para su funcionamiento, está formado por los siguientes componentes integrados en un chip (10), tal y como se indica en la Figura 1.

- Una fuente óptica integrada que comprende un láser de retroalimentación distribuida (100) o láser DFB integrado: En una posible realización, el dispositivo emplea como fuente óptica un láser DFB centrado en 1550 nm y cuya potencia óptica máxima (en un extremo; "single side", en inglés) a esta longitud de onda es de 6 mili watts. Este laser se emplea de forma continua pudiéndose a su vez realizar un ajuste fino de +-3 nm. Presenta un ancho de línea de 5 Mhz y un consumo máximo estimado de 150 miliamperios.

Adicionalmente, si por algún motivo es necesaria más potencia, el dispositivo puede contar con una entrada auxiliar óptica (101) optimizada mediante el empleo de un convertidor de tamaño de punto o convertidor SSC limitando las perdidas por acoplo a menos de 2 dB.

- Una etapa de modulación que comprende:

- un modulador de amplitud (110): Representado en la Figura 3 explicada más abajo en detalle, el modulador de amplitud (110) está implementado mediante un interferómetro de Mach-Zehnder balanceado, al cual se aplica una corriente eléctrica en una de sus ramas. Mediante este método se pueden conseguir ratios de extinción superiores a los 20 dB y con un ancho de banda superior a los 25 Ghz;

- un modulador de fase (120): Modulador de fase estándar extralargo que puede llegar a una variación de fase de hasta 3 pi.

- Una pluralidad de atenuadores de potencia: Debido a que es necesaria la drástica atenuación de la señal óptica, se usan múltiples atenuadores ópticos variables (141, 142, 143, 144) o atenuadores VOA ("Variable Optical Attenuator", en inglés). Además, para ajustar el dispositivo a las dimensiones máximas del dado o pastilla (DIE, en inglés; es el espacio reservado para el diseño/chip dentro de la oblea donde se fabrican los chips, oblea que es cortada en múltiples trozos según un patrón y cada trozo, llamado dado o DIE, contiene una copia del circuito) y a la sucesión de atenuaciones pasiva en cascada, se emplea al menos un divisor de potencia regulable (N1, N2), cuya estructura se representa en la Figura 2, descrita más abajo que comprende al menos un divisor de potencia fijo (151, 152) que es un interferómetro multimodal o acopiador MMI. En vez de atenuar la señal simplemente, un primer divisor de potencia (151) desvía parte de la señal a una primera salida (161) que a la vez sirve como control para la estimación de potencia o a una segunda salida (162) que, a través de un segundo divisor de potencia (152), simplemente reparte la potencia entre dos módulos del dispositivo.

- Un detector homodino (189): Se emplea un divisor de potencia regulable como estructura base del detector, que permite poder equilibrar las salidas de dicho detector.

En la Figura 1, se muestra además al menos un detector (180 181, 182) que comprende un fotodiodo (DO, D1, D2) y la salida del detector es la salida eléctrica del fotodiodo (DO, D1, D2), que pasa a un amplificador de transimpedancia (190 191, 192) o TIA (Transimpedance Amplifier, en inglés). La salida de un primer fotodiodo (DO), integrado en la primera salida (161) del dispositivo se usa en un módulo de estimación de potencia (1001) para poder chequear las modulaciones de amplitud y fase y ver qué potencias son necesarias después de modular. Opcionalmente, se incorpora un módulo de amplificación (1002) que se usa para balancear las señales de salida de los fotodiodos (D1, D2) que están en la segunda salida (162) del dispositivo, de tal forma que tengan la misma potencia. Para este propósito de balance en potencia del detector homodino (189), se emplea un tercer divisor de potencia variable (N3) que comprende un tercer divisor de potencia fijo (153).

- Una salida óptica (199) cuántica, optimizada mediante el empleo de un convertidor de tamaño de punto o convertidor SSC. La salida óptica (199) comprende un acopiador (198) o convertidor SSC para reducir las pérdidas de inserción. Además, opcionalmente, incluye un VOA (142).

En caso de que la señal óptica sea pulsada, una de las salidas de un divisor inicial (150) mostrado en la Figura 1 que se conecta a la salida de la fuente puede comprender un retardo óptico (160).

En la Figura 2, se muestra toda la estructura del circuito que funciona como divisor de potencia variable o regulable (N1, N2); dicha estructura es básicamente la misma tanto para un primer divisor de potencia (N1) regulable integrado entre la línea óptica principal del chip (10) y el primer fotodiodo (DO) de chequeo de potencia como para un segundo divisor de potencia regulable (N2) entre integrado la salida óptica (199) cuántica principal y el detector homodino (189), ilustrados en la Figura 4. El divisor de potencia variable o regulable (N1, N2), por ejemplo, divisor 1/99 a 5.5mA, comprende un primer divisor de potencia fijo (151) que es un acopiador MMI 1x2 que divide la potencia 50/50 y un segundo divisor de potencia regulable (152) que es un MMI 2x2. La configuración inicial hace que se comporte como un divisor 50/50 si no se le aplica ninguna señal de control. La estructura del circuito de esta Figura 2, que es similar a la representada en la Figura 3 como se explica a continuación, comprende además dos moduladores de amplitud (220), ninguno de los cuales debe confundirse con el modulador de amplitud (110) ilustrado en la Figura 1 y la Figura 4 que se describe más adelante. Además, en las Figuras 2 y 3 se

representan las señales de control de los elementos activos; dichas señales de control se corresponden con un generador de corriente continua (130) que se puede ajustar para modificar el punto de trabajo, siendo el generador de corriente continua (130) un elemento externo al chip que se le proporciona a éste mediante electrónica externa.

En la Figura 3, se muestra toda la estructura del circuito que funciona como modulador de amplitud (110) y que es similar a la representada en la Figura 2, pero el segundo divisor de potencia regulable (152), que es un acopiador MMI 2x2 en el divisor de potencia variable de la Figura 2, en el modulador de amplitud es un divisor de potencia 1-2 50/50 actuando como mezclador implementado por un MMI 2x2.

En la Figura 4, se añade al chip (10), o PIC, un circuito de pruebas (300) que consta de tres fotodiodos y un láser DFB. El circuito de pruebas (300) es una estructura de test que se puede emplear para estudiar el acople entre dos guías de ondas muy próximas entre sí, así como para testeo inicial de los láseres y fotodiodos del PIC tanto en alta como en baja frecuencia.

REIVINDICACIONES

1. Un transmisor de clave cuántica de variable continua, caracterizado por que comprende integrados dentro de un chip (10), que es un circuito integrado fotónico,fabricado en tecnología de fosfuro de indio, los siguientes componentes:

- una fuente óptica integrada que comprende un láser de retroalimentación distribuida (100) entregando una señal de potencia óptica en una salida de la fuente óptica; - una doble salida que consta de una salida óptica (199) para la transmisión óptica de la clave cuántica y una salida eléctrica (162) para la transmisión eléctrica de la clave cuántica;

- una etapa de modulación conectada a la salida de la fuente óptica que comprende un modulador de amplitud (110) implementado mediante un interferómetro de Mach¬Zehnder balanceado y un modulador de fase (120), el modulador de amplitud (110) y el modulador de fase (120) conectados en serie entregando una señal modulada en una rama superior de la doble salida;

- un divisor de potencia regulable (N2) que comprende al menos un divisor de potencia (151, 152) para desviar parte de la señal de potencia óptica a una rama inferior de la doble salida que actúa como piloto, donde Ja parte de la señal desviada a la rama inferior se mezcla con la señal modulada procedente de la rama superior de la doble salida;

- un detector homodino (189) configurado para equilibrar la salida óptica (199).

2. El transmisor de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que la fuente óptica integrada además comprende una entrada auxiliar óptica (101) que incluye un convertidor de tamaño de punto.

3. El transmisor de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el láser de retroalimentación distribuida (100) está centrado en una longitud de onda de 1550 nm y tiene una potencia óptica máxima a dicha longitud de onda de 6 mili watts.

4. El transmisor de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el modulador de fase (120) tiene una variación máxima de fase de 3 pi.

5. El transmisor de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que la salida óptica (199) envía una señal óptica fuera del chip (10) mediante un convertidor de tamaño de punto.

6. El transmisor de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el chip (10) tiene unas dimensiones de 12 milímetros de largo por 2 milímetros de ancho.

7. El transmisor de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el detector homodino (189) comprende un tercer divisor de potencia fijo (153) integrado en un tercer divisor de potencia variable (N3) configurado para balancear en potencia el detector homodino (189).

8. El transmisor de acuerdo con la reivindicación 7, caracterizado por que el detector homodino (189) además comprende al menos un par de atenuadores ópticos variables (143, 144) a la salida del tercer divisor de potencia fijo (153) y un par de fotodiodos (D1, D2) conectados a la salida de los atenuadores ópticos variables (143, 144) respectivamente, donde la salida eléctrica de los fotodiodos (D1, D2) es la salida eléctrica (162) del transmisor.

9. El transmisor de acuerdo con la reivindicación 8, caracterizado por que el detector homodino (189) además comprende un módulo de amplificación (1002) configurado para balancear las señales de salida de los fotodiodos (D1, D2) el módulo de amplificación (1002) comprendiendo un amplificador de transimpedancia (191, 192) a la salida de cada uno de los fotodiodos (D1, D2) en la salida eléctrica (162) del transmisor.

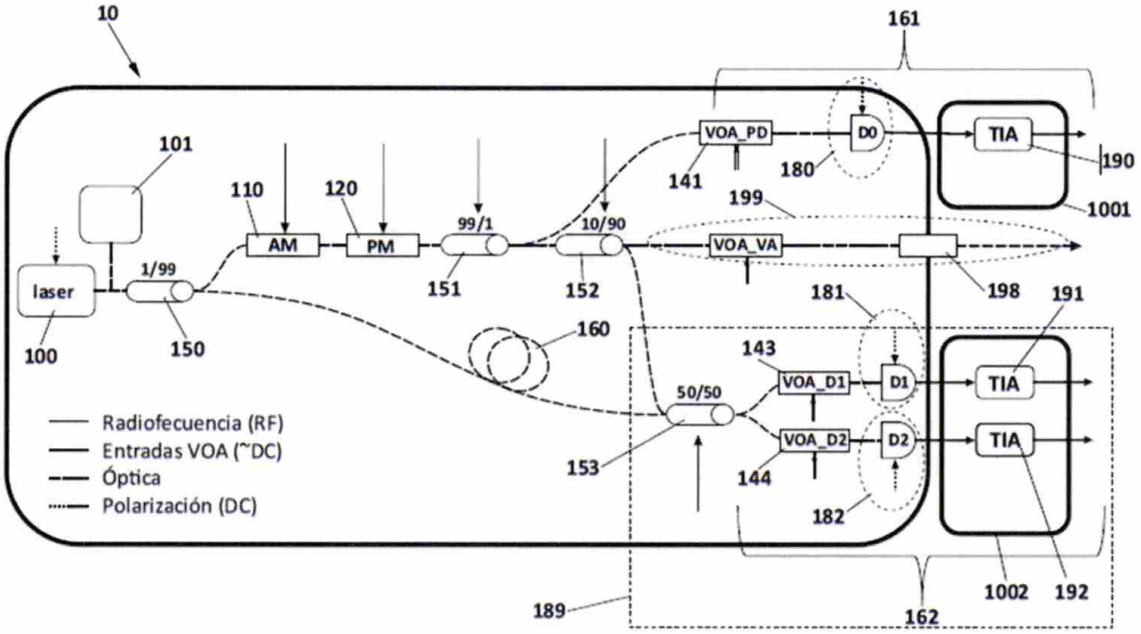
10
161
101
110
120
99/1
10/90
VOA_PD
D0
TIA
190
141
180
199
1001
AM
PM
VOA_VA
laser
1/99
151
152
198
181
191
100
150
160
143
VOA_D1
D1
TIA
50/50
VOA_D2
D2
TIA
153
144
182
Radiofecuencia (RF)
Entradas VOA (~DC)
Óptica
Polarización (DC)
189
162
1002
192

FIG. 1

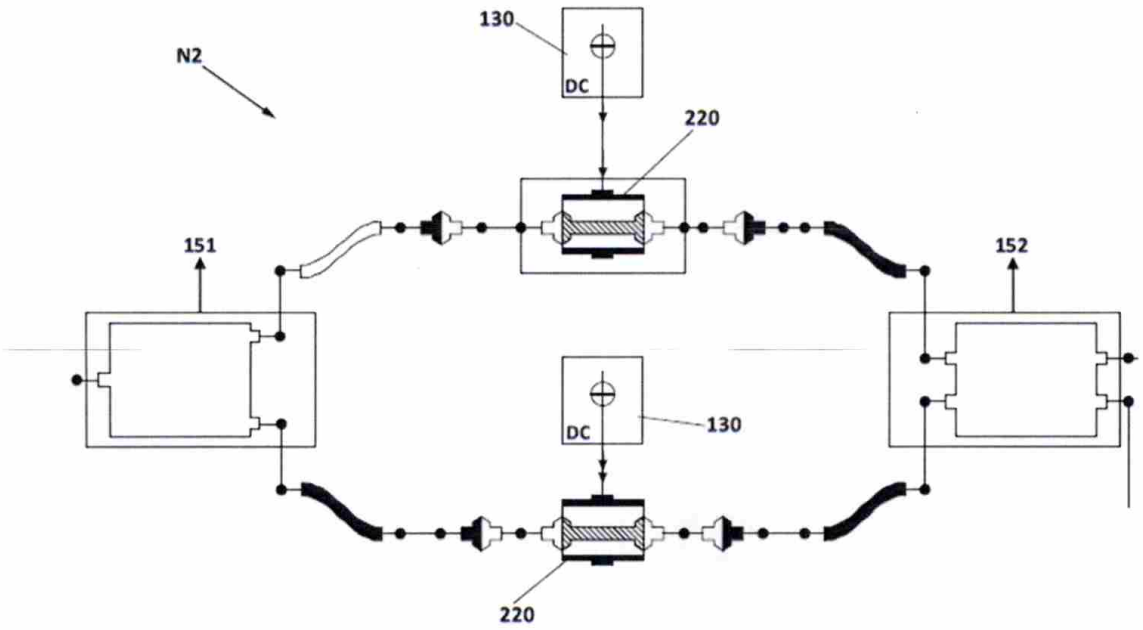
N2
130
DC
220
151
152
DC
130
220

FIG. 2

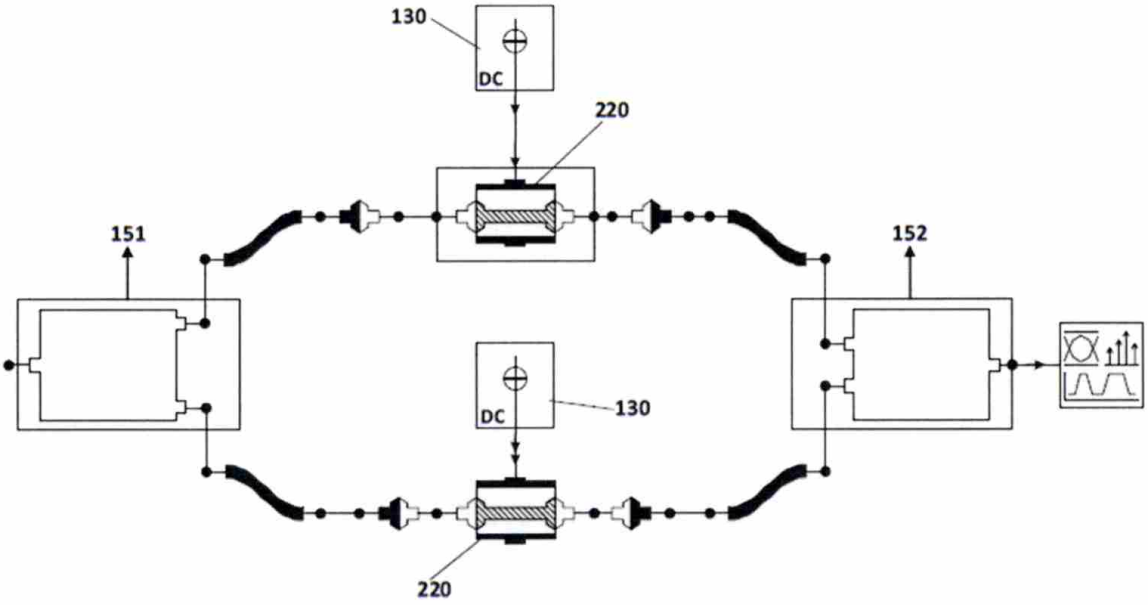
130
DC
220
151
152
DC
130
220

FIG. 3

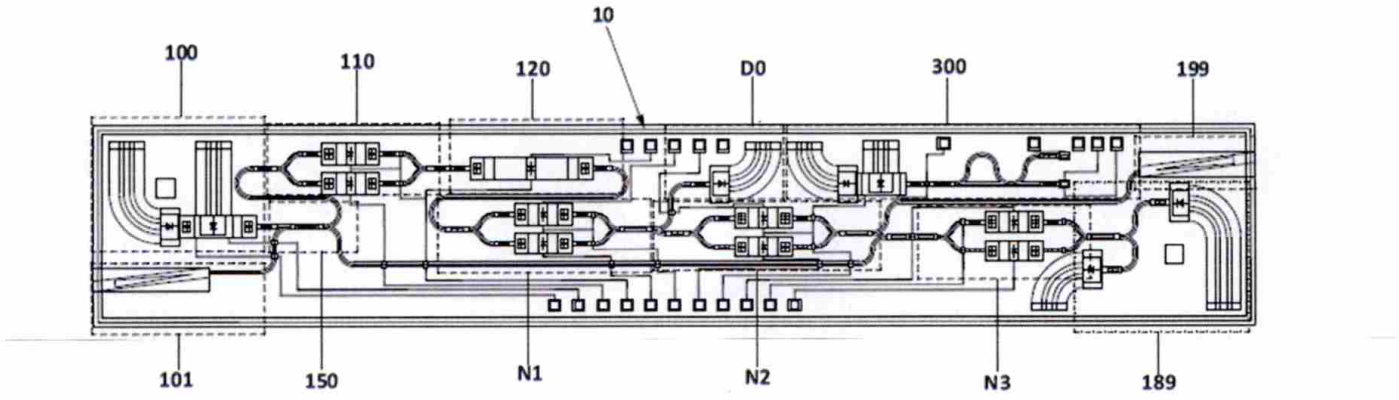
10
100
110
120
D0
300
199
101
150
N1
N2
N3
189

FIG. 4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 202100100

(22) Fecha de presentación de la solicitud: 28.09.2021

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/08*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	ZHANG G et al. Integrated Chip for Continuous-variable Quantum Key Distribution using Silicon Photonic Fabrication. 2018 Conference on Lasers and Electro-Optics (CLEO), 20180513 OSA. 13/05/2018, Páginas 1 - 2. Todo el documento	1-9
A	ERVEN C et al. Chip-scale integrated quantum technologies. 2015 Photonics North, 20150609 IEEE. 09/06/2015, Páginas 1, <DOI:10.1109/PN.2015.7569202>. Todo el documento	1-9
A	THOMPSON MARK G. Large-Scale Integrated Quantum Photonic Technologies for Communications and Computation. 2019 Optical Fiber Communications Conference and Exhibition (OFC), 20190303 OSA. 03/03/2019, Páginas 1 - 3. Todo el documento	1-9
A	WO 2016099565 A1 (NOKIA TECHNOLOGIES OY et al.) 23/06/2016, Todo el documento	1-9
A	EP 3335368 A1 (NOKIA TECHNOLOGIES OY) 20/06/2018, Todo el documento	1-9
A	US 9906311 B1 (DEROSE CHRISTOPHER et al.) 27/02/2018, Todo el documento	1-9

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
21.07.2022	M. Muñoz Sanchez	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, XPIEE, XPI3E, NPL