(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 717 708**

(51) Int. CI.:

***H04B 10/50*** (2013.01)
***H04B 10/516*** (2013.01)
***H04B 10/532*** (2013.01)
***H04B 10/54*** (2013.01)
***H04B 10/70*** (2013.01)
***H04L 9/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.08.2013 PCT/US2013/055430**

(87) Fecha y número de publicación internacional: **20.03.2014 WO14042822**

(96) Fecha de presentación y número de la solicitud europea: **16.08.2013 E 13837039 (0)**

(97) Fecha y número de publicación de la concesión europea: **13.02.2019 EP 2885886**

(54) Título: **Sistema de comunicaciones cuánticas con dispositivos fotónicos integrados**

(30) Prioridad:

**17.08.2012 US 201261684502 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**24.06.2019**

(73) Titular/es:

**TRIAD NATIONAL SECURITY, LLC (100.0%)**
**Los Alamos National Laboratory, P.O. Box 1663, MS A187**
**Los Alamos, NM 87545, US**

(72) Inventor/es:

**NORDHOLT, JANE ELIZABETH;**
**PETERSON, CHARLES GLEN;**
**NEWELL, RAYMOND THORSON y**
**HUGHES, RICHARD JOHN**

(74) Agente/Representante:

**SÁEZ MAESO, Ana**

## DESCRIPCIÓN

Sistema de comunicaciones cuánticas con dispositivos fotónicos integrados.

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica el beneficio de la solicitud de patente provisional de Estados Unidos núm. 61/684,502, presentada el 17 de agosto de 2012.

Campo

La descripción se refiere a métodos y aparatos para transmitir y recibir comunicaciones cuánticas.

Reconocimiento del apoyo gubernamental.

Esta invención se realizó con el apoyo del gobierno bajo el contrato núm. DE-AC52-06NA25396 otorgado por el Departamento de Energía de Estados Unidos. El gobierno tiene ciertos derechos en la invención.

Antecedentes

En la comunicación cuántica, dos partes intercambian información codificada en estados cuánticos. Normalmente, los estados cuánticos son propiedades especialmente definidas de los fotones, tales como los pares de estados de polarización (*por ejemplo,* 0° y 90°, o 45° y 135°) o estados de base circular (*por ejemplo,* izquierdo y derecho). A través de la comunicación cuántica ("QC"), las dos partes producen una serie de bits aleatorios compartidos que solo ellos conocen, y que luego pueden usarse como claves secretas en el posterior cifrado y descifrado de los mensajes.

Un tercero puede, en teoría, espiar la QC entre las dos partes. Sin embargo, tal espionaje perturba la QC, introduciendo anomalías que las dos partes previstas pueden detectar. Mediante el uso de la comunicación convencional, las dos partes procesan posteriormente los resultados de la QC para eliminar cualquier información parcial adquirida por un intruso, y forman claves secretas compartidas de la información restante que resulta de la QC.

Por ejemplo, de acuerdo con un enfoque general de la QC, un transmisor establece el estado cuántico de la información binaria, hace un registro de cómo establece el estado cuántico y transmite la información. La Tabla 1 muestra un ejemplo de estados cuánticos y bases para diferentes polarizaciones de fotones. Para las bases y estados mostrados en la Tabla 1, el transmisor selecciona una base (rectilínea, diagonal o circular), establece el estado de polarización de un fotón en la base seleccionada y registra el valor del bit (0 o 1), la base de envío seleccionada y el tiempo de transmisión.

Tabla 1. Ejemplo de bases y estados cuánticos.

| **Base** | **0** | **1** |
|---|---|---|
| Rectilínea (+) | 90° | 0° |
| Diagonal (×) | 45° | 135° (o -45°) |
| Circular | Izquierda | Derecha |

Un receptor recibe la información binaria, mide el estado cuántico de la información y registra cómo midió el estado cuántico. El estado medido depende de cómo el receptor realiza la medición (*por ejemplo,* con base de medida rectilínea o diagonal). Se espera que el transmisor y el receptor registren diferentes valores de bits en algunos casos debido a que el transmisor y el receptor a veces establecen/miden la información codificada en estado cuántico de diferentes maneras. Por lo tanto, después de intercambiar información en estados cuánticos, el transmisor y el receptor comparan sus registros de cómo se establecieron y midieron los estados cuánticos. Para esta comparación, el transmisor y el receptor intercambian información a través de un canal público. Luego, el transmisor y el receptor producen una serie de bits (claves) compartidos a partir de la información codificada para los cuales los estados cuánticos fueron establecidos y medidos de la misma manera por el transmisor y el receptor.

Si se usan las bases y estados rectilíneos y diagonales que se muestran en la Tabla 1, el receptor selecciona una base (rectilínea o diagonal), mide el estado de polarización en la base seleccionada y registra el valor del bit medido y la base de medición. Ninguna posible base de medición puede distinguir los cuatro estados, por lo que el receptor adivina esencialmente sea rectilínea o diagonal. Si la base de medición coincide con la base de envío, el receptor debe medir el valor de bit correcto. Sin embargo, si la base de medición no coincide con la base de envío, es probable que el valor del bit medido sea correcto o incorrecto. Por ejemplo, si la base de envío es diagonal para el valor de bit 0 (estado de polarización de 45°) pero la base de medición es rectilínea, los valores de bit medidos de 0 (90°) y 1 (0°) son igualmente probables. El transmisor y el receptor comparan la base de envío y la base de medición para un fotón determinado, y mantienen el valor de bit para un fotón si la base de envío y la base de medición coinciden.

Si un intruso intercepta y mide un fotón, la medición perturba el estado cuántico del fotón. El intruso solo puede adivinar la base de envío original cuando recodifica y retransmite el fotón al destino deseado. En el momento de la medición por el receptor, no se detecta el espionaje. En cambio, para los subconjuntos de los valores de bits para los cuales la base de envío y la base de medición coinciden, el transmisor y el receptor comparan los valores de paridad. Los valores de paridad deben coincidir exactamente, si el sistema se sintoniza adecuadamente y está libre de imperfecciones en la transmisión y la recepción. El espionaje introduce discrepancias notables en los valores de los bits, lo que permite que el transmisor y el receptor detecten el espionaje, corrijan las claves y establezcan un límite superior en la información parcial del intruso.

Una cadena de bits sin errores compartida por el transmisor y el receptor puede entonces amplificarse la privacidad (por ejemplo, mediante hash con una función de hashing) para reducir su longitud. (O, los bits pueden simplemente eliminarse, pero esto carece de ventajas de la amplificación de la privacidad). La longitud final de la cadena de bits compartida puede depender de la cantidad de errores detectados. Acortar la cadena de bits compartida con amplificación de la privacidad reduce el conocimiento y el espionaje puede tener un nivel arbitrariamente bajo, por lo general, mucho menos que un solo bit.

Desafortunadamente, los sistemas de QC prácticos, especialmente, aquellos que usan fibras ópticas, muestran errores incrementados debido a las dificultades para establecer los estados apropiados de polarización (SOP) en un receptor debido a la birrefringencia de las fibras, que puede ser grande y variable. En presencia de birrefringencia de fibra, las tasas de error de bits aumentan, y puede ser imposible identificar los estados y las bases de polarización deseados.

Los sistemas de QC actuales también tienden a ser costosos y difíciles de implementar. Por ejemplo, las fuentes de fotón único son, generalmente, sistemas voluminosos y complicados que requieren temperaturas criogénicas u otros entornos operativos especialmente controlados. Sin embargo, reemplazar dichas fuentes con sistemas más prácticos tiende a comprometer la seguridad de la QC.

El documento CN101572600 describe un dispositivo de distribución de clave cuántica. Una ruta óptica principal del dispositivo se forma conectando secuencialmente una fuente de fotones, un circulador óptico, un divisor/combinador de haz de polarización óptica de cuatro puertos, un canal cuántico, un modulador de fase y un espejo de rotación de Faraday de 90 grados. Dos partes de comunicación (una parte de control primaria y una parte de control secundaria) se conectan entre sí a través del canal cuántico. Un puerto de salida de reflexión del circulador óptico en la parte de control principal se conecta secuencialmente con un polarizador y un detector de fotón único para constituir una parte de detección; un puerto de reflexión del divisor/combinador de haz de polarización óptica de cuatro puertos se conecta con el espejo de rotación de Faraday de 90 grados, y un puerto de transmisión se conecta secuencialmente con el modulador de fase y el espejo de rotación de Faraday de 90 grados, lo que constituye una parte de carga de información. El canal cuántico de la parte de control secundaria se conecta secuencialmente con el modulador de fase y el espejo de rotación de Faraday de 90 grados para constituir la parte de carga de información. La combinación del divisor/combinador de haz de polarización óptica de cuatro puertos con el espejo de rotación de Faraday de 90 grados elimina el efecto de birrefringencia de los dispositivos ópticos y las fibras ópticas y mejora la estabilidad de un sistema.

El documento WO2012039595 describe un aparato y un método para codificar de forma dual el protocolo de fase coherente en el Sistema de Distribución de Clave cuántica (QKD) que, mediante el uso de una fuente de láser coherente, se describe un modulador de intensidad y un modulador de fase. El sistema comprende dos niveles de codificación y seis tipos de bits de señuelo para mejorar aún más la seguridad de las claves secretas. El sistema comprende un modulador de intensidad para la codificación de intensidad en donde se codifica una clave secreta, medios para generar un tren de pulsos con bits '1' para pulso de coherencia débil (WCP) y bits 'O' para pulso de vacío; y un modulador de fase para codificación de fase diferencial comprende la clave secreta codificada de intensidad codificada adicionalmente con bits T para la diferencia de fase de 0; bits '0' para la diferencia de fase de TT para impulso de coherencia débil (WCP); y bits de señuelo para otra orientación de diferencia de fase de pulso de vacío y WCP.

Resumen

De acuerdo con un primer aspecto de la presente invención, se proporciona un transmisor de comunicación cuántica como se describe en la reivindicación 1.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un método como se describe en la reivindicación 10.

Los transmisores de comunicación cuántica (QC) comprenden un láser configurado para producir un flujo óptico, un modulador de polarización configurado para modular el flujo óptico a fin de codificar datos en al menos dos bases de polarización ortogonales, un sistema de control de polarización configurado para transformar el flujo óptico modulado de manera que el flujo óptico modulado se envía a una salida del transmisor en las bases de polarización de salida diferentes a las asociadas con la modulación de polarización, y un atenuador variable configurado para aplicar una atenuación variable al flujo óptico de manera que los datos también se codifiquen en dos o más estados de señuelo, cada estado de señuelo corresponde a un valor predeterminado para un número promedio de fotones. Una entrada de modulación de

polarización puede acoplarse al sistema de control de polarización y configurarse para seleccionar la base de salida del transmisor.

En algunos ejemplos, los dos o más estados de señuelo comprenden un estado de vacío, un primer estado correspondiente a un número de fotones promedio menor que 1 y un segundo estado correspondiente a un número de fotones promedio menor que el número de fotones promedio del primer estado. Las bases de polarización pueden seleccionarse entre (R, L), (H, V) y (D, A). En algunos ejemplos, el atenuador variable es un primer atenuador variable y el sistema de modulación de polarización comprende al menos un segundo atenuador variable configurado para generar pulsos brillantes para la calibración de la polarización a una frecuencia predeterminada. El modulador de polarización, el atenuador variable y el láser pueden construirse sobre un sustrato de silicio para formar parte de un circuito CMOS.

En algunas implementaciones, los transmisores de QC también comprenden un detector de fotones, un divisor de guía de ondas y un sistema de control de estado de señuelo. El divisor de la guía de ondas se posiciona para recibir el flujo óptico corriente abajo del atenuador variable, y se configura para dirigir una primera porción del flujo óptico recibido al detector de fotones de acuerdo con una relación de división predeterminada y para dirigir una segunda porción del flujo óptico recibido hacia la salida del transmisor. El sistema de control de estado señuelo se acopla al detector de fotones y al atenuador variable y se configura para controlar la atenuación aplicada por el atenuador variable en función de la relación de división predeterminada y las mediciones realizadas por el detector de fotones de la primera porción del flujo óptico. En algunos ejemplos, el modulador de polarización, el atenuador variable, el láser y el detector de fotones se integran en un solo chip. El modulador de polarización y el atenuador variable pueden construirse en silicio mediante el uso de procesos CMOS, o en sustratos sin silicio. El láser y el detector de fotones pueden construirse sobre sustratos sin silicio y pueden colocarse en un circuito CMOS, o el láser y el detector de fotones pueden construirse sobre silicio.

Los receptores de QC comprenden un primer detector asociado con un SOP en una primera base y un segundo detector asociado con un SOP es un conjugado de segunda base para la primera base. Un sistema de modulación de polarización se configura para modular selectivamente un flujo óptico recibido que tiene el SOP en la primera y la segunda base para dirigir los componentes correspondientes del flujo óptico en cada uno de los primeros y segundos SOP al primer y al segundo detector correspondientes, respectivamente, de esta manera, se mapean los SOP recibidos en los SOP de la primera y la segunda base. En ejemplos típicos, las bases de polarización se seleccionan entre (R, L), (H, V) y (D, A). Un sistema de detección de estado de señuelo se configurado para estimar la transmitancia del fotón único del flujo óptico en base a las mediciones del detector de fotones del flujo óptico.

El sistema de detección de estado de señuelo puede acoplarse al primer y al segundo detector para recibir una señal de detección de fotones de cada uno de los detectores. El sistema de detección de estado de señuelo puede configurarse para generar distribuciones de fotones para el flujo en función de las señales de detección de fotones, donde cada distribución de fotones se caracteriza por un número promedio de fotones. El sistema de detección de estado de señuelo puede configurarse para comparar las distribuciones de fotones que tienen diferentes números de fotones promedio respectivos y para determinar una secuencia de bits en base a la comparación. Una de las distribuciones de fotones puede corresponder a un estado de vacío y el sistema de detección de estado de señuelo puede configurarse para estimar eventos de fondo del primer y el segundo detector en función de la distribución de fotones de estado de vacío.

Los métodos de QC comprenden recibir un flujo óptico que se codifica por polarización de acuerdo con al menos dos bases ortogonales y que se asocia con al menos dos estados de señuelo. Los estados de polarización del flujo recibido se ajustan para producir un estado de polarización en cada una de las bases ortogonales, y el flujo se decodifica dirigiendo el flujo en el estado de polarización producido a un detector asociado. Los eventos de detección de fotones producidos por el flujo que se asocian con uno de al menos dos estados de señuelo se comparan con los eventos de detección de fotones producidos por el flujo que se asocian con otro de al menos dos estados de señuelo. Una transmisión de fotón único del flujo óptico se estima en base a la comparación. En algunos ejemplos, el flujo recibido se asocia con al menos dos bases ortogonales conjugadas.

En algunas implementaciones, los métodos de QC también comprenden estimar cuál de los eventos de detección de fotones corresponde a señales de fotón único y seleccionar una secuencia de bits mediante el uso de las señales de fotón único. Los métodos de QC pueden comprender generar distribuciones de fotones a partir de los eventos de detección de fotones, en donde la estimación de la transmitancia del fotón único se basa, al menos en parte, en las distribuciones de fotones.

Los métodos comprenden aplicar una modulación de amplitud a un flujo óptico en base a un flujo de datos de entrada de acuerdo con dos o más estados de señuelo predeterminados para producir un flujo óptico de estado señuelo, y aplicar una modulación de polarización al flujo óptico en base al flujo de datos de entrada para producir un flujo óptico modulado por polarización asociado con estados conjugados de polarización (SOP) seleccionados de al menos dos bases ortogonales, en donde las bases ortogonales se seleccionan para compensar al menos parcialmente la birrefringencia de transmisión. El flujo óptico modulado por polarización puede codificarse en estados de fase de un Mach-Zehnder. El flujo óptico de estado de señuelo modulado por polarización se transmite a un receptor. Los SOP pueden seleccionarse de manera que un flujo óptico recibido tenga estados de polarización en forma rectilínea, diagonal o circular. En ejemplos típicos, la birrefringencia de transmisión se asocia con la propagación en una fibra óptica.

En algunos ejemplos, la modulación de polarización se asocia con SOP seleccionados de tres bases ortogonales que corresponden a cuatro SOP equidistantes en un gran círculo en la esfera de Poincaré y dos intersecciones de un eje del gran círculo y la esfera de Poincaré. En otros ejemplos, la modulación de polarización se aplica modulando el flujo óptico en las bases iniciales y luego aplicando una modulación de polarización para producir los estados de polarización en al menos dos bases. La aplicación de la modulación de amplitud al flujo óptico puede ser de acuerdo con tres estados de señuelo predeterminados. Los estados señuelo pueden comprender un estado de vacío, un primer estado correspondiente a un número de fotones promedio menor que 1 y un segundo estado correspondiente a un número de fotones promedio menor que el número de fotones promedio del primer estado. La aplicación de la modulación de amplitud puede comprender asignar uno de los dos o más estados de señuelo a cada pulso del flujo óptico.

Los transmisores comprenden un láser configurado para producir un flujo óptico que comprende pulsos de fotón múltiple y único y un modulador de amplitud configurado para modular la amplitud del flujo óptico para asociar los pulsos del flujo óptico con un número promedio de fotones seleccionado entre dos o más estados de señuelo predeterminados. Un modulador de fase o polarización se configura para modular el flujo óptico para asociar los pulsos del flujo óptico con un estado de polarización seleccionado de al menos dos bases de polarización ortogonales. Un detector de fotones y un divisor de guía de onda se posicionan para recibir el flujo óptico corriente abajo desde el modulador de fase y la lógica de control de estado de señuelo. El divisor se configura para dirigir una primera porción del flujo óptico recibido al detector de fotones de acuerdo con una relación de división predeterminada y para dirigir una segunda parte del flujo óptico recibido hacia una salida del transmisor. La lógica de control del estado de señuelo se acopla al detector de fotones y al modulador de fase y se configura para controlar la atenuación aplicada por el modulador de amplitud en base a la relación de división predeterminada y las mediciones realizadas por el detector de fotones de la primera porción del flujo óptico.

El láser, el modulador de amplitud, el modulador de fase, el detector de fotones, el divisor de guía de ondas y la lógica de control del estado de señuelo pueden acoplarse a un sustrato para formar un transmisor a escala de chip. El modulador de fase, el modulador de amplitud y el divisor de guía de onda pueden construirse sobre un sustrato de silicio para formar parte de un circuito CMOS, o sobre sustratos que no sean de silicio. El láser y el detector de fotones pueden construirse en sustratos sin silicona y pueden colocar en un circuito CMOS, o se pueden construir en sustratos de silicio usando procesos CMOS.

Los anteriores y otros objetos, características y ventajas de la tecnología descrita se harán más evidentes a partir de la siguiente descripción detallada, que procede con referencia a las figuras adjuntas.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques de un transceptor de comunicación cuántica generalizada (QC).
La Figura 2 es un diagrama de bloques de una implementación de ejemplo de un receptor codificado por polarización.
La Figura 3 es un diagrama de bloques de un transmisor de codificación de polarización representativo.
La Figura 4 es un diagrama de bloques de una implementación de ejemplo de un transmisor de QC.
La Figura 5 es un diagrama de bloques de una implementación de fibra de ejemplo de un receptor codificado por polarización.
La Figura 6 es un diagrama de bloques de un método representativo del lado del transmisor.
La Figura 7 es un diagrama de bloques de una implementación de ejemplo de un transmisor de estado señuelo.
La Figura 8 es un diagrama de bloques de otra implementación de ejemplo de un transmisor de estado señuelo.
La Figura 9 es un diagrama de bloques de una implementación de ejemplo de un sistema de estado de señuelo.
La Figura 10 es un diagrama de bloques de una implementación de ejemplo de un transmisor de estado señuelo.
Las Figuras 11 y 12 son diagramas de entornos operativos de ejemplo en los que las claves se adquieren a través de QC, se difunden y se usan para el cifrado, la autenticación y el control de acceso.
La Figura 13 es una ilustración de un ejemplo de un módulo transmisor microóptico de QC.
Las Figuras 14 y 15 son ilustraciones de ejemplos de módulos transmisores microópticos integrados de estado de señuelo.
La Figura 16 es un diagrama de bloques de una implementación a escala de chip de ejemplo de un transmisor de estado señuelo.
La Figura 17 es un diagrama de bloques de un método del lado del transmisor para generar un flujo óptico de estado de señuelo codificado por polarización.

Descripción detallada

Como se usa en esta solicitud y en las reivindicaciones, las formas en singular “un”, “una”, y “el/la” incluyen las formas en plural a menos que el contexto establezca claramente lo contrario. Adicionalmente, el término "incluye" significa "comprende". Además, el término "acoplado" no excluye la presencia de elementos intermedios entre los elementos acoplados.

Los sistemas, aparatos y métodos descritos en la presente descripción no deben interpretarse como limitantes de ninguna manera. En su lugar, la presente descripción se dirige a todas las características y aspectos nuevos y no obvios de las diversas modalidades descritas, solo y en diversas combinaciones y subcombinaciones entre sí. Los sistemas, métodos y aparatos descritos no se limitan a ningún aspecto o característica específica o combinaciones de los mismos, ni los sistemas, métodos y aparatos descritos requieren que una o más de las ventajas específicas estén presentes o que se

resuelvan los problemas. Cualquier teoría de operación debe facilitar la explicación, pero los sistemas, métodos y aparatos descritos no se limitan a tales teorías de operación.

Aunque las operaciones de algunos de los métodos descritos se describen en un orden secuencial particular para una presentación conveniente, debe entenderse que esta forma de descripción abarca la reordenación, a menos que el lenguaje específico que se expone a continuación requiera un orden particular. Por ejemplo, las operaciones descritas secuencialmente pueden, en algunos casos, reordenarse o realizarse al mismo tiempo. Además, por razones de simplicidad, las figuras adjuntas pueden no mostrar las diversas formas en que los sistemas, métodos y aparatos descritos pueden usarse junto con otros sistemas, métodos y aparatos. Además, la descripción a veces usa términos como "producir" y "proporcionar" para describir los métodos descritos. Estos términos son abstracciones de alto nivel de las operaciones reales que se realizan. Las operaciones reales que corresponden a estos términos variarán en dependencia de la implementación particular y son fácilmente perceptibles por un experto en la técnica.

Para mayor comodidad en la siguiente descripción, los estados lineales seleccionados de polarización (SOP) se denominan rectilíneos horizontales, rectilíneos verticales, diagonales y antidiagonales con respecto a un sistema de coordenadas XYZ en el que una dirección de propagación de un haz óptico es a lo largo de un eje Z. Los SOP rectilíneos horizontales y verticales son polarizaciones lineales ortogonales que se encuentran a lo largo de un eje + X y un eje + Y, respectivamente. Por conveniencia, estas pueden denominarse polarizaciones "H" y "V", respectivamente. La polarización diagonal ("D") y una polarización antidiagonal ("A") son polarizaciones lineales ortogonales que se orientan a lo largo de un eje girado 45 grados desde el eje + X hacia el eje + Y, y orientadas a lo largo de un eje girado 45 grados desde el eje + X hacia el eje - Y, respectivamente. Los pares de polarización H, V y D, A forman las bases de polarización respectivas referidas por conveniencia como una base rectilínea y una base diagonal. La base rectilínea es una "base ortogonal", denominada así porque los estados de polarización que forman la base (los estados de polarización H y V) son ortogonales. Igualmente, la base diagonal es una "base ortogonal", denominada así porque los estados de polarización que forman la base (los estados de polarización D y A) son ortogonales. Las bases rectilíneas y diagonales son ejemplos de las denominadas "bases conjugadas". En otras palabras, los SOP que forman la base rectilínea (H, V) se conjugan con los SOP que forman la base diagonal (D, A). Es decir, la medición de un SOP seleccionado de cualquiera de las bases aleatoriza la medición de un SOP seleccionado de la otra base.

Será evidente que los SOP y las bases de polarización descritos anteriormente son solo SOP y bases representativas, y pueden seleccionarse otros SOP y bases mediante el uso de otras polarizaciones lineales, polarizaciones circulares o polarizaciones elípticas. Por ejemplo, puede usarse una base circular que consiste en polarizaciones circulares izquierda y derecha (L, R). Esta base circular es también una "base ortogonal" ya que los estados de polarización L y R son ortogonales. Se selecciona cualquier sistema de coordenadas particular para una descripción conveniente, y pueden usarse otras coordenadas. En la siguiente descripción, los ejes y orientaciones de las placas de onda (placas de retardo o retardadores) u otros componentes ópticos dependientes de la polarización pueden describirse con respecto a este mismo sistema de coordenadas.

Los SOP pueden describirse convenientemente dentro de un sistema de coordenadas tridimensional en base a la esfera de Poincaré en la que las polarizaciones lineales se representan por puntos en un plano XY, y se representan la polarización circular derecha (RCP) y la polarización circular izquierda (LCP) como puntos situados en la parte superior e inferior (es decir, los polos) de la esfera de Poincaré. Otros puntos en la esfera de Poincaré representan polarizaciones elípticas.

Como se discutió anteriormente, los sistemas de QC a menudo se basan en la transmisión y detección de flujos ópticos modulados por polarización que tienen SOP en dos bases conjugadas. Dichos SOP pueden representarse en la esfera de Poincaré como 4 puntos equidistantes en un gran círculo. Las selecciones básicas comunes de H, V y D, A corresponden a 4 puntos equidistantes en un plano ecuatorial; la selección básica H, V y R, L corresponde a 4 puntos de equidistancia en un plano vertical que incluye polos de la esfera de Poincaré. La fibra óptica a menudo introduce una significativa birrefringencia variable en el tiempo, de manera que un flujo óptico modulado de base dual recibido de una fibra óptica puede incluir SOP correspondientes a cuatro puntos equidistantes en un gran círculo en la esfera de Poincaré, pero diferentes de los del transmisor. La fibra de birrefringencia hace girar el gran círculo asociado con las bases de polarización transmitidas, pero los SOP recibidos permanecen separados en un gran círculo que tiene una rotación arbitraria con respecto a las bases de polarización.

Mientras que la QC generalmente se basa en cuatro SOP de dos bases ortogonales conjugadas, un SOP de cada una de las bases es suficiente para definir un gran círculo. Por ejemplo, un SOP H de una base H, V y un SOP A de una base A, D son adecuados para definir un gran círculo. En la decodificación, el mapeo de un SOP recibido de una primera base transmitida a un primer detector predeterminado SOP de una base de primer detector se asocia con el mapeo del segundo SOP ortogonal recibido al segundo SOP de la base de primer detector. Además, los SOP recibidos asociados con una segunda base (una base conjugada) se asignan de manera similar a los SOP de la segunda base. Con cuatro SOP equidistantes en un gran círculo en la esfera de Poincaré, una sola rotación de magnitud adecuada sobre un eje adecuado asigna los cuatro SOP a los SOP equidistantes en cualquier gran círculo. Por ejemplo, los SOP ortogonales en cada una de las dos bases conjugadas pueden asignarse a cualquier par de bases L, R o H, V o A, D. En algunos esquemas, pueden usarse SOP de tres o más bases ortogonales conjugadas, y estas bases pueden mapearse de manera similar.

*Componentes representativos del sistema de QC*

Como se muestra en la Figura 1, un transmisor/receptor QC representativo incluye una pluralidad de módulos ópticos o elementos ópticos 110 adaptados para la comunicación óptica en el espacio libre. Los módulos ópticos 110 transmiten información binaria para la cual se mide la modulación del estado cuántico (mediante un receptor de QC). Los módulos ópticos 110 también pueden proporcionar un transceptor de red adaptado para transmitir y recibir información en un canal público a través de la fibra óptica, transmitiendo y recibiendo información binaria para la cual la modulación del estado cuántico no es medida por un receptor de QC.

Entre los módulos ópticos 110, el láser y el modulador con electrónica de controlador 112 incluyen un láser adaptado para generar fotones para la transmisión de QC y un modulador adaptado para modular el estado cuántico (*por ejemplo,* estado de polarización) de salida del láser. El modulador se acopla ópticamente al láser y puede implementarse, por ejemplo, con un modulador de niobato de litio que modula el estado de polarización entre 0°, 45°, 90° y -45°, correspondiendo típicamente a una o más bases de polarización conjugadas. Alternativamente, el modulador se implementa con otro tipo de modulador de cristal integrado u óptico integrado. La elección del modulador es específica de la implementación y puede depender, por ejemplo, de la idoneidad del modulador para la longitud de onda específica de la luz del láser, la frecuencia de operación del modulador y/o la pureza de estado para los estados de polarización producidos. En algunas implementaciones, se proporcionan láseres para cada estado de polarización.

El atenuador óptico variable 114 se acopla ópticamente al láser. El atenuador se adapta para reducir los fotones por pulso del láser, lo que mejora la seguridad del QC al frustrar los intentos de espionaje que interceptan fotones adicionales. El fotodiodo de avalancha del monitor ("APD") 117 está dividido de otros módulos por el divisor de fibra óptica 116 y se adaptado para medir el número de fotones por pulso del láser usado para la QC. Por ejemplo, el APD 117 se implementa con uno o más detectores de fotones InGaAs. El APD 117 proporciona información usada para controlar el láser y el atenuador 114 para la QC. Otro detector (no mostrado) recibe información como un receptor de fibra óptica convencional para comunicación no cuántica.

El procesador/matriz de compuerta programable en campo ("FPGA") con la lógica de protocolo 120 controla diferentes operaciones como parte de la QC. En particular, el procesador/FPGA 120, que se acoplado eléctricamente al módulo 112, se configura para coordinar las operaciones del láser y el modulador a través de la electrónica del controlador incluida con el láser y el modulador 112. Un generador de números aleatorios genera una serie de bits aleatorios para números aleatorios de alta calidad. Con el control de polarización de alta fidelidad, el procesador/FPGA 120 controla la polarización de los fotones con el modulador para codificar bits aleatorios como diferentes estados de polarización de acuerdo con un protocolo de QC. El procesador/FPGA 120 controla el número de fotones por pulso (medido con el APD 117) para la QC. A través del control del láser y el atenuador óptico variable 114, el procesador/FPGA 120 puede reducir selectivamente los fotones por pulso del láser a un nivel promedio de un fotón único por pulso u otro nivel promedio predeterminado (*por ejemplo* estado de señuelo).

El procesador/FPGA 120 controla la sincronización y el patrón de los pulsos de fotones producidos por el láser para la QC. El procesador/FPGA 120 también controla el tiempo y los pulsos de los pulsos de mayor potencia (los denominados pulsos "brillantes") producidos para la sincronización, la comunicación no cuántica y/u otros fines.

Para otros aspectos del protocolo de QC, el procesador/FPGA 120 controla las operaciones asociadas con el registro del estado cuántico y la base de envío por impulso para la QC, la transmisión de las bases de envío registradas y, de cualquier otra manera, el procesamiento de los elementos del protocolo de QC convencionales. El procesador/FPGA 120 puede coordinar las operaciones para la amplificación de la privacidad y los estados de señuelo para mejorar aún más la seguridad. La amplificación de la privacidad reduce la longitud de una cadena de bits compartida (por ejemplo, mediante el hashing con una función hash) para reducir la información parcial que un intruso podría haber ganado. La longitud final de la cadena puede establecerse en dependencia de la cantidad de errores detectados. En algunos ejemplos, la fuente es una fuente de fotón único. Sin embargo, también pueden usarse fuentes de fotón único imperfectas, como fuentes de láser débiles. Los estados de señuelo o pulsos que tienen diferentes números de fotones promedio pueden transmitirse con fuentes imperfectas, de manera que la tasa de error y el número de pulsos de fotón único en una cadena de bits pueden determinarse y usarse para regular el grado de amplificación de la privacidad.

La memoria 122 almacena una o más teclas. Por ejemplo, la memoria 122 almacena claves cuánticas. En algunas implementaciones, la memoria 122 es una memoria segura y las claves se almacenan en forma cifrada. La memoria 122 puede fabricarse junto con los módulos ópticos integrados 110 o colocarse por separado.

El lector biométrico 140 es un escáner u otro módulo adaptado para aceptar marcas biométricas de un usuario. Por ejemplo, el lector biométrico 140 es un escáner de huellas dactilares. El procesador/FPGA 120 puede incluir una lógica para cifrar las marcas biométricas con una clave almacenada en la memoria segura 122. O bien, uno o más módulos de cifrado (no mostrados) pueden proporcionar dicha funcionalidad de cifrado.

La pantalla táctil 150 acepta la entrada del usuario (*por ejemplo,* a un teclado numérico) que puede cifrarse junto con las marcas biométricas como parte de la autenticación del usuario. La pantalla táctil 150 también muestra información al usuario (*por ejemplo,* un recuento de claves cuánticas en la memoria 122, un aviso para contactar a una autoridad

confiable para hacer claves cuánticas, un aviso para iniciar una comunicación segura con otro o un aviso para otra función y acepta la entrada del usuario.

Fuera de los módulos ópticos integrados 110, la mayoría de los módulos funcionales pueden implementarse con componentes estándar para dispositivos portátiles o no portátiles. Entre los módulos ópticos integrados 110, muchos de los módulos (*por ejemplo,* el atenuador 114), el monitor APD 117, el divisor 116 y el receptor codificado con polarización 118 pueden implementarse con componentes estándar para la comunicación por fibra óptica u óptica a granel. Otros módulos funcionales (*por ejemplo,* FPGA) pueden implementarse con componentes de control que se han usado con transmisores de QC convencionales para: (1) producir estados de polarización específicos con un modulador de fibra óptica; (2) regular la producción de QC cronometrada exacto y pulsos brillantes en un patrón conocido disciplinado con GPS 190 (no se muestra) o un oscilador o reloj atómico, para que la autoridad confiable rastree el tiempo y las variaciones de tiempo cuando se realiza la QC; (3) monitorear el número promedio de fotones por pulso mediante el uso del sistema de temporización y el APD 117; (4) controlar la polarización de APD, la activación y la electrónica discriminadora; (5) procesar elementos de control de protocolo de QC convencionales, *por ejemplo,* para rastrear, corregir e intercambiar información de estado de polarización. El receptor 118 se configura para entregar bits codificados como un estado particular de polarización a un detector correspondiente. Para la QC que usa dos bases conjugadas, se proporcionan cuatro detectores D1-D4, o se cambia la luz entre las bases y solo se proporcionan dos detectores.

*Transmisores/receptores de codificación de polarización representativos*

En los ejemplos típicos, las unidades receptoras/transmisoras se configuran para enviar y recibir datos convencionales, pero los receptores y transmisores representativos se describen por separado a continuación para una ilustración conveniente. En algunos ejemplos, la transmisión cuántica es unidireccional, y un transmisor cuántico (y ningún receptor cuántico) se configura para transmitir a un receptor cuántico remoto sin un transmisor cuántico. Si bien en algunos ejemplos se muestran elementos ópticos a granel, pueden usarse ópticas basadas en fibra, tales como los divisores de potencia de fibra óptica y las lentes externas y los componentes a granel no son necesarios.

Un receptor codificado por polarización representativo 200 que separa los estados de polarización de las bases D, A y R, L (u otras bases) se ilustra en la Figura 2. Un primer controlador de polarización 202 se sitúa para recibir un flujo óptico de entrada codificado por polarización y dirigir un flujo óptico modulado a un divisor de haz no polarizador (NPBS) 204. El controlador de polarización 202 puede implementarse como una serie de exprimidores piezoeléctricos situados alternativamente a 0 y 45 grados a lo largo de una longitud de fibra óptica. En general, se proporcionan al menos tres o cuatro exprimidores, de manera que pueden proporcionarse retardos de fase variables a lo largo de ejes alternos. Dicho dispositivo puede convertir cualquier SOP en cualquier otro SOP en dependencia de los voltajes de control de entrada. Una primera parte del flujo codificado y modulado se dirige a un segundo controlador de polarización 206 y al primer divisor de haz de polarización (PBS) 208. El PBS 208 transmite un componente del flujo óptico en un estado lineal de polarización a un detector 216 (D3) y un componente en un SOP ortogonal lineal a un detector 218 (D4), con los componentes mostrados en la Figura 2 correspondientes a los SOP R, L, respectivamente. Una segunda parte del flujo codificado y modulado se dirige desde el NPBS 204 a un segundo PBS 210, de manera que los componentes lineales ortogonales del flujo codificado y modulado se dirigen a los detectores 220, 221 (D1, D2), con los componentes mostrados en la Figura 2 como los SOP A, D, respectivamente.

Un detector/amplificador detector se acopla a los detectores D1-D4 y a un controlador modulador 234 y un procesador de detección cuántica 236. El controlador del modulador 234 se configura para establecer modulaciones adecuadas de manera que cada uno de los detectores D1-D4 reciba un estado de polarización seleccionado de una de las dos bases. Por ejemplo, D1 y D2 se acoplan para recibir SOP lineales (A, D), y D3 y D4 se acoplan para recibir SOP circulares (R, L). En ejemplos típicos, la detección de QC usa un conjunto adicional de cuatro detectores lineales, para permitir la corrección de la birrefringencia de la fibra y los componentes de control de polarización asociados, pero estos no se muestran en la Figura 2. Los moduladores de polarización pueden ser dispositivos de guía de onda, moduladores electro ópticos a granel o controladores de polarización basados en piezoeléctricos. Los cambios de birrefringencia en las fibras ópticas son lo suficientemente lentos en algunos casos, por lo que no se requiere una modulación de polarización de alta velocidad, pero el ancho de banda de modulación de polarización en un receptor tiende a depender de la implementación. El receptor de la Figura 2 se basa en dos bases de polarización predeterminadas.

El receptor 200 de la Figura 2 puede operarse de la siguiente manera, en el cual los períodos de tiempo de QC se alternan con los períodos de calibración en los que se usan flujos ópticos de mayor potencia (flujos "brillantes"). En un ejemplo, el receptor 202 se configura para dirigir los componentes de un flujo óptico de entrada en A, D, R, L SOP (mediante el uso de bases diagonales y circulares) a los detectores D1, D2, D3, D4, respectivamente. En respuesta a un flujo óptico "brillante" en un primer SOP, por ejemplo, un SOP A, el controlador modulador 202 ajusta el controlador de polarización para maximizar sustancialmente el flujo óptico recibido en el detector D1. En respuesta a un flujo óptico "brillante" en un SOP D con la misma modulación aplicada por el controlador 202 de polarización, el flujo óptico en el detector D1 se minimiza sustancialmente y el flujo óptico en el detector D2 se maximiza sustancialmente. Con este ajuste del modulador 202, los estados de polarización A, D pueden decodificarse apropiadamente. En respuesta a un flujo óptico "brillante" en un SOP de la segunda base, tal como un SOP R, el controlador de polarización 206 se ajusta (con el controlador de polarización 202 establecido como se describió anteriormente) de manera que el flujo óptico en el detector D3 se maximice. Con las modulaciones de los controladores de polarización 202, 206 fijas, cada uno de los detectores D1-D4

recibe porciones de flujo óptico en SOP predeterminados. Se apreciará que un SOP A se dirige al detector D1 en el mismo ajuste de control que el SOP D se dirige al detector D2 porque las polarizaciones transmitidas permanecen opuestas en un gran círculo en la esfera de Poincaré, independientemente de cualquier birrefringencia a lo largo de la trayectoria entre el transmisor y el receptor. Cualquier rotación en la esfera de Poincaré que devuelve la modulación A transmitida a una modulación A en el detector devuelve la óptica modulada D; flujo al SOP D. De manera similar, ajustar un controlador para que el SOP R transmitido se dirija a un detector D3 necesariamente dirige el SOP L transmitido al detector D4, ya que estos SOP se encuentran en una posición opuesta en la esfera de Poincaré.

Con referencia a la Figura 3, un transmisor de codificación de polarización 300 incluye un láser 302 que produce un flujo óptico que se dirige a un modulador de amplitud 304 y un controlador de polarización 306 a través de un retardador de media onda 303. Si se usa un controlador de polarización total, este retardador puede omitirse. El modulador de amplitud 304 se configura para controlar un número medio de fotones por bit en la QC para que sea un número predeterminado de fotones, típicamente un número entre cero y uno, atenuando el flujo óptico del láser. Además, el modulador de amplitud 304 se configura para proporcionar sustancialmente menos atenuación en la transmisión de las llamadas "ráfagas brillantes" para uso en un receptor para corregir los cambios de polarización en la propagación. La modulación de polarización cuántica se aplica al flujo óptico mediante un controlador de polarización 306 y el flujo modulado se dirige a la óptica de salida 308 para el acoplamiento a una fibra óptica u otro medio de transmisión. Una porción del flujo óptico se dirige por un reflector 309 a un polarímetro 310 que se configura para determinar uno o más SOP en el flujo óptico. Un controlador 312 se acopla a la polarización modular 306, al modulador de amplitud 304 y al polarímetro 310 para ajustar la modulación de polarización para que se corresponda con las bases seleccionadas. Además, el controlador 312 puede ajustar el modulador de amplitud 304, así como también recibir y almacenar en buffer los datos que van a transmitirse desde una fuente de datos 314. Mientras que el controlador de polarización 306 puede implementarse de varias maneras, para la codificación de polarización de alta velocidad puede usarse un convertidor TE/TM de guía de onda tal como un dispositivo $LiNBO_3$. El retardador 303 se ajusta para proporcionar polarizaciones TE y TM aproximadamente iguales en el controlador de polarización 306, y el controlador puede variar el voltaje aplicado para que la salida SOP se varíe a lo largo de un gran círculo en la esfera de Poincaré que pasa a través de los polos. Si se desea, puede usarse un modulador de polarización que permita asignar cualquier SOP de entrada a cualquier SOP de salida y el retardador 303 sería innecesario. Los voltajes correspondientes a los SOP A, D, R, L se usan para la modulación de datos. En algunos casos, se proporciona una entrada 320 para que un receptor remoto pueda especificar bases de polarización adecuadas para la modulación en el transmisor 300, de manera que el flujo óptico recibido esté en las bases definidas en el receptor.

Con referencia a la Figura 4, un transmisor 400 acoplado a fibra incluye un láser 402 que dirige un flujo óptico a un aislador 404 y un retardador 408 de onda media. Un modulador de fase 410 recibe el flujo óptico desde el retardador 408 y dirige un flujo modulado por polarización a una fibra 412 en base a datos de una fuente de datos 414. El modulador de fase 410 sirve como un retardador de voltaje variable, con un eje fijo y puede proporcionarse como un dispositivo de guía de onda óptico integrado (por ejemplo, un dispositivo GaAs) que produce diferencias de fase dependientes del voltaje en polarizaciones TE y TM. El modulador de fase 410 se configura para modular un flujo óptico de entrada para proporcionar una salida codificada de polarización en cualquiera de los cuatro SOP de dos bases conjugadas, una base (A, D) y una base (R, L) como se muestra en la Figura 4. Normalmente, los voltajes de activación del modulador necesarios para producir los SOP seleccionados se determinan en un procedimiento de calibración en el que la tensión de activación del modulador varía mientras que el SOP resultante se evalúa con un polarímetro. Para una salida acoplada de fibra, el SOP de salida del modulador se mide después de que la fibra interviene introduciendo cierta birrefringencia. El retardador se configura correctamente para el sistema con un modulador monofásico cuando la exploración del modulador de fase produce un gran círculo en la esfera de Poincaré. Luego pueden elegirse cuatro SOP separados en el gran círculo para dos bases ortogonales conjugadas.

Con referencia a la Figura 5, un receptor de polarización 500 incluye un primer controlador de polarización 501 tal como un modulador óptico integrado que se conecta a un acoplador de fibra 502. El acoplador de fibra 502 es independiente de la polarización y dirige una porción del flujo óptico recibido a un acoplador de fibra dependiente de la polarización 506 que entrega componentes de polarización ortogonales a los detectores SOP L, R correspondientes en el módulo detector 508. El acoplador de fibra 502 también dirige una porción del flujo óptico recibido a un controlador de polarización 510 y un acoplador de fibra dependiente de la polarización 512 que entrega componentes de polarización ortogonales a los detectores SOP D, A correspondientes en el módulo detector 514. Un controlador 520 proporciona voltajes de accionamiento adecuados para los controladores de polarización 501, 510. Cuando se ajusta apropiadamente, se recibe un L SOP en un detector L correspondiente, no se recibe en un detector R y se recibe a ½ amplitud (igualmente) en los detectores A, D. Otros SOP se dirigen de manera similar. En general, un primer SOP en una primera base se dirige preferentemente a un detector asociado con el primer SOP y la primera base, y no a un detector asociado con un segundo SOP en la primera base. Este primer SOP de la primera base se dirige igualmente a los detectores asociados con la segunda base.

En los ejemplos anteriores, el receptor incluye cuatro detectores (uno para cada SOP de dos bases conjugadas), pero, en otros ejemplos, solo se usa un detector para cada base. Por ejemplo, si se aplica una modulación de manera que un SOP lineal, como un SOP H, se dirija a un primer detector, generalmente se dirige necesariamente un SOP V para que esté disponible para un segundo detector que no necesita ser suministrado. Además, mientras que la corrección de polarización puede aplicarse en un receptor como se muestra arriba, pueden proporcionarse correcciones de polarización similares en un transmisor, o pueden distribuirse entre el transmisor y el receptor.

Un método del lado del transmisor representativo se ilustra en la Figura 6. En 602, se seleccionan una o más bases de polarización conjugadas para compensar la birrefringencia medida o esperada en la transmisión. En 604, un flujo óptico se modula (codifica) con respecto a estas bases, y en 606, se transmite el flujo óptico modulado. En algunos ejemplos, las bases se seleccionan de manera que después de la transmisión, el flujo modulado por polarización sea en una o más de una base rectilínea, una base diagonal o una base circular.

*Sistemas de QC de estado de señuelo representativos*

Para los sistemas de QC que carecen de una verdadera fuente de fotón único, como los sistemas que usan fuentes de láser débiles, los estados de señuelo pueden proporcionar una mayor seguridad. Las fuentes de láser débiles pueden ser ventajosas sobre las fuentes de fotón único debido a su menor costo y menor tamaño. Sin embargo, debido a que las fuentes de láser débiles producen algunos pulsos de fotón múltiple, las transmisiones de QC pueden ser menos seguras. Estas fuentes emiten fotones de acuerdo con una distribución de Poisson con un número promedio de fotones de μ. Algunos pulsos no contienen fotones, algunos pulsos contienen un fotón único, mientras que otros pulsos contienen dos o más fotones. Las fuentes que emiten pulsos con más de un fotón son susceptibles a ataques de división de números de fotones (PNS) cuando se usan para la QC. Durante un ataque PNS, un intruso intercepta la QC y elimina uno de los fotones de los pulsos de fotón múltiple. El intruso oculto almacena el fotón eliminado hasta que el receptor previsto anuncie la base seleccionada para la medición. Esta información puede transmitirse a través del canal público cuando se intercambian registros entre el transmisor y el receptor. A continuación, el intruso mide el fotón en la misma base y aprende el valor del bit sin introducir ningún error en la QC. De esta manera, el intruso puede potencialmente obtener un conocimiento completo de la serie de bits (claves) compartidos entre el receptor y el transmisor sin ser detectado.

Para reducir el riesgo de ataques PNS y aumentar la seguridad, la velocidad de los pulsos de fotón múltiple debe reducirse, por ejemplo, reduciendo el número medio de fotones, μ, para la fuente del láser. Sin embargo, la reducción de μ puede aumentar las tasas de error porque la proporción de recuentos oscuros del detector probablemente también aumentará. El riesgo de ataques PNS también puede eliminarse sustancialmente mediante el uso de estados de señuelo. Al seguir un protocolo de estado de señuelo, puede colocarse un límite inferior en una transmitancia de un fotón único, incluidas las pérdidas del receptor, y, por lo tanto, en el número de detecciones por el receptor que se originaron a partir de fotones únicos. En consecuencia, puede determinarse el riesgo o la exposición a los ataques PNS, y se mejora la seguridad de la QC.

En un sistema de QC de estado de señuelo, un transmisor produce una señal de QC que alterna entre dos o más valores para μ. Normalmente, a cada bit se le asigna aleatoriamente un valor para μ por el transmisor, y cada valor μ corresponde a un estado de señuelo diferente. Por ejemplo, pueden asignarse diferentes probabilidades a cada valor μ, y las probabilidades pueden representar la probabilidad de generar un estado de señuelo particular. Los estados de señuelo se producen mediante la atenuación controlada de la señal de QC mediante el uso de un modulador de amplitud o un atenuador variable. Para una señal de bit dada, un interlocutor no sabrá qué valor de μ se usó para producir la señal y, por lo tanto, tratará todas las señales de fotón único de la misma manera, independientemente del estado del señuelo. Una vez que la transmisión de QC ha finalizado, el transmisor y el receptor pueden comparar el número de eventos de detección para cada transmisión μ diferente y colocar límites estrictos en la transmitancia de un fotón único del canal. Los estados de señuelo permiten a las partes estimar la probabilidad de que se transmita un pulso de fotón único y, por lo tanto, estimar la seguridad de la QC. La medida en que la transmitancia de un fotón único puede delimitarse también puede depender del tiempo de adquisición o del tiempo dedicado a la recopilación de eventos de detección. Es decir, puede lograrse una mayor tasa de producción de bits secretos aumentando el tiempo de adquisición.

En general, un mayor número de valores μ o niveles diferentes permite una mejor caracterización de los parámetros del canal. Las implementaciones descritas en la presente descripción usan un protocolo de tres niveles de estado de señuelo; sin embargo, también se prevén sistemas con más o menos de tres niveles. En un protocolo de estado de señuelo de tres niveles, un transmisor conmuta entre tres valores para μ: $\mu_0$, $\mu_1$y $\mu_2$. Típicamente, $\mu_0$ corresponde a un valor alto para μ, $\mu_1$ corresponde a un valor moderado, y $\mu_2$ corresponde a un valor bajo. En un sistema de estado de señuelo de tres niveles ilustrativo, $\mu_2$ es aproximadamente igual a cero y $\mu_1 << \mu_0$. En otro ejemplo, los tres valores para μ son aproximadamente 0,5, 0,1 y 0, mientras que en otros ejemplos los valores μ están entre aproximadamente 0,25 y aproximadamente 0,5, entre aproximadamente 0,05 y aproximadamente 0,1, y entre aproximadamente $1 \times 10^{-5}$ y alrededor de $1 \times 10^{-2}$. También pueden usarse otros valores para μ y, por lo general, se seleccionan en función de los parámetros del canal para optimizar el rendimiento. Un estado señuelo que tiene μ sustancialmente igual a cero puede denominarse estado de vacío. La proximidad de μ a cero depende del modulador de amplitud o atenuador usado para producir el estado. Por ejemplo, como un modulador de amplitud tiene una relación de extinción finita, un estado de vacío generado por un modulador de amplitud tiene un valor de μ mayor que cero, tal como aproximadamente el 1,0% de $\mu_0$ o menos. Los estados de vacío pueden usarse para proporcionar una estimación de la probabilidad de detección de fondo y conteos oscuros para un sistema en particular.

Las probabilidades y los valores para μ pueden seleccionarse realizando simulaciones para maximizar la tasa de bits secreta para varios parámetros de canal. Por ejemplo, los valores de μ óptimos o casi óptimos pueden depender de la longitud de la transmisión, como en las longitudes de enlace particulares. Puede encontrarse una discusión adicional de la selección del valor μ, por ejemplo, en Rosenberg y otros, Long-Distance Decoy-State Quantum Key Distribution in

Optical Fiber, Phys. Rev. Lett. 98, 010503 (2007), que se incorpora en la presente descripción como referencia en su totalidad.

El receptor en el sistema de QC en estado de señuelo genera distribuciones de fotones a partir de la señal codificada en estado de señuelo recibida mediante el uso de uno o más detectores sensibles a fotones únicos. El receptor es capaz de distinguir, en base a la distribución de los eventos del detector de fotones, un valor μ para cada estado de señuelo de la QC recibida. El transmisor y el receptor intercambian, generalmente a través de un canal público, información que indica el valor μ asignado a cada bit. Los eventos de detección del receptor deben generar distribuciones que correspondan con los valores de μ seleccionados por el transmisor, de cualquier otra manera se detecta un interceptor. El transmisor y el receptor pueden comparar los eventos de detección para los diferentes valores de μ para estimar la transmitancia de fotón único y para determinar las porciones de bits que provienen de pulsos de fotón único y de fotón múltiple.

En un protocolo de estado de señuelo de tres niveles ilustrativo, un estado de vacío $\mu_2$ se usa primero para proporcionar una estimación de la probabilidad de detección de fondo y conteos oscuros. Una vez que el transmisor le informa al receptor qué señales corresponden a un estado de vacío, el conteo de eventos de detección del receptor para esas señales proporciona una estimación de la probabilidad de detección de fondo y de conteo oscuro. Los niveles de confianza también pueden determinarse a partir de la estimación. A continuación, los eventos de fondo y de conteo oscuro se restan de los eventos de detección para $\mu_1$. Esto proporciona una estimación y niveles de confianza para la transmitancia de fotón único, ya que la mayoría de los eventos restantes son señales de fotón único. Esta estimación puede usarse para determinar el número de eventos $\mu_0$que corresponden a señales de fotón único.

Los protocolos de estado de señuelo pueden usarse junto con cualquiera de los transmisores/receptores de codificación de polarización descritos en la presente descripción.

*Transmisores/receptores de estado de señuelo representativos*

Una implementación de un transmisor de estado de señuelo 700 se ilustra en la Figura 7. Un láser de telecomunicación 710 emite pulsos de fotones que son guiados a través de un aislador 712 y una óptica de acoplamiento 714 a una guía de onda o fibra 716. La guía de onda o fibra 716 transporta los fotones a una fibra óptica 788 acoplada a un conector de fibra 790. El conector de fibra 790 puede ser FC-UPC u otro conector conocido en la técnica. Un detector de telecomunicaciones 718 detecta los fotones recibidos a través del conector de fibra 790 como parte de una comunicación óptica no cuántica convencional.

Un láser cuántico 750 se configura para generar pulsos de fotones para una transmisión de QC. Los pulsos de fotones generados por el láser 750 son guiados a través de un aislador 752 y una óptica de acoplamiento 754 a una guía de ondas 755. La guía de ondas 755 incluye un atenuador 760 que puede usarse para desactivar el láser cuántico 750 de manera efectiva. La guía de ondas 755 también incluye dos atenuadores variables o moduladores de amplitud 762, 764 y un controlador de polarización o modulador de fase 770. Uno de los atenuadores variables 762, 764 es típicamente un atenuador de alta velocidad usado para generar estados de señuelo, mientras que el otro atenuador variable se usa para la calibración de birrefringencia como se explicó anteriormente al producir períodos alternos de flujo "brillante". El atenuador de alta velocidad es lo suficientemente rápido como para generar una señal con diferentes valores de μ para cada pulso o bit, y se configura de acuerdo con un protocolo de estado de señuelo predeterminado. El atenuador de calibración puede ser de alta o baja velocidad, en dependencia de la frecuencia con la que se realice la calibración. Por ejemplo, la calibración puede realizarse cada pocos segundos o cada milisegundo. También pueden incluirse atenuadores adicionales a lo largo de la guía de onda 755 para obtener un nivel de atenuación deseado. El controlador de polarización 770 se configura para aplicar la modulación de polarización cuántica a la señal recibida como se describió anteriormente.

La guía de onda 755 transporta los pulsos de fotones a la fibra óptica 788 acoplada al conector de fibra 790. Los pulsos de fotones luego se transmiten por fibra a uno o más receptores (no mostrados). Sin embargo, en algunas implementaciones, la señal generada por el transmisor 700 se transmite por espacio libre en lugar de por cable de fibra óptica. En la unión de múltiples guías de onda, el circulador 783 dirige la luz de una guía de onda a otra guía de onda en dependencia de la dirección de propagación de la luz. La luz del conector de fibra 790 se envía al detector de telecomunicaciones 718, y la luz del láser de telecomunicaciones 710 o láser cuántico 750 se dirige hacia el conector de fibra 790. El circulador 785 de manera similar dirige la luz de fibra a fibra en dependencia de la dirección de propagación de la luz.

Un controlador 792 con lógica de protocolo controla los atenuadores variables 762, 764 para producir los impulsos codificados en estado de señuelo predeterminado. La lógica de protocolo también controla el controlador de polarización 770 para modular el estado de polarización de los impulsos de estado de señuelo y, de esta manera, producir impulsos codificados de polarización. Los detectores de fotones 782, 784 se acoplan al control de la lógica de protocolo y se usan con fines de retroalimentación de la QC. Los detectores de fotones 782, 784 miden porciones del flujo óptico de QC y se usan para configurar o calibrar el sistema de QC. Por ejemplo, el detector de fotones 782 puede configurarse para determinar uno o más SOP del flujo óptico, y la lógica de protocolo puede usar la retroalimentación del detector de fotones 782 para controlar el controlador de polarización 770 de manera que se realice la modulación de polarización cuántica deseada. Igualmente, el detector de fotones 784 puede configurarse para determinar los valores de μ, y la lógica de protocolo puede usar la retroalimentación del detector de fotones 782 para controlar el atenuador variable de alta velocidad

762 de manera que se produzcan los estados de señuelo deseados. Adicional o alternativamente, el detector de fotones 782 puede usarse para la calibración del sistema y la normalización del láser cuántico 750 para interoperar con el láser de telecomunicaciones 710.

En general, uno o ambos detectores de fotones 782, 784 pueden usarse para evaluar si los pulsos del láser cuántico 750 son pulsos de fotón único o para detectar estados de señuelo. En algunas implementaciones, los detectores 782, 784 son detectores de fotón único capaces de detectar fotones individuales. Por ejemplo, los detectores pueden ser APD, tales como InGaAs o InP APD, que funcionan en modo Geiger. En otros ejemplos, los detectores pueden ser sensores de borde de transición (TES), que son sensibles a la detección de fotón único. El detector también puede ser un diodo PIN que se integra en muchos pulsos.

Sin embargo, los detectores de fotones no necesitan ser detectores de fotón único para determinar los valores de μ si, por ejemplo, se establece una relación de división de guía de onda precisa y predeterminada. Por ejemplo, un divisor de guía de onda 774 puede configurarse para dividir el flujo óptico de manera precisa, de manera que un número predeterminado de fotones continúe hasta el conector de fibra 790 y un número mucho mayor de fotones continúe hasta el detector de fotones 784. En un ejemplo, la relación es de aproximadamente 10,000 a 1, con aproximadamente 10,000 fotones dirigidos al detector de fotones 784 por cada fotón dirigido a la salida del transmisor en el conector de fibra 790. De esta manera, el detector 784 no necesita ser sensible a un fotón único porque los valores de μ pueden determinarse mediante el uso de la señal medida por el detector 784 y la relación de división. En el ejemplo con una relación de división de 10,000 a 1, si el detector 784 midiera un número promedio de fotones de 5000, el valor de μ para la señal de salida sería 0,5. El detector 784 se acopla a la lógica de protocolo y a uno o más de los atenuadores variables 762, 764 para controlar el número de fotones en la señal de salida en base a la señal medida por el detector 784 y la relación de división de la guía de onda predeterminada. La atenuación puede aumentarse si la señal de fotón medida es más grande de lo deseado, o disminuir si la señal es más pequeña de lo deseado. Por lo tanto, el número promedio de fotones en la salida QC puede determinarse por la división de la guía de onda y la medida de la señal por el detector 784, sin la necesidad de detectores sensibles a fotones únicos. Adicional o alternativamente, un divisor 772 puede configurarse de manera similar para dividir el flujo óptico de manera precisa de manera que un número predeterminado de fotones continúe hacia el circulador 783 y un número mucho mayor de fotones continúe hasta el detector de fotones 782.

Los componentes de enfriamiento termoeléctrico (TEC) (no mostrados) pueden usarse para enfriar los láseres 710, 750 y los detectores de fotones 782, 784 a una temperatura de funcionamiento adecuada. Los componentes o calentadores TEC también pueden proporcionar estabilización de la temperatura para los atenuadores y/o el controlador de polarización.

La Figura 7 muestra dos láseres. Alternativamente, la implementación 700 puede usar un láser único como el láser de telecomunicaciones 710 y el láser cuántico 750. Si es así, el atenuador 762 facilita la conmutación entre los pulsos de estado señuelo para operar como un láser cuántico y los pulsos brillantes para operar como un láser de telecomunicaciones. Además, para la información de estado cuántico que se codifica en estados de base diagonal y estados de base circular, en lugar de un controlador de polarización, puede usarse un modulador de fase para cambiar la polarización de diagonal a izquierda, o para cambiar la polarización de antidiagonal a derecha.

En las implementaciones descritas en la presente descripción, los láseres funcionan típicamente en longitudes de onda de telecomunicaciones (sin embargo, otras longitudes de onda son posibles), y los componentes ópticos usados en los sistemas de QC se seleccionan para ser compatibles con la longitud de onda operacional. Por ejemplo, el láser cuántico 750 puede operar a una longitud de onda de telecomunicaciones apropiada (como 1310 nm o 1550 nm para la transmisión de fibra), y el controlador de polarización 770 puede ser un modulador de niobato de litio. Alternativamente, el láser cuántico 750 puede operar en otra longitud de onda adecuada (como 780 nm para la transmisión en el espacio libre) y el controlador de polarización 770 puede ser un modulador de arseniuro de galio (GaAs).

La Figura 8 ilustra una implementación similar a la de la Figura 7, pero en el que se usan otras guías de onda en lugar de fibras ópticas. Como se muestra en la Figura 8, un láser de telecomunicaciones 810, un detector de telecomunicaciones 818 y un láser cuántico 850 se acoplan a las guías de onda 816, 820, 855, respectivamente. La óptica de acoplamiento 888 acopla ópticamente la guía de onda 855 a un conector de fibra 890. En lugar de los circuladores como se muestra en la Figura. 7, las guías de onda en la implementación 800 de la Figura 8 tienen la forma de que la luz se dirige como se desea.

Una implementación de un sistema de QC de estado de señuelo se muestra en la Figura 9. Un transmisor de estado de señuelo 900 incluye un láser 902 que produce un flujo óptico que se dirige a lo largo de una fibra 904 a un atenuador variable 908 y un controlador de polarización o modulador de fase 910. El atenuador variable 908 se configura de acuerdo con un protocolo de estado de señuelo predeterminado para producir pulsos de fotones que tienen valores de μ seleccionados, y puede implementarse mediante el uso de uno o más atenuadores. Además, el atenuador variable 908 se configura para proporcionar una atenuación sustancialmente menor en la transmisión de las llamadas "ráfagas brillantes" para su uso en un receptor para corregir los cambios de polarización en la propagación. El controlador de polarización 910 se configura para aplicar la modulación de polarización cuántica al flujo óptico codificado en estado de señuelo. El flujo modulado por polarización se dirige a la óptica de salida 912 y se propaga en el espacio libre a la óptica

de acoplamiento 918 para acoplarse a la fibra 920. Una porción del flujo óptico se dirige por un reflector 914 a un polarímetro 916 que se configura para determinar uno o más SOP en el flujo óptico.

Uno o más controladores (no mostrados) se acoplan al controlador de polarización 910, el atenuador variable 908 y el polarímetro 916 para ajustar la modulación de polarización para que se corresponda con las bases seleccionadas y para ajustar la atenuación variable 908 para que se corresponda con los niveles de estado de señuelo seleccionados El transmisor 900 puede incluir uno o más detectores de fotones (no mostrados) acoplados al controlador para calibrar la transmisión de QC.

La fibra 920 transmite el flujo óptico desde el transmisor 900 a un receptor 901 que se configura para separar los estados de polarización de la QC recibida. Un primer controlador de polarización 922 se sitúa para recibir el flujo óptico codificado por polarización desde el transmisor 900 y para dirigir el flujo óptico a lo largo de una fibra 924. El flujo óptico se divide entonces de manera que una primera porción se dirige a lo largo de una fibra 928 a un divisor de haz polarizador (PBS) 930 y una segunda porción se dirige a un controlador de polarización 926 y a un PBS 932. Los PBS 930 y PBS 932 dirigen componentes lineales ortogonales directos del flujo óptico recibido a lo largo de las trayectorias P1, P2 y P3, P4, respectivamente. Los controladores de polarización 922 y 926 se acoplan a un controlador (no se muestra) y se configuran de manera que cada una de las rutas P1, P2, P3, P4 se dirija a detectores configurados para recibir estados de polarización seleccionados de una de las dos bases predeterminadas.

El conmutador 934 dirige el flujo óptico a lo largo de la trayectoria P1 al detector 944 o al detector de fotón único 942. El conmutador 936 dirige el flujo óptico a lo largo de la trayectoria P2 al detector 948 o al detector de fotón único 946. El conmutador 938 dirige el flujo óptico a lo largo de la trayectoria P3 al detector 952 o al detector de fotón único 950. El conmutador 940 dirige el flujo óptico a lo largo de la trayectoria P4 al detector 956 o al detector de fotón único 954. Los conmutadores 934, 936, 938, 940 pueden implementarse mediante el uso de un interferómetro Mach-Zehnder, por ejemplo. En algunos ejemplos, el conmutador se configura para aplicar cambios de relación de extinción de aproximadamente 27 dB o más. Esto provoca un cambio significativo en el brillo del láser con un único paso rápido. Más generalmente, los conmutadores actúan como atenuadores variables.

Los detectores de fotón único 942, 946, 950, 954 se acoplan a un procesador (no mostrado), que incluye lógica para analizar eventos de detección de fotones y/o producir distribuciones de fotones basadas en los eventos. El procesador se configura para estimar la transmitancia de un fotón único y para calcular los niveles de confianza de la transmitancia en base a los valores de μ medidos. El procesador puede configurarse adicionalmente para calcular los valores de μ en función de los eventos de detección de fotones y para estimar la probabilidad de detección de fondo y de conteo oscuro en base a los eventos de detección de estado de vacío. El procesador también puede comparar los valores de μ medidos del receptor con los valores de μ de un receptor y determinar qué valores de bit provienen de los pulsos de fotón único para seleccionar los bits secretos de la transmisión de QC.

Una implementación de un transmisor de QC de estado de señuelo 1000 se ilustra en la Figura 10. El transmisor 1000 incluye un láser 1002 que dirige un flujo óptico a un aislador 1004 y un retardador de onda media 1008. Un modulador de intensidad "lenta" 1010 recibe el flujo óptico del retardador 1008 y se configura para producir un flujo óptico que se modula en intensidad aproximadamente cada 1 a 10 ms con fines de calibración. El flujo óptico se recibe por un modulador de intensidad "rápida" 1012, que se configura para modular la intensidad del flujo recibido aproximadamente cada 1 a 10 ns o más rápido. Normalmente, el modulador de intensidad lenta 1010 se configura para atenuar el flujo en al menos 60 dB o más, mientras que el modulador de intensidad rápida 1012 se configura para atenuar el flujo en aproximadamente 20 dB o más. El modulador de intensidad rápida 1012 se configura para generar estados de señuelo en base a datos de una fuente de datos 1022.

El modulador 1012 dirige un flujo modulado en estado señuelo a un polarizador lineal 1014 y un retardador de onda media 1016. Un modulador de polarización 1020 modula la polarización del flujo óptico recibido del estado de señuelo en base a los datos de la fuente de datos 1022 para proporcionar una salida codificada de polarización en cualquiera de los cuatro SOP de dos bases conjugadas, una base (A, D) y una Base (R, L) como se muestra en la Figura 10. Pueden elegirse cuatro SOP separados en un gran círculo en la esfera de Poincaré para dos bases ortogonales conjugadas.

*Ejemplos de entornos operativos para transmisores/receptores de QC*

La Figura 11 muestra un ejemplo de entorno operativo 1100 en el que varios dispositivos de usuario adquieren claves a través de QC con una autoridad confiable 1101. Los dispositivos de usuario incluyen una tarjeta de QC 1102 que se acopla con una estación base 1103, un teléfono móvil 1107 que tiene una tarjeta de QC, un satélite 1109 y varios ordenadores 1106 conectados a un transmisor de QC convencional 1105. Un dispositivo de usuario generalmente indica un sistema de computación asociado con un usuario y puede ser para un usuario individual o para una empresa, institución financiera o institución gubernamental como usuario.

La autoridad de confianza 1101 se implementa mediante el uso de un sistema informático configurado para autenticar a un usuario, producir claves cuánticas en comunicación con un dispositivo de usuario (o un transmisor de QC convencional 1105) y almacenar las claves cuánticas. La tarjeta de QC 1102 se acopla con una estación base 1103, que proporciona una conexión de red con la autoridad de confianza 1101 y puede proporcionar energía eléctrica a la tarjeta de QC 1102.

La tarjeta de QC 1102 se involucra en la QC con la autoridad confiable 1101 para producir claves cuánticas y luego almacena las claves cuánticas en la memoria segura. En general, la tarjeta de QC 1102 combina las ventajas de la tecnología de tarjeta inteligente con las ventajas de la distribución de claves cuánticas.

En algunas modalidades, la tarjeta de QC 1102 incluye un transmisor de QC. En implementaciones de ejemplo, la tarjeta de QC se hace relativamente barata y portátil al miniaturizar el transmisor de QC, o reducir de cualquier otra manera la huella del transmisor. Por ejemplo, la tarjeta de QC puede incluir módulos microelectroópticos integrados capaces de producir estados de señuelo y una señal codificada de polarización que contiene impulsos que tienen cualquiera de los cuatro estados de polarización no ortogonales. O bien, la tarjeta de QC puede fabricarse como un único chip. En comparación con los transmisores de QC convencionales, el transmisor de QC en la tarjeta de QC puede ser un transmisor de baja potencia. No obstante, en la medida en que el consumo de energía pueda ser una preocupación, la tarjeta de QC puede obtener energía eléctrica de la estación base a la que se acopla la tarjeta de QC para la distribución de claves cuánticas. Por lo tanto, en algunas implementaciones, la tarjeta de QC es liviana y robusta, y puede empaquetarse en un teléfono móvil u otro dispositivo para el cual el tamaño, el peso y el consumo de energía limitados son atributos convenientes.

Para generar claves cuánticas, un usuario inserta la tarjeta de QC 1102 en la estación base 1103. Normalmente, como condición previa para la distribución de claves cuánticas, la autoridad de confianza 1101 autentica al usuario. Por ejemplo, la tarjeta de QC 1102 transmite información de autenticación a la autoridad de confianza 1101. La tarjeta de QC 1102 puede configurarse para que acepte un escaneo de huellas dactilares y un número de identificación personal ("PIN") del usuario, cifre el PIN y los datos de escaneo de huellas dactilares, y transmita el material cifrado a la autoridad confiable 1101 para compararlo con la información proporcionada previamente a la autoridad de confianza 1101. Alternativamente, la tarjeta de QC 1102 acepta otra información biométrica y/u otra información que identifique al usuario.

Si el usuario está autenticado, la tarjeta de QC 1102 se involucra en la QC con la autoridad de confianza 1101, y la tarjeta de QC 1102 y la autoridad de confianza 1101 producen números aleatorios secretos de calidad criptográfica para las claves cuánticas. La tarjeta de QC 1102 almacena las claves cuánticas resultantes en la memoria segura de la tarjeta de QC 1102. La tarjeta de QC 1102 puede usar posteriormente las claves cuánticas o distribuir las claves cuánticas a otro dispositivo para su uso.

En la Figura 11, la estación base 1103 se conecta a la autoridad confiable 1101 sobre la fibra instalada 1104. La fibra 1104 instalada se usa como un canal cuántico para la distribución de claves cuánticas punto a punto entre la tarjeta de QC 1102 y la autoridad confiable 1101, por ejemplo, para la transmisión de una señal de QC. En la Figura 11, la fibra instalada 1104 también se usa como un canal público para intercambiar información no cuántica entre la tarjeta de QC 1102 y la autoridad confiable 1101, por ejemplo, información de autenticación, información no cuántica sobre las bases de medición, estados de señuelo seleccionados/medidos, bases de registro en la QC y/o información de clave no secreta de la autoridad de confianza 1101. Alternativamente, la tarjeta de QC 1102 y la autoridad confiable 1101 comunican información no cuántica sobre otro tipo de medios de red (*por ejemplo,* cobre, RF) o espacio libre (óptico), o en una red de fibra que tenga otra topología de red.

El teléfono móvil 1107 incluye una tarjeta de QC 1102, así como también componentes de teléfonos móviles convencionales. El teléfono móvil 1107 se acopla con una estación base 1108 que se adapta para conectarse al teléfono móvil 1107 y proporciona una conexión de red a la autoridad de confianza 1101. La estación base 1108 del teléfono móvil también puede proporcionar energía eléctrica y una conexión de datos para la sincronización de la información en el teléfono móvil 1107. El teléfono móvil 1107 almacena las claves cuánticas producidas por la tarjeta de QC 1102 y la autoridad confiable 1101.

En los ejemplos mostrados en la Figura 11, el sistema informático que implementa la autoridad de confianza 1101 tiene un receptor de QC. Alternativamente, el sistema informático que implementa la autoridad de confianza 1101 tiene un transmisor de QC, y la otra parte de QC incluye un receptor de QC.

Las claves cuánticas tienen una fuerte seguridad de envío, y la Figura 12 muestra un ejemplo de entorno operativo 1120 en el que una tarjeta de QC 1102 distribuye las claves cuánticas obtenidas mediante la distribución de claves cuánticas con la autoridad de confianza 1101. Una tarjeta de QC 1102 puede distribuir claves cuánticas almacenadas en un teléfono móvil 1117 o en el ordenador de un usuario 1116. Por ejemplo, la tarjeta de QC 1102 transmite las claves cuánticas a través de una conexión de fibra punto a punto o una conexión inalámbrica. O bien, una tarjeta de QC 1102 proporciona claves cuánticas a un centro de control de satélites 1113, que carga las claves cuánticas a un satélite 1118.

Una vez que se obtienen las claves cuánticas, se establece una comunicación segura y un dispositivo de usuario puede comunicarse de forma segura con otro dispositivo de usuario directamente o a través de una red pública como Internet. O bien, el dispositivo del usuario puede usar una clave cuántica para autenticarse en otro dispositivo del usuario u obtener acceso a una instalación a través de un dispositivo de control de acceso. Las claves cuánticas pueden usarse para la comunicación o autenticación segura entre múltiples usuarios de acuerdo con cualquier protocolo disponible para la administración de claves (*por ejemplo,* gestión de claves simétricas) y/o autenticación.

Los transmisores/receptores de QC descritos en la presente descripción pueden implementarse con cualquiera de las técnicas de distribución de clave cuántica, incluida la tarjeta de QC/marco de autoridad confiable, que se describe en la solicitud de patente de Estados Unidos núm. 12/895,720, titulada "Quantum Key Distribution Using Card, Base Station y Trusted Authority", de Nordholt y otros, que se incorpora en la presente descripción como referencia en su totalidad.

*Implementación microóptica integrada representativa*

Para algunas aplicaciones de QC, puede ser ventajoso producir transceptores o receptores ilustrativos descritos en la presente descripción como un sistema o módulo microóptico integrado para reducir el costo y el tamaño. Por ejemplo, en un entorno operativo que involucra la distribución de claves cuánticas, una tarjeta de QC se usa para obtener claves cuánticas y participar en otras comunicaciones cuánticas. Si la tarjeta de QC incluye un transmisor y/o receptor de QC, entonces el tamaño de estos componentes puede establecer límites en el tamaño del dispositivo de la tarjeta de QC. Implementar el transmisor y/o el receptor como un módulo microóptico integrado puede facilitar la producción de una tarjeta de QC que es relativamente económica, de menor tamaño y, en algunos casos, portátil. En algunos ejemplos, los dispositivos de QC microópticos integrados tienen una longitud inferior a aproximadamente 200 mm y un ancho inferior a aproximadamente 50 mm. Sin embargo, otros tamaños son posibles.

Con referencia a las Figuras 7 y 8, los componentes ilustrados pueden seleccionarse para ser componentes microópticos e integrarse para reducir el tamaño y el costo del transceptor. Por ejemplo, aunque la Figura 7 muestra el láser cuántico 750 separado del controlador de polarización 770, el láser cuántico 750 y el controlador de polarización 770 pueden integrarse más estrechamente, potencialmente con un modulador de amplitud en el mismo módulo. Igualmente, el controlador de polarización 770 y uno o más de los atenuadores 760, 762, 764 pueden combinarse o integrarse en un solo modulador de intensidad/polarización. Además, los láseres 710 y 750 pueden reemplazarse por un láser de un único chip, y los detectores 782 y 784 no necesitan ser detectores de fotón único donde se usa una división de guía de onda precisa. Todas las ópticas de acoplamiento, lentes, aisladores y divisores pueden implementarse mediante el uso de lentes en miniatura y otros componentes microópticos.

Otros transmisores/receptores representativos ilustrados o descritos en la presente descripción también pueden implementarse como un sistema microóptico integrado mediante la selección de componentes microópticos. Por ejemplo, los componentes electroópticos pueden obtenerse por separado y colocarse sobre un sustrato rígido, tal como una mesa microóptica de silicio. Pueden usarse lentes, placas de onda, aisladores y divisores de haz para acoplar los componentes. Puede usarse una placa de onda o un retardador variable como controlador de polarización; sin embargo, pueden usarse uno o más moduladores electroópticos en lugar de o además de la placa de onda (o retardador variable). Los moduladores pueden acoplarse mediante el uso de lentes miniaturizadas en posición micro para colimar y enfocar la luz desde la guía de onda de un modulador al siguiente. La luz que sale del dispositivo puede ser a través del espacio libre o en una fibra óptica. Si la salida es de espacio libre, generalmente es conveniente proporcionar un filtrado espacial, por ejemplo, mediante el uso de un orificio de salida para reducir la luz no modulada que entra en la salida.

Un transmisor de QC integrado ilustrativo 1300 se ilustra en la Figura 13. El transmisor 1300 incluye múltiples dispositivos a escala de chip que se han acoplado en un espacio libre en un módulo integrado, como se muestra. El transmisor 1300 incluye un chip láser 1302 que dirige un flujo óptico a una lente en miniatura 1304, un aislador 1306 y un retardador de onda media 1308. Una lente 1310 acopla el flujo en un modulador de polarización 1312, que sirve como un retardador de voltaje variable, y puede proporcionarse como un chip modulador de polarización GaAs que produce diferencias de fase dependientes de voltaje entre las polarizaciones TE y TM. El modulador de polarización 1312 se configura para modular un flujo óptico de entrada para proporcionar una salida codificada de polarización en cualquiera de los cuatro SOP de dos bases conjugadas. Pueden elegirse cuatro SOP separados en un gran círculo en la esfera de Poincaré para los cuatro SOP. El flujo modulado por polarización se acopla luego en una fibra 1314. Por ejemplo, la fibra 1314 puede ser una fibra monomodo conectorizada FC-UPC. El módulo 1300 puede incluir componentes adicionales, tales como refrigeradores termoeléctricos o calentadores para la estabilización de la temperatura del modulador 1312, el láser 1302 y/o otros componentes. Se proporcionan uno o más terminales eléctricos 1316 para suministrar señales de control o transmisión al láser 1302, el modulador 1312 y/u otros componentes del transmisor 1300.

Un transmisor de QC 1400 de estado de señuelo integrado se ilustra en la Figura 14. El transmisor 1400 incluye múltiples dispositivos a escala de chip que se han acoplado en un espacio libre en un módulo integrado, como se muestra. El transmisor 1400 incluye un láser 1402 que dirige un flujo óptico a una lente en miniatura 1404, un aislador 1406 y una placa de onda 1408. El láser 1402 es un chip láser, como un láser de diodo DFB o DBR. El aislador 1406 y la placa de onda 1408 se configuran para ajustar la polarización del flujo óptico recibido según sea apropiado para la entrada en un modulador acústico óptico 1410.

El modulador acústico óptico 1410 recibe el flujo óptico de la placa de onda 1408 y se configura para producir un flujo óptico que se modula en intensidad aproximadamente cada 1 a 10 ms con fines de calibración. El flujo óptico luego se recibe por una lente 1412, que dirige el flujo óptico a un modulador de intensidad 1414 Mach-Zehnder. El Mach-Zehnder 1414 se configura para modular la intensidad del flujo óptico recibido aproximadamente cada 1 a 10 ns o más rápido para generar estados de señuelo de acuerdo con un protocolo de estado de señuelo predeterminado. El Mach-Zehnder 1414 dirige un flujo óptico de estado señuelo hacia una lente 1416, un polarizador lineal 1418, una placa de onda 1420, una lente 1422 y un modulador de polarización GaAs 1424. El modulador de polarización 1424 modula la polarización del flujo

óptico recibido para proporcionar una salida codificada de polarización en cualquiera de los cuatro SOP de dos bases conjugadas. La salida se dirige a una fibra con lente 1426. Alternativamente, puede usarse una fibra conectorizada.

El módulo 1400 puede incluir componentes adicionales, tales como refrigeradores termoeléctricos o calentadores para la estabilización de la temperatura del modulador 1424, el láser 1402 y/u otros componentes. Además, cuando se implemente, el módulo 1400 se conectará a las fuentes de alimentación y no se muestra la electrónica del controlador.

Se ilustra otro transmisor de QC de estado de señuelo integrado 1500 ilustrativo en la Figura 15. El transmisor 1500 incluye múltiples dispositivos a escala de chip que se han acoplado en un espacio libre en un módulo integrado, como se muestra. El transmisor 1500 incluye un láser 1502 que dirige un flujo óptico a una lente en miniatura 1504, un aislador 1506 y una placa de onda 1508. El láser 1502 es un chip láser, como un láser de diodo DFB o DBR. El aislador 1506 protege al láser de los efectos de retroalimentación. La placa de onda 1508 se configura para rotar la polarización de manera que los flujos TE y TM que salen del modulador sean sustancialmente iguales.

Un atenuador 1510 accionado mecánicamente recibe el flujo óptico de la placa de onda 1508 y se configura para producir un flujo óptico que se modula en intensidad aproximadamente cada 1 a 10 ms con fines de calibración. El flujo óptico luego se recibe por una lente 1512, que dirige el flujo óptico a un modulador de intensidad 1514 de Mach-Zehnder. El Mach-Zehnder 1514 se configura para modular la intensidad del flujo recibido aproximadamente cada 1 a 10 ns o más rápido para generar estados de señuelo de acuerdo con un protocolo de estado de señuelo predeterminado. El Mach-Zehnder 1514 dirige un flujo óptico de estado señuelo hacia una lente 1516, un polarizador lineal 1518, una placa de onda 1520, una lente 1522 y un modulador de polarización GaAs 1524. El modulador de polarización 1524 modula la polarización del flujo óptico recibido para proporcionar una salida codificada de polarización en cualquiera de los cuatro SOP de dos bases conjugadas. La salida se dirige a una fibra con lente 1526.

El módulo 1500 puede incluir componentes adicionales, tales como refrigeradores termoeléctricos o calentadores para la estabilización de la temperatura del modulador 1524, el láser 1502 y/u otros componentes. Además, cuando se implemente, el módulo 1500 se conectará a las fuentes de alimentación y no se muestra la electrónica del controlador.

Mientras que las soluciones de QC convencionales tienden a ser caras y difíciles de implementar, los componentes de QC con transmisores/receptores microópticos integrados pueden fabricarse a un costo menor y con un tamaño menor.

*Implementación representativa a escala de chip*

Como se indicó anteriormente con respecto a los módulos microópticos integrados, reducir el tamaño de un transmisor/receptor de QC puede ser ventajoso cuando se implementa en una tarjeta de QC u otro dispositivo de usuario de QC. Igualmente, las implementaciones a escala de chip reducen aún más el tamaño de los transmisores/receptores al tiempo que reducen la complejidad, lo que permite un empaquetado aún más pequeño del sistema a un costo reducido. Por ejemplo, los transmisores/receptores de QC a escala de chip pueden facilitar la producción de una tarjeta de QC como parte de un ordenador portátil o dispositivo móvil.

En una implementación a escala de chip, los componentes ópticos del transmisor/receptor de QC se integran en un solo chip, creando un circuito optoelectrónico integrado. Los componentes pueden integrarse monolíticamente mediante el uso de procesos de fabricación compatibles con CMOS, o el chip puede ser un circuito híbrido que incluye una combinación de componentes fabricados con diferentes materiales/sustratos no necesariamente compatibles con CMOS. Por ejemplo, los componentes ópticos pueden basarse en la fotónica de silicio y fabricarse mediante el uso de procesos CMOS. Alternativamente, los componentes ópticos pueden fabricarse mediante el uso de otras técnicas, como en múltiples sustratos, y luego integrarse. Por ejemplo, la electrónica puede fabricarse por separado e integrarse como un chip en los chips CMOS, u otros componentes, como los láseres y los detectores, pueden fabricarse por separado y luego "colocarse" en el circuito del CMOS. Preferentemente, todos los componentes del transmisor o receptor de QC se integran a nivel de chip en el mismo sustrato. Por ejemplo, los láseres, moduladores, detectores, etcétera no se fabrican por separado, sino como parte del mismo chip. La electrónica también se integra, por lo que no se requieren chips de controladores electrónicos separados o módulos de múltiples chips.

Normalmente, las lentes no se usan para acoplar la luz entre los componentes ópticos en la escala del chip. El acoplamiento entre dispositivos electroópticos puede realizarse mediante el uso de guías de onda en los mismos o diferentes sustratos. El acoplamiento de las guías de onda en diferentes sustratos puede hacerse cortando los sustratos deseados a través de la guía de onda y luego uniendo las dos guías de onda. Puede ser conveniente reducir una o más de las guías de onda donde las guías de onda se unen entre sí para facilitar el ajuste de la luz entre los dos sustratos. Además, pueden introducirse microópticas en una guía de onda donde los elementos microópticos no pueden hacerse fácilmente directamente sobre el sustrato de la guía de onda. Por ejemplo, puede introducirse una placa de onda cortando una pequeña ranura a través de una guía de onda para que la placa de onda pueda usarse para cambiar o hacer girar el estado de polarización de la luz en la guía de onda. La salida de luz de la implementación a escala de chip puede ser en fibra óptica o en espacio libre. Preferentemente, no se emiten modos ópticos no deseados o no modulados.

La Figura 16 es un diagrama de bloques de una implementación a escala de chip ilustrativo de un transmisor 1600. El transmisor 1600 incluye un chip 1610 que contiene un circuito optoelectrónico integrado configurado para generar una

señal de QC. El transmisor 1600 también puede incluir otros componentes/módulos no ilustrados en la Figura 16. Todos los componentes ilustrados del chip de QC 1610 pueden ser componentes CMOS integrados monolíticamente (incluidos los componentes fotónicos de silicio), o los componentes pueden formar un circuito híbrido, con algunos componentes CMOS y otros componentes que no son CMOS.

Un láser con electrónica de controlador 1612 genera una señal de QC que se acopla a una guía de onda 1614. El láser puede ser un láser fabricado por CMOS, tal como un láser de silicio, acoplado a la electrónica del controlador CMOS, o el láser puede ser un láser sin silicio. Por ejemplo, en un circuito híbrido en el que el láser se fabrica por separado de otros componentes del chip, el láser puede acoplarse en la parte superior del chip a través de espejos de giro óptico. En algunos ejemplos, el láser se forma a partir de estructuras DFB construidas sobre el silicio, como por ejemplo mediante la implantación de emisores. Alternativamente, el láser puede ser un láser fuera del chip acoplado a la fibra en el chip, por ejemplo, mediante el uso de un borde o un acoplador de rejilla. El láser 1612 se configura para generar transmisiones cuánticas y, opcionalmente, para producir también transmisiones de telecomunicaciones. La guía de onda 1614 puede ser una guía de onda de silicio o una guía de onda formada sobre un sustrato distinto del silicio. También pueden incorporarse guías de onda adicionales que no se muestran en el chip de QC 1610 para facilitar el acoplamiento de la luz entre los componentes ópticos.

La señal de QC se acopla desde la guía de ondas 1614 a un modulador de amplitud con la electrónica del controlador 1616 configurada para producir estados de señuelo predeterminados y para producir pulsos "brillantes" para la calibración del sistema de QC. Luego, la señal se acopla a un modulador de fase con la electrónica del controlador 1618 configurada para modular el estado de polarización de los impulsos recibidos para producir una señal de QC codificada por polarización. El modulador de amplitud 1616 y el modulador de fase 1618 pueden ser componentes separables conectados por una guía de onda, o integrados en un solo componente. Cada modulador puede ser un único modulador o comprender una serie de moduladores. Por ejemplo, el modulador de amplitud 1616 puede ser una serie de moduladores de amplitud, unidos entre sí para lograr la atenuación deseada.

En algunas implementaciones, los moduladores se hacen en el mismo sustrato y se unen mediante guías de onda hechas en ese sustrato. Por ejemplo, los moduladores pueden ser cualquier modulador óptico de silicio conocido en la técnica, como los que se describen en las siguientes referencias: Reed, y otros, "Silicon Optical Modulators", Nature Photonics 4, 518-526 (2010), y Liow y otros, "Silicon Modulators and Germanium Photodetectors on SOI: Monolithic Integration, Compatibility, and Performance Optimization," IEEE J Quantum Electron. 16, 307-315 (2010), todos los cuales se incorporan como referencia en la presente descripción. Los moduladores ópticos de silicio pueden integrarse monolíticamente en una plataforma CMOS con electrónica del controlador CMOS y conectarse entre sí (y a otros componentes fotónicos de silicio) mediante el uso de guías de onda de silicio. En otras implementaciones, los moduladores se fabrican en diferentes sustratos seleccionados para optimizar el rendimiento de cada modulador en particular. Los moduladores que no son de silicio pueden colocarse en un circuito CMOS para formar un circuito híbrido integrado, y los componentes fabricados en diferentes sustratos pueden unirse uniendo guías de onda o mediante el uso de otras técnicas.

Los moduladores se acoplan ópticamente a un divisor de guía de onda 1620 preciso configurado para dirigir una porción de la señal a una salida de fibra o espacio libre 1624 y una porción de la señal a un detector de retroalimentación 1622. El detector 1622 puede ser un detector integrado CMOS, como un fotodetector SiGe o Ge, o el detector puede ser un detector fabricado sin CMOS. Por ejemplo, en un circuito híbrido en el que el detector se fabrica por separado de otros componentes del chip, la luz puede acoplarse a través de espejos de giro óptico en el detector situado en la parte superior del chip. El detector 1620 se configura para medir el estado de polarización y/o el estado de señuelo de la señal de QC. Preferentemente, el divisor 1620 de la guía de onda se fabrica con precisión de manera que el detector 1620 no necesita ser sensible a fotones únicos para medir los valores de μ, y la salida 1624 transmite los impulsos de estado de señuelo o fotones únicos deseados al receptor remoto (no se muestra).

La lógica 1630 se fabrica mediante el uso de procesos CMOS y contiene una lógica de protocolo para controlar diferentes operaciones del chip de QC 1610. La lógica 1630 se configura para coordinar las operaciones del láser 1612 y los moduladores 1616, 1618, de manera que el transmisor 1600 produzca la señal de QC del estado de señuelo modulada por la polarización deseada. Por ejemplo, la lógica 1630 puede incluir un generador de números aleatorios u otra tecnología para generar una serie de bits aleatorios. La lógica 1630 puede programarse con un protocolo de QC predeterminado para controlar el modulador de fase 1618 para codificar bits aleatorios con diferentes estados de polarización y para controlar el modulador de amplitud 1616 para codificar bits aleatorios con diferentes estados de señuelo. La lógica 1630 puede acoplarse eléctricamente al detector de retroalimentación 1622 para facilitar el control del modulador de fase 1618 y el modulador de amplitud 1616. La lógica 1630 también puede controlar el tiempo para generar señales de QC, pulsos "brillantes" para calibración, comunicación no cuántica y/u otras señales.

Un método del lado del transmisor representativo se ilustra en la Figura 17. En 1700, se seleccionan uno o más estados de señuelo para mejorar la seguridad en un sistema que transmite pulsos de láser débiles. En 1702, se seleccionan una o más bases de polarización conjugadas para compensar la birrefringencia medida o inesperada en la transmisión. En 1704, los flujos ópticos se modulan (codifican) con respecto a las bases seleccionadas, y en 1706, los flujos ópticos se modulan en amplitud en función de los estados de señuelo seleccionados. En 1708, se transmite el flujo óptico de estado de señuelo codificado por polarización.

En algunos ejemplos, las bases se seleccionan de manera que después de la transmisión, el flujo modulado por polarización sea en una o más de una base rectilínea, una base diagonal o una base circular. En algunos ejemplos, los flujos ópticos se codifican por polarización antes de que se aplique la modulación de amplitud de estado de señuelo, mientras que en otros ejemplos se aplica la modulación de amplitud de estado de señuelo antes de la modulación de polarización. En otro ejemplo, la modulación de polarización y la modulación de amplitud se aplican de manera sustancialmente simultánea, por ejemplo, mediante el mismo componente.

En vista de las muchas modalidades posibles a las que pueden aplicarse los principios de la tecnología descrita, debe reconocerse que las modalidades ilustradas son solo ejemplos preferidos y no deben tomarse como limitantes. Reclamamos como nuestra invención todo lo que entra dentro del alcance de las reivindicaciones adjuntas.

Reivindicaciones

1. Un transmisor de comunicación cuántica (700/1000), que comprende:
un láser (750/1002) configurado para producir un flujo óptico;
un modulador de polarización (770/1020) configurado para modular el flujo óptico a fin de codificar datos en al menos dos bases de polarización ortogonales;
un primer atenuador variable (762/1010) configurado para aplicar una primera atenuación variable al flujo óptico para permitir que un receptor realice una calibración de birrefringencia; y
un segundo atenuador variable (764/1012) configurado para aplicar una segunda atenuación variable al flujo óptico de manera que los datos también se codifiquen en dos o más estados señuelo, cada estado señuelo corresponde a un valor predeterminado para un número promedio de fotones, en donde el segundo atenuador variable se configura para operar más rápido que el primer atenuador variable.

2. El transmisor de la reivindicación 1, que comprende además uno o más atenuadores adicionales en serie con el primer atenuador variable y el segundo atenuador variable.

3. El transmisor de la reivindicación 1, en donde el segundo atenuador variable se configura para aplicar la segunda atenuación variable al flujo óptico antes de que el primer atenuador variable aplique la primera atenuación variable al flujo óptico.

4. El transmisor de la reivindicación 1, en donde el primer atenuador variable se configura para aplicar la primera atenuación variable al flujo óptico antes de que el segundo atenuador variable aplique la segunda atenuación variable al flujo óptico.

5. El transmisor de la reivindicación 1, que comprende además:
una entrada de modulación de polarización acoplada al sistema de control de polarización y configurada para seleccionar la base de salida del transmisor;
en donde dos o más estados de señuelo comprenden un estado de vacío, un primer estado correspondiente a un número de fotones promedio menor que 1, y un segundo estado correspondiente a un número de fotones promedio menor que el número de fotones promedio del primer estado; y
en donde las bases de polarización se seleccionan de (R, L); (H, V); y (D, A).

6. El transmisor de la reivindicación 1, en donde el modulador de polarización, el primer atenuador variable y el segundo atenuador variable y los divisores de guía de onda se construyen sobre un sustrato de silicio para formar parte de un circuito CMOS.

7. El transmisor de la reivindicación 1, en donde el modulador de polarización, el primer atenuador variable y el segundo atenuador variable se construyen sobre un sustrato de silicio para formar parte de un circuito CMOS y el láser se acopla en el circuito CMOS.

8. El transmisor de la reivindicación 1, que comprende además:
un detector de fotones;
un divisor de guía de onda posicionado para recibir el flujo óptico corriente abajo del primer atenuador variable, y el segundo atenuador variable, el divisor se configura para dirigir una primera parte del flujo óptico recibido al detector de fotones de acuerdo con una relación de división predeterminada y para dirigir una segunda porción del flujo óptico recibido hacia la salida del transmisor; y
un sistema de control de estado de señuelo acoplado al menos al detector de fotones y al segundo atenuador variable y configurado para controlar la segunda atenuación aplicada por el segundo atenuador variable en base a la relación de división predeterminada y las mediciones hechas por el detector de fotones de la primera porción del flujo óptico.

9. El transmisor de la reivindicación 8, en donde el modulador de polarización, el primer atenuador variable y el segundo atenuador variable se construyen sobre silicio mediante el uso de procesos CMOS, y el láser y el detector de fotones se construyen sobre sustratos que no son de silicio, y el modulador de polarización, el atenuador variable, el láser y el detector de fotones se integran en un solo chip.

10. Un método, que comprende:
aplicar una primera modulación de amplitud a un flujo óptico mediante el uso de un primer atenuador variable (762/1010) para permitir que un receptor realice una calibración de birrefringencia;
aplicar una segunda modulación de amplitud al flujo óptico mediante el uso un segundo atenuador variable (764/1012) en base a un flujo de datos de entrada de acuerdo con dos o más estados de señuelo predeterminados, en donde el segundo atenuador variable opera más rápido que el primer atenuador variable;
aplicar una modulación de polarización (770/1020) al flujo óptico en base al flujo de datos de entrada para producir un flujo óptico modulado por polarización asociado con estados de polarización (SOP) seleccionados de al menos dos bases ortogonales; y
transmitir la polarización del flujo óptico del estado de señuelo modulado.

11. El método de la reivindicación 10, que comprende además aplicar una o más modulaciones de amplitud adicionales al flujo óptico.

12. El método de la reivindicación 10, en donde la primera modulación de amplitud se aplica al flujo óptico antes de que la segunda modulación de amplitud se aplique al flujo óptico.

13. El método de la reivindicación 10, en donde la segunda modulación de amplitud se aplica al flujo óptico antes de que la primera modulación de amplitud se aplique al flujo óptico.

14. El método de la reivindicación 10, en donde la modulación de polarización se aplica en tres bases ortogonales que corresponden a cuatro SOP equidistantes en un gran círculo en la esfera Poincare y dos intersecciones de un eje del gran círculo y la esfera Poincare.

15. El método de la reivindicación 10,
en donde dos o más estados de señuelo comprenden un estado de vacío, un primer estado correspondiente a un número de fotones promedio menor que 1, y un segundo estado correspondiente a un número de fotones promedio menor que el número de fotones promedio del primer estado; y
en donde la aplicación de la segunda modulación de amplitud comprende asignar uno de los dos o más estados de señuelo a cada pulso del flujo óptico.

FIG. 1

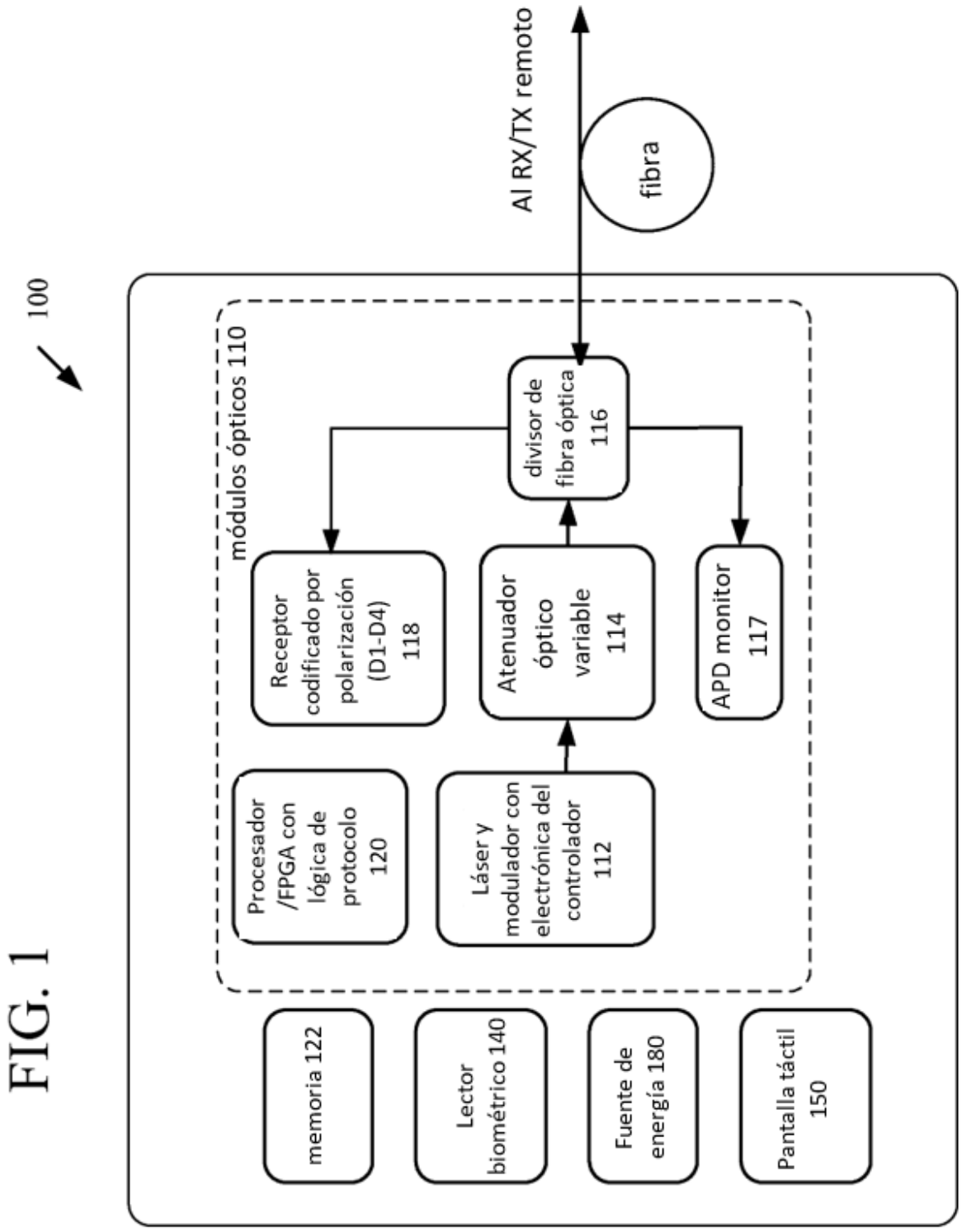
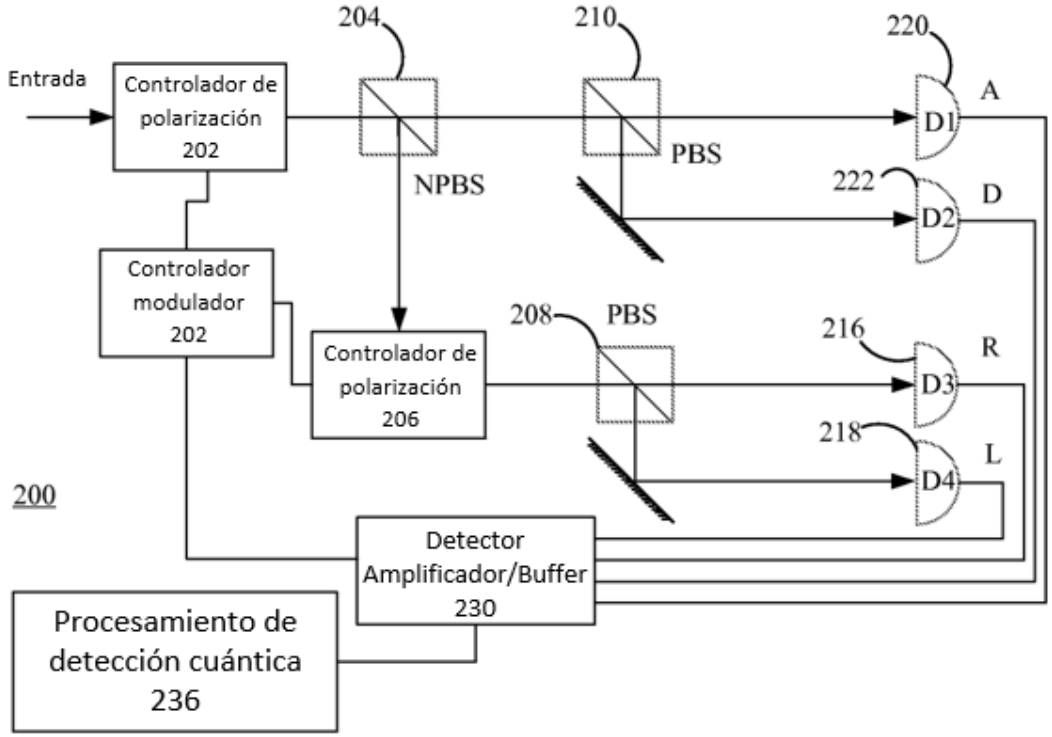

100
Al RX/TX remoto
fibra
módulos ópticos 110
divisor de fibra óptica 116
Receptor codificado por polarización (D1-D4) 118
Atenuador óptico variable 114
APD monitor 117
Procesador /FPGA con lógica de protocolo 120
Láser y modulador con electrónica del controlador 112
memoria 122
Lector biométrico 140
Fuente de energía 180
Pantalla táctil 150

FIG. 2


Entrada
Controlador de polarización 202
204
210
220
A
D1
PBS
NPBS
222
D
D2
Controlador modulador 202
208
PBS
216
R
D3
Controlador de polarización 206
218
L
D4
200
Detector Amplificador/Buffer 230
Procesamiento de detección cuántica 236

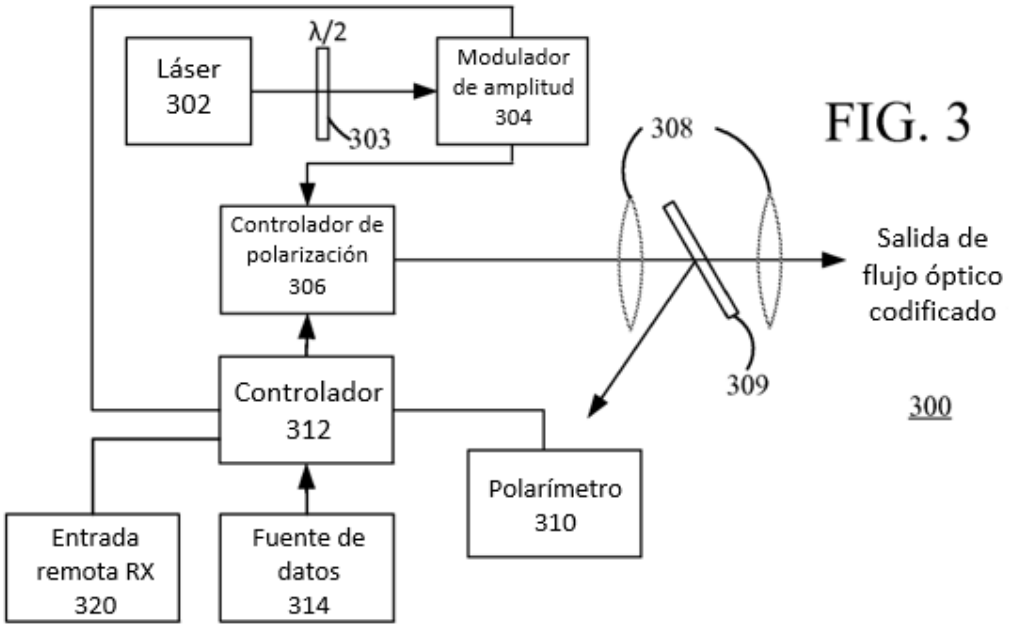
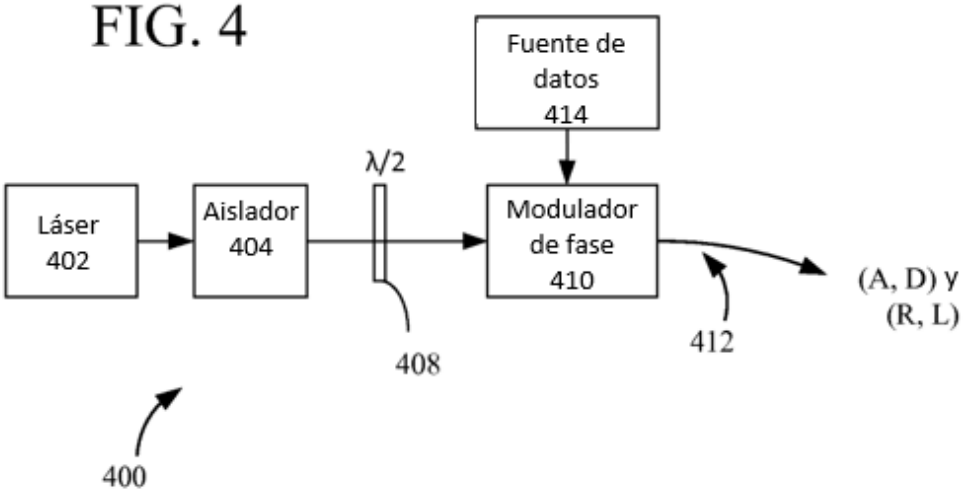

Láser 302
λ/2
303
Modulador de amplitud 304
308
Controlador de polarización 306
Salida de flujo óptico codificado
Controlador 312
309
300
Polarímetro 310
Entrada remota RX 320
Fuente de datos 314

FIG. 3

FIG. 4


Fuente de datos 414
λ/2
Láser 402
Aislador 404
Modulador de fase 410
(A, D) y (R, L)
412
408
400

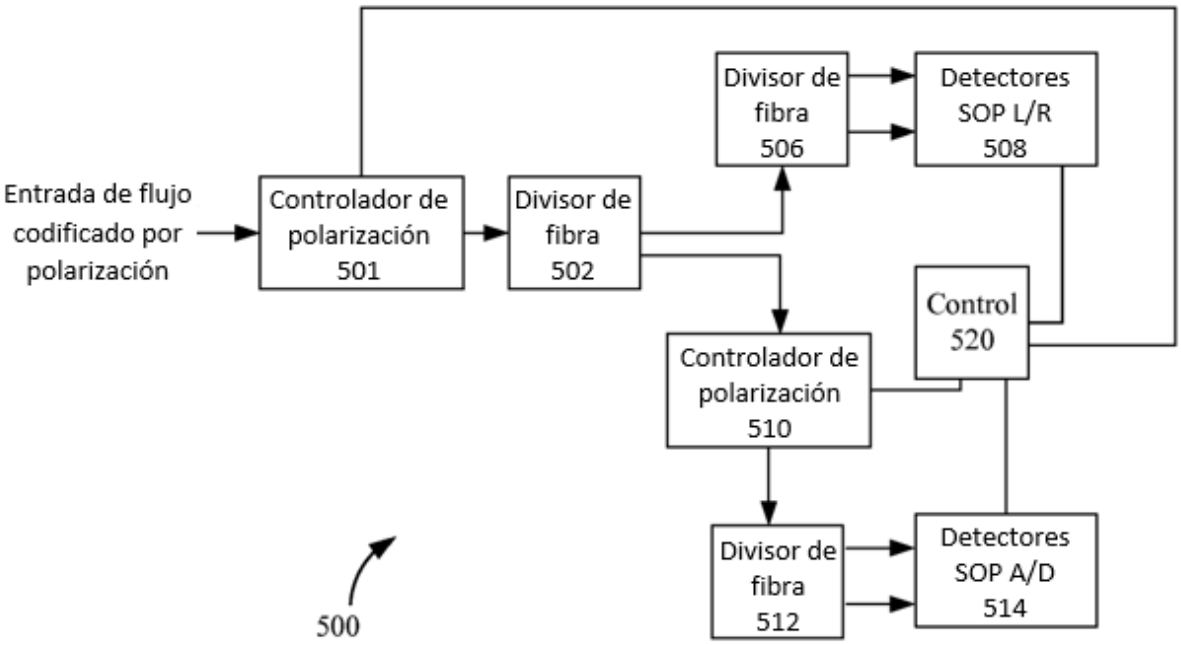

Divisor de fibra 506
Detectores SOP L/R 508
Entrada de flujo codificado por polarización
Controlador de polarización 501
Divisor de fibra 502
Control 520
Controlador de polarización 510
Divisor de fibra 512
Detectores SOP A/D 514
500

FIG. 5

FIG. 6

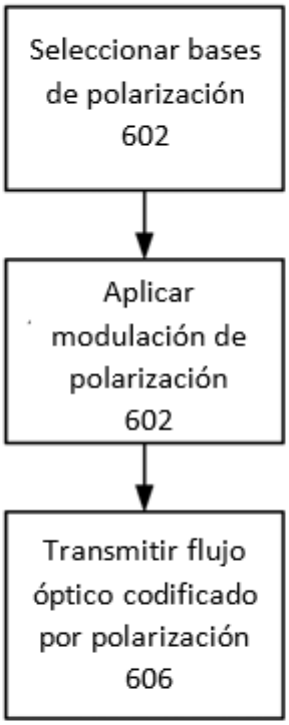

Seleccionar bases de polarización 602
Aplicar modulación de polarización 602
Transmitir flujo óptico codificado por polarización 606

FIG. 7

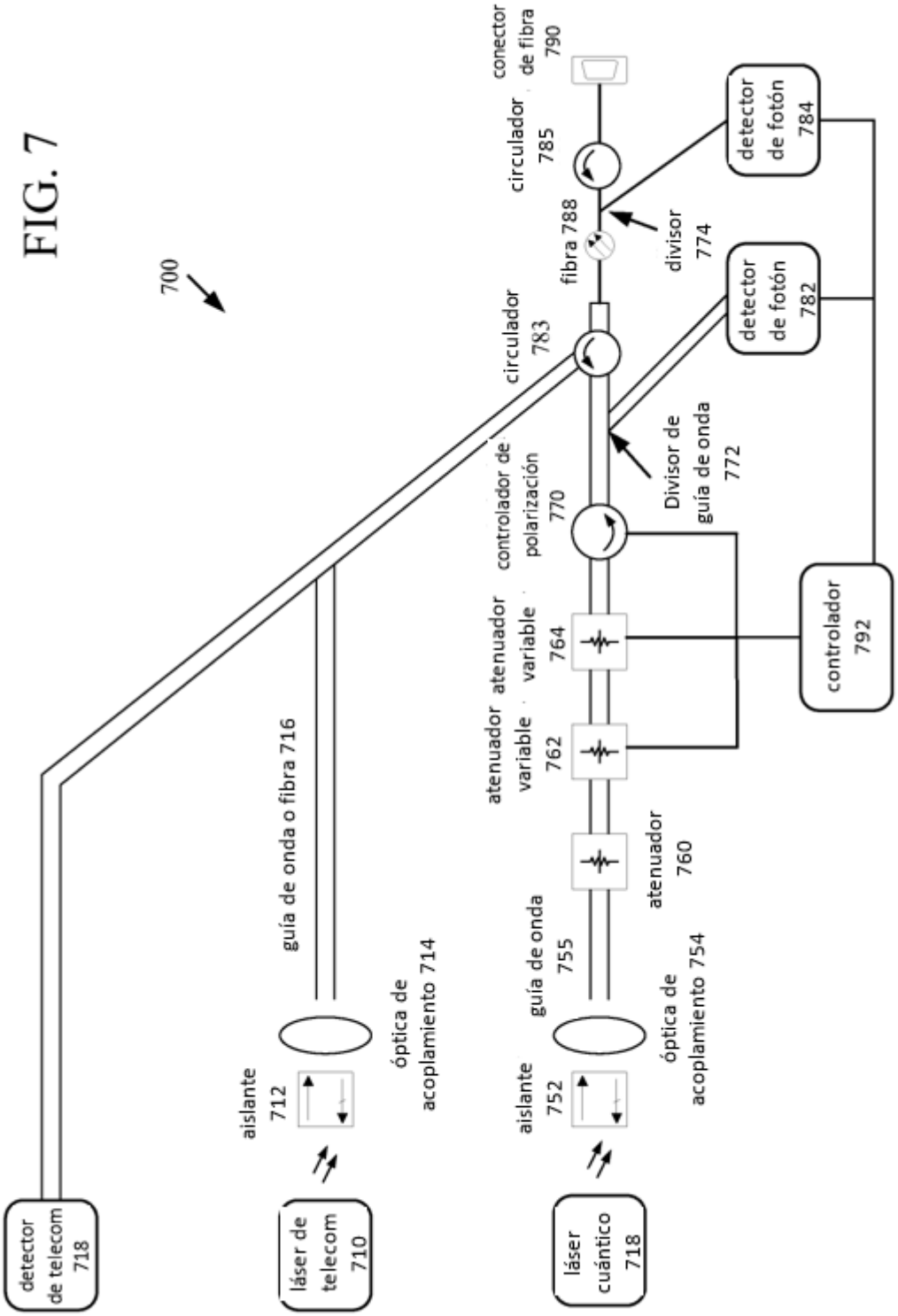
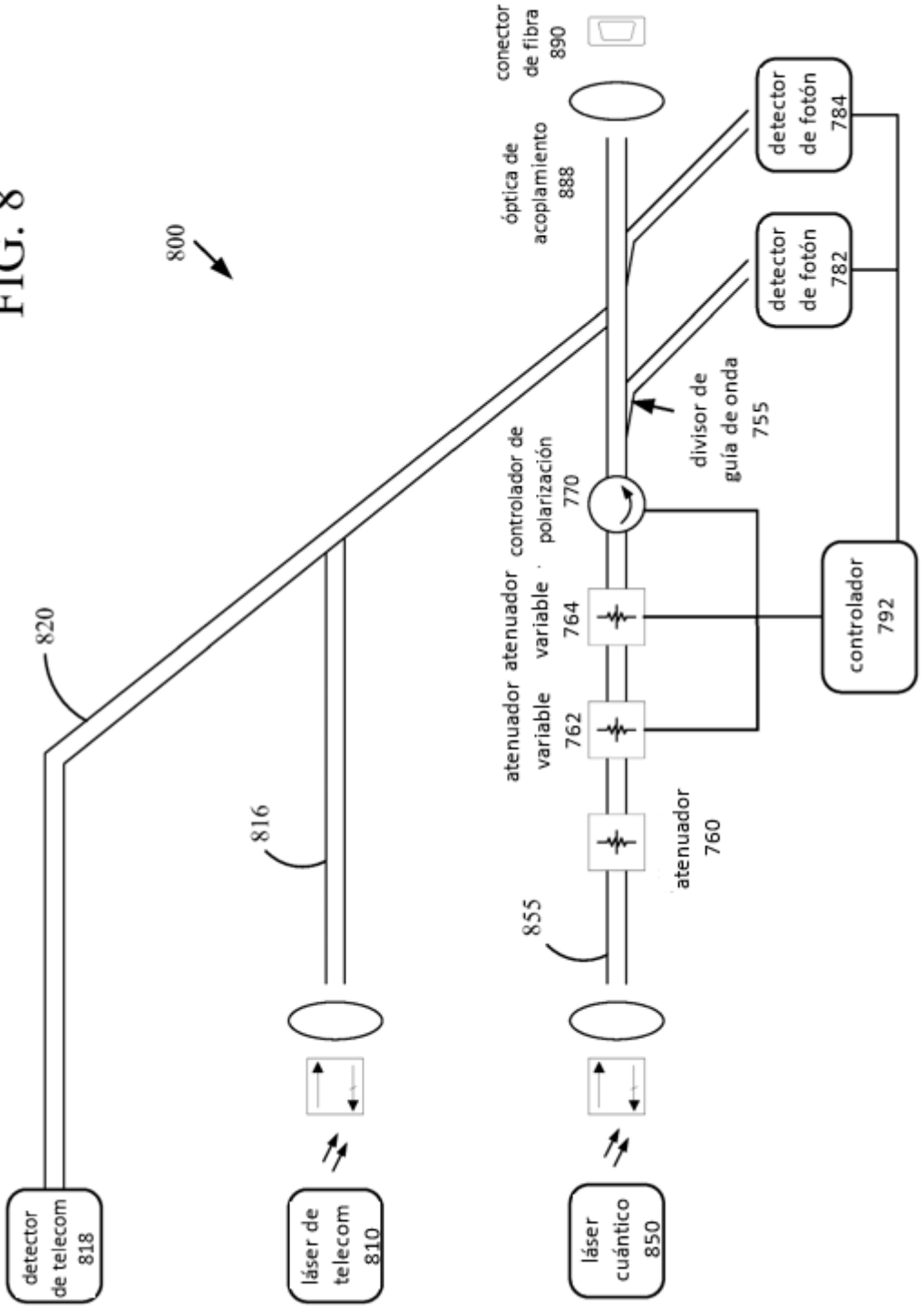

700
detector de telecom 718
láser de telecom 710
aislante 712
guía de onda o fibra 716
óptica de acoplamiento 714
láser cuántico 718
aislante 752
guía de onda 755
óptica de acoplamiento 754
atenuador 760
atenuador variable 762
atenuador variable 764
controlador de polarización 770
Divisor de guía de onda 772
circulador 783
fibra 788
circulador 785
conector de fibra 790
divisor 774
detector de fotón 782
detector de fotón 784
controlador 792

FIG. 8


800
820
816
855
detector de telecom 818
láser de telecom 810
láser cuántico 850
atenuador 760
atenuador variable 762
atenuador variable 764
controlador de polarización 770
divisor de guía de onda 755
óptica de acoplamiento 888
conector de fibra 890
detector de fotón 782
detector de fotón 784
controlador 792

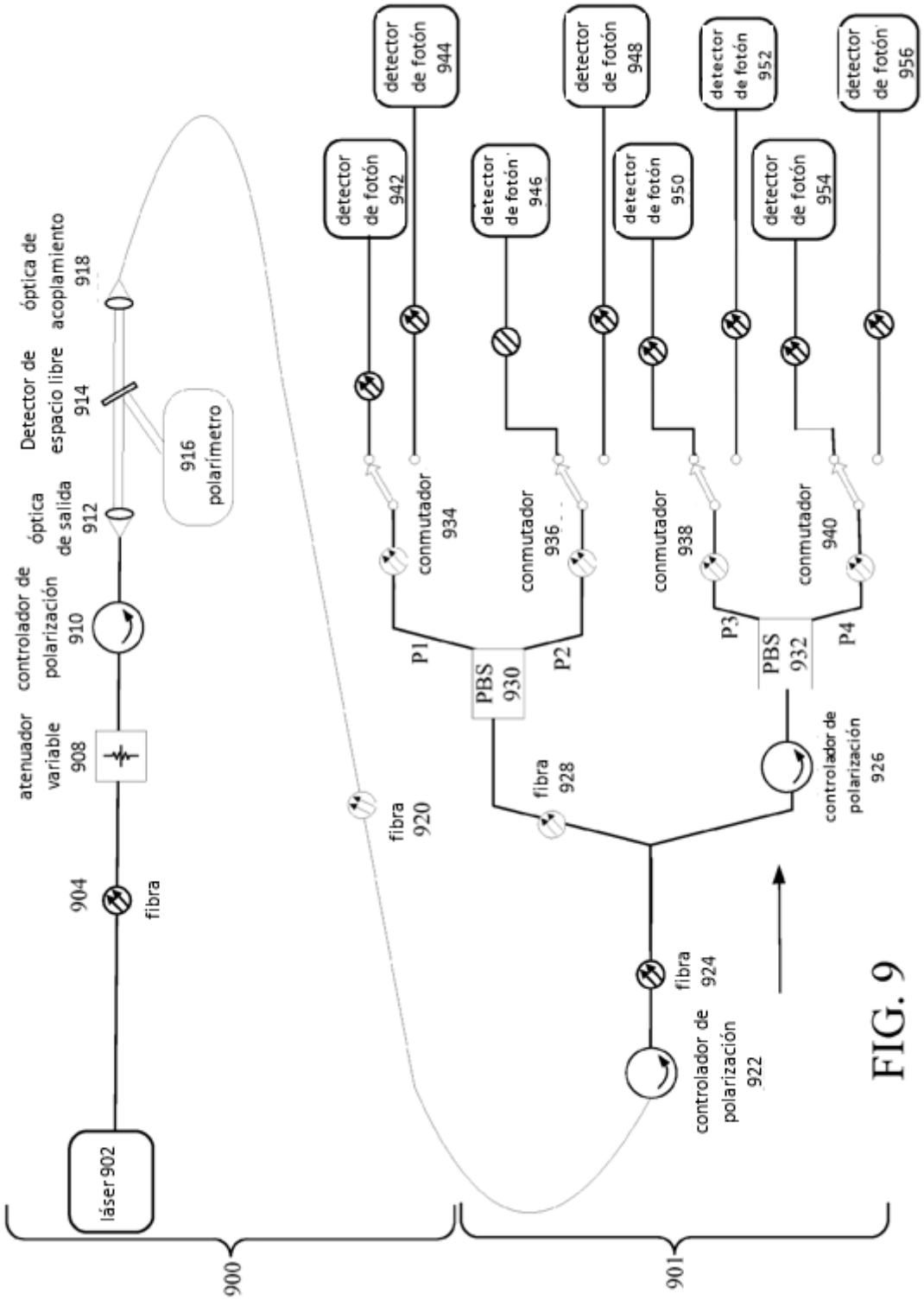

láser 902
fibra
904
atenuador variable 908
controlador de polarización 910
óptica de salida 912
Detector de espacio libre 914
óptica de acoplamiento 918
916 polarímetro
fibra 920
controlador de polarización 922
fibra 924
PBS 930
fibra 928
P1
P2
PBS 932
P3
P4
controlador de polarización 926
conmutador 934
conmutador 936
conmutador 938
conmutador 940
detector de fotón 942
detector de fotón 944
detector de fotón 946
detector de fotón 948
detector de fotón 950
detector de fotón 952
detector de fotón 954
detector de fotón 956
900
901

FIG. 9

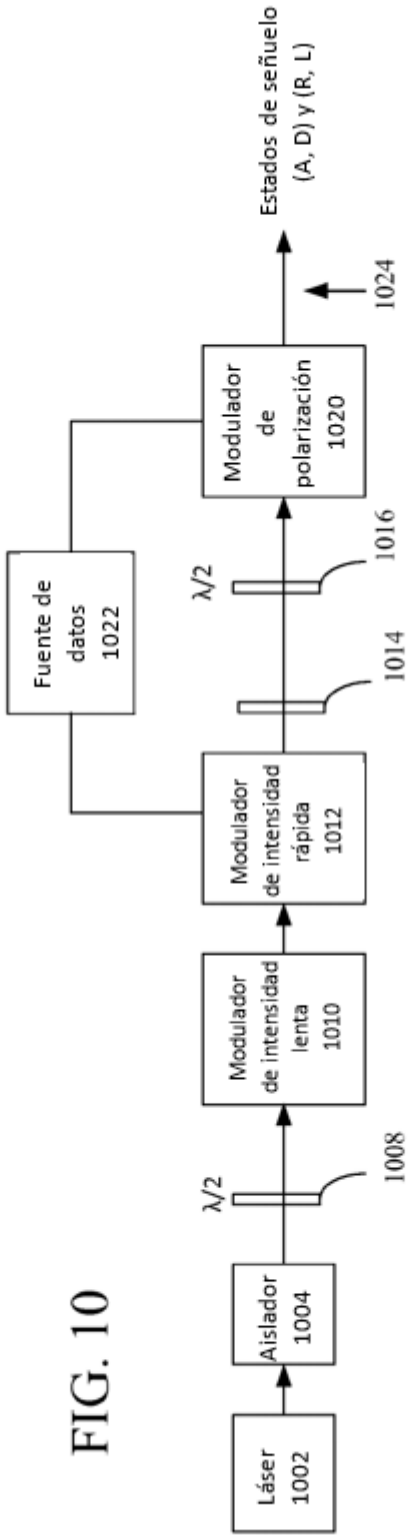

Estados de señuelo
(A, D) y (R, L)
1024
Modulador de polarización 1020
1016
λ/2
1014
Fuente de datos 1022
Modulador de intensidad rápida 1012
Modulador de intensidad lenta 1010
1008
λ/2
Aislador 1004
Láser 1002
1000

FIG. 10

FIG. 11

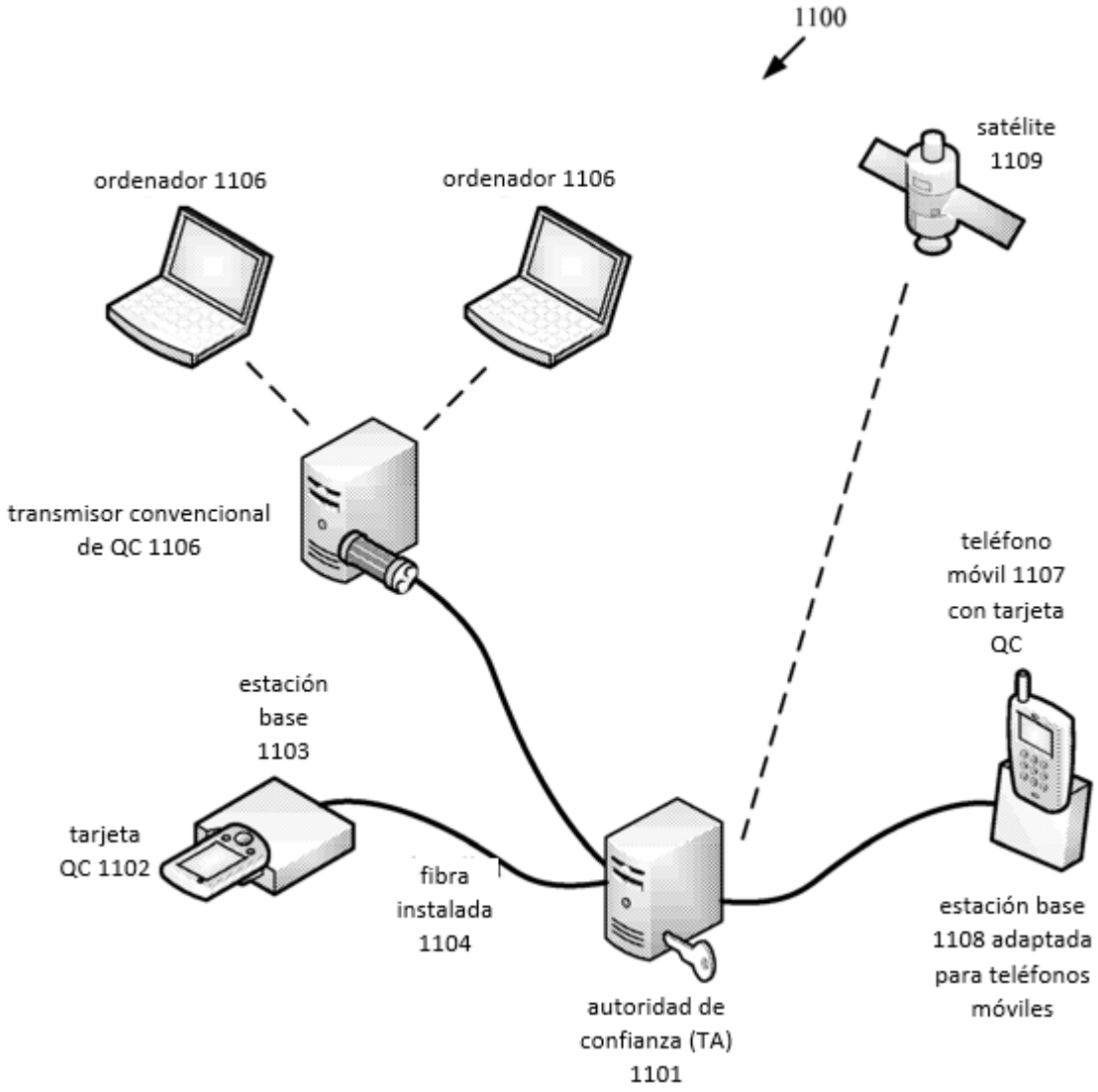
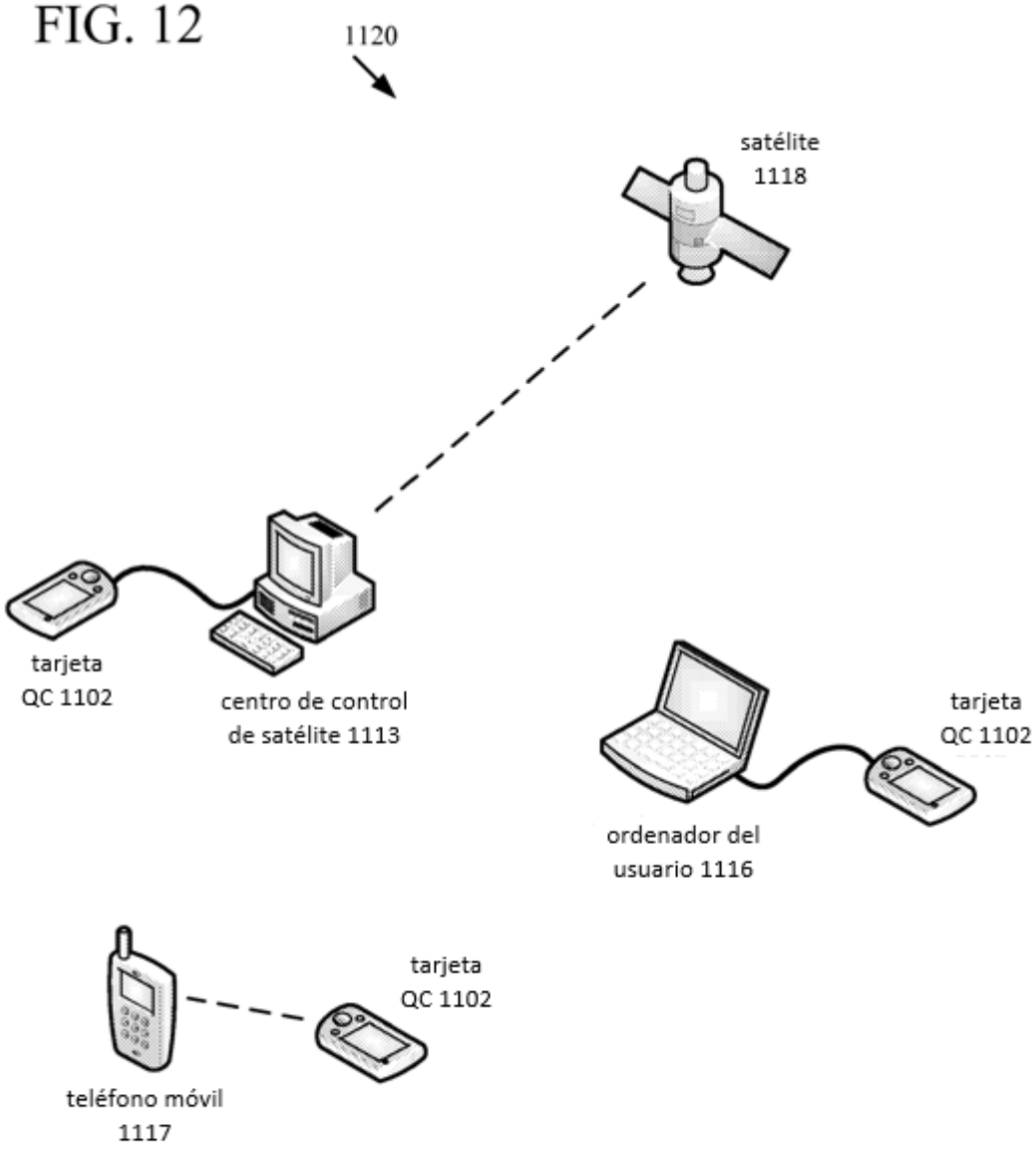

1100
satélite
1109
ordenador 1106
ordenador 1106
transmisor convencional
de QC 1106
teléfono
móvil 1107
con tarjeta
QC
estación
base
1103
tarjeta
QC 1102
fibra
instalada
1104
estación base
1108 adaptada
para teléfonos
móviles
autoridad de
confianza (TA)
1101

FIG. 12


1120
satélite
1118
tarjeta
QC 1102
centro de control
de satélite 1113
tarjeta
QC 1102
ordenador del
usuario 1116
tarjeta
QC 1102
teléfono móvil
1117

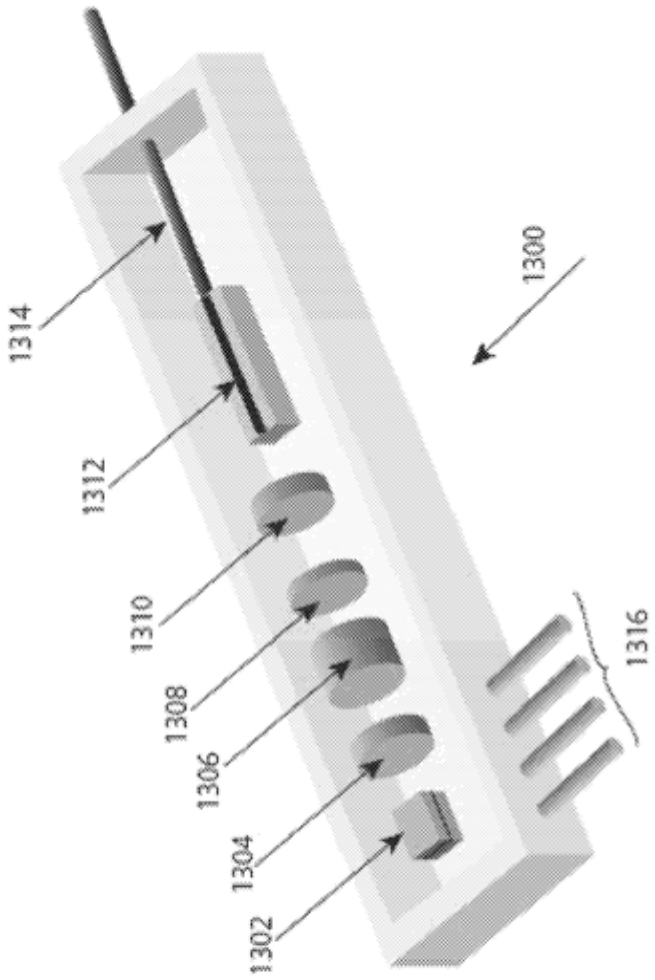



FIG. 13

FIG. 14

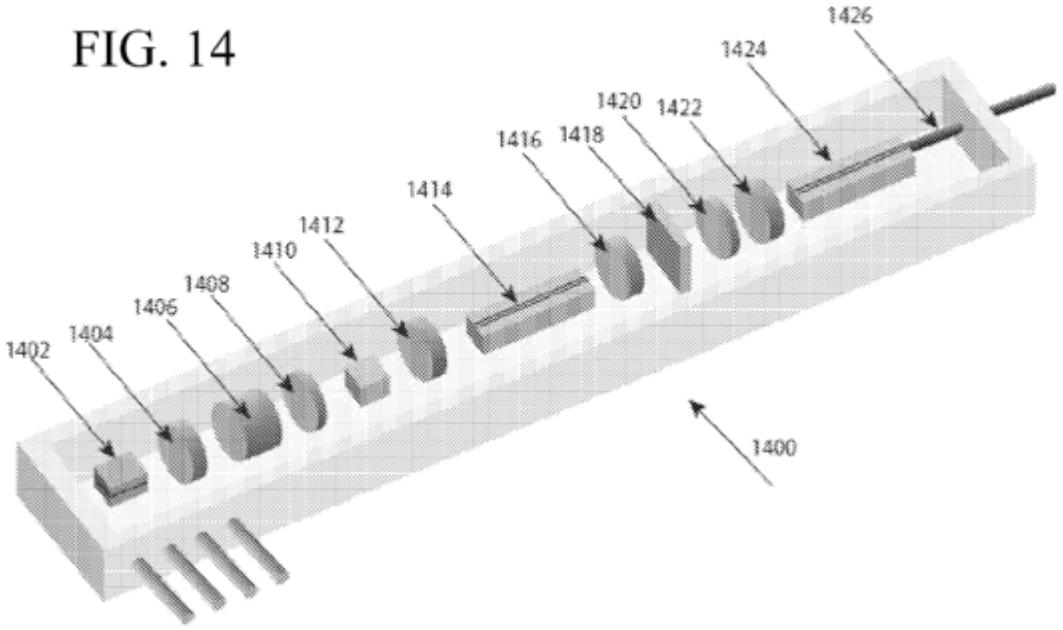

1426
1424
1420
1422
1416
1418
1414
1412
1410
1408
1406
1404
1402
1400

FIG. 15

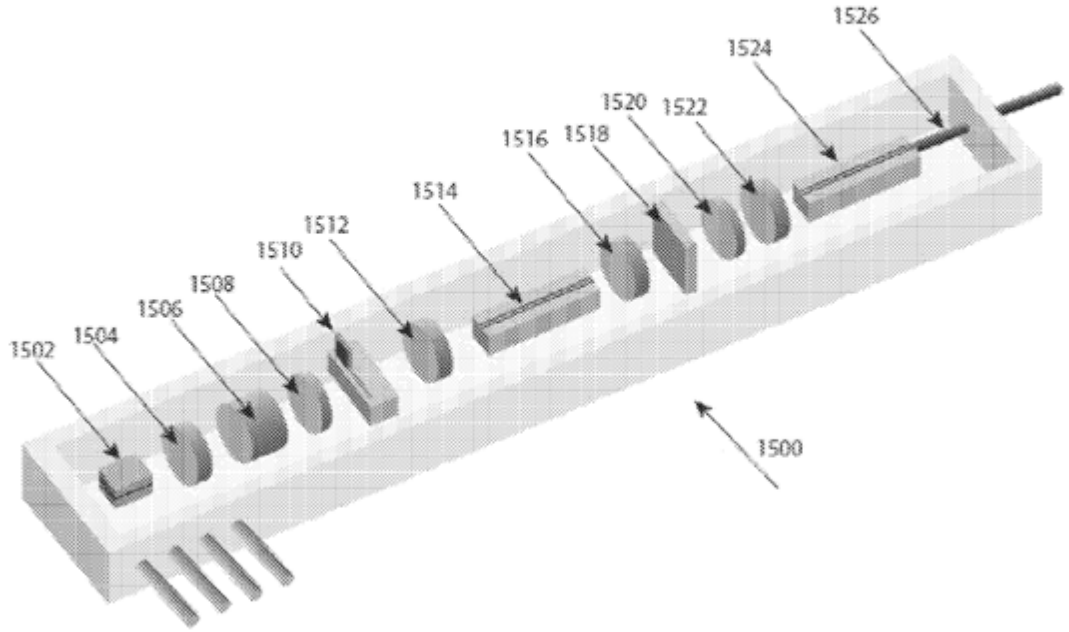

1526
1524
1520
1522
1516
1518
1514
1512
1510
1508
1506
1504
1502
1500

FIG. 16

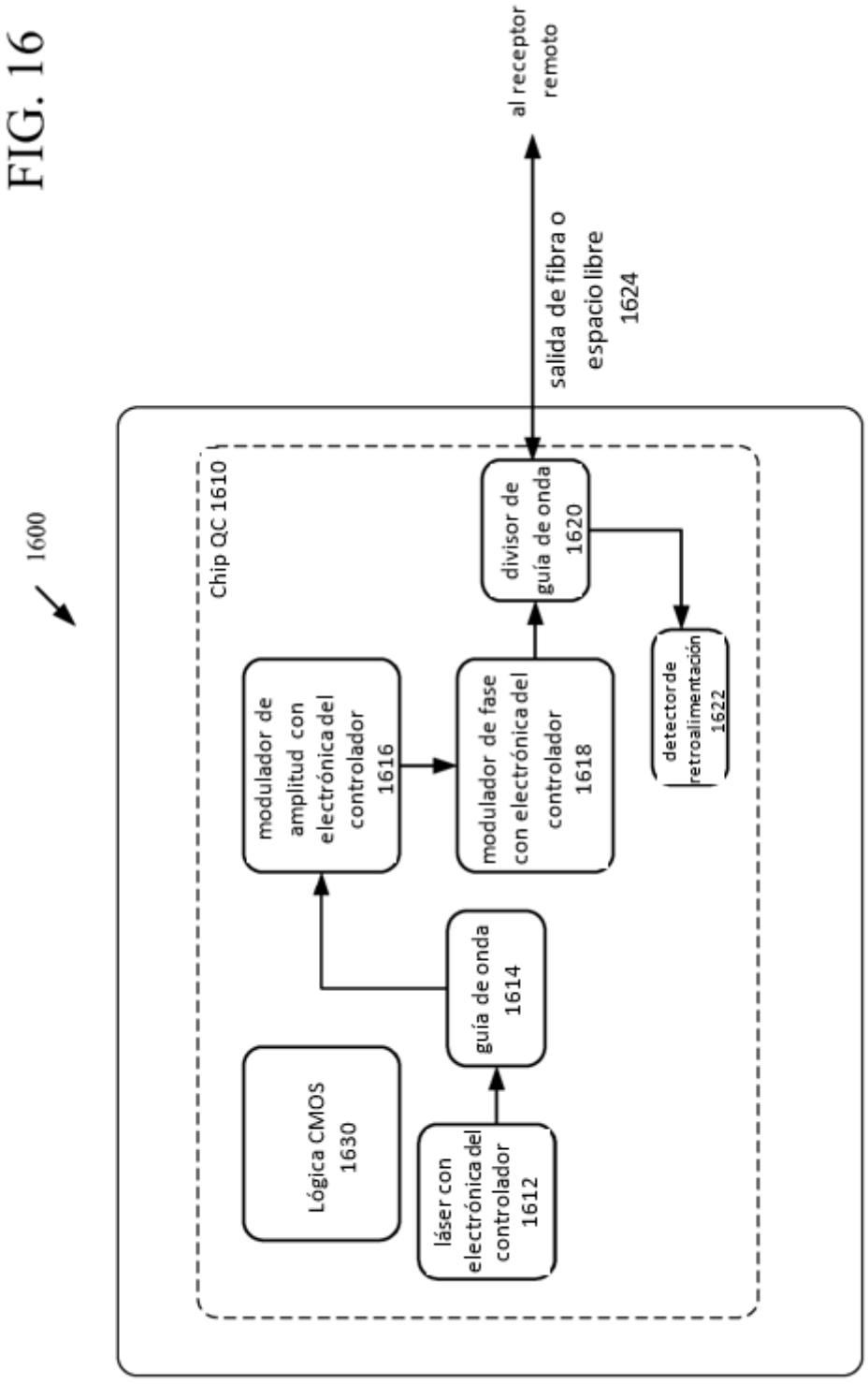
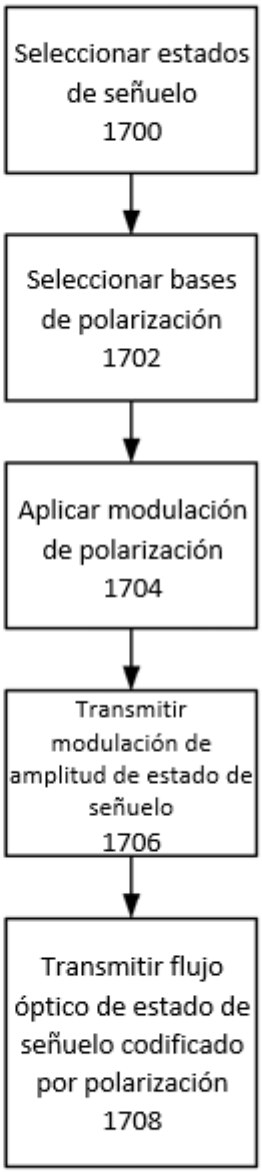

1600
Chip QC 1610
Lógica CMOS 1630
láser con electrónica del controlador 1612
guía de onda 1614
modulador de amplitud con electrónica del controlador 1616
modulador de fase con electrónica del controlador 1618
divisor de guía de onda 1620
detector de retroalimentación 1622
salida de fibra o espacio libre 1624
al receptor remoto

FIG. 17


Seleccionar estados de señuelo 1700
Seleccionar bases de polarización 1702
Aplicar modulación de polarización 1704
Transmitir modulación de amplitud de estado de señuelo 1706
Transmitir flujo óptico de estado de señuelo codificado por polarización 1708