

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 980 162**

51 Int. Cl.:

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: **22.07.2019 PCT/CN2019/097103**

87 Fecha y número de publicación internacional: **30.01.2020 WO20020100**

96 Fecha de presentación y número de la solicitud europea: **22.07.2019 E 19841875 (8)**

97 Fecha y número de publicación de la concesión europea: **24.04.2024 EP 3820076**

54 Título: **Dispositivo y sistema de transmisión de claves cuánticas**

30 Prioridad:

23.07.2018 CN 201810813907

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

30.09.2024

73 Titular/es:

**HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian,
Longgang District
Shenzhen, Guangdong 518129, CN**

72 Inventor/es:

**LI, ZHENGYU;
XIAO, XINHUA y
WU, YUPING**

74 Agente/Representante:

PONS ARIÑO, Ángel

ES 2 980 162 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Dispositivo y sistema de transmisión de claves cuánticas

5 Sector técnico

Esta solicitud se refiere al sector de las tecnologías de las comunicaciones cuánticas y, en particular, a un aparato y sistema de transmisión de claves cuánticas.

10 Antecedentes

Las comunicaciones cuánticas seguras son una nueva tecnología de comunicaciones desarrollada en los últimos 30 años. Las comunicaciones cuánticas seguras son una combinación de propiedades cuánticas y criptografía convencional. En las comunicaciones cuánticas seguras, la seguridad de las comunicaciones se garantiza principalmente basándose en los principios y propiedades básicos de la mecánica cuántica. Actualmente, una de las tecnologías más prácticas en las comunicaciones cuánticas seguras es la transmisión de claves cuánticas. En la transmisión de claves cuánticas, se transporta una clave aleatoria en una señal cuántica para su transmisión.

15

20

En la técnica anterior, cuando se realiza la transmisión de claves cuánticas, un extremo de la transmisión puede generar una señal del oscilador local y una señal cuántica, y transmitir la señal del oscilador local y la señal cuántica a un extremo de recepción a través de un mismo canal. Debido a que la intensidad luminosa de la señal del oscilador local es mucho mayor que la intensidad luminosa de la señal cuántica, la señal del oscilador local fácilmente provoca interferencias con la señal cuántica. Para reducir la diafonía causada por la señal del oscilador local a la señal cuántica, el extremo de transmisión generalmente puede aislar la señal del oscilador local de la señal cuántica mediante multiplexación por división del tiempo y multiplexación por polarización. La multiplexación por división del tiempo significa que un punto del tiempo de envío de la señal del oscilador local es diferente de un punto del tiempo de envío de la señal cuántica, y la multiplexación por polarización significa que las direcciones de polarización de la señal del oscilador local y de la señal cuántica son ortogonales cuando la señal del oscilador local y la señal cuántica entran en una fibra óptica.

25

30

Cuando se utiliza la multiplexación por división del tiempo para transmitir la señal del oscilador local y la señal cuántica, después de recibir la señal del oscilador local y la señal cuántica, el extremo de recepción necesita introducir una diferencia de trayectoria óptica adicional para compensar una latencia entre la señal cuántica y la señal del oscilador local. En consecuencia, el extremo de recepción no puede utilizar un chip óptico integrado y no puede ser miniaturizado. Sin embargo, cuando se utiliza la multiplexación por polarización para transmitir la señal del oscilador local y la señal cuántica, una relación de extinción finita de un multiplexor de polarización limita la intensidad de la señal del oscilador local y, en consecuencia, disminuye la relación de señal a ruido del extremo de recepción.

35

40

El Informe del Grupo de ETSI sobre Distribución de Claves Cuánticas (ETSI GR QKD 003 v2.1.1) analiza componentes e interfaces internas, incluidas implementaciones de QKD de variable continua. En un esquema de oscilador local transmitido, el transmisor produce un estado de oscilador local y un estado de señal que tiene una referencia de fase bien definida. Por lo tanto, ambos pulsos deberían provenir de la misma fuente láser. En una implementación práctica, el pulso láser puede ser dividido mediante un acoplador óptico altamente desequilibrado con los dos puertos de salida correspondientes a una intensidad alta y baja para el canal del oscilador local y al canal de señal cuántica, respectivamente. La señal cuántica es modulada y multiplexada en el oscilador local antes de ser enviada al canal de transmisión. Para separar ambos canales sin grandes pérdidas, se puede utilizar multiplexación por polarización. En el emisor, la señal y el oscilador local se acoplan a los dos puertos de entrada de un divisor de haz de polarización (Polarising Beam Splitter, PBS). En el puerto de salida, una polarización corresponde a la señal y, la otra, al oscilador local. De este modo, los dos pulsos se propagan con un estado de polarización ortogonal en el canal de transmisión. En el receptor, se recuperan los estados iniciales de polarización de los pulsos.

45

50

55

LID et al analizan "Synchronization Schemes for Continuous-Variable Quantum Key Distribution" en la revista Proceedings of SPIE, vol. 10244, páginas 1024408-1 a 1024408-5. Tal como se analiza en ese artículo, la sincronización del reloj es crucial para que un sistema práctico de distribución de claves cuánticas de variable continua obtenga con precisión el resultado de la medición. Se presentan tres esquemas de sincronización diferentes para un sistema de distribución de claves cuánticas de variable continua para demostrar el esquema óptimo. El rendimiento del esquema de sincronización se evalúa midiendo el exceso de ruido, que es el parámetro crítico para el sistema de distribución de claves cuánticas de variable continua. Los resultados del experimento muestran que obtener la señal de sincronización del oscilador local tiene la implementación física más simple y un efecto de sincronización superior, pero se requiere un oscilador local más fuerte. La transmisión de señales de sincronización y señales cuánticas en la misma fibra mediante multiplexación por división de la longitud de onda también es una excelente manera de proporcionar un reloj estable cuando no tenemos en cuenta el dispositivo físico ni la fuente de longitud de onda.

60

65

Compendio

5 Esta solicitud da a conocer un aparato y sistema de transmisión de claves cuánticas, para resolver el problema de que un extremo de recepción no puede ser miniaturizado y la relación de señal a ruido disminuye cuando una señal cuántica y una señal del oscilador local son aisladas una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Las soluciones técnicas son las siguientes:

10 Según un primer aspecto, se da a conocer un aparato de envío de claves cuánticas tal como se establece en la reivindicación 1.

15 En esta realización de esta solicitud, el aparato de envío de claves cuánticas puede ajustar una dirección de polarización de la señal cuántica y una dirección de polarización de la señal de referencia mediante la utilización de un controlador de polarización, y enviar una señal del oscilador local y una señal cuántica ajustada a diferentes fibras ópticas para su transmisión. De esta manera, la señal del oscilador local y la señal cuántica ya no necesitan estar aisladas una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Sobre esta base, en un receptor de señales cuánticas en un extremo de recepción, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación de latencia, y el extremo de recepción puede ser integrado y miniaturizado. Además, la multiplexación por polarización ya no es necesaria en la transmisión de la señal del oscilador local y la señal cuántica. Por lo tanto, la intensidad de la señal del oscilador local no está limitada por una relación de extinción finita de un multiplexor de polarización, y se mejora la relación de señal a ruido recibida. Además, ya no es necesario realizar el aislamiento mediante multiplexación por división del tiempo. Por lo tanto, no es necesario asignar ningún recurso en una fibra óptica utilizada para transmitir la señal cuántica para transmitir la señal del oscilador local. En otras palabras, todos los recursos de la fibra óptica se pueden utilizar para transmitir la señal cuántica. Esto mejora la proporción de transmisión de la señal cuántica en una unidad de tiempo.

30 En una posible implementación, la intensidad luminosa de la segunda señal óptica es mayor que la intensidad luminosa de la tercera señal óptica.

En una posible implementación, el aparato incluye, además, un receptor y un procesador, donde el receptor está configurado para: recibir información de control de la dirección de polarización y enviar la información de control de la dirección de polarización, al procesador;

40 el procesador está configurado para: procesar la información de control de la dirección de polarización para obtener una primera señal de control, y enviar la primera señal de control, al módulo de control de la polarización; y

el módulo de control de la polarización está configurado específicamente para ajustar la dirección de polarización de la primera señal modulada y la dirección de polarización de la segunda señal modulada sobre la base de la primera señal de control.

45 La información de control de la dirección de polarización puede ser información de ángulo que es retroalimentada por un extremo de recepción sobre la base de un resultado de detección generado al detectar la señal de referencia y la señal del oscilador local, y que se utiliza para indicar un ángulo de polarización que necesita ser ajustado.

50 En una posible implementación, el módulo de generación de señales cuánticas incluye un generador de números aleatorios cuánticos, un procesador y un modulador; el generador de números aleatorios cuánticos está configurado para: generar un número aleatorio y enviar el número aleatorio al procesador; el procesador está configurado para: generar la clave aleatoria basándose en el número aleatorio y generar una señal de control cuántica basándose en la clave aleatoria; y está configurado, además, para: generar una señal de control de referencia basándose en los datos de referencia almacenados, y enviar la señal de control cuántica y la señal de control de referencia, al modulador; y el modulador está configurado para: modular la tercera señal óptica basándose en la señal de control cuántica para obtener la primera señal modulada, modular la tercera señal óptica basándose en la señal de control de referencia para obtener la segunda señal modulada, y enviar la primera señal modulada y la segunda señal modulada, al módulo de control de la polarización.

60 En una posible implementación, el módulo de control de la polarización incluye un controlador de polarización y un atenuador; el controlador de polarización está configurado para: ajustar la dirección de polarización de la primera señal modulada y la dirección de polarización de la segunda señal modulada, y enviar una primera señal modulada ajustada y una segunda señal modulada ajustada, al atenuador; y el atenuador está configurado para: atenuar la primera señal modulada ajustada para obtener la señal cuántica, y atenuar la

segunda señal modulada ajustada para obtener la señal de referencia.

5 En una posible implementación, el módulo de control de la polarización incluye un controlador de polarización y un atenuador; el atenuador está configurado para: atenuar la primera señal modulada y la segunda señal modulada para obtener una primera señal modulada atenuada y una segunda señal modulada atenuada, y enviar la primera señal modulada atenuada y la segunda señal modulada atenuada al controlador de polarización; y el controlador de polarización está configurado para: ajustar una dirección de polarización de la primera señal modulada atenuada para obtener la señal cuántica, y atenuar una dirección de polarización de la segunda señal modulada atenuada para obtener la señal de referencia.

10 En una posible implementación, la longitud de onda de la segunda señal óptica es diferente de la longitud de onda de otra señal óptica transmitida a través de la primera fibra óptica, y la longitud de onda de la tercera señal óptica es diferente de la longitud de onda de otra señal óptica transmitida a través de la segunda fibra óptica.

15 En una posible implementación, la segunda fibra óptica se utiliza, además, para transmitir una señal óptica coherente, y la dirección de transmisión de la señal óptica coherente transmitida a través de la segunda fibra óptica es opuesta a la dirección de transmisión de la señal cuántica transmitida sobre la segunda fibra óptica.

20 En esta realización de esta solicitud, el controlador de polarización está dispuesto en una ruta de transmisión de señal cuántica del aparato de envío de claves cuánticas, y ajusta una dirección de polarización de la señal cuántica basándose en la información de control de la dirección de polarización que es retroalimentada por un aparato de recepción de claves cuánticas basándose en el resultado de la detección. De esta manera, la señal cuántica y la señal del oscilador local que son recibidas por el aparato de recepción de claves cuánticas pueden tener una misma dirección de polarización o tener una diferencia de dirección de polarización fija, o la señal cuántica recibida siempre puede ser estabilizada en una dirección de polarización. Esto puede mejorar el efecto de interferencia entre la señal cuántica y la señal del oscilador local, y garantizar aún más la precisión del resultado de una detección. Además, la señal cuántica generada debe pasar a través del controlador de polarización antes de ser enviada a la segunda fibra óptica para su transmisión. El propio controlador de polarización atenúa la señal hasta cierto punto. Por lo tanto, cuando se atenúa una tercera señal óptica modulada para obtener la señal cuántica, el atenuador puede reducir correspondientemente la intensidad de atenuación de la señal. Esto reduce la carga de trabajo del atenuador y no afecta a la intensidad de la señal del oscilador local.

35 Según un segundo aspecto, se da a conocer un aparato de recepción de claves cuánticas, según la reivindicación 9.

40 En esta realización de esta solicitud, el aparato de recepción de claves cuánticas puede recibir la señal del oscilador local y la señal cuántica que se transmiten a través de dos fibras ópticas diferentes, y controlar la dirección de polarización de la señal del oscilador local o la señal cuántica utilizando el módulo de control de la polarización dispuesto en una ruta de transmisión de la señal del oscilador local o una ruta de transmisión de la señal cuántica. En un proceso de transmisión, la señal del oscilador local y la señal cuántica no están aisladas una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Por lo tanto, en el aparato de recepción de claves cuánticas, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación de la latencia, y el aparato de recepción de claves cuánticas puede ser integrado y miniaturizado. Además, la intensidad de la señal del oscilador local no está limitada por una relación de extinción finita de un multiplexor de polarización, y se mejora la relación de señal a ruido del extremo de recepción. Además, el módulo de control de la polarización ajusta la dirección de polarización de la señal del oscilador local o de la señal cuántica. De esta manera, la señal del oscilador local y la señal cuántica pueden tener la misma dirección de polarización o tener una diferencia de dirección de polarización fija, o la señal del oscilador local siempre puede ser estabilizada en una dirección de polarización. Esto puede mejorar el efecto de interferencia entre la señal cuántica y la señal del oscilador local, y garantizar aún más la precisión del resultado de una detección.

55 Según un tercer aspecto, se da a conocer un aparato de recepción de claves cuánticas tal como se establece en la reivindicación 10.

60 En esta realización de esta solicitud, no se puede disponer un módulo de control de la polarización en el aparato de recepción de claves cuánticas. En cambio, el primer divisor de haz de polarización y el segundo divisor de haz de polarización se utilizan para realizar la división del haz en la señal del oscilador local, la señal cuántica y la señal de referencia. A continuación, el primer detector heterodino cuántico y el segundo detector heterodino cuántico se utilizan para medir una componente regular de la señal de referencia y una componente regular de la señal cuántica, calcular, además, el parámetro de señal basándose en la componente regular de la señal de referencia y, finalmente, procesar la componente regular de la señal cuántica basándose en el parámetro de la señal para obtener la clave inicial, para eliminar el impacto causado por la rotación de la polarización y garantizar la precisión de la información de clave obtenida.

Según un cuarto aspecto, se da a conocer un sistema de transmisión de claves cuánticas tal como se establece en la reivindicación 11.

5 Los efectos técnicos conseguidos en el segundo aspecto, el tercer aspecto y el cuarto aspecto son similares a los conseguidos utilizando los medios técnicos correspondientes en el primer aspecto. Los detalles no se describen de nuevo en la presente memoria.

10 Las soluciones técnicas dadas a conocer en esta solicitud tienen al menos los siguientes efectos beneficiosos:

En esta realización de esta solicitud, se da a conocer el aparato de envío de claves cuánticas, y puede ajustar la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia mediante la utilización de un controlador de polarización, y enviar la señal del oscilador local y la
15 señal cuántica ajustada a diferentes fibras ópticas, para su transmisión. De esta manera, la señal del oscilador local y la señal cuántica ya no necesitan estar aisladas una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Sobre esta base, en un receptor de señales cuánticas en un extremo de recepción, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación de latencia, y el extremo de recepción puede ser integrado y miniaturizado. Además, la
20 señal del oscilador local y la señal cuántica ya no necesitan estar aisladas una de otra mediante la multiplexación por polarización. Por lo tanto, la intensidad de la señal del oscilador local no está limitada por una relación de extinción finita de un multiplexor de polarización, y se mejora la relación de señal a ruido del extremo de recepción. Además, ya no es necesario realizar el aislamiento mediante multiplexación por división del tiempo. Por lo tanto, no es necesario asignar ningún recurso en una fibra óptica utilizada para
25 transmitir la señal cuántica para transmitir la señal del oscilador local. En otras palabras, todos los recursos de la fibra óptica se pueden utilizar para transmitir la señal cuántica. Esto mejora la proporción de transmisión de la señal cuántica en una unidad de tiempo.

Breve descripción de los dibujos

30 La figura 1 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

35 la figura 2 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

la figura 3 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

40 la figura 4 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

la figura 5 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

45 la figura 6 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

50 la figura 7 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

la figura 8 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud;

55 la figura 9 es un diagrama estructural esquemático de un aparato de recepción de claves cuánticas, según una realización de esta solicitud;

la figura 10 es un diagrama estructural esquemático de un aparato de recepción de claves cuánticas, según una realización de esta solicitud;

60 la figura 11 es un diagrama estructural esquemático de un aparato de recepción de claves cuánticas según un ejemplo antecedente que queda fuera del alcance de las reivindicaciones adjuntas;

65 la figura 12 es un diagrama estructural esquemático de un aparato de recepción de claves cuánticas, según una realización de esta solicitud;

la figura 13 es un diagrama estructural esquemático de un aparato de recepción de claves cuánticas, según una realización de esta solicitud;

5 la figura 14 es un diagrama estructural esquemático de un sistema de transmisión de claves cuánticas, según una realización de esta solicitud; y

la figura 15 es un diagrama estructural esquemático de un sistema de transmisión de claves cuánticas, según una realización de esta solicitud.

10 Descripción de las realizaciones

Para aclarar aún más los objetivos, las soluciones técnicas y las ventajas de esta solicitud, a continuación se describen adicionalmente, en detalle, las implementaciones de esta solicitud, con referencia a los dibujos adjuntos.

15

La figura 1 es un diagrama estructural esquemático de un aparato de envío de claves cuánticas, según una realización de esta solicitud. Tal como se muestra en la figura 1, el aparato incluye un láser 101, un divisor de haz 102, un módulo de generación de señales cuánticas 103 y un controlador de polarización 104.

20

El láser 101 está configurado para emitir una primera señal óptica. El divisor de haz 102 está configurado para: recibir la primera señal óptica, dividir la primera señal óptica en una segunda señal óptica y una tercera señal óptica, enviar la segunda señal óptica a través de una primera fibra óptica, y enviar la tercera señal óptica al módulo de generación de señales cuánticas 103. El módulo de generación de señales cuánticas 103 está configurado para: modular la tercera señal óptica para obtener una señal cuántica y una señal de referencia, y enviar la señal cuántica y la señal de referencia al controlador de polarización 104, donde la señal cuántica lleva una clave aleatoria a transmitir. El controlador de polarización 104 está configurado para: ajustar una dirección de polarización de la señal cuántica y una dirección de polarización de la señal de referencia, y enviar una señal cuántica ajustada y una señal de referencia ajustada, a través de una segunda fibra óptica. Opcionalmente, la intensidad luminosa de la segunda señal óptica es mayor que la intensidad luminosa de la tercera señal óptica.

25

30

35

Por ejemplo, el láser 101 puede ser un láser que puede generar una señal óptica polarizada linealmente de ancho de línea estrecho, puede ser un láser que emite una señal láser de pulso que tiene una relación de fase estable, o puede ser un láser que emite una señal láser continua. El láser 101 incluye un puerto de salida. El láser 101 puede emitir la primera señal óptica a través del puerto de salida. Opcionalmente, cuando posteriormente se transmiten señales a través de la primera fibra óptica y la segunda fibra óptica, también se pueden transmitir otras señales ópticas a través de la primera fibra óptica y la segunda fibra óptica. Por ejemplo, también se pueden transmitir señales ópticas coherentes clásicas a través de la primera fibra óptica y la segunda fibra óptica. Sobre esta base, en esta realización de esta solicitud, el láser 101 puede emitir la primera señal óptica cuya longitud de onda es diferente de las longitudes de onda de las otras señales ópticas transmitidas a través de la primera fibra óptica y la segunda fibra óptica.

40

45

El divisor de haz 102 puede incluir un puerto de entrada y dos puertos de salida. El puerto de entrada del divisor de haz 102 está conectado al puerto de salida del láser 101. El divisor de haz 102 puede recibir, a través del puerto de entrada incluido, la primera señal óptica enviada por el láser 101, y dividir la primera señal óptica en la segunda señal óptica y la tercera señal óptica basándose en una relación de división de haz del divisor de haz 102. La intensidad luminosa de la señal de un oscilador local suele ser alta. Por lo tanto, después de la división del haz, se puede utilizar una señal óptica con mayor intensidad de luz como segunda señal óptica, y se puede utilizar una señal óptica con menor intensidad de luz como tercera señal óptica. La relación de división de haz del divisor de haz 102 puede ser 10:90, 1:99 o similar.

50

55

Después de dividir la primera señal óptica en la segunda señal óptica y la tercera señal óptica, el divisor de haz 102 puede emitir la segunda señal óptica a través de un primer puerto de salida incluido, y emitir la tercera señal óptica a través de un segundo puerto de salida incluido. Cabe señalar que el primer puerto de salida del divisor de haz 102 puede ser conectado directamente a la primera fibra óptica, o el primer puerto de salida del divisor de haz 102 puede ser conectado a la primera fibra óptica utilizando un acoplador. De esta manera, la segunda señal óptica emitida desde el primer puerto de salida se envía como la señal del oscilador local a través de la primera fibra óptica. El segundo puerto de salida del divisor de haz 102 puede ser conectado al módulo de generación de señales cuánticas 103. De esta manera, el divisor de haz 102 puede enviar la tercera señal óptica al módulo de generación de señales cuánticas 103 a través del segundo puerto de salida.

60

65

El módulo de generación de señales cuánticas 103 puede recibir la tercera señal óptica enviada por el divisor de haz 102, y modular la tercera señal óptica basándose en la clave aleatoria y en los datos de referencia, para obtener la señal cuántica que transporta la clave aleatoria y la señal de referencia que transporta.

Por ejemplo, haciendo referencia a la figura 2, el módulo de generación de señales cuánticas 103 puede incluir un generador de números aleatorios cuánticos 1031, un módulo de procesamiento 1032, un modulador 1033 y un atenuador 1034. El generador de números aleatorios cuánticos 1031 está configurado para: generar un número aleatorio y enviar el número aleatorio al módulo de procesamiento 1032. Después de recibir el número aleatorio enviado por el generador de números aleatorios cuánticos 1031, el módulo de procesamiento 1032 puede procesar el número aleatorio según un protocolo o un estándar, para generar la clave aleatoria, y generar, basándose en la clave aleatoria, una señal de control utilizada para controlar el modulador 1033 para modular la señal cuántica. Asimismo, el módulo de procesamiento 1032 puede generar además, basándose en los datos de referencia almacenados, una señal de control, utilizada para controlar que el modulador 1033 module la señal de referencia. A continuación, el módulo de procesamiento 1032 puede enviar las dos señales de control anteriores, al modulador 1033. El modulador 1033 puede modular la tercera señal óptica basándose en las dos señales de control anteriores, para obtener la señal cuántica y la señal de referencia, y permitir que la señal cuántica y la señal de referencia se ubiquen en diferentes bandas de frecuencia. El modulador 1033 envía una señal modulada al atenuador 1034. El atenuador 1034 atenúa la intensidad de la señal modulada, para obtener la señal cuántica que transporta la clave aleatoria y la señal de referencia que transporta los datos de referencia.

Opcionalmente, en una posible implementación, el módulo de generación de señales cuánticas 103 puede enviar la señal cuántica y la señal de referencia en un modo de división del tiempo. En otras palabras, en un período de tiempo, el módulo de procesamiento 1032 en el módulo de generación de señales cuánticas 103 puede generar, basándose en la clave aleatoria, una señal de control cuántica utilizada para controlar el modulador 1033 y, a continuación, controlar, basándose en la señal de control cuántica, el modulador 1033, para realizar la modulación, para obtener la señal cuántica. En otro período de tiempo diferente del período de tiempo, el módulo de procesamiento 1032 puede generar, basándose en los datos de referencia, una señal de control de referencia utilizada para controlar el modulador 1033 y, a continuación, controlar, basándose en la señal de control de referencia, el modulador 1033, para realizar modulación, para obtener la señal de referencia.

Opcionalmente, además de enviar la señal cuántica y la señal de referencia en un modo de multiplexación por división del tiempo o multiplexación por división de la frecuencia, el módulo de generación de señales cuánticas 103 también puede enviar la señal cuántica y la señal de referencia en un modo de multiplexación por polarización. Es decir, cuando el módulo de generación de señales cuánticas 103 introduce la señal cuántica y la señal de referencia en un canal, la dirección de polarización de la señal cuántica puede ser ortogonal a la dirección de polarización de la señal de referencia. En este caso, el modulador puede ser un modulador de polarización dual, por ejemplo, un modulador de polarización dual-desplazamiento de fase en cuadratura (Dual Polarization-Quadrature Phase Shift Keying, DP-QPSK).

El controlador de polarización 104 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El controlador de polarización 104 puede recibir, a través del primer puerto de entrada incluido, la señal cuántica y la señal de referencia que son enviadas por el módulo de generación de señales cuánticas 103, y recibir una primera señal de control a través del segundo puerto de entrada. A continuación, el controlador de polarización 104 puede ajustar la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia basándose en la primera señal de control, y emitir la señal cuántica ajustada y la señal de referencia ajustada a través del puerto de salida incluido. El puerto de salida del controlador de polarización 104 puede ser conectado directamente a la segunda fibra óptica, o puede ser conectado a la segunda fibra óptica mediante el uso de un acoplador. De esta manera, la señal cuántica ajustada y la señal de referencia ajustada emitidas desde el puerto de salida del controlador de polarización 104 pueden ser enviadas a través de la segunda fibra óptica.

Cabe señalar que la primera señal de control puede ser una señal de control que se genera mediante un aparato de recepción de claves cuánticas sobre la base de un resultado de detección obtenido detectando la señal de referencia y la señal del oscilador local, y que es retroalimentado por el aparato de recepción de claves cuánticas.

Opcionalmente, en una posible implementación, el aparato de recepción de claves cuánticas solo puede generar información de control de la dirección de polarización basándose en el resultado de detección obtenido al detectar la señal de referencia y la señal del oscilador local, y retroalimentar la información de control de la dirección de polarización, y el aparato de envío de claves cuánticas procesa la información de control de la dirección de polarización para obtener, además, la primera señal de control. En este caso, haciendo referencia a la figura 3, el aparato de envío de claves cuánticas puede incluir, además, un receptor 105 y un procesador 106. El receptor 105 está configurado para: recibir información de control de la dirección de polarización y enviar la información de control de la dirección de polarización, al procesador 106; El procesador 106 está configurado para: recibir la información de control de la dirección de polarización, procesar la información de control de la dirección de polarización para obtener la primera señal de control, y enviar la primera señal de control al controlador de polarización 104. El controlador de polarización 104 está configurado específicamente para ajustar la dirección de polarización de la señal cuántica y la dirección de

polarización de la señal de referencia basándose en la primera señal de control.

5 Cabe señalar que el receptor 105 puede incluir un puerto de entrada y un puerto de salida. El receptor 105 puede recibir, a través del puerto de entrada, la información de control de la dirección de polarización retroalimentada por el aparato de recepción de claves cuánticas. La información de control de la dirección de polarización puede ser información de ángulo utilizada para indicar un ángulo de polarización que necesita ser ajustado. Después de recibir la información de control de la dirección de polarización, el receptor 105 puede enviar la información de control de la dirección de polarización al procesador 106 a través del puerto de salida.

10 El procesador 106 puede incluir un puerto de entrada y un puerto de salida. El puerto de entrada incluido en el procesador 106 está conectado al puerto de salida del receptor 105. De esta manera, el procesador 106 puede recibir, a través del puerto de entrada incluido, la información de control de la dirección de polarización enviada por el receptor 105. El puerto de salida incluido en el procesador 106 puede ser conectado al
15 segundo puerto de entrada del controlador de polarización 104. De esta manera, después de procesar la información de control de la dirección de polarización para obtener la primera señal de control, el procesador 106 puede enviar la primera señal de control al controlador de polarización 104 a través del puerto de salida incluido.

20 El aparato de recepción de claves cuánticas normalmente codifica la información del ángulo de polarización que necesita ser ajustado y, a continuación, envía información del ángulo codificada. Por lo tanto, después de que el receptor 105 envía la información de control de la dirección de polarización recibida al procesador 106, el procesador 106 puede decodificar la información de control de la dirección de polarización de acuerdo con un protocolo o un estándar negociado con el aparato de recepción de claves cuánticas de antemano, para
25 obtener el ángulo de polarización que necesita ser ajustado. A continuación, el procesador 106 puede generar una señal analógica basándose en el ángulo de polarización, donde la señal analógica es la primera señal de control utilizada para controlar el controlador de polarización 104 para ajustar la dirección de polarización.

30 Después de recibir la primera señal de control a través del segundo puerto de entrada, el controlador de polarización 104 puede ajustar, basándose en la primera señal de control, las direcciones de polarización de la señal cuántica y la señal de referencia que son enviadas por el módulo de generación de señales cuánticas 103, para obtener la señal cuántica ajustada y la señal de referencia ajustada.

35 Opcionalmente, en una posible implementación, haciendo referencia a la figura 4, el aparato de envío de claves cuánticas puede incluir además un divisor de haz 107 y un módulo de generación de señal de referencia 108, para aumentar la intensidad luminosa de la señal de referencia, de modo que cuando las fases y la polarización de las dos fibras ópticas cambien relativamente rápido, un extremo de recepción pueda restaurar con mayor precisión, basándose en la señal de referencia, información de clave transportada
40 en la señal cuántica.

Un puerto de entrada del divisor de haz 107 está conectado al segundo puerto de salida del divisor de haz 102, un primer puerto de salida del divisor de haz 107 está conectado al modulador 1033 incluido en el módulo de generación de señales cuánticas 103, y un segundo puerto de salida del divisor de haz 107 está
45 conectado al módulo de generación de señal de referencia 108. De esta manera, el divisor de haz 107 puede recibir, a través del puerto de entrada incluido, la tercera señal óptica enviada por el divisor de haz 102 a través del segundo puerto de salida. Después de recibir la tercera señal óptica, el divisor de haz 107 puede dividir la tercera señal óptica en dos señales ópticas. El divisor de haz 107 puede enviar una de las dos señales ópticas al modulador 1033 a través del primer puerto de salida incluido, y enviar la otra señal óptica
50 al módulo de generación de señal de referencia a través del segundo puerto de salida.

El modulador 1033 en el módulo de generación de señales cuánticas 103 puede recibir la señal óptica enviada por el divisor de haz 107, y modular la señal óptica recibida basándose en el método descrito anteriormente, de modo que una primera señal de referencia y la señal cuántica estén ubicadas en diferentes
55 bandas de frecuencia.

El módulo de generación de señal de referencia 108 puede recibir la otra señal óptica enviada por el divisor de haz 107, y modular la señal óptica recibida para obtener una segunda señal de referencia. La segunda señal de referencia está situada en una banda de frecuencia diferente de las bandas de frecuencia en las que se encuentran la primera señal de referencia y la señal cuántica.
60

Por ejemplo, el módulo de generación de señal de referencia 108 puede incluir un desplazador de frecuencia 1081, un módulo de procesamiento 1082, un modulador 1083 y un atenuador 1084. El segundo puerto de salida del divisor de haz 107 está conectado a un puerto de entrada del desplazador de frecuencia 1081. De esta manera, el desplazador de frecuencia 1081 puede recibir, a través del puerto de entrada incluido, la otra
65 señal óptica enviada por el divisor de haz 107. Después de recibir la señal óptica enviada por el divisor de

haz 107, el desplazador de frecuencia 1081 puede realizar un pequeño cambio de frecuencia en la señal óptica recibida. A continuación, el desplazador de frecuencia 1081 puede enviar una señal óptica de frecuencia desplazada al modulador 1083.

5 El módulo de procesamiento 1082 puede generar, basándose en los datos de referencia almacenados, una señal de control utilizada para controlar el modulador 1083 para modular la segunda señal de referencia. A continuación, el módulo de procesamiento 1082 puede enviar la señal de control al modulador 1083 a través de un puerto de salida.

10 El modulador 1083 incluye dos puertos de entrada y un puerto de salida. Un primer puerto de entrada del modulador 1083 puede ser conectado a un puerto de salida del desplazador de frecuencia 1081. De esta manera, el modulador 1083 puede recibir, a través del primer puerto de entrada incluido, la señal óptica de frecuencia desplazada enviada por el desplazador de frecuencia 1081. Un segundo puerto de entrada del modulador 1083 está conectado al puerto de salida del módulo de procesamiento 1082. De esta manera, el
 15 modulador 1083 puede recibir, a través del segundo puerto de entrada incluido, la señal de control que se utiliza para modular la segunda señal de referencia y que es enviada por el módulo de procesamiento 1082. Después de recibir la señal de control enviada por el módulo de procesamiento 1082, el modulador 1083 puede modular, basándose en la señal de control, la señal óptica recibida con desplazamiento de frecuencia enviada por el desplazador de frecuencia 1081, y enviar una señal modulada al atenuador 1084 a través del
 20 puerto de salida. La señal modulada y la primera señal de referencia transportan los mismos datos de referencia.

Después de recibir la señal modulada, el atenuador 1084 puede atenuar la señal modulada para obtener la segunda señal de referencia, y enviar la segunda señal de referencia al controlador de polarización 104.

25 El controlador de polarización 104 puede recibir la primera señal de referencia, la señal cuántica y la segunda señal de referencia. El controlador de polarización 104 puede recibir, además, la primera señal de control y ajustar una dirección de polarización de la primera señal de referencia, la dirección de polarización de la señal cuántica y la dirección de polarización de la segunda señal de referencia basándose en la primera
 30 señal de control. A continuación, el controlador de polarización puede emitir una primera señal de referencia ajustada en la dirección de polarización, la señal cuántica ajustada en la dirección de polarización y una segunda señal de referencia ajustada en la dirección de polarización a través del puerto de salida incluido y la segunda fibra óptica.

35 En esta realización de esta solicitud, la intensidad luminosa de la señal cuántica es muy baja. Por lo tanto, es difícil implementar una alta intensidad luminosa para la primera señal de referencia generada junto con la señal cuántica. Sin embargo, en esta implementación, el módulo de generación de señal de referencia está dispuesto en el aparato de envío de claves cuánticas y, por lo tanto, la segunda señal de referencia puede ser generada utilizando el módulo de generación de señal de referencia independiente. De esta manera, la
 40 intensidad luminosa de la segunda señal de referencia se puede controlar por separado, para permitir que la intensidad luminosa de la segunda señal de referencia sea mayor que la intensidad luminosa de la primera señal de referencia. De esta manera, la primera señal de referencia y la segunda señal de referencia se envían simultáneamente al extremo de recepción, y el extremo de recepción recibe dos señales de referencia. En otras palabras, la intensidad luminosa de la señal de referencia aumenta considerablemente.
 45 Sobre esta base, la información de clave contenida en la señal cuántica se puede restaurar con mayor precisión basándose en la señal de referencia.

Opcionalmente, el módulo de generación de señales cuánticas 103 puede incluir un generador de números aleatorios cuánticos 1031, un módulo de procesamiento 1032 y un modulador 1033; y el módulo de generación de señal de referencia 108 puede incluir un desplazador de frecuencia 1081, un módulo de procesamiento 1082 y un modulador 1083. Las funciones de los componentes anteriores son las mismas que las descritas en la realización de la figura 5, y los detalles no se describen aquí nuevamente. Tanto un extremo de salida del modulador 1033 como un extremo de salida del modulador 1083 están conectados al controlador de polarización 104. Después del ajuste de la polarización, se envía una señal ajustada a un
 50 atenuador 109 para obtener una primera señal de referencia ajustada, una segunda señal de referencia ajustada y la señal cuántica ajustada, y la primera señal de referencia ajustada, la segunda señal de referencia ajustada y la señal cuántica se envían a través de la segunda fibra óptica. Opcionalmente, la intensidad luminosa de una señal enviada por el divisor de haz 107 al módulo de generación de señal de referencia 108 es mayor que la intensidad luminosa de una señal enviada por el divisor de haz 107 al módulo de generación de señales cuánticas 103.
 55 60

En esta realización de esta solicitud, el aparato de envío de claves cuánticas puede enviar la señal del oscilador local a través de la primera fibra óptica, y enviar la señal cuántica ajustada y la señal de referencia ajustada a través de la segunda fibra óptica. La primera fibra óptica y la segunda fibra óptica pueden ser
 65 fibras ópticas que están especialmente dispuestas entre el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas, y que se utilizan para comunicaciones cuánticas. Opcionalmente, en una

5 posible implementación, considerando un escenario en el que se utilizan dos fibras para transmitir señales ópticas coherentes en un sistema de comunicaciones coherente clásico para implementar comunicación bidireccional, en esta realización de esta solicitud, un sistema de comunicaciones cuánticas que incluye el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas puede compartir las dos
 10 fibras ópticas con el sistema de comunicaciones coherente clásico para la transmisión de señales. En otras palabras, la primera fibra óptica y la segunda fibra óptica en esta realización de esta solicitud no solo pueden ser utilizadas para comunicaciones cuánticas, sino también para transmitir señales ópticas coherentes en el sistema de comunicaciones coherente clásico. Sobre esta base, para distinguir entre la segunda señal óptica transmitida a través de la primera fibra óptica y otra señal óptica coherente transmitida a través de la primera
 15 fibra óptica, la longitud de onda de la segunda señal óptica puede ser diferente de la longitud de onda de la otra señal óptica coherente en la primera fibra óptica. Además, para distinguir entre la señal cuántica y la señal de referencia que se transmiten a través de la segunda fibra óptica y otra señal óptica coherente transmitida a través de la segunda fibra óptica, la longitud de onda de la tercera señal óptica utilizada para generar la señal cuántica y la señal de referencia también puede ser diferente de la longitud de onda de la
 otra señal óptica coherente transmitida a través de la segunda fibra óptica. Opcionalmente, la dirección de transmisión de la señal óptica coherente transmitida a través de la segunda fibra óptica es opuesta a la dirección de transmisión de la señal cuántica transmitida a través de la segunda fibra óptica.

20 En esta realización de esta solicitud, se da a conocer el aparato de envío de claves cuánticas, y puede ajustarse la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia mediante la utilización de un controlador de polarización, y enviar la señal del oscilador local y la señal cuántica ajustada a diferentes fibras ópticas, para su transmisión. De esta manera, la señal del oscilador local y la señal cuántica ya no necesitan estar aisladas una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Sobre esta base, en un aparato de recepción de claves
 25 cuánticas que sirve como extremo de recepción, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación de la latencia, y el extremo de recepción puede ser integrado y miniaturizado. Además, la intensidad de la señal del oscilador local no está limitada por una relación de extinción finita de un multiplexor de polarización, y se mejora la relación de señal a ruido de un extremo de recepción. Además, ya no es necesario realizar el aislamiento mediante multiplexación por división del tiempo. Por lo tanto, no es necesario asignar ningún recurso en una fibra óptica utilizada para transmitir la
 30 señal cuántica para transmitir la señal del oscilador local. En otras palabras, todos los recursos de la fibra óptica se pueden utilizar para transmitir la señal cuántica. Esto mejora la proporción de transmisión de la señal cuántica en una unidad de tiempo.

35 Además, cuando la señal del oscilador local y la señal cuántica se transmiten respectivamente a través de dos fibras ópticas, la rotación de polarización de la señal del oscilador local es diferente de la rotación de polarización de la señal cuántica en un proceso de transmisión. Por lo tanto, para garantizar que el aparato de recepción de claves cuánticas puede obtener un resultado de detección más preciso después de recibir la señal del oscilador local y la señal cuántica, el controlador de polarización 104 puede estar dispuesto en el
 40 aparato de envío de claves cuánticas. El controlador de polarización 104 ajusta la dirección de polarización de la señal cuántica basándose en la información de control de la dirección de polarización que es retroalimentada por el aparato de recepción de claves cuánticas basándose en el resultado de la detección. De esta manera, la señal cuántica y la señal del oscilador local que son recibidas por el aparato de recepción de claves cuánticas pueden tener una misma dirección de polarización o tener una diferencia de dirección de polarización fija, o la señal cuántica recibida siempre puede ser estabilizada en una dirección de polarización. Esto puede mejorar el efecto de interferencia entre la señal cuántica y la señal del oscilador local, y
 45 garantizar aún más la precisión del resultado de la detección.

50 Cabe señalar, además, que, en esta realización de esta solicitud, el controlador de polarización está dispuesto en una ruta de transmisión de la señal cuántica. La señal cuántica generada debe pasar a través del controlador de polarización antes de ser enviada a la segunda fibra óptica para su transmisión. El propio controlador de polarización atenúa la señal hasta cierto punto. Por lo tanto, cuando se atenúa una tercera señal óptica modulada para obtener la señal cuántica, el atenuador puede reducir correspondientemente la intensidad de atenuación de la señal. Esto reduce la carga de trabajo del atenuador.

55 En la realización anterior, el controlador de polarización está dispuesto después del módulo de generación de señales cuánticas. Opcionalmente, el controlador de polarización puede estar dispuesto alternativamente dentro del módulo de generación de señales cuánticas.

60 Con referencia a la figura 6, se da a conocer otro aparato de envío de claves cuánticas. Tal como se muestra en la figura 6, el aparato incluye un láser 201, un divisor de haz 202, un módulo de generación de señales cuánticas 203 y un módulo de control de la polarización 204. El módulo de generación de señales cuánticas 203 incluye un generador de números aleatorios cuánticos 2031, un módulo de procesamiento 2032 y un modulador 2033. El módulo de control de la polarización 204 incluye un controlador de polarización 2041 y un atenuador 2042.

Para conocer la función del láser 201, consulte la explicación y descripción del láser 101 en la realización anterior. Para conocer la función del divisor de haz 202, consulte la explicación y descripción del divisor de haz 102 en la realización anterior. En esta realización de esta solicitud, los detalles no se describen nuevamente en la presente memoria.

5

Cabe señalar que el generador de números aleatorios cuánticos 2031 incluido en el módulo de generación de señales cuánticas 203, está configurado para: generar un número aleatorio, y enviar el número aleatorio al módulo de procesamiento 2032.

10

Después de recibir el número aleatorio enviado por el generador cuántico de números aleatorios 2031, el módulo de procesamiento 2032 puede procesar el número aleatorio según un protocolo o un estándar, para generar una clave aleatoria, y generar, basándose en la clave aleatoria, una señal de control utilizada para controlar el modulador 2033 para modular una señal cuántica. Además, el módulo de procesamiento 2032 puede generar además, basándose en datos de referencia almacenados, una señal de control utilizada para

15

controlar el modulador 2033 para modular una señal de referencia. A continuación, el módulo de procesamiento 2032 puede enviar las dos señales de control anteriores, al modulador 2033.

20

El modulador 2033 puede recibir las señales de control enviadas por el módulo de procesamiento 2032, recibir una tercera señal óptica enviada por el divisor de haz 202, modular la tercera señal óptica basándose en las señales de control, para obtener la señal cuántica y la señal de referencia, y permiten ubicar la señal cuántica y la señal de referencia en diferentes bandas de frecuencia. El modulador 2033 envía una señal modulada al controlador de polarización 2041.

25

El controlador de polarización 2041 puede configurarse para: recibir una primera señal de control y la señal modulada que es enviada por el modulador 2033, ajustar una dirección de polarización de la señal modulada sobre la base de la primera señal de control, y enviar una señal ajustada en la dirección de polarización, al atenuador 2042. La primera señal de control puede ser una señal de control que se genera mediante un aparato de recepción de claves cuánticas sobre la base de un resultado de detección obtenido detectando la señal de referencia y la señal del oscilador local, y que es retroalimentado por el aparato de recepción de claves cuánticas.

30

35

El atenuador 2042 está configurado para: atenuar la intensidad de la señal ajustada en la dirección de polarización, para obtener la señal cuántica que transporta la clave aleatoria y la señal de referencia que transporta los datos de referencia, y enviar la señal cuántica y la señal de referencia a través de una segunda fibra óptica.

40

Opcionalmente, el aparato de envío de claves cuánticas puede incluir, además, un aparato de recepción 205 y un procesador 206. Para las funciones del aparato de recepción 205 y el procesador 206, consulte las funciones del receptor 105 y el procesador 106 en la realización anterior. En esta realización de esta solicitud, los detalles no se describen nuevamente en la presente memoria.

45

En esta realización de esta solicitud, el controlador de polarización está dispuesto entre el modulador y el atenuador, es decir, el controlador de polarización puede estar dispuesto en una ruta de transmisión de la señal cuántica. Debido a que el propio controlador de polarización atenúa una señal hasta cierto punto, el controlador de polarización está dispuesto antes del atenuador. Por lo tanto, se reduce la intensidad de una señal cuya dirección de polarización se ajusta mediante el controlador de polarización. De esta manera, el atenuador puede reducir apropiadamente la intensidad de atenuación al atenuar la señal ajustada en la dirección de polarización. Esto reduce la carga de trabajo del atenuador.

50

En esta realización, el controlador de polarización está dispuesto en la ruta de transmisión de la señal cuántica y está configurado para ajustar una dirección de polarización de la señal cuántica y una dirección de polarización de la señal de referencia. Opcionalmente, en una posible implementación, el controlador de polarización puede estar dispuesto alternativamente en una ruta de transmisión de señal del oscilador local, es decir, está configurado para ajustar una dirección de polarización de la señal del oscilador local. A

55

continuación se describe en detalle una implementación en la que el controlador de polarización está dispuesto en la ruta de transmisión de la señal del oscilador local.

60

Con referencia a la figura 7, se da a conocer otro aparato de envío de claves cuánticas. El aparato incluye un láser 301, un divisor de haz 302, un controlador de polarización 303 y un módulo de generación de señales cuánticas 304.

65

El láser 301 está configurado para emitir una primera señal óptica. El divisor de haz 302 está configurado para: recibir la primera señal óptica, dividir la primera señal óptica en una segunda señal óptica y una tercera señal óptica, enviar la segunda señal óptica al controlador de polarización 303, y enviar la tercera señal óptica al módulo de generación de señales cuánticas 304, donde la intensidad luminosa de la segunda señal óptica es mayor que la intensidad luminosa de la tercera señal óptica. El controlador de polarización 303 está

configurado para: ajustar una dirección de polarización de la segunda señal óptica y enviar una segunda señal óptica ajustada a través de una primera fibra óptica. El módulo de generación de señales cuánticas 304 está configurado para: modular la tercera señal óptica para obtener una señal cuántica y una señal de referencia, y enviar la señal cuántica y la señal de referencia a través de una segunda fibra óptica.

5

Para conocer la función del láser 301, consulte la explicación y descripción del láser 101 en la realización anterior. En esta realización de esta solicitud, los detalles no se describen nuevamente en la presente memoria.

10

El divisor de haz 302 puede incluir un puerto de entrada y dos puertos de salida. El puerto de entrada del divisor de haz 302 está conectado al puerto de salida del láser 301. El divisor de haz 302 puede recibir, a través del puerto de entrada incluido, la primera señal óptica enviada por el láser 301, y dividir la primera señal óptica en la segunda señal óptica y la tercera señal óptica basándose en una relación de división de haz del divisor de haz 302. La intensidad luminosa de la señal de un oscilador local suele ser alta. Por lo tanto, después de la división del haz, se puede utilizar una señal óptica con mayor intensidad luminosa como la segunda señal óptica, y se puede utilizar una señal óptica con menor intensidad luminosa como la tercera señal óptica. La relación de división del haz del divisor de haz 302 puede ser 10:90, 1:99 o similar.

15

20

Después de dividir la primera señal óptica en la segunda señal óptica y la tercera señal óptica, el divisor de haz 302 puede emitir la segunda señal óptica a través de un primer puerto de salida incluido, y emitir la tercera señal óptica a través de un segundo puerto de salida incluido. Cabe señalar que el primer puerto de salida del divisor de haz 302 está conectado a un primer puerto de entrada del controlador de polarización 303. De esta manera, la segunda señal óptica puede ser enviada al controlador de polarización 303 a través del primer puerto de salida del divisor de haz. El segundo puerto de salida del divisor de haz 302 puede ser conectado al módulo de generación de señales cuánticas 304. De esta manera, el divisor de haz 302 puede enviar la tercera señal óptica al módulo de generación de señales cuánticas 304 a través del segundo puerto de salida.

25

30

El controlador de polarización 303 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El controlador de polarización 303 puede recibir, a través del primer puerto de entrada incluido, la segunda señal óptica enviada por el divisor de haz 302, y recibir una primera señal de control a través del segundo puerto de entrada. A continuación, el controlador de polarización 303 puede ajustar la dirección de polarización de la segunda señal óptica basándose en la primera señal de control, y emitir la segunda señal óptica ajustada a través del puerto de salida incluido. El puerto de salida del controlador de polarización 303 puede ser conectado directamente a la primera fibra óptica, o puede ser conectado a la primera fibra óptica mediante el uso de un acoplador o un circulador. De esta manera, el controlador de polarización 303 puede enviar la segunda señal óptica ajustada como la señal del oscilador local a través de la primera fibra óptica.

35

40

Cabe señalar que la primera señal de control puede ser una señal de control que se genera mediante un aparato de recepción de claves cuánticas sobre la base de un resultado de detección obtenido detectando la señal de referencia y la señal del oscilador local, y que es retroalimentado por el aparato de recepción de claves cuánticas.

45

50

Opcionalmente, en una posible implementación, el aparato de envío de claves cuánticas puede incluir, además, un aparato de recepción 305 y un procesador 306. En este caso, el aparato de recepción de claves cuánticas puede generar información de control de la dirección de polarización basándose en el resultado de la detección obtenido al detectar la señal de referencia y la señal del oscilador local, y retroalimentar la información de control de la dirección de polarización. El aparato de envío de claves cuánticas puede recibir la información de control de la dirección de polarización utilizando el aparato de recepción 305, y el procesador 306 procesa la información de control de la dirección de polarización para obtener la primera señal de control.

55

Para las funciones del aparato de recepción 305 y el procesador 306, consulte las funciones del receptor 105 y el procesador 106 en la realización anterior. En esta realización de esta solicitud, los detalles no se describen nuevamente en la presente memoria.

60

Para una implementación del módulo de generación de señales cuánticas 304, consulte una implementación relacionada del módulo de generación de señales cuánticas 103 mostrado en la figura 4 en la realización anterior, o consulte una implementación relacionada del módulo de generación de señales cuánticas 203 mostrado en la figura 6 en la realización anterior. En esta realización de esta solicitud, los detalles no se describen nuevamente en la presente memoria.

65

Cabe señalar que un puerto de salida del módulo de generación de señales cuánticas 304 puede ser conectado directamente a la segunda fibra óptica, o puede ser conectado a la segunda fibra óptica mediante el uso de un acoplador o un circulador. De esta manera, después de generar la señal cuántica y la señal de

referencia, el módulo de generación de señales cuánticas 304 puede enviar la señal cuántica y la señal de referencia a través de la segunda fibra óptica.

5 Opcionalmente, tal como se muestra en la figura 8, el aparato de envío de claves cuánticas incluye, además,
 un divisor de haz 307 y un módulo de generación de señal de referencia 308. El divisor de haz 307 está
 configurado para: dividir la tercera señal óptica en dos señales ópticas y enviar una señal óptica al módulo de
 generación de señales cuánticas 304 y la otra señal óptica al módulo de generación de señales de referencia
 308. Para el módulo de generación de señales de referencia, consulte una implementación relacionada del
 módulo de generación de señales de referencia 108 mostrado en la figura 5 en la realización anterior. Esto no
 10 está limitado en esta solicitud.

En esta realización de esta solicitud, el aparato de envío de claves cuánticas puede ajustar la dirección de
 polarización de la señal cuántica y la dirección de polarización de la señal de referencia mediante el uso de
 un controlador de polarización, y enviar una señal del oscilador local y una señal cuántica ajustada a
 15 diferentes fibras ópticas para su transmisión. De esta manera, la señal del oscilador local y la señal cuántica
 ya no necesitan estar aisladas una de otra mediante multiplexación por división del tiempo y multiplexación
 por polarización. Sobre esta base, en un aparato de recepción de señales cuánticas en un extremo de
 recepción, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación
 de la latencia, y el extremo de recepción puede ser integrado y miniaturizado. Además, ya no es necesario
 20 realizar el aislamiento mediante multiplexación por división del tiempo. Asimismo, la intensidad de la señal del
 oscilador local no está limitada por una relación de extinción finita de un multiplexor de polarización, y se
 mejora la relación de señal a ruido recibida. Además, ya no es necesario realizar el aislamiento mediante
 multiplexación por división del tiempo. Por lo tanto, no es necesario asignar ningún recurso en una fibra
 óptica utilizada para transmitir la señal cuántica para transmitir la señal del oscilador local. En otras palabras,
 25 todos los recursos de la fibra óptica se pueden utilizar para transmitir la señal cuántica. Esto mejora la
 proporción de transmisión de la señal cuántica en una unidad de tiempo.

Además, cuando la señal del oscilador local y la señal cuántica se transmiten respectivamente a través de
 dos fibras ópticas, la rotación de polarización de la señal del oscilador local es diferente de la rotación de
 30 polarización de la señal cuántica en un proceso de transmisión. Por lo tanto, para garantizar que el aparato
 de recepción de claves cuánticas puede obtener un resultado de detección más preciso después de recibir la
 señal del oscilador local y la señal cuántica, el controlador de polarización puede estar dispuesto en el
 aparato de envío de claves cuánticas. El controlador de polarización ajusta la dirección de polarización de la
 señal cuántica basándose en la información de control de la dirección de polarización que es retroalimentada
 35 por el aparato de recepción de claves cuánticas basándose en el resultado de la detección. De esta manera,
 la señal del oscilador local y la señal cuántica que son recibidas por el aparato receptor de claves cuánticas
 pueden tener una misma dirección de polarización o tener una diferencia de dirección de polarización fija, o la
 señal del oscilador local recibida puede estabilizarse siempre en una dirección de polarización. Esto puede
 mejorar el efecto de interferencia entre la señal cuántica y la señal del oscilador local, y garantizar aún más la
 40 precisión del resultado de la detección.

En las realizaciones anteriores, se describe principalmente el aparato de envío de claves cuánticas
 proporcionado en las realizaciones de esta solicitud. El aparato de envío de claves cuánticas no solo puede
 45 enviar la señal del oscilador local y la señal cuántica a diferentes fibras ópticas para su transmisión, sino que
 también puede ajustar la dirección de polarización de la señal cuántica o la señal del oscilador local. De esta
 manera, después de que se produce una rotación de polarización diferente, la señal del oscilador local y la
 señal cuántica que son recibidas por el aparato de recepción de claves cuánticas que sirve como extremo de
 recepción pueden tener una misma dirección de polarización o tener una diferencia de dirección de
 polarización fija, o la señal del oscilador local o la señal cuántica que es recibida por el aparato de recepción
 50 de claves cuánticas siempre puede ser estabilizada en una dirección de polarización. Esto garantiza la
 precisión del resultado de la detección. Opcionalmente, en una posible implementación, el aparato de envío
 de claves cuánticas puede no incluir el controlador de polarización. Es decir, el aparato de envío de claves
 cuánticas puede ser solo responsable de enviar la señal del oscilador local y la señal cuántica a diferentes
 fibras ópticas para su transmisión, y el aparato de recepción de claves cuánticas ajusta la dirección de
 55 polarización de la señal del oscilador local o la señal cuántica recibida, para garantizar que después de que
 se produce una rotación de polarización diferente, la señal del oscilador local y la señal cuántica puedan
 tener la misma dirección de polarización o tener una diferencia de dirección de polarización fija.

Sobre la base de la descripción anterior, con referencia a la figura 9, una realización de esta solicitud da a
 60 conocer un aparato de recepción de claves cuánticas. El aparato incluye un módulo de detección cuántica
 401 y un módulo de control de la polarización 402.

El módulo de control de la polarización 402 está configurado para: recibir una señal del oscilador local desde
 una primera fibra óptica, ajustar una dirección de polarización de la señal del oscilador local y enviar una
 65 señal del oscilador local ajustada al módulo de detección cuántica 401. El módulo de detección cuántica 401
 está configurado para: recibir una señal cuántica y una señal de referencia desde una segunda fibra óptica, y

detectar la señal del oscilador local ajustada, la señal cuántica y la señal de referencia para obtener resultados de detección, donde la señal cuántica lleva una clave aleatoria, y los resultados de la detección incluyen información de clave de la clave aleatoria.

5 Por ejemplo, en una posible implementación, haciendo referencia a la figura 10, el módulo de control de la polarización 402 puede incluir un controlador de polarización 4021. En este caso, el controlador de polarización 4021 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El primer puerto de entrada del controlador de polarización 4021 puede ser conectado directamente a la primera fibra óptica, o el primer puerto de entrada del controlador de polarización 4021 puede ser conectado a la primera fibra óptica mediante la utilización de un acoplador o un circulador. El controlador de polarización 4021 puede recibir, a través del primer puerto de entrada, la señal del oscilador local enviada por un aparato de envío de claves cuánticas a través de la primera fibra óptica. El controlador de polarización 4021 puede recibir, a través del segundo puerto de entrada, una segunda señal de control que es generada por el módulo de detección cuántica 401 antes de un punto del tiempo actual basándose en el resultado de la detección de la señal del oscilador local y en la señal de referencia. A continuación, el controlador de polarización puede ajustar la dirección de polarización de la señal del oscilador local a una primera dirección de polarización basándose en la segunda señal de control, y enviar la señal del oscilador local ajustada al módulo de detección cuántica, donde la primera dirección de polarización puede ser la misma que la dirección de polarización de la señal cuántica, o puede haber una diferencia de dirección fija entre la primera dirección de polarización y la dirección de polarización de la señal cuántica.

La señal de referencia transporta datos de referencia, y los datos de referencia son negociados de antemano por el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas. Además, la dirección de polarización de la señal de referencia es la misma que la dirección de polarización de la señal cuántica. Además, cabe señalar que, si el controlador de polarización 4021 recibe la señal del oscilador local por primera vez, el controlador de polarización 4021 ajusta la señal del oscilador local a una dirección de polarización preestablecida, y envía la señal del oscilador local ajustada al módulo de detección cuántica 401. En otras palabras, si la señal del oscilador local se recibe por primera vez, durante el primer ajuste, el ajuste de la dirección de polarización de la señal del oscilador local a una primera dirección de polarización es ajustar la señal del oscilador local a la dirección de polarización preestablecida.

El módulo de detección cuántica 401 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El módulo de detección cuántica 401 puede recibir, a través del primer puerto de entrada incluido, la señal cuántica y la señal de referencia que envía el aparato de envío de claves cuánticas a través de la segunda fibra óptica. El módulo de detección cuántica 401 puede recibir la señal del oscilador local ajustada a través del segundo puerto de entrada incluido. Si la señal cuántica y la señal de referencia se envían en un modo de multiplexación por división de la frecuencia, al recibir la señal cuántica y la señal de referencia, el módulo de detección cuántica 401 puede extraer la señal de referencia de una banda de frecuencia en la que se encuentra la señal de referencia, y detectar una señal de interferencia entre la señal de referencia y la señal del oscilador local ajustada, para obtener un valor de medición de datos de referencia. Si una desviación entre el valor de medición de los datos de referencia y los datos de referencia almacenados no es mayor que una desviación permitida, indica que un efecto de interferencia entre la señal de referencia y la señal del oscilador local ajustada es relativamente bueno, es decir, la dirección de polarización de la señal del oscilador local ajustada es apropiada. La dirección de polarización de la señal de referencia ajustada es la misma que la dirección de polarización de la señal cuántica ajustada. Por lo tanto, un efecto de interferencia entre la señal del oscilador local y la señal cuántica ajustada también es relativamente bueno. Sobre esta base, el módulo de detección cuántica 401 puede medir una señal de interferencia entre la señal cuántica y la señal del oscilador local ajustada, para obtener un resultado de detección, y obtener además la información de clave de la clave aleatoria basándose en el resultado de la detección.

Ciertamente, si una desviación entre el valor de medición de los datos de referencia y los datos de referencia almacenados es mayor que una desviación permitida, indica que el efecto de interferencia entre la señal de referencia y la señal del oscilador local ajustada es relativamente malo. En este caso, es necesario ajustar de manera continua la dirección de polarización de la señal del oscilador local. Por lo tanto, el módulo de detección cuántica 401 puede generar la segunda señal de control basándose en la diferencia entre el valor de medición de los datos de referencia y los datos de referencia, y enviar la segunda señal de control al controlador de polarización 4021 a través del puerto de salida.

Opcionalmente, si la señal de referencia y la señal cuántica se envían en un modo de multiplexación por división del tiempo, al recibir la señal de referencia, el módulo de detección cuántica 401 puede ajustar de manera continua la dirección de la señal del oscilador local para determinar una dirección de polarización que es de la señal del oscilador local y que se obtiene cuando el efecto de interferencia entre la señal de referencia y la señal del oscilador local es el mejor. Cuando se recibe la señal cuántica, la señal del oscilador local se ajusta basándose en la dirección de polarización finalmente determinada de la señal del oscilador local, para mejorar el efecto de interferencia entre la señal del oscilador local ajustada y la señal cuántica, y

garantizar aún más la precisión del resultado de una detección.

5 El módulo de detección cuántica 401 puede ser un detector cuántico para detectar una señal en una dirección de polarización única, o puede ser un detector cuántico para detectar señales en direcciones de polarización ortogonales. Esto no está limitado en esta solicitud.

10 El controlador de polarización 4021 puede incluir, además, el segundo puerto de entrada. El segundo puerto de entrada está conectado al puerto de salida del módulo de detección cuántica 401 y se utiliza para recibir la segunda señal de control enviada por el módulo de detección cuántica 401. El controlador de polarización 4021 ajusta, basándose en la segunda señal de control, la dirección de polarización de una señal del oscilador local actualmente recibida; reenvía una señal del oscilador local ajustada al módulo de detección cuántica; y cuando la diferencia entre un valor de medición de datos de referencia detectado por el módulo de detección cuántica 401 y los datos de referencia no es mayor que la desviación permitida, ajusta una dirección de polarización de una señal del oscilador local recibida posteriormente basándose en una dirección de polarización de una señal del oscilador local finalmente ajustada.

En un ejemplo antecedente, con referencia a la figura 11, el módulo de control de la polarización 402 puede incluir un controlador de polarización 4021, un divisor de haz 4022 y un analizador de polarización 4023.

20 El divisor de haz 4022 está configurado para: recibir la señal del oscilador local desde la primera fibra óptica, dividir la señal del oscilador local en una cuarta señal óptica y una quinta señal óptica, enviar la cuarta señal óptica al analizador de polarización 4023, y enviar la quinta señal óptica al controlador de polarización 4021, donde la intensidad luminosa de la cuarta señal óptica es menor que la intensidad luminosa de la quinta señal óptica. El analizador de polarización 4023 está configurado para: recibir la cuarta señal óptica, analizar la dirección de polarización de la cuarta señal óptica, generar una tercera señal de control basándose en la dirección de polarización de la cuarta señal óptica y la dirección de polarización objetivo, y enviar la tercera señal de control al controlador de polarización 4021. El controlador de polarización 4021 está configurado para: recibir la quinta señal óptica y la tercera señal de control, ajustar la dirección de polarización de la quinta señal óptica a la dirección de polarización objetivo basándose en la tercera señal de control, y enviar una quinta señal óptica ajustada al módulo de detección cuántica 401. El módulo de detección cuántica 401 está configurado específicamente para: recibir la quinta señal óptica ajustada, recibir la señal cuántica y la señal de referencia de la segunda fibra óptica, y detectar la quinta señal óptica ajustada, la señal cuántica y la señal de referencia, para obtener los resultados de la detección.

35 Cabe señalar que, en esta implementación, el divisor de haz 4022 incluye un puerto de entrada, un primer puerto de salida y un segundo puerto de salida. El puerto de entrada del divisor de haz 4022 puede ser conectado directamente a la primera fibra óptica, o puede ser conectado a la primera fibra óptica mediante el uso de un acoplador o un circulador. De esta manera, el divisor de haz 4022 puede recibir, a través del puerto de entrada incluido, la señal del oscilador local enviada por un aparato de envío de claves cuánticas a través de la primera fibra óptica. A continuación, el divisor de haz 4022 puede dividir la señal del oscilador local recibida en la cuarta señal óptica y la quinta señal óptica basándose en una relación de división de haz específica. La cuarta señal óptica se utiliza para analizar una dirección de polarización y puede tener una intensidad luminosa relativamente baja. La quinta señal óptica se utiliza como señal del oscilador local para interferir con la señal cuántica y la señal de referencia. Por lo tanto, es necesario garantizar una intensidad luminosa específica para la quinta señal óptica. Sobre esta base, cuando se realiza la división del haz mediante el divisor de haz 4022, la intensidad luminosa de la cuarta señal óptica puede ser relativamente baja. Por ejemplo, la relación de división de haz puede ser 1:99. Cuando la división del haz se realiza basándose en la relación de división de haz, se obtienen la cuarta señal óptica que representa el 1 % de la señal del oscilador local y la quinta señal óptica que representa el 99 % de la señal del oscilador local.

50 Después de obtener la cuarta señal óptica y la quinta señal óptica, el divisor de haz 4022 puede enviar la cuarta señal óptica al analizador de polarización 4023 a través del primer puerto de salida, y enviar la quinta señal óptica al controlador de polarización 4021 a través del segundo puerto de salida.

55 El analizador de polarización 4023 puede incluir un puerto de entrada y un puerto de salida. El puerto de entrada está conectado al primer puerto de salida del divisor de haz 4022. De esta manera, el analizador de polarización 4023 puede recibir la cuarta señal óptica a través del puerto de entrada. Después de recibir la cuarta señal óptica, el analizador de polarización puede analizar la dirección de polarización de la cuarta señal óptica, comparar la dirección de polarización objetivo con la dirección de polarización que es de la cuarta señal óptica y que se obtiene mediante análisis, y generar la tercera señal de control basándose en la diferencia entre la dirección de polarización de la cuarta señal óptica y la dirección de polarización objetivo. La tercera señal de control sale a través del puerto de salida incluido.

65 El controlador de polarización 4021 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El primer puerto de entrada está conectado al segundo puerto de salida del divisor de haz 4022. De esta manera, el controlador de polarización 4021 puede recibir la quinta señal óptica emitida

por el divisor de haz 4022. El segundo puerto de entrada está conectado al puerto de salida del analizador de polarización 4023. De esta manera, el controlador de polarización 4021 puede recibir la tercera señal de control emitida por el analizador de polarización 4023. El controlador de polarización 4021 puede ajustar la dirección de polarización de la quinta señal óptica a la dirección de polarización objetivo basándose en la tercera señal de control recibida, y enviar la quinta señal óptica ajustada al módulo de detección cuántica 401 a través del puerto de salida.

Cabe señalar que una desviación de dirección entre la dirección de polarización objetivo y una dirección de polarización de la señal cuántica no es mayor que un valor preestablecido. Cuando la desviación de la dirección es 0, indica que la dirección de polarización de la señal cuántica es la misma que la dirección de polarización de la señal del oscilador local. En este caso, un efecto de interferencia entre la señal cuántica y la señal del oscilador local es el mejor. Ciertamente, si la desviación de dirección es mayor que 0, a medida que aumenta la desviación de dirección, el efecto de interferencia entre la señal del oscilador local y la señal cuántica se deteriora gradualmente. Por lo tanto, el valor preestablecido puede ser minimizado tanto como sea posible. Por ejemplo, el valor preestablecido puede ser 5°, 8° o 10°.

El módulo de detección cuántica 401 puede recibir la quinta señal óptica ajustada enviada por el controlador de polarización 4021, y detectar una señal de interferencia entre la quinta señal óptica ajustada y la señal cuántica, para obtener un resultado de detección que incluye la información de clave de la clave aleatoria.

Opcionalmente, la potencia de la señal del oscilador local se atenúa en un proceso de transmisión. Por lo tanto, para garantizar el efecto de interferencia entre la señal del oscilador local y la señal cuántica, la potencia de la señal del oscilador local debe alcanzar un valor específico. Sobre esta base, se puede disponer además un amplificador óptico en el aparato de recepción de claves cuánticas. El amplificador óptico puede estar dispuesto antes del módulo de control de la polarización, o puede estar dispuesto entre el módulo de control de la polarización y el módulo de detección cuántica. En otras palabras, el aparato de recepción de claves cuánticas puede recibir y amplificar, utilizando el amplificador óptico, la señal del oscilador local transmitida a través de la primera fibra óptica, y a continuación enviar una señal del oscilador local amplificada al módulo de control de la polarización para ajustar la dirección de polarización. Alternativamente, el aparato de recepción de claves cuánticas puede ajustar, utilizando el módulo de control de la polarización, la dirección de polarización de la señal del oscilador local, introducir la señal del oscilador local ajustada en el amplificador óptico para la amplificación de potencia y, a continuación, emitir una señal desde el oscilador local amplificada, al módulo de detección cuántica.

El aparato de recepción de claves cuánticas puede recibir la señal del oscilador local y la señal cuántica que se transmiten a través de dos fibras ópticas diferentes, y obtener el resultado de la detección basándose en la señal del oscilador local recibida y en la señal cuántica recibida. En un proceso de transmisión, no es necesario aislar la señal cuántica y la señal del oscilador local una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Por lo tanto, en el aparato de recepción de claves cuánticas, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación de la latencia, y el aparato de recepción de claves cuánticas puede ser integrado y miniaturizado. Además, la señal del oscilador local y la señal cuántica ya no necesitan estar aisladas una de otra mediante la multiplexación por polarización. Por lo tanto, la intensidad de la señal del oscilador local no está limitada por una relación de extinción finita de un multiplexor de polarización, y se mejora la relación de señal a ruido del extremo de recepción.

Además, la rotación de polarización de la señal del oscilador local es diferente de la rotación de polarización de la señal cuántica cuando se transmiten en las dos fibras ópticas. Por lo tanto, en el aparato de recepción de claves cuánticas, el módulo de control de la polarización puede estar dispuesto en una trayectoria de transmisión de señal del oscilador local para ajustar la dirección de polarización de la señal del oscilador local. De esta manera, la señal del oscilador local ajustada y la señal cuántica pueden tener la misma dirección de polarización o tener una diferencia de dirección de polarización fija, o la señal del oscilador local ajustada siempre puede estabilizarse en una dirección de polarización. Esto puede mejorar el efecto de interferencia entre la señal cuántica y la señal del oscilador local, y garantizar aún más la precisión del resultado de la detección.

En los aparatos de recepción de claves cuánticas proporcionados en la figura 9 a la figura 11, el módulo de control de la polarización está dispuesto en la ruta de transmisión de la señal del oscilador local para ajustar la dirección de polarización de la señal del oscilador local. Opcionalmente, en una posible implementación, el módulo de control de la polarización puede estar dispuesto alternativamente en una ruta de transmisión de señal cuántica del aparato de recepción de claves cuánticas, y la dirección de polarización de la señal cuántica se ajusta, para garantizar que una desviación de dirección entre la dirección de polarización de la señal cuántica y la dirección de polarización de la señal del oscilador local no son mayores que un valor preestablecido.

Por ejemplo, haciendo referencia a la figura 12, se da a conocer un aparato de recepción de claves

cuánticas. El aparato incluye un módulo de detección cuántica 501 y un módulo de control de la polarización 502.

5 El módulo de control de la polarización 502 está configurado para: recibir una señal cuántica y una señal de referencia desde una segunda fibra óptica, ajustar una dirección de polarización de la señal cuántica y una dirección de polarización de la señal de referencia, y enviar una señal cuántica ajustada y una señal de referencia ajustada al módulo de detección cuántica 501. El módulo de detección cuántica 501 está configurado para: recibir una señal del oscilador local desde una primera fibra óptica y detectar la señal del oscilador local, la señal cuántica ajustada y la señal de referencia ajustada, para obtener resultados de detección.

15 Cabe señalar que el módulo de control de la polarización 502 puede ser un controlador de polarización. El módulo de control de la polarización 502 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El primer puerto de entrada del módulo de control de la polarización 502 puede ser conectado directamente a la segunda fibra óptica, o el primer puerto de entrada del controlador de polarización 502 puede ser conectado a la segunda fibra óptica utilizando un acoplador o un circulador. El módulo de control de la polarización 502 puede recibir, a través del primer puerto de entrada, la señal cuántica y la señal de referencia que son enviadas por un aparato de envío de claves cuánticas a través de la segunda fibra óptica. El módulo de control de la polarización 502 puede recibir, a través del segundo puerto de entrada, una cuarta señal de control que es generada por el módulo de detección cuántica 501 antes de un punto del tiempo actual basándose en el resultado de la detección de la señal del oscilador local y la señal de referencia. A continuación, el módulo de control de la polarización 502 puede ajustar la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia a una primera dirección de polarización basándose en la cuarta señal de control, y enviar la señal cuántica ajustada y la señal de referencia ajustada, al módulo de detección cuántica 501.

30 La señal de referencia transporta datos de referencia, y los datos de referencia son negociados de antemano por el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas. Además, la dirección de polarización de la señal de referencia es la misma que la dirección de polarización de la señal cuántica. Además, cabe señalar que, si el módulo de control de la polarización 502 recibe la señal cuántica y la señal de referencia por primera vez, el módulo de control de la polarización 502 ajusta la señal cuántica y la señal de referencia a una dirección de polarización preestablecida, y envía la señal cuántica ajustada y la señal de referencia ajustada, al módulo de detección cuántica 501. En otras palabras, si la señal cuántica y la señal de referencia se reciben por primera vez, durante el primer ajuste, el ajuste de la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia a una primera dirección de polarización es ajustar la señal cuántica y la señal de referencia a la dirección de polarización preestablecida.

40 El módulo de detección cuántica 501 puede incluir un primer puerto de entrada, un segundo puerto de entrada y un puerto de salida. El módulo de detección cuántica 501 puede recibir, a través del primer puerto de entrada incluido, la señal del oscilador local enviada por el aparato de envío de claves cuánticas a través de la primera fibra óptica. El módulo de detección cuántica 501 puede recibir, a través del segundo puerto de entrada incluido, la señal cuántica ajustada y la señal de referencia ajustada que son enviadas por el módulo de control de la polarización 502. Si la señal cuántica y la señal de referencia se envían en un modo de multiplexación por división de la frecuencia, al recibir la señal cuántica y la señal de referencia, el módulo de detección cuántica 501 puede extraer la señal de referencia de una banda de frecuencia en la que se encuentra la señal de referencia, y detectar una señal de interferencia entre la señal de referencia y la señal del oscilador local ajustada, para obtener un valor de medición de datos de referencia. Si una desviación entre el valor de medición de los datos de referencia almacenados no es mayor que una desviación permitida, indica que un efecto de interferencia entre la señal de referencia ajustada y la señal del oscilador local es relativamente bueno, es decir, la dirección de polarización de la señal de referencia ajustada es apropiada. La dirección de polarización de la señal de referencia es la misma que la dirección de polarización de la señal cuántica. Por lo tanto, el efecto de interferencia entre la señal del oscilador local ajustada y la señal cuántica también es relativamente bueno. Sobre esta base, el módulo de detección cuántica 501 puede medir una señal de interferencia entre la señal cuántica y la señal del oscilador local ajustada, para obtener un resultado de detección, y obtener, además, la información de clave de la clave aleatoria basándose en el resultado de la detección.

60 Ciertamente, si una desviación entre el valor de medición de los datos de referencia y los datos de referencia almacenados es mayor que una desviación permitida, indica que un efecto de interferencia entre la señal de referencia y la señal del oscilador local ajustada es relativamente malo. En este caso, es necesario ajustar de manera continua la dirección de polarización de la señal del oscilador local. Por lo tanto, el módulo de detección cuántica 501 puede generar la cuarta señal de control basándose en la diferencia entre el valor de medición de los datos de referencia y los datos de referencia, y enviar la cuarta señal de control al módulo de control de la polarización 502 a través del puerto de salida.

El módulo de control de la polarización 502 puede recibir, a través del segundo puerto de entrada incluido, la cuarta señal de control enviada por el módulo de detección cuántica 501; ajustar, basándose en la cuarta señal de control, la dirección de polarización de una señal cuántica actualmente recibida y la dirección de polarización de una señal de referencia actualmente recibida; volver a enviar una señal cuántica ajustada y una señal de referencia ajustada al módulo de detección cuántica 501; y cuando la diferencia entre un valor de medición de datos de referencia detectado por el módulo de detección cuántica 501 y los datos de referencia no es mayor que la desviación permitida, ajustar la dirección de polarización de una señal cuántica recibida posteriormente y la dirección de polarización de una señal de referencia recibida posteriormente basándose en una dirección de polarización de una señal cuántica finalmente ajustada y en una dirección de polarización de una señal de referencia finalmente ajustada.

Opcionalmente, si la señal de referencia y la señal cuántica se envían en un modo de multiplexación por división del tiempo, al recibir la señal de referencia, el módulo de control de la polarización 502 puede ajustar de manera continua la dirección de la señal de referencia para determinar una dirección de polarización que es de la señal de referencia y que se obtiene cuando el efecto de interferencia entre la señal de referencia y la señal del oscilador local es el mejor. Cuando se recibe la señal cuántica, la señal del oscilador local se ajusta basándose en la dirección de polarización finalmente determinada de la señal del oscilador local, para mejorar el efecto de interferencia entre la señal del oscilador local ajustada y la señal cuántica, y garantizar aún más la precisión del resultado de una detección.

El aparato de recepción de claves cuánticas puede recibir la señal del oscilador local y la señal cuántica que se transmiten a través de dos fibras ópticas diferentes, y obtener el resultado de la detección basándose en la señal del oscilador local recibida y en la señal cuántica recibida. En un proceso de transmisión, no es necesario aislar la señal cuántica y la señal del oscilador local una de otra mediante multiplexación por división del tiempo y multiplexación por polarización. Por lo tanto, en el aparato de recepción de claves cuánticas, no es necesario introducir ninguna diferencia de trayectoria óptica adicional para la compensación de la latencia, y el aparato de recepción de claves cuánticas puede ser integrado y miniaturizado. Además, el aparato de recepción de claves cuánticas ya no necesita realizar una compensación de polarización. Esto reduce los componentes adicionales y las pérdidas de línea.

Además, la rotación de polarización de la señal del oscilador local es diferente de la rotación de polarización de la señal cuántica cuando se transmiten en las dos fibras ópticas. Por lo tanto, en el aparato de recepción de claves cuánticas, el módulo de control de la polarización puede estar dispuesto en una trayectoria de transmisión de la señal del oscilador local para ajustar la dirección de polarización de la señal del oscilador local. De esta manera, la señal del oscilador local ajustada y la señal cuántica pueden tener la misma dirección de polarización o tener una diferencia de dirección de polarización fija, o la señal del oscilador local ajustada siempre puede estabilizarse en una dirección de polarización. Esto puede mejorar el efecto de interferencia entre la señal cuántica y la señal del oscilador local, y garantizar aún más la precisión del resultado de la detección.

El aparato de recepción de claves cuánticas descrito en las realizaciones anteriores utiliza principalmente el módulo de control de la polarización para evitar la inconsistencia de la rotación de polarización causada cuando la señal cuántica y la señal del oscilador local se transmiten a través de diferentes fibras ópticas. Opcionalmente, en una posible implementación, el aparato de recepción de claves cuánticas puede evitar alternativamente la inconsistencia de la rotación de polarización en otra implementación.

Por ejemplo, haciendo referencia a la figura 13, se da a conocer un aparato de recepción de claves cuánticas. El aparato incluye un primer divisor de haz de polarización 601, un segundo divisor de haz de polarización 602, un primer detector heterodino cuántico 603, un segundo detector heterodino cuántico 604 y un procesador 605.

El primer divisor de haz de polarización 601 está configurado para: recibir una señal de oscilador local desde una primera fibra óptica, dividir la señal de oscilador local en una sexta señal óptica y una séptima señal óptica, enviar la sexta señal óptica al primer detector heterodino cuántico, y enviar la séptima señal óptica al segundo detector heterodino cuántico.

Cabe señalar que el primer divisor de haz de polarización 601 puede incluir un puerto de entrada, un primer puerto de salida y un segundo puerto de salida. El primer puerto de entrada del primer divisor de haz de polarización 601 puede conectarse directamente a la primera fibra óptica, o el puerto de entrada del primer divisor de haz de polarización 601 puede conectarse a la primera fibra óptica utilizando un acoplador o un circulador. El primer divisor de haz de polarización 601 puede recibir, a través del primer puerto de entrada, la señal del oscilador local enviada por un aparato de envío de claves cuánticas a través de la primera fibra óptica. A continuación, el primer divisor de haz de polarización 601 puede dividir la señal del oscilador local en la sexta señal óptica y la séptima señal óptica, emitir la sexta señal óptica a través del primer puerto de salida y emitir la séptima señal óptica a través del segundo puerto de salida.

El segundo divisor de haz de polarización 602 está configurado para: recibir una señal cuántica y una señal de referencia de una segunda fibra óptica, dividir la señal de referencia en una octava señal óptica y una novena señal óptica, dividir la señal cuántica en una décima señal óptica y una undécima señal óptica, enviar la octava señal óptica y la décima señal óptica al primer detector heterodino cuántico, y enviar la novena señal óptica y la undécima señal óptica al segundo detector heterodino cuántico, donde la señal cuántica lleva una clave aleatoria.

Cabe señalar que el segundo divisor de haz de polarización 602 puede incluir un puerto de entrada, un primer puerto de salida y un segundo puerto de salida. El primer puerto de entrada del segundo divisor de haz de polarización 602 puede conectarse directamente a la primera fibra óptica, o el puerto de entrada del segundo divisor de haz de polarización 602 puede conectarse a la primera fibra óptica utilizando un acoplador o un circulador. El segundo divisor de haz de polarización 602 puede recibir, a través del puerto de entrada, la señal cuántica y la señal de referencia que son enviadas por el aparato de envío de claves cuánticas a través de la segunda fibra óptica.

La señal cuántica y la señal de referencia pueden ser enviadas mediante multiplexación por división del tiempo. Por lo tanto, al recibir la señal de referencia, el segundo divisor de haz de polarización 602 puede dividir la señal de referencia en la octava señal óptica y la novena señal óptica, emitir la octava señal óptica a través del primer puerto de salida y emitir la novena señal óptica a través del segundo puerto de salida. Al recibir la señal cuántica, el segundo divisor de haz de polarización 602 puede dividir la señal cuántica en la décima señal óptica y la undécima señal óptica, emitir la décima señal óptica a través del primer puerto de salida y emitir la undécima señal óptica a través del segundo puerto de salida.

El primer detector heterodino cuántico 603 está configurado para: recibir la sexta señal óptica, la octava señal óptica y la décima señal óptica, detectar una señal de interferencia entre la sexta señal óptica y la octava señal óptica para obtener una componente regular de la octava señal óptica, detectar una señal de interferencia entre la sexta señal óptica y la décima señal óptica para obtener una componente regular de la décima señal óptica, y enviar la componente regular de la octava señal óptica y la componente regular de la décima señal óptica señal, al procesador 605.

Al recibir la sexta señal óptica y la octava señal óptica, el primer detector heterodino cuántico 603 puede detectar la señal de interferencia entre la sexta señal óptica y la octava señal óptica para obtener la componente regular de la octava señal óptica y enviar la componente regular de la octava señal óptica al procesador 605. Al recibir la décima señal óptica, el primer detector heterodino cuántico 603 puede detectar la señal de interferencia entre la décima señal óptica y la sexta señal óptica para obtener la componente regular de la décima señal óptica, y enviar la componente regular de la décima señal óptica al procesador 605.

El segundo detector heterodino cuántico 604 está configurado para: recibir la séptima señal óptica, la novena señal óptica y la undécima señal óptica, detectar una señal de interferencia entre la séptima señal óptica y la novena señal óptica para obtener una componente regular de la novena señal óptica, detectar una señal de interferencia entre la séptima señal óptica y la undécima señal óptica para obtener una componente regular de la undécima señal óptica, y enviar la componente regular de la novena señal óptica y la componente regular de la undécima señal óptica, al procesador 605.

Cuando el primer detector heterodino cuántico 603 recibe la octava señal óptica, el segundo detector heterodino cuántico 604 puede recibir la novena señal óptica. En este caso, el segundo detector heterodino cuántico 604 puede detectar la señal de interferencia entre la novena señal óptica y la séptima señal óptica para obtener la componente regular de la novena señal óptica, y enviar la componente regular de la novena señal óptica, al procesador 605. Cuando el primer detector heterodino cuántico 603 recibe la décima señal óptica, el segundo detector heterodino cuántico 604 puede recibir la undécima señal óptica. En este caso, el segundo detector heterodino cuántico 604 puede detectar la señal de interferencia entre la undécima señal óptica y la séptima señal óptica para obtener el componente regular de la undécima señal óptica, y enviar la componente regular de la undécima señal óptica al procesador 605.

El procesador 605 recibe la componente regular de la octava señal óptica, la componente regular de la décima señal óptica, la componente regular de la novena señal óptica y la componente regular de la undécima señal óptica, procesa la componente regular de la octava señal óptica y la componente regular de la novena señal óptica para obtener un parámetro de señal, y procesa la componente regular de la décima señal óptica y la componente regular de la undécima señal óptica basándose en el parámetro de señal para obtener una clave inicial, donde la clave inicial incluye información de clave de la clave aleatoria.

Cuando el procesador 605 recibe la componente regular que es de la octava señal óptica y que es enviada por el primer detector heterodino cuántico 603 y la componente regular que es de la novena señal óptica y que es enviada por el segundo detector heterodino cuántico, el procesador 605 puede procesar la componente regular de la octava señal óptica y la componente regular de la novena señal óptica para

obtener el parámetro de señal, donde el parámetro de señal puede incluir una primera transmitancia de intensidad, una segunda transmitancia de intensidad, una primera fase y una segunda fase. La primera transmitancia de intensidad es una transmitancia de intensidad de una señal emitida desde el primer puerto de salida del segundo divisor de haz de polarización 602 después de que la señal de referencia entra en el
 5 segundo divisor de haz de polarización 602. La segunda transmitancia de intensidad es una transmitancia de intensidad de una señal emitida desde el primer puerto de salida del primer divisor de haz de polarización 601 después de que la señal del oscilador local entra en el primer divisor de haz de polarización 601. La primera fase es una fase que es de la novena señal óptica cuando el segundo detector heterodino cuántico 604 recibe la novena señal óptica y que se determina sobre la base de una fase de la octava señal óptica
 10 cuando el primer detector heterodino cuántico 603 recibe la octava señal óptica. La segunda fase es una fase que es de la sexta señal óptica cuando el primer detector heterodino cuántico 603 recibe la sexta señal óptica y que se determina sobre la base de la fase de la octava señal óptica cuando el primer detector heterodino cuántico 603 recibe la octava señal óptica.

15 Al recibir la componente regular que es de la décima señal óptica y que es enviada por el primer detector heterodino cuántico 603 y la componente regular que es de la undécima señal óptica y que es enviada por el segundo detector heterodino cuántico, el procesador 605 puede procesar la componente regular de la décima señal óptica y la componente regular de la undécima señal óptica basándose en el parámetro de señal determinado para obtener la clave inicial, donde la clave inicial incluye la información de clave de la clave
 20 aleatoria.

Opcionalmente, en una posible implementación, el aparato de envío de claves cuánticas puede enviar la señal cuántica y la señal de referencia en un modo de multiplexación por división de la frecuencia. De esta
 25 manera, el segundo divisor de haz de polarización 602 recibe simultáneamente la señal cuántica y la señal de referencia, divide la señal cuántica y la señal de referencia en una duodécima señal óptica y una decimotercera señal óptica, emite la duodécima señal óptica a través del primer puerto de salida, y emite la decimotercera señal óptica a través del segundo puerto de salida.

30 Al recibir la duodécima señal óptica, el primer detector heterodino cuántico 603 puede detectar la señal de interferencia entre la duodécima señal óptica y la sexta señal óptica para obtener la componente regular de la décima señal óptica, y enviar la componente regular de la duodécima señal óptica, al procesador 605. Al recibir la decimotercera señal óptica, el segundo detector heterodino cuántico 604 puede detectar la señal de interferencia entre la decimotercera señal óptica y la séptima señal óptica para obtener la componente regular de la decimotercera señal óptica, y enviar la componente regular de la decimotercera señal óptica al
 35 procesador 605.

Después de recibir la componente regular de la duodécima señal óptica y la componente regular de la decimotercera señal óptica, el procesador 605 puede extraer una primera componente regular de la señal de referencia de la componente regular de la duodécima señal óptica, extraer una segunda componente regular
 40 de la señal de referencia a partir de la componente regular de la decimotercera señal óptica, determinar un parámetro de señal basándose en la primera componente regular y en la segunda componente regular de la señal de referencia, y procesar una componente regular de la señal cuántica en la duodécima señal óptica y una componente regular de la decimotercera señal óptica basándose en el parámetro de señal para obtener una clave inicial.

45 La señal de referencia y la señal cuántica se envían mediante multiplexación por división de la frecuencia, y se ocupan diferentes bandas de frecuencia para la señal de referencia y la señal cuántica. Por lo tanto, basándose en una banda de frecuencia en la que está situada la señal de referencia, el procesador 605 puede extraer por separado, de la componente regular de la duodécima señal óptica y de la componente
 50 regular de la decimotercera señal óptica, una componente regular en la banda de frecuencia en la que se localiza la señal de referencia, para obtener la primera componente regular y la segunda componente regular de la señal de referencia.

55 En esta realización de esta solicitud, el aparato de recepción de claves cuánticas puede realizar la división del haz en la señal del oscilador local, la señal cuántica y la señal de referencia utilizando el primer divisor del haz de polarización y el segundo divisor del haz de polarización, medir la componente regular de la señal de referencia y la componente regular de la señal cuántica utilizando el primer detector heterodino cuántico y el segundo detector heterodino cuántico, calcular el parámetro de señal basándose en la componente regular de la señal de referencia y, finalmente, procesar la componente regular de la señal cuántica basándose en el
 60 parámetro de señal para obtener la clave inicial. Se puede aprender que, en esta realización de esta solicitud, puede que no sea necesario disponer un módulo de control de la polarización en el aparato de recepción de claves cuánticas. Según el método anterior, se puede eliminar el impacto causado por la rotación de la polarización y se puede garantizar la precisión de la información de clave obtenida.

65 El aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas que se utilizan para la transmisión de clave cuántica se han descrito principalmente en las realizaciones anteriores. A continuación,

una realización de esta solicitud da a conocer un sistema de transmisión de claves cuánticas.

5 Con referencia a la figura 14, se da a conocer un sistema de transmisión de claves cuánticas. El sistema puede incluir un aparato de envío de claves cuánticas 701, un aparato de recepción de claves cuánticas 702, una primera fibra óptica 703 y una segunda fibra óptica 704. El aparato de envío de claves cuánticas 701 y el aparato de recepción de claves cuánticas 702 se comunican entre sí a través de la primera fibra óptica 703 y de la segunda fibra óptica 704, la primera fibra óptica 703 está configurada para transmitir una señal del oscilador local, y la segunda fibra óptica 704 está configurada para transmitir una señal cuántica y una señal de referencia.

10 Cabe señalar que el aparato de envío de claves cuánticas 701 en el sistema de transmisión de claves cuánticas puede ser cualquier aparato de envío de claves cuánticas mostrado en la figura 1 a la figura 8. En este caso, el aparato de recepción de claves cuánticas 702 puede ser un aparato de recepción de claves cuánticas que no incluye un dispositivo configurado para controlar una dirección de polarización. Por ejemplo, el aparato de recepción de claves cuánticas 702 puede incluir un módulo de detección cuántica y no incluye un módulo de control de la polarización.

15 Opcionalmente, el aparato de recepción de claves cuánticas 702 en el sistema de transmisión de claves cuánticas puede ser cualquier aparato de recepción de claves cuánticas mostrado en la figura 9 a la figura 13. En este caso, el aparato de envío de claves cuánticas 701 puede no incluir un controlador de polarización. Por ejemplo, el aparato de envío de claves cuánticas 701 puede incluir un láser, un divisor de haz y un módulo de generación de señales cuánticas, y no incluye el controlador de polarización. El aparato de envío de claves cuánticas 701 puede incluir alternativamente un láser, un divisor de haz, un módulo de generación de señales cuánticas y un módulo de generación de señal de referencia, y no incluye el controlador de polarización.

20 Opcionalmente, en una posible implementación, el aparato de envío de claves cuánticas 701 en el sistema de transmisión de claves cuánticas puede ser cualquier aparato de envío de claves cuánticas mostrado en la figura 1 a la figura 8, y el aparato de recepción de claves cuánticas 702 en el sistema de transmisión de claves cuánticas puede ser cualquier aparato de recepción de claves cuánticas mostrado en la figura 9 a la figura 13.

25 Opcionalmente, considerando que se utilizan dos fibras ópticas para transmitir señales ópticas coherentes en un sistema de comunicaciones coherente clásico para implementar comunicación bidireccional, y que el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas en esta realización de esta solicitud también se comunican entre sí a través de dos fibras ópticas, el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas en esta realización de esta solicitud pueden compartir dos fibras ópticas con el sistema de comunicaciones coherente clásico para transmitir señales.

30 Sobre esta base, con referencia a la figura 15, una realización de esta solicitud da a conocer un sistema de transmisión de claves cuánticas en el que una señal cuántica y una señal óptica coherente se transmiten de manera híbrida. El sistema incluye una primera estación base de comunicaciones 80 y una segunda estación base de comunicaciones 90. La primera estación base de comunicaciones 80 y la segunda estación base de comunicaciones 90 implementan comunicación bidireccional a través de una primera fibra óptica y una segunda fibra óptica.

35 La primera estación base de comunicaciones 80 incluye un aparato de envío de claves cuánticas 801, un primer aparato de envío óptico coherente 802, un primer aparato de recepción óptica coherente 803, un primer acoplador 804 y un segundo acoplador 805.

40 La segunda estación base de comunicaciones 90 incluye un aparato de recepción de claves cuánticas 901, un segundo aparato de recepción óptica coherente 902, un segundo aparato de envío óptico coherente 903, un tercer acoplador 904 y un cuarto acoplador 905.

45 Cabe señalar que, para las implementaciones del aparato de envío de claves cuánticas 801 y el aparato de recepción de claves cuánticas 901, consulte las implementaciones del aparato de envío de claves cuánticas 701 y el aparato de recepción de claves cuánticas 702 mostrados en la figura 14.

50 El primer aparato de envío óptico coherente 802 está conectado a la primera fibra óptica utilizando el primer acoplador, y está configurado para enviar una señal óptica coherente al segundo aparato de recepción óptica coherente 902 a través de la primera fibra óptica. El segundo aparato de envío óptico coherente 903 está conectado a la segunda fibra óptica mediante el uso del cuarto acoplador, y está configurado para enviar una señal óptica coherente al primer aparato de recepción óptica coherente 803 a través de la segunda fibra óptica. En otras palabras, el primer aparato de envío óptico coherente 802 y el segundo aparato de recepción óptica coherente 902 pueden ser utilizado para transmitir una señal coherente desde la primera estación base de comunicaciones 80 a la segunda estación base de comunicaciones 90. El segundo aparato de envío

óptico coherente 903 y el primer aparato de recepción óptica coherente 803 pueden ser utilizados para transmitir una señal coherente desde la segunda estación base de comunicaciones 90 a la primera estación base de comunicaciones 80.

5 Además, una señal del oscilador local enviada por el aparato de envío de claves cuánticas 801 y la señal óptica coherente enviada por el primer aparato de envío óptico coherente 802 se transmiten simultáneamente a través de la primera fibra óptica. Por lo tanto, tanto el aparato de envío de claves cuánticas 801 como el primer aparato de envío óptico coherente 802 pueden conectarse a la primera fibra óptica utilizando el primer acoplador 804. De esta manera, al recibir la señal del oscilador local enviada por el aparato de envío de
10 claves cuánticas 801 y la señal óptica coherente enviada por el primer aparato de envío óptico coherente 802, el primer acoplador 804 puede acoplar la señal del oscilador local y la señal óptica coherente, y enviar una señal acoplada a través de la primera fibra óptica conectada. La longitud de onda de la señal del oscilador local es diferente de la longitud de onda de la señal óptica coherente.

15 En consecuencia, el tercer acoplador 904 está conectado a la primera fibra óptica. De esta manera, el tercer acoplador 904 puede recibir la señal que se transmite a través de la primera fibra óptica y que se obtiene acoplando la señal óptica coherente y la señal del oscilador local, y desacoplar la señal recibida para obtener la señal del oscilador local y la señal óptica coherente que es enviada por el primer aparato de envío óptico coherente 802. A continuación, el tercer acoplador 904 puede enviar, al segundo aparato de recepción óptica
20 coherente 902, la señal óptica coherente enviada por el primer aparato de envío óptico coherente 802, y enviar la señal del oscilador local al aparato de recepción de claves cuánticas 901.

Cabe señalar, además, que el aparato de envío de claves cuánticas 801 está conectado a la segunda fibra óptica mediante el uso del segundo acoplador 805. De esta manera, el aparato de envío de claves cuánticas
25 801 puede enviar una señal cuántica y una señal de referencia al segundo acoplador 805. A continuación, el segundo acoplador 805 envía la señal cuántica y la señal de referencia al cuarto acoplador 905 a través de la segunda fibra óptica. Adicionalmente, el segundo acoplador 805 puede ser configurado, además, para: recibir una señal óptica coherente enviada por el cuarto acoplador 905 a través de la segunda fibra óptica, y enviar la señal óptica coherente al primer aparato de recepción óptica coherente 803.

30 El cuarto acoplador 905 está configurado para: recibir la señal cuántica y la señal de referencia de la segunda fibra óptica, y enviar la señal cuántica y la señal de referencia, al aparato de recepción de claves cuánticas 901. Adicionalmente, el cuarto acoplador 905 está configurado, además, para: recibir la señal óptica coherente enviada por el segundo aparato de envío óptico coherente 903, y enviar la señal óptica coherente
35 al primer aparato de recepción óptica coherente 803 a través de la segunda fibra óptica y del segundo acoplador.

El primer acoplador 804, el segundo acoplador 805, el tercer acoplador 904 y el cuarto acoplador 905 pueden ser cada uno de ellos un acoplador selectivo de longitud de onda, por ejemplo, puede ser un acoplador
40 multiplexado por división de la longitud de onda (Wavelength Division Multiplexing, WDM).

Opcionalmente, en una posible implementación, en el sistema de transmisión de claves cuánticas, la primera estación base de comunicaciones puede incluir una pluralidad de aparatos de envío de claves cuánticas. En consecuencia, la segunda estación base de comunicaciones puede incluir aparatos de recepción de claves
45 cuánticas cuya cantidad es igual a una cantidad de aparatos de envío de claves cuánticas, y la pluralidad de aparatos de envío de claves cuánticas en la primera estación base de comunicaciones corresponden uno a uno a los aparatos de recepción de claves cuánticas en la segunda estación base de comunicaciones.

Además, la primera estación base de comunicaciones puede incluir, además, una pluralidad de aparatos de
50 recepción de claves cuánticas. En consecuencia, la segunda estación base de comunicaciones puede incluir aparatos de envío de claves cuánticas que corresponden uno a uno a la pluralidad de aparatos de recepción de claves cuánticas, para implementar la transmisión bidireccional de una señal cuántica.

En esta realización de esta solicitud, el aparato de envío de claves cuánticas y el aparato de recepción de
55 claves cuánticas pueden compartir dos fibras ópticas con un sistema de comunicaciones coherente clásico para transmitir señales. De este modo se integra y miniaturiza un extremo de recepción, se reducen componentes adicionales y pérdidas de línea y se transmiten de manera híbrida una señal óptica coherente clásica y una señal cuántica.

60 Los expertos en la materia pueden comprender que todas o algunas de las etapas de los procedimientos en las realizaciones pueden ser implementadas mediante un programa que le proporcione indicaciones a un hardware relevante. El programa puede almacenarse en un medio de almacenamiento legible por ordenador. El medio de almacenamiento puede ser una memoria de solo lectura, un disco magnético, un disco óptico o similares.
65

REIVINDICACIONES

1. Un aparato de envío de claves cuánticas, en el que el aparato comprende un láser (201), un divisor de haz (202), un módulo de generación de señales cuánticas (203) y un módulo de control de la polarización (204);
 5 el láser (201) está configurado para emitir una primera señal óptica;
- el divisor de haz (202) está configurado para: recibir la primera señal óptica, dividir la primera señal óptica en una segunda señal óptica y una tercera señal óptica, enviar la segunda señal óptica a través de una primera
 10 fibra óptica, y enviar la tercera señal óptica al módulo de generación de señales cuánticas (203);
- el módulo de generación de señales cuánticas (203) está configurado para: modular la tercera señal óptica para obtener una primera señal modulada y una segunda señal modulada, y enviar la primera señal modulada y la segunda señal modulada al módulo de control de la polarización, en el que la primera señal
 15 modulada transporta una clave aleatoria a transmitir, y la segunda señal modulada transporta datos de referencia a transmitir; y
- el módulo de control de la polarización (204) está configurado para: ajustar una dirección de polarización de la primera señal modulada y una dirección de polarización de la segunda señal modulada, y atenuar la
 20 intensidad de la luz de la primera señal modulada y la intensidad de la luz de la segunda señal modulada para obtener una señal cuántica y una señal de referencia, en donde la señal cuántica y la señal de referencia se envían a través de una segunda fibra óptica,
- en donde la señal de referencia transporta datos de referencia, y los datos de referencia son negociados de
 25 antemano por el aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas,
- en donde la dirección de polarización de la señal de referencia es la misma que la dirección de polarización de la señal cuántica.
2. El aparato según la reivindicación 1, en el que la intensidad luminosa de la segunda señal óptica es mayor
 30 que la intensidad luminosa de la tercera señal óptica.
3. El aparato según la reivindicación 1 o 2, en el que el aparato comprende, además, un aparato de recepción (205) y un procesador (206);
 35 el receptor (205) está configurado para: recibir información de control de la dirección de polarización y enviar la información de control de la dirección de polarización, al procesador (206);
- el procesador (206) está configurado para: procesar la información de control de la dirección de polarización para obtener una primera señal de control, y enviar la primera señal de control al módulo de control de la
 40 polarización (204); y
- el módulo de control de la polarización (204) está configurado para ajustar la dirección de polarización de la primera señal modulada y la dirección de polarización de la segunda señal modulada basándose en la
 45 primera señal de control.
4. El aparato según la reivindicación 1 o 2, en el que el módulo de generación de señales cuánticas (203) comprende un generador de números aleatorios cuánticos (2031), un módulo de procesamiento (2032) y un
 50 modulador (2033);
- el generador de números aleatorios cuánticos (2031) está configurado para: generar un número aleatorio y enviar el número aleatorio al módulo de procesamiento (2032);
- el módulo de procesamiento (2032) está configurado para: generar la clave aleatoria basándose en el
 55 número aleatorio, y generar una señal de control cuántica basándose en la clave aleatoria; y está configurado, además, para: generar una señal de control de referencia basándose en los datos de referencia almacenados, y enviar la señal de control cuántica y la señal de control de referencia, al modulador (2033); y
- el modulador (2033) está configurado para: modular la tercera señal óptica sobre la base de la señal de
 60 control cuántica para obtener la primera señal modulada, modular la tercera señal óptica sobre la base de la señal de control de referencia para obtener la segunda señal modulada, y enviar la primera señal modulada señal y la segunda señal modulada al módulo de control de la polarización (204).
5. El aparato según la reivindicación 4, en el que el módulo de control de la polarización (204) comprende un
 65 controlador de polarización (2041) y un atenuador (2042);

el controlador de polarización (2041) está configurado para: ajustar la dirección de polarización de la primera señal modulada y la dirección de polarización de la segunda señal modulada, y enviar una primera señal modulada ajustada y una segunda señal modulada ajustada al atenuador (2042); y

5 el atenuador (2042) está configurado para: atenuar la primera señal modulada ajustada para obtener la señal cuántica, y atenuar la segunda señal modulada ajustada para obtener la señal de referencia.

6. El aparato según la reivindicación 4, en el que el módulo de control de la polarización (204) comprende un controlador de polarización (2041) y un atenuador (2042);

10 el atenuador (2042) está configurado para: atenuar la primera señal modulada y la segunda señal modulada para obtener una primera señal modulada atenuada y una segunda señal modulada atenuada, y enviar la primera señal modulada atenuada y la segunda señal modulada atenuada, al controlador de polarización (2041); y

15 el controlador de polarización (2041) está configurado para: ajustar una dirección de polarización de la primera señal modulada atenuada para obtener la señal cuántica, y atenuar una dirección de polarización de la segunda señal modulada atenuada para obtener la señal de referencia.

20 7. El aparato según la reivindicación 1 o 2, en el que la longitud de onda de la segunda señal óptica es diferente de la longitud de onda de otra señal óptica transmitida a través de la primera fibra óptica, y la longitud de onda de la tercera señal óptica es diferente de la longitud de onda de otra señal óptica transmitida a través de la segunda fibra óptica.

25 8. El aparato según la reivindicación 1 o 2, en el que la segunda fibra óptica se utiliza, además, para transmitir una señal óptica coherente, y la dirección de transmisión de la señal óptica coherente transmitida a través de la segunda fibra óptica es opuesta a la dirección de transmisión de la señal cuántica transmitida sobre la segunda fibra óptica.

30 9. Un aparato de recepción de claves cuánticas, en el que el aparato comprende un módulo de detección cuántica (401) y un módulo de control de la polarización (402);

35 el módulo de control de la polarización (402) está configurado para: recibir una señal del oscilador local desde una primera fibra óptica, ajustar una dirección de polarización de la señal del oscilador local y enviar una señal del oscilador local ajustada al módulo de detección cuántica; y

40 el módulo de detección cuántica (401) está configurado para: recibir una señal cuántica y una señal de referencia desde una segunda fibra óptica, y detectar la señal del oscilador local ajustada, la señal cuántica y la señal de referencia para obtener resultados de detección, en donde la señal de referencia transporta datos de referencia negociados de antemano por un aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas, la señal cuántica transporta una clave aleatoria, y los resultados de la detección comprenden información de clave de la clave aleatoria; o

45 el módulo de control de la polarización (402) está configurado para: recibir una señal cuántica y una señal de referencia desde una segunda fibra óptica, ajustar la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia, y enviar la señal cuántica ajustada y la señal de referencia ajustada, al módulo de detección cuántica (401); y

50 el módulo de detección cuántica (401) está configurado para: recibir una señal del oscilador local desde una primera fibra óptica y detectar la señal del oscilador local, la señal cuántica ajustada y la señal de referencia ajustada, para obtener resultados de detección.

55 en donde la dirección de polarización de la señal de referencia es la misma que la dirección de polarización de la señal cuántica, el módulo de control de la polarización (402) comprende un controlador de polarización (4021); y

bien:

60 a) el controlador de polarización (4021) está configurado para: recibir la señal del oscilador local desde la primera fibra óptica, ajustar la dirección de polarización de la señal del oscilador local a una primera dirección de polarización y enviar la señal del oscilador local ajustada al módulo de detección cuántica (401);

65 el módulo de detección cuántica (401) está configurado para: recibir la señal del oscilador local ajustada; recibir la señal cuántica y la señal de referencia desde la segunda fibra óptica; detectar una señal de interferencia entre la señal del oscilador local ajustada y la señal de referencia para obtener un valor de medición de datos de referencia; y, si una desviación entre el valor de medición de los datos de referencia y

los datos de referencia almacenados no es mayor que una desviación permitida, detectar una señal de interferencia entre la señal cuántica y la señal del oscilador local ajustada, para obtener los resultados de la detección; o bien, si una desviación entre el valor de medición de los datos de referencia y los datos de referencia almacenados es mayor que una desviación permitida, generar una segunda señal de control basándose en el valor de medición de los datos de referencia, y enviar la segunda señal de control al controlador de polarización (4021); y

el controlador de polarización (4021) está configurado, además, para: recibir la segunda señal de control, actualizar la dirección de polarización de la señal del oscilador local basándose en la segunda señal de control y reenviar la señal del oscilador local ajustada al módulo de detección cuántica (401); o bien

b) el controlador de polarización (4021) está configurado para: recibir la señal cuántica y la señal de referencia desde la segunda fibra óptica, ajustar la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia a una primera dirección de polarización, y enviar la señal cuántica ajustada y la señal de referencia ajustada al módulo de detección cuántica (401);

el módulo de detección cuántica (401) está configurado para: recibir la señal cuántica ajustada y la señal de referencia ajustada; recibir la señal del oscilador local desde la primera fibra óptica; detectar una señal de interferencia entre la señal de referencia ajustada y la señal del oscilador local para obtener un valor de medición de datos de referencia; y, si la desviación entre el valor de medición de los datos de referencia y los datos de referencia almacenados no es mayor que una desviación permitida, detectar una señal de interferencia entre la señal cuántica ajustada y la señal del oscilador local, para obtener los resultados de la detección; o bien, si la desviación entre el valor de medición de los datos de referencia y los datos de referencia almacenados es mayor que una desviación permitida, generar una cuarta señal de control basándose en el valor de medición de los datos de referencia y enviar la cuarta señal de control al controlador de polarización (4021); y

el controlador de polarización (4021) está configurado, además, para: recibir la cuarta señal de control, actualizar la dirección de polarización de la señal cuántica y la dirección de polarización de la señal de referencia sobre la base de la cuarta señal de control, y reenviar la señal cuántica ajustada y la señal de referencia ajustada, al módulo de detección cuántica (401).

10. Un aparato de recepción de claves cuánticas, en el que el aparato comprende un primer divisor de haz de polarización (601), un segundo divisor de haz de polarización (602), un primer detector heterodino cuántico (603), un segundo detector heterodino cuántico (604) y un procesador (605);

el primer divisor de haz de polarización (601) está configurado para: recibir una señal de oscilador local desde una primera fibra óptica, dividir la señal de oscilador local en una sexta señal óptica y una séptima señal óptica, enviar la sexta señal óptica al primer detector heterodino cuántico (603), y enviar la séptima señal óptica al segundo detector heterodino cuántico (604);

el segundo divisor de haz de polarización (602) está configurado para: recibir una señal cuántica y una señal de referencia desde una segunda fibra óptica, dividir la señal de referencia en una octava señal óptica y una novena señal óptica, dividir la señal cuántica en una décima señal óptica y una undécima señal óptica, enviar la octava señal óptica y la décima señal óptica al primer detector heterodino cuántico (603), y enviar la novena señal óptica y la undécima señal óptica al segundo detector heterodino cuántico (604), en donde la señal de referencia transporta datos de referencia negociados de antemano por un aparato de envío de claves cuánticas y el aparato de recepción de claves cuánticas y la señal cuántica transporta una clave aleatoria;

el primer detector heterodino cuántico (603) está configurado para: detectar una señal de interferencia entre la sexta señal óptica y la octava señal óptica para obtener una componente regular de la octava señal óptica, detectar una señal de interferencia entre la sexta señal óptica y la décima señal óptica para obtener una componente regular de la décima señal óptica, y enviar la componente regular de la octava señal óptica y la componente regular de la décima señal óptica al procesador (605);

el segundo detector heterodino cuántico (604) está configurado para: detectar una señal de interferencia entre la séptima señal óptica y la novena señal óptica para obtener una componente regular de la novena señal óptica, detectar una señal de interferencia entre la séptima señal óptica y la undécima señal óptica para obtener una componente regular de la undécima señal óptica, y enviar la componente regular de la novena señal óptica y la componente regular de la undécima señal óptica, al procesador (605); y

el procesador (605) está configurado para: procesar la componente regular de la octava señal óptica y la componente regular de la novena señal óptica para obtener un parámetro de señal, y procesar la componente regular de la décima señal óptica y la componente regular de la undécima señal óptica basándose en el parámetro de señal para obtener una clave inicial, en donde la clave inicial comprende

información de clave de la clave aleatoria.

- 5 11. Un sistema de transmisión de claves cuánticas, en el que el sistema de transmisión de claves cuánticas comprende un aparato de envío de claves cuánticas y un aparato de recepción de claves cuánticas;
- el aparato de envío de claves cuánticas es el aparato según cualquiera de las reivindicaciones 1 a 8; y
- el aparato de recepción de claves cuánticas es el aparato según la reivindicación 9.

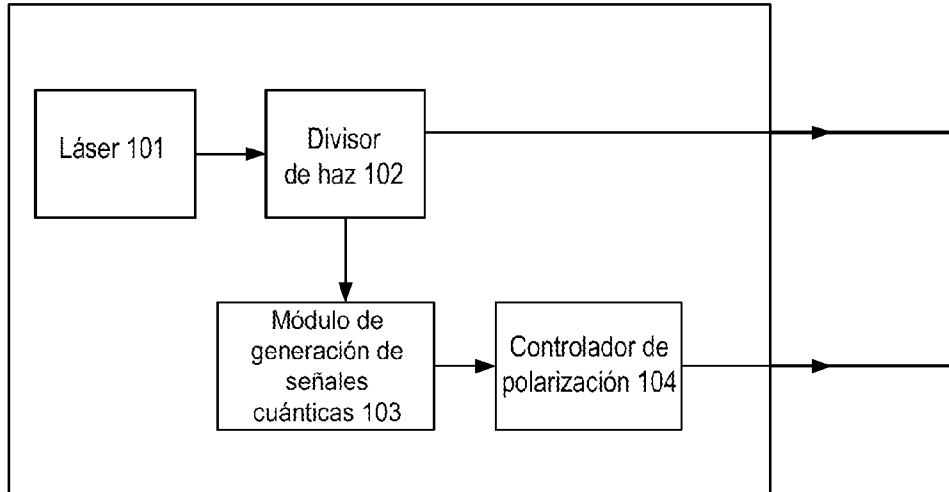


FIG. 1

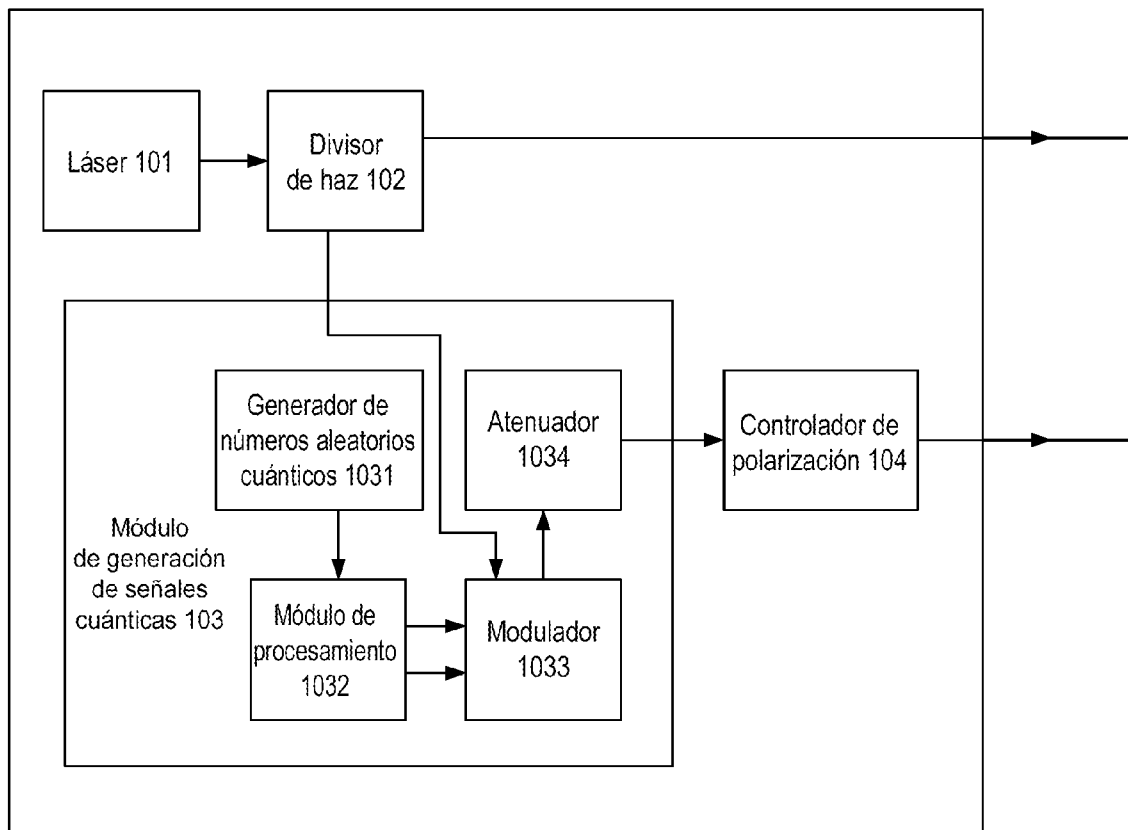


FIG. 2

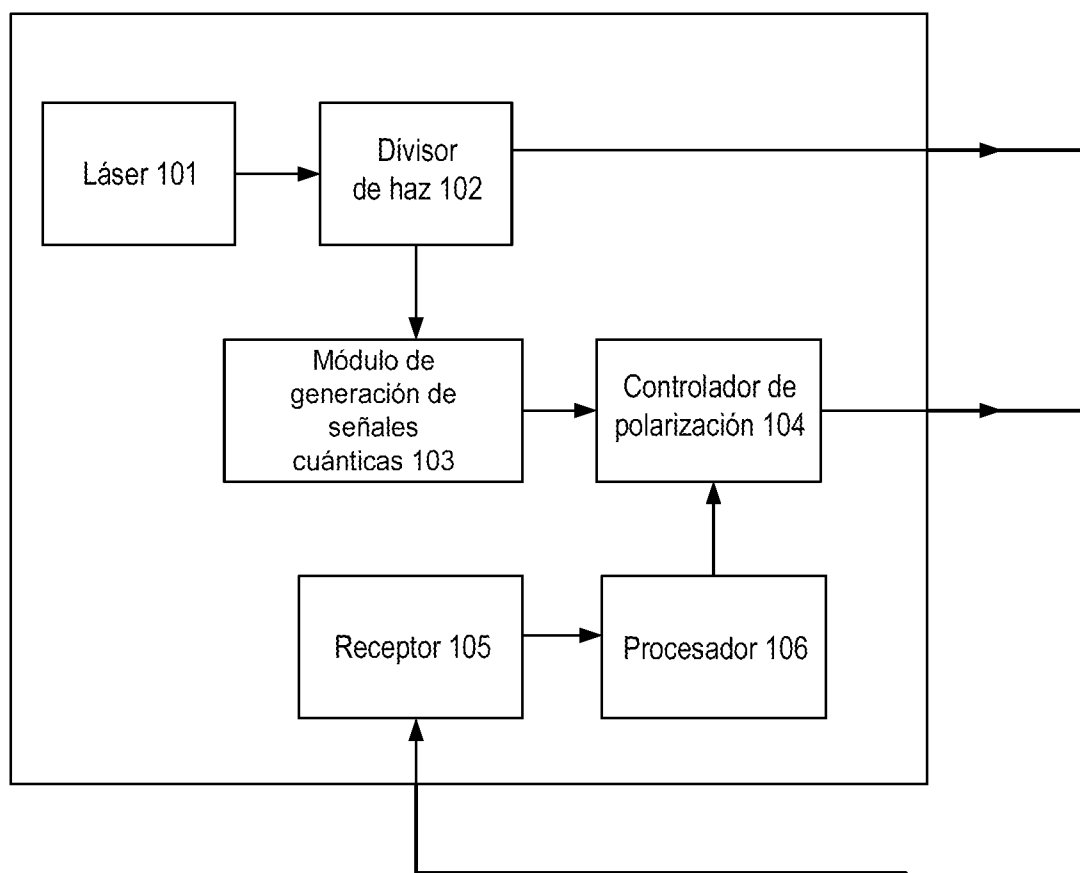


FIG. 3

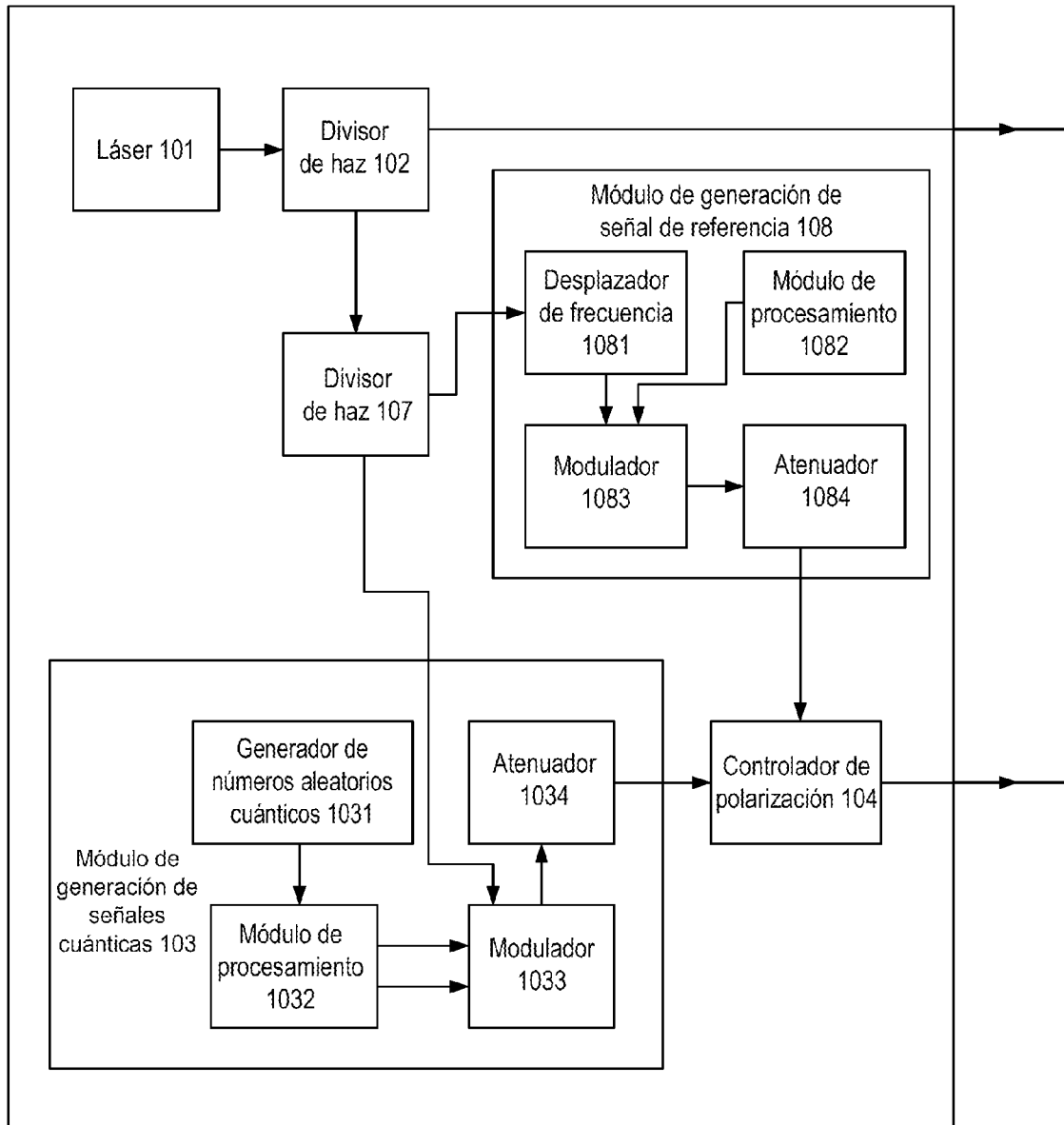


FIG. 4

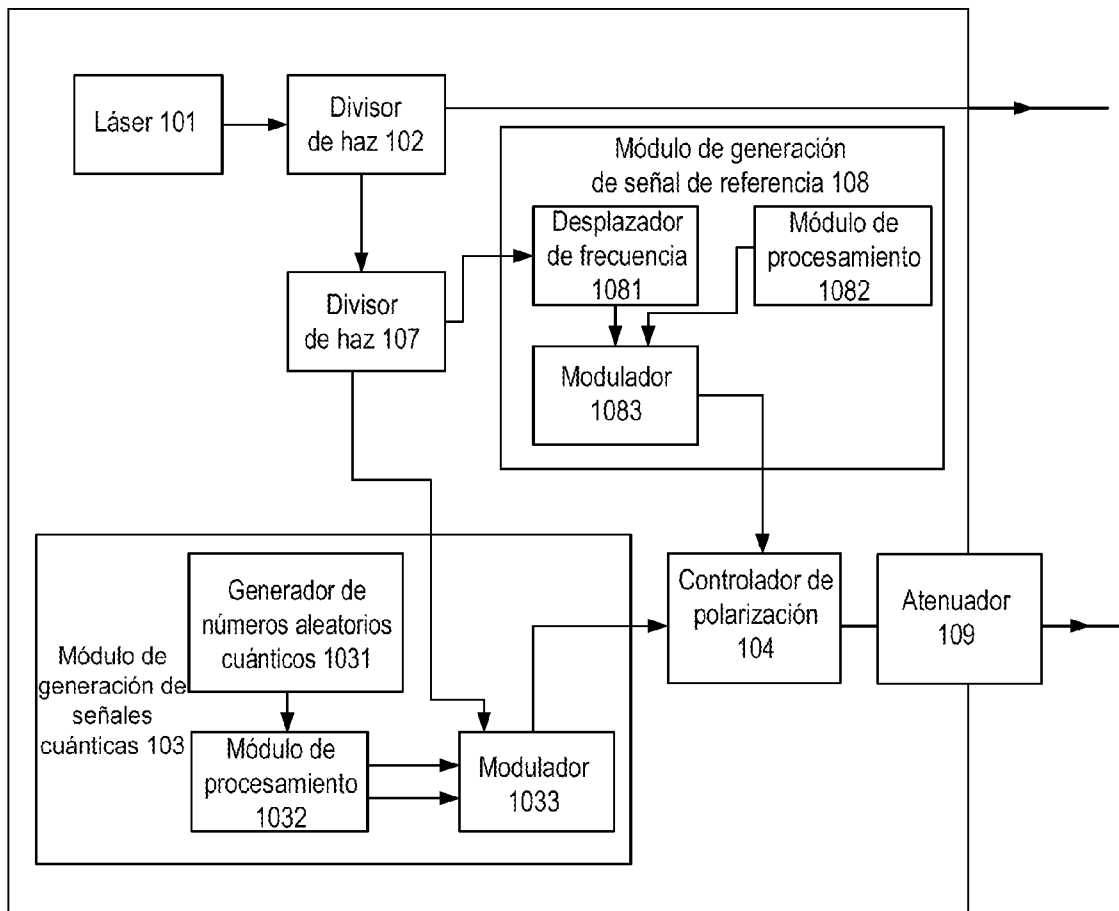


FIG. 5

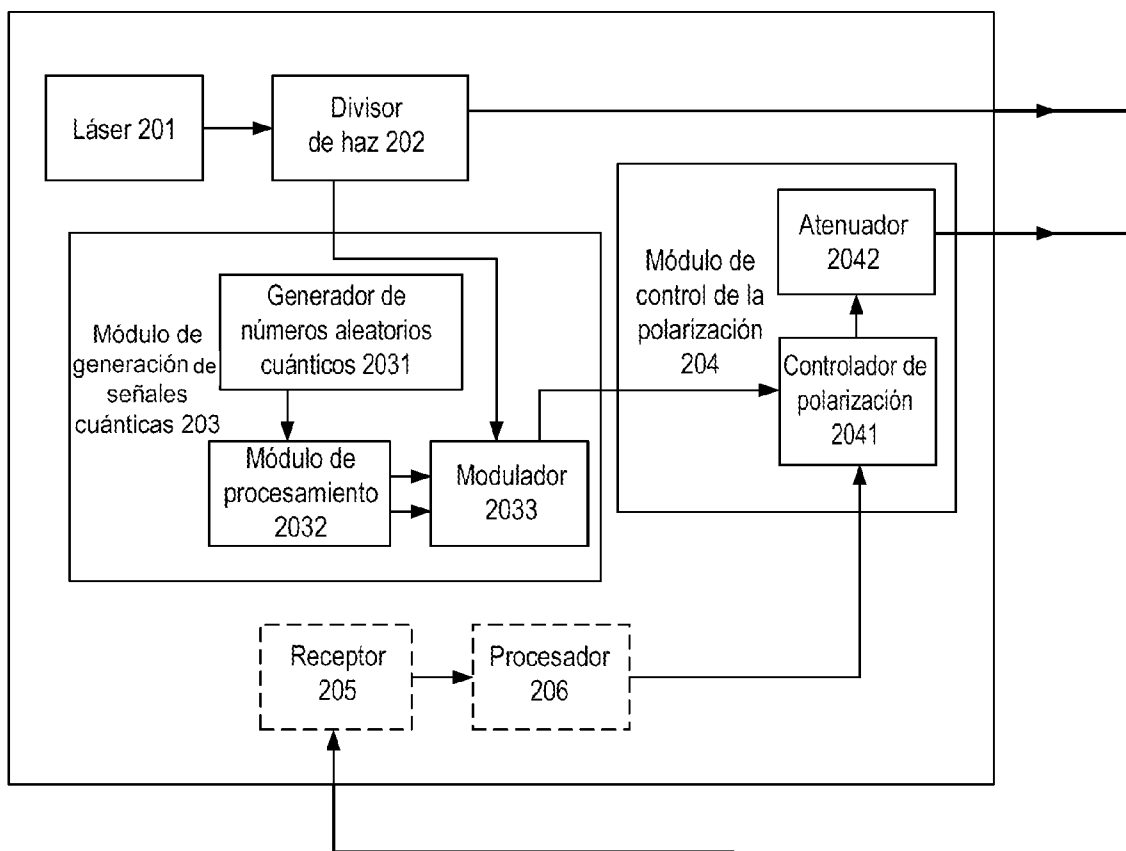


FIG. 6

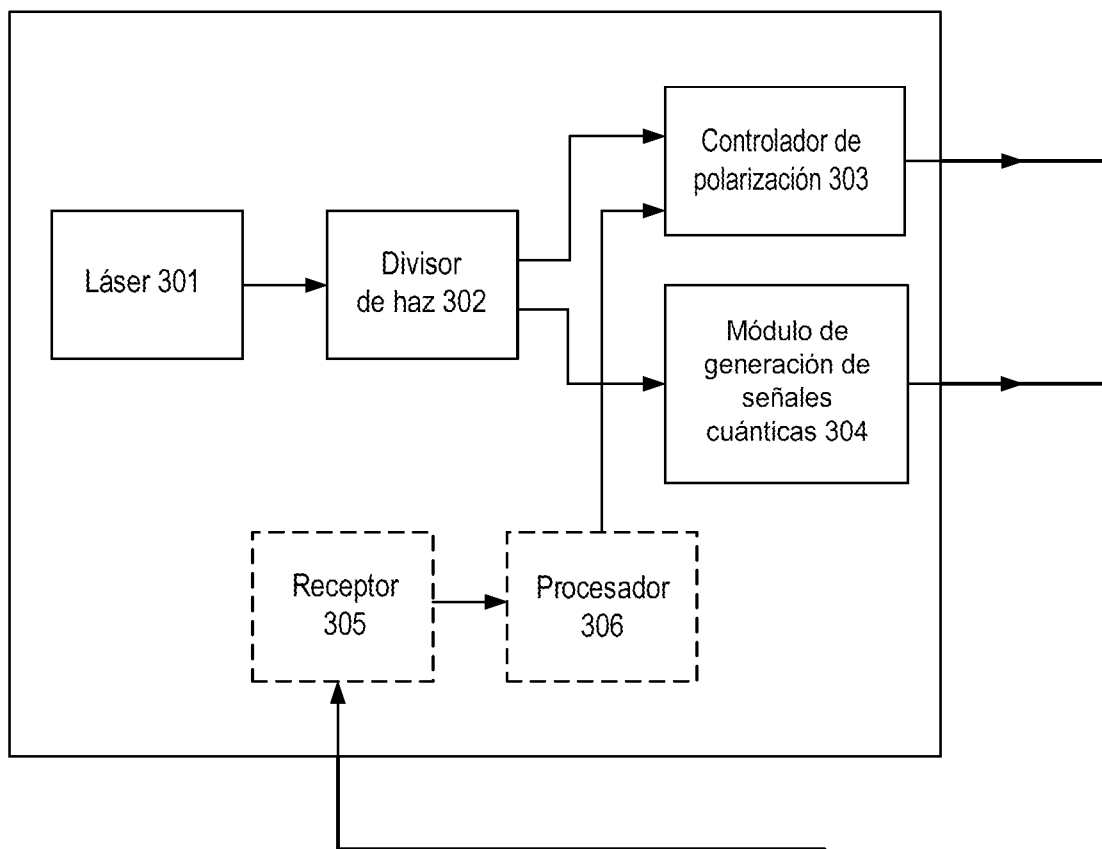


FIG. 7

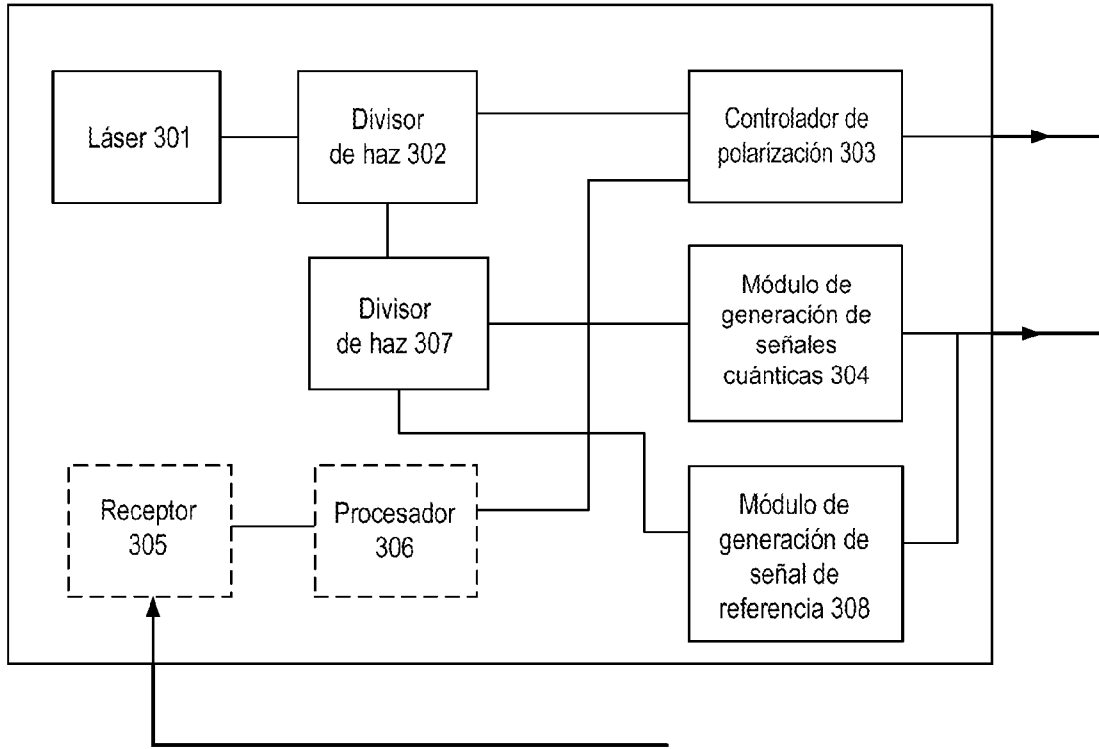


FIG. 8

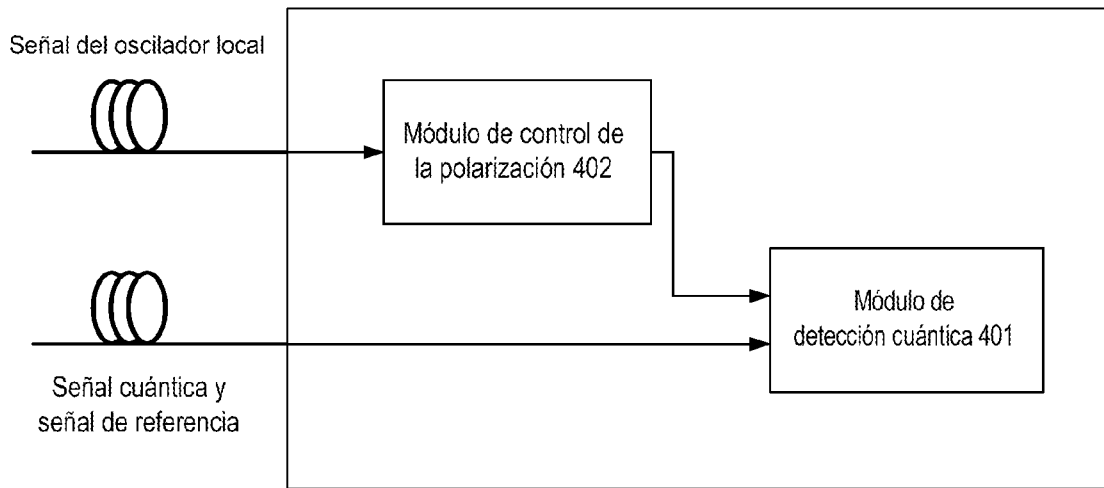


FIG. 9

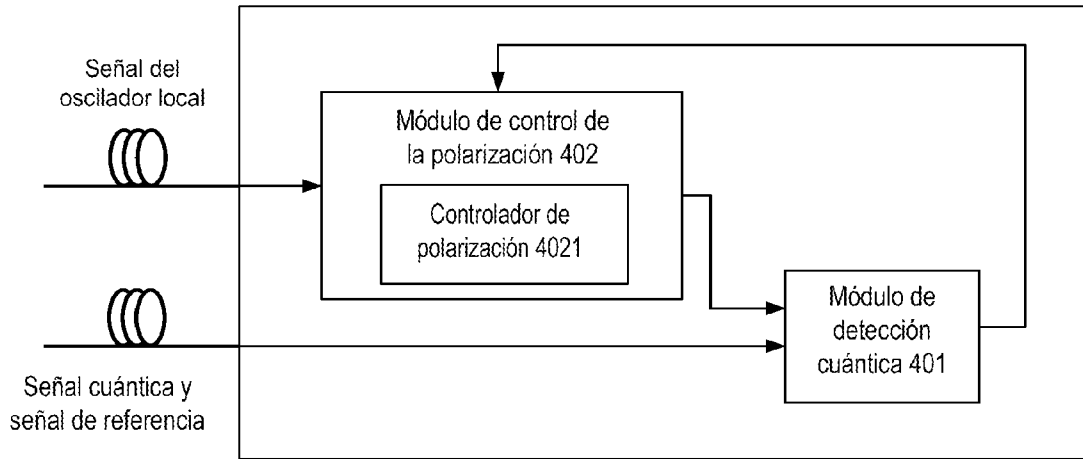


FIG. 10

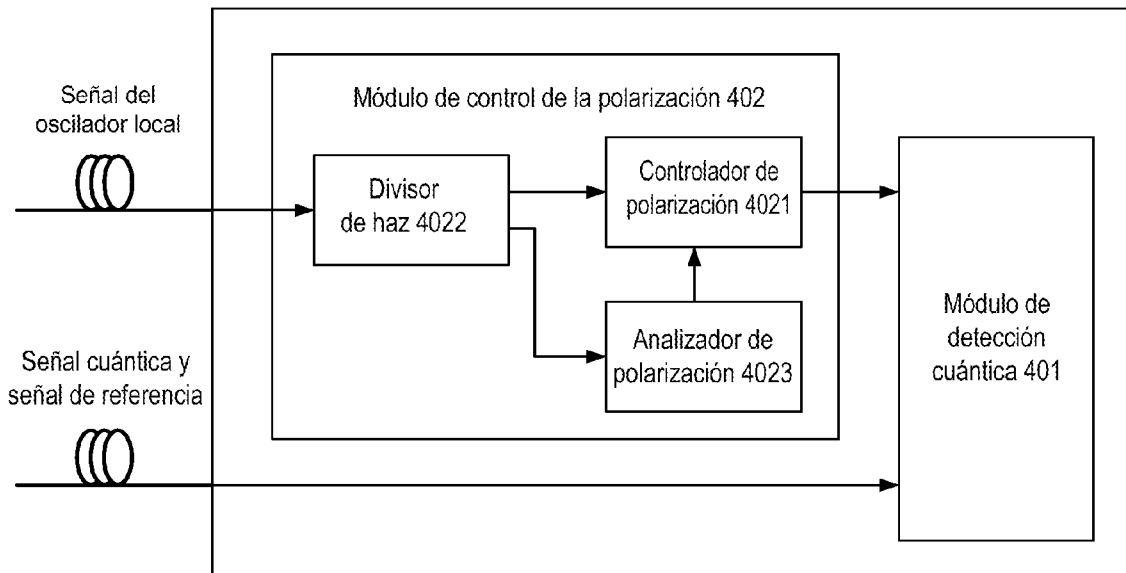


FIG. 11

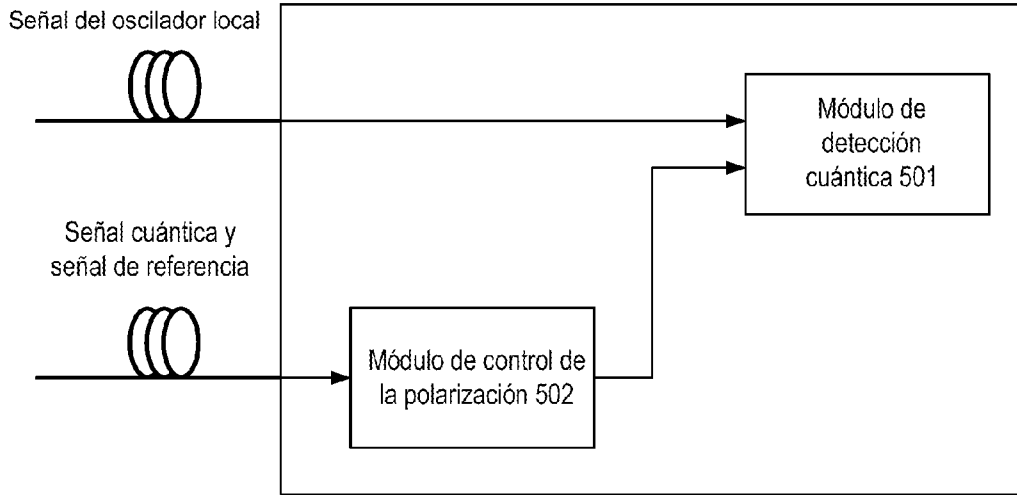


FIG. 12

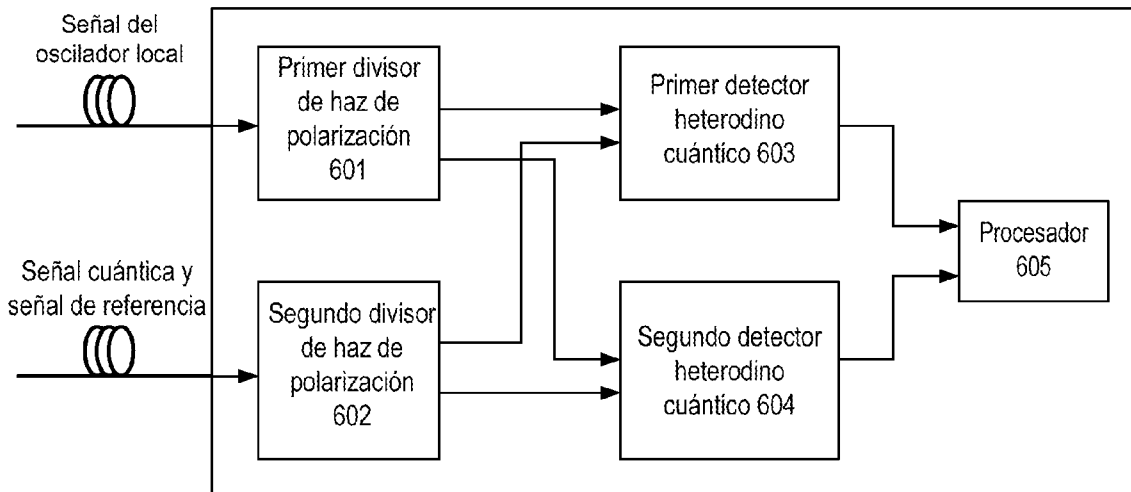


FIG. 13

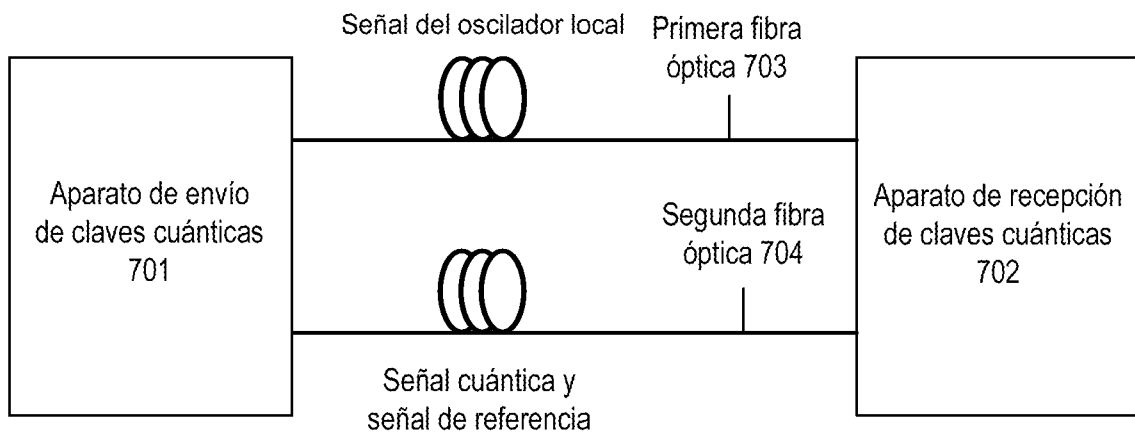


FIG. 14

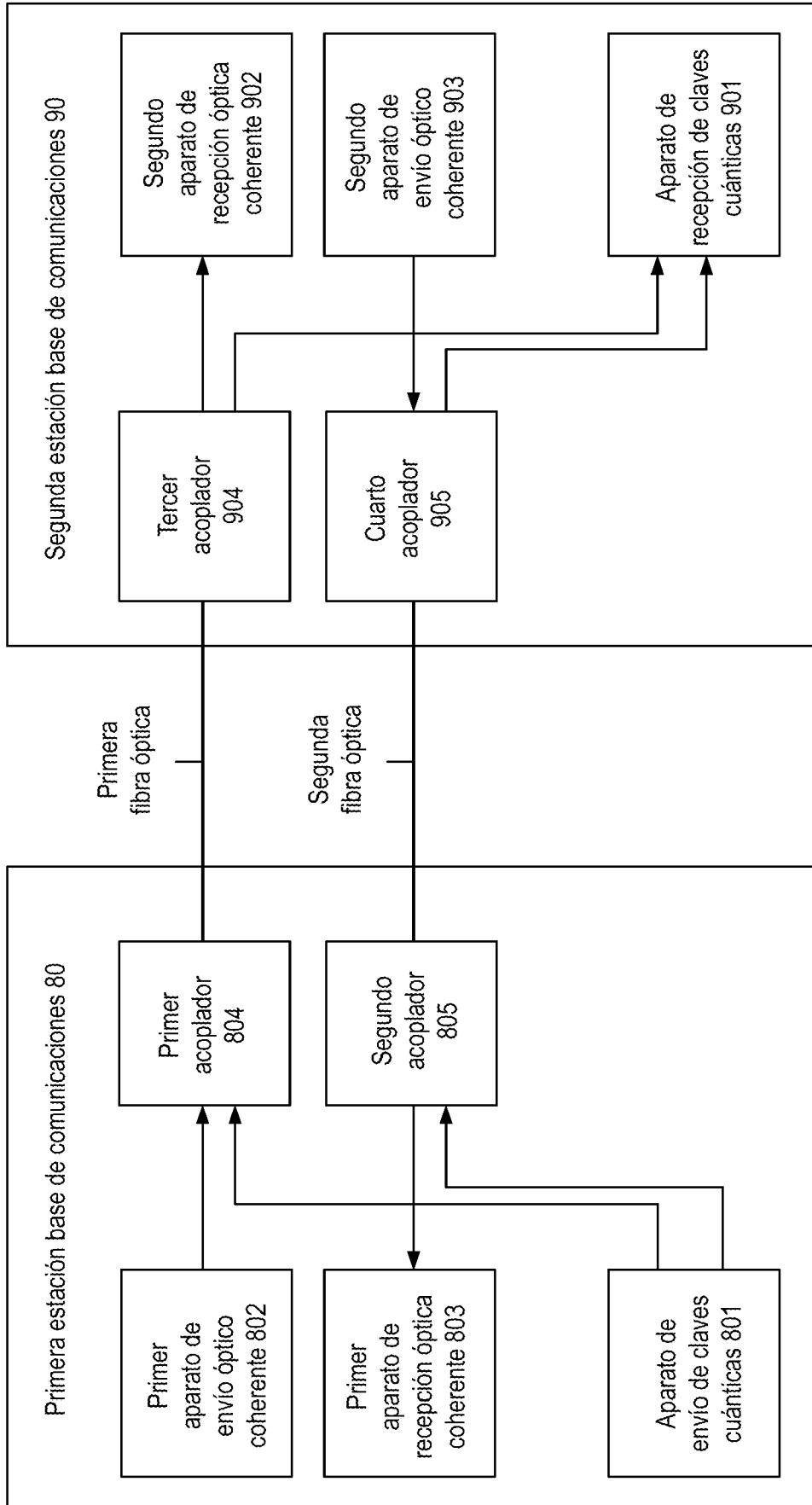


FIG. 15