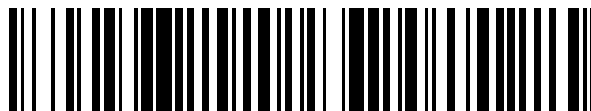


(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



(11) Número de publicación: **2 425 693**

(21) Número de solicitud: 201230385

(51) Int. Cl.:

H04L 9/08

(2006.01)

(12)

SOLICITUD DE PATENTE

A1

(22) Fecha de presentación:

14.03.2012

(43) Fecha de publicación de la solicitud:

16.10.2013

(56) Se remite a la solicitud internacional:

PCT/ES2013/070157

(71) Solicitantes:

**UNIVERSIDAD POLITÉCNICA DE VALENCIA
(100.0%)
CAMINO DE VERA, S/N
46022 VALENCIA ES**

(72) Inventor/es:

**CAPMANY FRANCOY, Jose;
MORA ALMERICH, Jose y
RUIZ ALBA GAYA, Antonio**

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

(54) Título: **SISTEMA DE DISTRIBUCION DE CLAVE CUANTICA BASADO EN MODULACION DE FRECUENCIA Y FASE DIFERENCIAL**

(57) Resumen:

Sistema de distribución de clave cuántica basado en modulación de frecuencia y fase diferencial. Combina la técnica de modulación en frecuencia y la técnica de fase diferencial de forma que en el emisor (15) se emplean dos osciladores (18, 18a) cuya fase se modula tomando valores 0 o π mediante la utilización de desfasadores (19). La señal eléctrica modulada en fase se aplica a un modulador electro-óptico (17, 17a) para realizar una modulación en frecuencia sobre una fuente óptica que emite pulsos con un fotón. La señal se recibe en un receptor (16) que mediante un modulador electro-óptico (22, 22a) al que se aplica una frecuencia con desfase 0, produce una interferencia entre dos frecuencias ópticas, que permite detectar en que frecuencia se recibe el fotón para obtener el bit enviado en función de la fase seleccionada por el emisor (16). El receptor envía al emisor la frecuencia en la se ha producido la detección, detectando dicho emisor el bit detectado por el receptor.

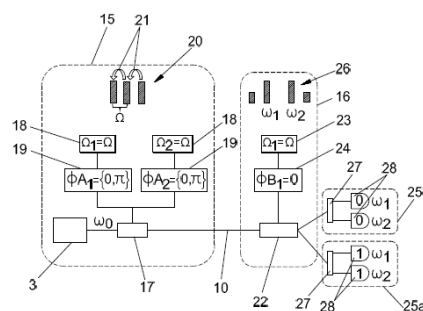


FIG. 2

DESCRIPCIÓN

Sistema de distribución de clave cuántica basado en modulación de frecuencia y fase diferencial

OBJETO DE LA INVENCION

5 La presente invención, tal y como se expresa en el enunciado de esta memoria descriptiva, se refiere a un sistema de distribución de clave cuántica que tiene por objeto distribuir la clave cuántica mediante una modulación en frecuencia y de fase diferencial para conseguir una mayor tasa de transmisión de la clave así como una mayor sencillez en el control del emisor y receptor.

10 En general, la invención es aplicable en los sistemas de comunicaciones cuánticas, y más concretamente en la distribución de claves cuánticas o criptografía cuántica para proporcionar medidas de seguridad adecuadas que garanticen la protección efectiva en las comunicaciones y los derechos de los usuarios, como por ejemplo sucede en muchos ámbitos como es el caso de aplicaciones bancarias, militares, aero-espaciales, firmas electrónicas y en transmisión de resultados electorales.

ANTECEDENTES DE LA INVENCION

15 En los sistemas de distribución de claves cuánticas es conocido el uso de dos tipos de algoritmos para cifrar la información de manera segura, que son los algoritmos de clave pública y los algoritmos de clave privada.

20 Dentro de los algoritmos de clave pública existen dos claves diferentes; una para cifrar la información, que es una clave pública; y otra para descifrarla que es una clave privada. La clave pública para cifrar la información es conocida por todos los usuarios, mientras que la clave privada para descifrarla solo es conocida por el destinatario del mensaje, de forma que éste es el único que puede descifrar la información. Este algoritmo se basa en la factorización de números primos para mantener la seguridad, lo cual resulta efectivo ya que los métodos que se requieren para atacar el sistema son poco eficientes, al resultar muy costoso para los computadores de hoy en día conseguir el mensaje, pues pueden tardar cientos de años.

25 Estos algoritmos de clave pública, aún siendo eficientes en el presente, presentan el problema de que no pueden asegurar que en un futuro se pueda encontrar un método más eficiente con el cual el atacante pueda reducir este tiempo. Así pues el algoritmo de clave pública no proporciona seguridad incondicional que implique que la información permanezca segura aún en el caso en el que se asuma un poder computacional infinito del atacante.

30 Respecto a los algoritmos de clave privada, la clave para cifrar el mensaje es la misma que para descifrarlo, por tanto, solo puede ser conocida por el emisor y el receptor. Estos algoritmos presentan seguridad incondicional siempre y cuando se use una sola vez la clave, es decir, no se puede usar la misma clave para mandar dos mensajes.

35 Estos algoritmos de clave privada presentan el problema de que se ha de garantizar la transmisión de una clave segura entre el emisor y el receptor para que puedan cifrar y descifrar el mensaje. Es aquí donde entran en juego los sistemas de distribución de clave, y más concretamente los sistemas de distribución de clave cuántica (QKD Quantum Key Distribution). Estos sistemas se basan en las leyes de la física cuántica para asegurar que la clave se transmite de manera segura entre el emisor y el receptor de tal manera que si un espía trata de adquirir información de esta clave producirá errores en la transmisión que el emisor y el receptor podrán detectar y de esta forma notar la presencia de un ataque. Ello es debido a que una clave cuántica, cuando se trata de leer cambia su estado.

40 La primera propuesta de un sistema QKD fue efectuada en 1984 por Charle Bennet y Gilles Brassard, que se basaba en un protocolo conocido como BB84 que ellos mismos inventaron. Esta técnica propone codificar los ceros y unos de las claves en el estado de polarización de fotones individuales. Gracias a las leyes de la física cuántica dichos bits no pueden ser interceptados, ya que si un espía los midiera, su estado cambiaría inmediatamente debido a que un sistema cuántico no puede ser medido sin perturbar el sistema en sí, tal y como ya fue comentado anteriormente.

45 En este protocolo, se lleva a cabo una etapa conocida con el nombre de reconciliación de bases, donde la mitad de los bits de la clave son descartados y resulta ser un paso fundamental para mantener la seguridad.

Posteriormente se han desarrollado varios sistemas de distribución de clave cuántica que desarrollan el protocolo BB84. Las tecnologías fotónicas han demostrado ser un medio adecuado para la implementación de sistemas QKD para la distribución de claves entre usuarios a varios cientos de kilómetros. Los sistemas propuestos para llevar a cabo el protocolo BB84 se puede agrupar en tres tipos:

- 50 a) El primero fue propuesto en 1992 por Bennet y sus colaboradores, que utilizaban la polarización de los fotones en un sistema QKD para transmitir la clave. Este sistema se enfrenta al problema de conservar la polarización de los estados a través del enlace de fibra óptica.
- b) El segundo tipo fue propuesto por Townsend y colaboradores en 1993, que se basa en el uso de retardos en los

fotones enviados y su análisis mediante el uso de interferómetros de fibra balanceados. El principal problema para trabajar con estos sistemas consiste en conseguir que los interferómetros de fibra no se desajusten debido a factores mecánicos y ambientales.

- 5 c) El tercer tipo fue propuesto en 1999 por J.M. Merolla y colaboradores; en el que se codifica la información en las bandas laterales que aparecen en una señal de luz modulada por una onda de radiofrecuencia. Estos sistemas se conocen como FC-QKD debido a su codificación en frecuencia (FC).

10 En cualquiera de los tres casos existe el problema de que la tasa de transferencia de bits es muy baja. Además la clave es codificada en estados cuánticos de forma que, para preservar la seguridad del sistema, solo un fotón puede llevar la información de cada bit. Debido a la dificultad de crear fuentes con un solo fotón se debe recurrir a fuentes semiclásicas donde la energía se reduce a niveles tales que se da la circunstancia de que la probabilidad de que un pulso lleve solo un fotón descienda al 10%. En consecuencia, aproximadamente el 90% de los pulsos enviados están vacíos de información. Si a este hecho se le añade la necesidad de utilizar en el destino un protocolo de destilación de clave la tasa de transferencia del bit se reduce aún más. Para incrementar esta tasa de bits se recurre a técnicas usadas en telecomunicaciones como la multiplexación de subportadora.

15 En el año 2002 se propone un nuevo protocolo basado en una técnica de uso común en sistemas de comunicaciones ópticas coherentes para QKD que consiste en la modulación de fase diferencial (DPS- Differential Phase Shift). Este protocolo, a diferencia del protocolo BB84, no necesita una etapa de reconciliación de bases, resultando más eficiente ya que no se descartan la mitad de los bits además de la mayor sencillez en la etapa de recepción. La principal desventaja que presentan los sistemas que funcionan con este protocolo es precisamente
20 que necesitan un interferómetro óptico en el transmisor y receptor, el cual resulta muy complejo de mantener estable frente a fluctuaciones ambientales. Además la ampliación de su capacidad de transmisión, que puede conseguirse al aumentar el número de caminos ópticos de forma considerable, complica sustancialmente la operación del sistema. A raíz de este protocolo se han desarrollado algunas variantes como el protocolo DQPS (diferencia de fase en cuadratura) cuya finalidad es proporcionar una mayor seguridad al sistema frente a ataques secuenciales.

25 Un ejemplo de un sistema QKD con DPS se describe en la Patente US 2010 0034390, cuyo contenido se describe en mayor detalle en el apartado de formas de realización preferidas de la invención, para facilitar la comprensión de la invención.

30 No existe un sistema que use el protocolo DPSK (DPS Keying) en combinación con modulación en frecuencia. La invención propone un nuevo sistema que realiza la distribución de clave cuántica basándose en la combinación de la técnica de modulación en frecuencia y la técnica de fase diferencial, lo que evita el uso de interferómetros ópticos en el dominio del tiempo en el transmisor y receptor.

DESCRIPCIÓN DE LA INVENCION

35 Para conseguir los objetivos y resolver los inconvenientes anteriormente indicados, la invención ha desarrollado un nuevo sistema de distribución de clave cuántica que emplea modulación de fase diferencial y modulación en frecuencia.

Para ello el sistema de la invención comprende un emisor que incluye una fuente de fotones pulsada con una frecuencia óptica ω_0 y una determinada tasa de repetición para modularla con una clave digital que envía a un receptor.

40 La invención se caracteriza por que el emisor además comprende dos osciladores de radiofrecuencia de diferentes frecuencias Ω_1 y Ω_2 y misma amplitud, cada uno de los cuales está conectado a un desfasador de radiofrecuencia Φ_{A1} y Φ_{A2} que pueden tomar los valores de desfase 0 y π para modular la fase de dichos osciladores. Además los dos desfasadores están conectados a un modulador electro-óptico, que a su vez está conectado a la fuente óptica de fotones, para realizar una modulación en frecuencia de la señal óptica, generando una portadora ω_0 y las bandas laterales $\omega_0 \pm \Omega_1$ y $\omega_0 \pm \Omega_2$, las cuales estarán desfasadas con un valor Φ_{A1} (0, π) y Φ_{A2} (0, π) respectivamente, de
45 forma que los desfases introducidos por Φ_{A1} y Φ_{A2} determinan la codificación digital de la clave que ha de detectarse en el receptor. El modulador electro-óptico envía la señal modulada al receptor por un canal de fibra óptica, a través del cual se recibe en el receptor.

Además, el emisor comprende medios convencionales de obtención de un bit detectado por el receptor, correspondiente a la clave enviada, a partir de la frecuencia óptica en la que el receptor ha detectado el fotón (según será explicado más adelante) y a partir del desfase de las frecuencias que fueron enviadas por el emisor. Para ello la frecuencia óptica en la que el receptor ha detectado el fotón se envía al emisor desde el receptor a través de un canal autenticado, como puede ser un canal público.

Además, el receptor del sistema de la invención, comprende al menos un oscilador de radiofrecuencia Ω_1 , que está conectado a un desfasador Φ_{B1} para establecer una fase inicial de valor 0 de la radiofrecuencia Ω_1 . El desfasador Φ_{B1} está conectado a un modulador electro-óptico que recibe las señales enviadas por el emisor y las modula mediante la frecuencia Ω_1 . Mediante la modulación descrita del receptor se produce una interferencia entre las

frecuencias ópticas consecutivas recibidas, generando distintas bandas laterales correspondientes a las frecuencias ópticas interferentes en función de las fases, que el emisor aplique a dichas señales interferentes. El modulador electro-óptico del receptor está dotado de dos salidas, y está configurado para enviar las frecuencias generadas en la interferencia cuyas fases son coincidentes a una de las salidas; y para enviar las frecuencias generadas en la interferencia cuyas fases no sean coincidentes a la otra salida.

Una de las salidas del modulador electro-óptico está conectada a un primer detector al que se envían las frecuencias generadas en la interferencia cuyas fases son coincidentes. El detector comprende un filtro óptico con dos ventanas de frecuencia correspondiente a cada una de las frecuencias que se pueden producir en la interferencia, y por tanto en las que se puede detectar un fotón. Cada una de dichas ventanas están conectadas a un contador de detección de fotones que permite discernir la frecuencia en la que se ha detectado un fotón: cuando un contador de fotones realiza una cuenta de un fotón, dicho contador indica a qué frecuencia se ha detectado el fotón correspondiente a la ventana a que está conectado. Por consiguiente, esta configuración permite distinguir en qué frecuencia se ha producido la detección de entre las frecuencias cuyas fases son coincidentes. Dicha detección se hace corresponder con un bit de la clave enviada. En dos realizaciones de la invención en las que el modulador electro-óptico del emisor y receptor, están constituidos por un modulador de banda lateral única, según se describe más adelante, la detección se hace corresponder con un "0"; es decir cuando se efectúa una detección entre las frecuencias cuyas fases son coincidentes se detecta un "0" correspondiente a la clave enviada y además el receptor sabe en qué frecuencia se ha realizado la detección. Obviamente la anterior detección también podría hacerse corresponder con un "1".

La otra salida del modulador se encuentra conectada a un segundo detector al que se envían las frecuencias generadas en la interferencia cuyas fases no son coincidentes, y que comprende un filtro óptico con una ventana de frecuencia correspondiente a cada una de las frecuencias de la interferencia en las que se puede detectar un fotón. En este caso, igualmente cada una de dichas ventanas se encuentra conectada a un contador de fotones de detección de la frecuencia en la que se ha detectado un fotón. Esta configuración permite distinguir la frecuencia en la que se ha producido la detección; que de acuerdo con las realizaciones de la invención en las que el modulador es de banda lateral única, se hace corresponder dicha detección con un "1". Es decir las frecuencias cuyas fases son coincidentes se van a corresponder a un "0" y las frecuencias cuyas fases no se corresponden se van a hacer corresponder con un "1", de acuerdo con las dos realizaciones de la invención en las que el modulador de banda lateral única.

En coherencia con lo anteriormente expuesto, respecto al emisor, el receptor también está dotado de medios para permitir enviar a dicho emisor, por un canal autenticado, la frecuencia óptica de interferencia en la que se ha producido la detección que se ha hecho corresponder a un bit, a partir de la cual el emisor obtiene el bit detectado por el receptor de forma convencional, tal y como se explica en el apartado de descripción de las formas de realización preferidas.

Hasta este punto se ha descrito la configuración básica de la invención, la cual puede adoptar tres configuraciones diferentes según el tipo del modulador electro-óptico empleado en el emisor y receptor. Las dos primeras realizaciones el modulador es un modulador de banda lateral única, según a continuación se describe.

Así, en una realización de la invención el modulador electro-óptico del emisor y receptor está constituido por un modulador de banda lateral única con un nivel de portadora óptica equivalente al de las bandas laterales generadas. En este caso uno de los osciladores de radiofrecuencia del emisor es de una frecuencia de oscilación de valor $\Omega_1 = \Omega$ y el otro oscilador es de una frecuencia el doble al anterior $\Omega_2 = 2\Omega$. En este caso el oscilador del receptor es de una frecuencia de valor igual a $\Omega_1 = \Omega$.

En otra realización de la invención el modulador electro-óptico del emisor y del receptor están constituidos por un modulador de banda lateral única con un nivel de portadora óptica superior al de las bandas laterales generadas. En este caso el receptor comprende dos osciladores de radiofrecuencia, de frecuencia igual a la de cada uno de los osciladores del emisor respectivamente (Ω_1 y Ω_2). Cada uno de dichos osciladores del receptor está conectado a un desfasador Φ_{B1} y Φ_{B2} para establecer una fase inicial del receptor igual a 0, y que están conectados al modulador electro-óptico del receptor para efectuar la modulación comentada.

En la última realización de la invención el modulador electro-óptico del emisor y receptor está constituido por un modulador de doble banda lateral. En este caso el receptor comprende dos osciladores de radiofrecuencia de frecuencia igual a la de los osciladores del emisor (Ω_1 y Ω_2), cada uno de los cuales está conectado a un desfasador Φ_{B1} y Φ_{B2} para establecer una fase inicial del receptor igual a 0, y que están conectados al modulador del receptor para efectuar la modulación comentada. En este caso los contadores se hacen corresponder con un "0" o un "1" dependiendo de la banda en la que se ha producido la detección. Así por ejemplo siendo las fases iguales si se detecta en la banda superior, se hace corresponder con un "0" y si detecta en la banda inferior se hace corresponder con un "1", y para el caso en que las fases no coincidan si se detecta en la banda inferior se hace corresponder con un "0" y si se detecta en la banda superior se hace corresponder con un "1".

En cualquiera de las realizaciones descritas de la invención no se requiere el uso de un desfasador óptico en el transmisor para producir las diferentes fases entre pulsos, tal y como se requiere en los moduladores DPSK

convencionales, cuya configuración se describe más adelante para facilitar la comprensión de la invención.

La invención tampoco requiere el empleo de un interferómetro en el receptor para poder detectar la clave cuántica, que a diferencia del estado de la técnica, la invención utiliza un modulador electro-óptico en el emisor el receptor, y no un interferómetro. Ello redundará en una mayor estabilidad del dispositivo en condiciones ambientales de uso real, soportando de mejor forma la fluctuación de temperatura, los cambios de polarización o las vibraciones que se puedan producir en el entorno en el que se encuentra instalado el sistema.

Además, la invención al utilizar la modulación DPSK adquiere las ventajas que ésta presenta, que consisten en una mayor eficiencia en la tasa de transmisión y mayor seguridad frente a los sistemas FC-QKD.

Por otro lado, al utilizar la invención la modulación en frecuencia modulada juntamente con el protocolo DPSK, consigue mayor estabilidad frente a los sistemas DPS, así como la posibilidad de incorporar fácilmente las técnicas de multiplexación de subportadora. También permite su aplicación en el protocolo DQPS (diferencia de fase en cuadratura) para aumentar aún más la seguridad en enlaces ópticos de mayor alcance.

La invención sustituye los caminos ópticos por subportadoras eléctricas a través de moduladores en cascada cuya diferencia efectiva es más robusta que una implementación real. De esta forma, es posible introducir un número elevado de osciladores de radiofrecuencia que permiten aumentar la seguridad y la eficiencia de transmisión de forma más sencilla.

Además la invención disminuye radicalmente el grado de complejidad del receptor en comparación con los sistemas FC-QKD, ya que la aleatoriedad se introduce de forma pasiva a través de codificación en frecuencia. Esto hace que la capacidad de extender esta tecnología a varios usuarios sea más competitiva al disminuir la complejidad del receptor lo que implica una reducción en el coste y su posterior mantenimiento.

La invención, al poderse adaptar a las técnicas conocidas de multiplexación cuántica de subportadora, permite aumentar la tasa de transmisión proporcionalmente al número de subportadoras que se utilicen.

A continuación para facilitar una mejor comprensión de esta memoria descriptiva, y formando parte integrante de la misma, se acompañan una serie de figuras en las que con carácter ilustrativo y no limitativo se ha representado el objeto de la invención.

BREVE ENUNCIADO DE LAS FIGURAS

Figura 1.- Muestra una vista esquemática de un ejemplo de realización del estado de la técnica en el que se realiza modulación DPS.

Figura 2.- Muestra un primer ejemplo de realización de la invención en el que el modulador electro-óptico está constituido por un modulador de banda lateral única con un nivel de portadora óptica igual al de las bandas laterales generadas.

Figura 3.- Muestra una segunda realización de la invención en la que el modulador electro-óptico se encuentra constituido por un modulador de banda lateral única pero en este caso con un nivel de portadora óptica superior al de las bandas laterales generadas.

Figura 4.- Muestra otra realización de la invención en la que el modulador electro-óptico está constituido por un modulador de doble banda lateral.

DESCRIPCIÓN DE LAS FORMAS DE REALIZACIÓN PREFERIDAS

A continuación se realiza una descripción de la invención basada en las figuras anteriormente comentadas.

En primer lugar y con ayuda de la figura 1 se describe un ejemplo de realización convencional en el que se utiliza modulación DPS. En este ejemplo, se prevé un transmisor 1 que comprende una fuente óptica 2 que proporciona fotones individuales con una tasa de repetición determinada. Además el emisor 1 está dotado de unos divisores de potencia 3 que forman una estructura interferométrica y que dividen el fotón por tres caminos diferentes a los que aplica un retardo, de forma que el retardo entre caminos consecutivos son iguales a T y el coeficiente de acoplo para cada camino es igual para garantizar la misma probabilidad en los tres caminos.

Los tres caminos se recombinan mediante interferómetros ópticos 4, cada uno de los cuales constituido por dos acopladores o divisores, de forma que el fotón recombinado en el último interferómetro 4 presenta en su salida 6 las señales 5 representadas en la figura 1. Las flechas 7 indican los tiempos en los que se pueden producir las interferencias en el receptor, según será descrito posteriormente.

Las señales 5 se aplican a un modulador de fase (PM) 8 que modula el fotón recombinado, de forma que cada pulso tendrá una fase aleatoria entre dos posibles valores de fase 0 y π que se aplican mediante dicho modulador 8. En este punto, el fotón es enviado al receptor 9 a través de un canal de fibra óptica 10. Dependiendo del desfase que se aplique en el modulador 8 se realiza la codificación de cada bit de la clave que se envía al receptor 9.

El receptor 9 comprende en su entrada un divisor de potencia 11 mediante el que se divide el fotón incidente por medio de dos caminos con un retardo entre ellos de T . El fotón es de nuevo recombinado por medio de un interferómetro óptico 12 en el que se produce una interferencia en los tiempos T_1 o T_2 . Con la referencia 14 se muestra la distribución en el tiempo de las señales obtenidas en la salida del interferómetro 12, el cual está dotado de dos salidas, en cada una de las cuales se incorpora un detector 13 y 13a, de forma que el detector 13 se corresponde a la detección de un bit "0" y el detector 13a se corresponde a la detección de un bit "1". Como solo hay un fotón, la aleatoriedad del sistema descansa en la incertidumbre del tiempo de detección T_1 o T_2 . Dependiendo de la diferencia de fase seleccionada por el emisor 1, el fotón seguirá el camino superior hacia el detector 13 o el camino inferior hacia el detector 13a. Así cuando la diferencia en fase es 0 seguirá el camino superior y se detectará en el detector 13 el cual se corresponde a la detección de un bit "0", y en caso que la diferencia de fase sea π seguirá el camino inferior, lo cual se corresponde con la detección de un bit "1".

Los detectores 13 y 13a, además detectan en que tiempo T_1 o T_2 se ha producido la interferencia, de forma que el receptor 9 envía por un canal autenticado, el tiempo T_1 o T_2 en el que se ha producido la detección.

Con esta información el emisor, al conocer las fases con las que ha realizado la modulación de la señal que ha enviado al receptor 9, y al conocer el tiempo T_1 o T_2 en el que el receptor 9 ha realizado la detección, obtiene la misma cadena de bits, teniendo en cuenta que la diferencia de fase entre pulsos consecutivos igual a 0 corresponde al bit "0", y la diferencia de fase π corresponde a un bit "1".

La seguridad de este sistema reside en el hecho de que el emisor 1 y receptor 9 en ningún momento intercambian el valor del bit detectado y tampoco el valor de las fases del otro tiempo no detectado, que necesita un posible espía para una clonación perfecta del estado cuántico asociado al bit enviado.

El estado de la técnica descrito constituye la base para poder entender la invención, la cual prevé tres posibles realizaciones distintas.

La primera realización de la invención se describe con ayuda de la figura 2, en la que el emisor 15 y el receptor 16 presentan una configuración que difiere sustancialmente respecto de la descrita en el estado de la técnica.

La invención también emplea una fuente de fotones individuales 3 con una frecuencia óptica ω_0 , pero en este caso la fuente 3 está conectada a un modulador electro-óptico 17 para realizar una modulación en frecuencia del fotón proporcionado por la fuente 3. Además el emisor 15 comprende dos osciladores de radiofrecuencia 18, de frecuencias Ω y 2Ω con la misma amplitud, cada uno de los cuales se encuentra conectado a un desfaseador de radiofrecuencia 19 con un valor Φ_{A1} y Φ_{A2} que pueden tomar los valores 0 y π , de forma que la fase de los osciladores 18 se modula mediante dichos desfaseadores de radiofrecuencia 19, y esta señal modulada se aplica al modulador electro-óptico 17 que realiza una modulación en frecuencia del fotón, que tiene la misma probabilidad a la salida de encontrarse en una de las siguientes frecuencias ópticas: ω_0 , $\omega_0 + \Omega$ y $\omega_0 + 2\Omega$. Para ello el modulador electro-óptico 17 está constituido por un modulador de banda lateral única. Además cada una de las frecuencias ópticas se desfasea con respecto a la frecuencia ω_0 un valor Φ_{A1} y Φ_{A2} que pueden tomar los valores 0 o π .

La referencia 20 representa las tres frecuencias ópticas en las que el fotón puede estar localizado y las flechas 21 indican entre que pulsos se va a producir la interferencia en el receptor 16.

En este caso cada bit de la clave cuántica es función del desfase que se aplique mediante los desfaseadores de radiofrecuencia 19.

La modulación en frecuencia se envía al receptor 16 a través de la fibra óptica 10, de forma que dicho receptor 16 comprende un modulador electro-óptico 22 de banda lateral única que está conectado a un oscilador 23 de frecuencia Ω a través de un desfaseador 24 que introduce una fase inicial de valor 0, es decir $\Phi_{B1} = 0$. Mediante esta configuración a la salida del modulador electro-óptico 22 interfieren las frecuencias ópticas consecutivas recibidas, y genera distintas bandas laterales correspondientes a las frecuencias ópticas en las que se produce la interferencia ω_1 o ω_2 en función de las fases de las señales interferentes. Como solo hay un fotón la aleatoriedad del sistema descansa en la incertidumbre de la frecuencia de detección ω_1 o ω_2 , que en este caso se corresponde con las frecuencias ópticas $\omega_1 = \omega_0$ o $\omega_2 = \omega_0 + \Omega$, ya que el modulador electro-óptico 22 lo que hace es desplazar las frecuencias consecutivas recibidas un valor de frecuencia Ω correspondiente a la frecuencia proporcionada por el oscilador 23.

El modulador electro-óptico 22 es un modulador convencional de banda lateral única que comprende dos salidas, de forma que en su salida superior envía las frecuencias generadas en la interferencia cuyas fases son coincidentes, en tanto que a la salida inferior envía las frecuencias generadas en la interferencia cuyas fases no son coincidentes.

La salida superior del modulador electro-óptico 22 está conectada a un primer detector 25, y su salida inferior a un segundo detector 25a.

Las señales que se obtienen en las salidas del modulador electro-óptico 22 se representan con la referencia 26.

El primer detector 25 se hace corresponder a la detección de un bit "0", que de acuerdo con lo anteriormente

descrito, se detecta en las frecuencias ω_1 o ω_2 cuando las fases son coincidentes. El segundo detector 25a se corresponde con una detección de un bit "1" que se detecta en las frecuencias ω_1 o ω_2 cuando las fases son diferentes. Para ello tanto el primer detector 25 como el segundo detector 25a comprenden un filtro óptico 27 cada uno de ellos dotado de dos ventanas de frecuencia correspondientes a cada una de las frecuencias de interferencia ω_1 y ω_2 en las que se puede detectar un fotón, de forma que cada una de dichas ventanas está conectada a un contador de fotones 28 que detecta la frecuencia ω_1 o ω_2 en la que se ha producido la detección del "0" o del "1".

De esta forma el receptor obtiene el bit de la clave enviada y, a su vez, envía al emisor 15 la frecuencia ω_1 o ω_2 en la que realizó la detección mediante un canal autenticado.

El emisor 15 está dotado de medios convencionales de obtención del bit detectado por el receptor, a partir de la frecuencia óptica que ha recibido ω_1 o ω_2 , ya que el emisor 15 conoce el desfase de las frecuencias que fueron enviadas, y por tanto puede saber que desfase 0 o π ha detectado el receptor mediante el modulador electro-óptico 22, lo que le permite obtener la misma cadena de bits que envió, teniendo en cuenta que la diferencia de fase entre frecuencias ópticas consecutivas igual a 0 corresponde al bit "0" y la diferencia de fase π corresponde al bit "1". Estos medios no se describen en mayor detalle por ser convencionales y no ser el objeto de la invención.

Con ayuda de la figura 3 se describe una segunda realización de la invención en la que el emisor 15 presenta una configuración similar a la descrita para el ejemplo anterior, pero en este caso los osciladores de radiofrecuencia 18a tienen frecuencias Ω_1 y Ω_2 con la misma amplitud. En este caso el modulador electro-óptico 17 es un modulador de banda lateral única en cuya salida tendrá las frecuencias ω_0 , $\omega_0 + \Omega_1$ y $\omega_0 + \Omega_2$, cuyas frecuencias ópticas en las que el fotón puede estar localizado se han representado con la referencia 20a y las flechas 21a indican entre que pulsos se va a producir la interferencia en el receptor 16.

En este caso, el fotón tendrá la misma probabilidad de encontrarse en las frecuencias $\omega_0 + \Omega_1$ y $\omega_0 + \Omega_2$ a la salida del modulador electro-óptico 17.

Estas señales se envían al receptor 16 mediante una fibra óptica 10, y se reciben en un modulador electro-óptico 22, pero que en este caso está alimentado por dos osciladores de radiofrecuencia 23a, con frecuencias Ω_1 y Ω_2 correspondientes a las frecuencias de los osciladores 18a, estando cada uno de dichos osciladores de radiofrecuencia 23a conectados al modulador electro-óptico 22 a través de sendos desfasadores 24a que proporcionan un desfase 0, al igual que en el caso anterior.

En esta realización la modulación realizada por el modulador electro-óptico 22 produce interferencias entre las frecuencias ópticas ω_0 , $\omega_0 + \Omega_1$ y $\omega_0 + \Omega_2$ recibidas a la entrada y las frecuencias ópticas generadas a partir de la portadora óptica ω_0 , es decir se producen las interferencias de interés en las frecuencias $\omega_1 = \omega_0 + \Omega_1$ o $\omega_2 = \omega_0 + \Omega_2$, lo cual está representado mediante la referencia 26a.

La detección del bit se realiza de forma equivalente a como fue descrito para el caso anterior, de forma que el receptor 16 envía la frecuencia ω_1 o ω_2 en la que ha realizado la detección del bit correspondiente, así el emisor conoce el bit recibido por el receptor según fue explicado en el caso anterior.

En la figura 4 se muestra una tercera realización de la invención en la que el emisor 15 presenta la particularidad de que el modulador electro-óptico es un modulador electro-óptico de doble banda lateral 17a, de forma que en su salida se obtiene la señal 20b y las posibles interferencias que pueden producirse en el receptor se representan mediante las flechas 21b.

En esta realización el modulador electro-óptico 22a del receptor 16 es un modulador de doble banda lateral en el que se producen las interferencias a frecuencias ópticas $\omega_1 = \omega_0 \pm \Omega_1$ y $\omega_2 = \omega_0 \pm \Omega_2$. Con la referencia 26b se muestra la salida superior del modulador electro-óptico 17a y con la referencia 26c la señal presente en la salida inferior. En este caso la aleatoriedad del sistema descansa en la incertidumbre de si la frecuencia óptica se produce en las bandas asociadas a la primera frecuencia eléctrica ω_1 o a la segunda ω_2 . Posteriormente, la diferencia de fase seleccionada por el transmisor determina si la interferencia se produce en la banda inferior $\omega_0 - \Omega_1$; $\omega_0 - \Omega_2$ o superior $\omega_0 + \Omega_1$; $\omega_0 + \Omega_2$, permitiendo de esta forma decodificar el bit. Por tanto, a diferencia de los dos esquemas anteriores, en esta configuración la codificación en fase se traduce en una codificación en frecuencia. En este caso cada filtro 27a discrimina entre la banda superior y la inferior.

En esta realización, si el fotón sigue el camino superior, se obtendrá un bit "0" cuando la detección del fotón se efectúe en las frecuencias ópticas de la banda superior, mientras que obtendrá un bit "1" cuando la detección del fotón se efectúe en la banda inferior. Si el fotón sigue el camino inferior se obtiene el caso complementario, debido a la diferencia de fase entre las dos salidas del modulador electro-óptico. Por tanto cuando el fotón sigue el camino inferior se detectará un bit "0" cuando el fotón se detecte en la banda inferior $\omega_0 - \Omega_1$ o $\omega_0 - \Omega_2$, y se detectará un bit "1" cuando se detecte en la banda superior $\omega_0 + \Omega_1$ o $\omega_0 + \Omega_2$. Debido a la complementariedad, la salida superior e inferior se unen para su conexión con los contadores 28 de acuerdo con las diferentes frecuencias de cada camino, según se ha explicado y tal y como se muestra en la figura 4.

REIVINDICACIONES

1.- SISTEMA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA BASADO EN MODULACIÓN DE FRECUENCIA Y FASE DIFERENCIAL, que comprende un emisor que incluye una fuente de fotones (3) pulsada con una frecuencia óptica ω_0 y una determinada tasa de repetición para modularla con una clave digital que envía un receptor; caracterizado por que el emisor (15) además comprende:

- dos osciladores de radiofrecuencia (18, 18a) de diferentes frecuencias Ω_1 y Ω_2 y misma amplitud;
- dos desfasadores de radiofrecuencia (19) Φ_{A1} y Φ_{A2} que pueden tomar valores de desfase seleccionados entre 0 y π y cada uno de los cuales está conectado a uno de dichos osciladores de radiofrecuencia para modular su fase; estando los desfasadores de radiofrecuencia (19) conectados a
- un modulador electro-óptico (17, 17a) que a su vez está conectado a la fuente óptica de fotones (3), para realizar una modulación en frecuencia de la señal óptica, generando una portadora ω_0 y bandas laterales $\omega_0 \pm \Omega_1$ y $\omega_0 \pm \Omega_2$ que están desfasadas con un valor Φ_{A1} (0, π) y Φ_{A2} (0, π) respectivamente, cuyos desfases determinan la codificación digital de la clave, enviando la señal modulada al receptor (16) por un canal de fibra óptica (10);
- medios convencionales de obtención de un bit, detectado por el receptor (16) correspondiente a la clave enviada, a partir de la frecuencia óptica en la que el receptor (16) ha detectado el fotón, y a partir del desfase de las frecuencias que fueron enviadas por el emisor (15); donde dicha frecuencia óptica se envía al emisor (15) desde el receptor (16) a través de un canal autenticado;

comprendiendo dicho receptor:

- al menos un oscilador de radiofrecuencia (23, 23a) Ω_1 que está conectado a
- un desfasador (24) Φ_{A1} para establecer una fase inicial de valor 0 del al menos oscilador de radiofrecuencia Ω_1 , que está conectado a
- un modulador electro-óptico (22, 22a) de recepción de las señales enviadas por el emisor (15) que las modula a la frecuencia Ω_1 , produciendo una interferencia entre dos frecuencias ópticas consecutivas recibidas, y genera distintas bandas laterales correspondientes a las frecuencias ópticas interferentes en función de las fases de dichas señales interferentes; comprendiendo el modulador dos salidas, y estando configurado para enviar las frecuencias generadas en la interferencia cuyas fases detectadas son coincidentes a una de las salidas; y para enviar las frecuencias generadas en la interferencia cuyas fases no son coincidentes a la otra salida; y estando la salida del modulador electro-óptico a la que se envían las frecuencias generadas en la interferencia cuyas fases detectadas son coincidentes conectada a
- un primer detector (25) de las frecuencias generadas en la interferencia cuyas fases detectadas son coincidentes y que comprende un filtro óptico (27) con al menos dos ventanas de frecuencia, correspondientes a cada una de las frecuencias de la interferencia en las que se puede detectar un fotón; donde cada ventana de frecuencia está conectada a un contador de fotones (28) de detección de la frecuencia en la que se ha detectado un fotón, para distinción de dicha frecuencia en la que se ha producido la detección; correspondiéndose dicha detección con la detección de un bit seleccionado entre un "0" y un "1";
- y estando la salida del modulador electro-óptico a la que se envían las frecuencias generadas en la interferencia cuyas fases detectadas no son coincidentes conectada a
- a un segundo detector (25a) de las frecuencias generadas en la interferencia cuyas fases no son coincidentes, y que comprende un filtro óptico (27) con al menos dos ventanas de frecuencia correspondientes a cada una de las frecuencias de la interferencia en las que se puede detectar un fotón; estando cada una de dichas ventanas conectadas a un contador de fotones (28) de detección de la frecuencia en la que se ha detectado un fotón, para distinción de dicha frecuencia en la que se ha producido la detección; correspondiéndose dicha detección con la detección de un bit seleccionado entre un "0" y un "1"
- medios para enviar al emisor por un canal autenticado la frecuencia óptica de interferencia en la que se ha producido la detección de un bit.

2.- SISTEMA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA BASADO EN MODULACIÓN DE FRECUENCIA Y FASE DIFERENCIAL, según reivindicación 1, caracterizado por que el modulador electro-óptico del emisor y receptor es un modulador de banda lateral única con un nivel de portadora óptica equivalente al de las bandas laterales generadas.

3.- SISTEMA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA BASADO EN MODULACIÓN DE FRECUENCIA Y FASE DIFERENCIAL, según reivindicaciones 1 y 2, caracterizado por que uno de los osciladores de radiofrecuencia del emisor es de una frecuencia de oscilación de valor $\Omega_1 = \Omega$ y el otro oscilador es de una frecuencia el doble $\Omega_2 = 2\Omega$;

en tanto que el oscilador del receptor es de una frecuencia de valor igual a la frecuencia Ω_1 .

4.- SISTEMA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA BASADO EN MODULACIÓN DE FRECUENCIA Y FASE DIFERENCIAL, según reivindicación 1, caracterizado por que el modulador electro-óptico del emisor y del receptor es un modulador de banda lateral única con un nivel de portadora óptica superior al de las bandas laterales generadas.

5.- SISTEMA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA BASADO EN MODULACIÓN DE FRECUENCIA Y FASE DIFERENCIAL, según reivindicaciones 1 y 4, caracterizado por que el receptor comprende dos osciladores de radiofrecuencia (23a) de frecuencia igual a la de los osciladores (18a) del emisor respectivamente (Ω_1 y Ω_2); y cada uno de dichos osciladores (23a) del receptor está conectado a un desfasador (24a) Φ_{B1} y Φ_{B2} para establecer una fase inicial de receptor igual a 0; y que a su vez están conectados al modulador (22) del receptor.

6.- SISTEMA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA BASADO EN MODULACIÓN DE FRECUENCIA Y FASE DIFERENCIAL, según reivindicación 1, caracterizado por que el modulador electro-óptico del emisor y receptor es un modulador de doble banda lateral (22a); y el receptor (16) comprende dos osciladores de radiofrecuencia (23a) de frecuencia igual a la de los osciladores (18a) del emisor respectivamente, y cada uno de dichos osciladores (23a) del receptor (15) está conectado a un desfasador (24a) para establecer un desfase inicial de receptor igual a 0, y que están conectados al modulador (22a) del receptor (15).

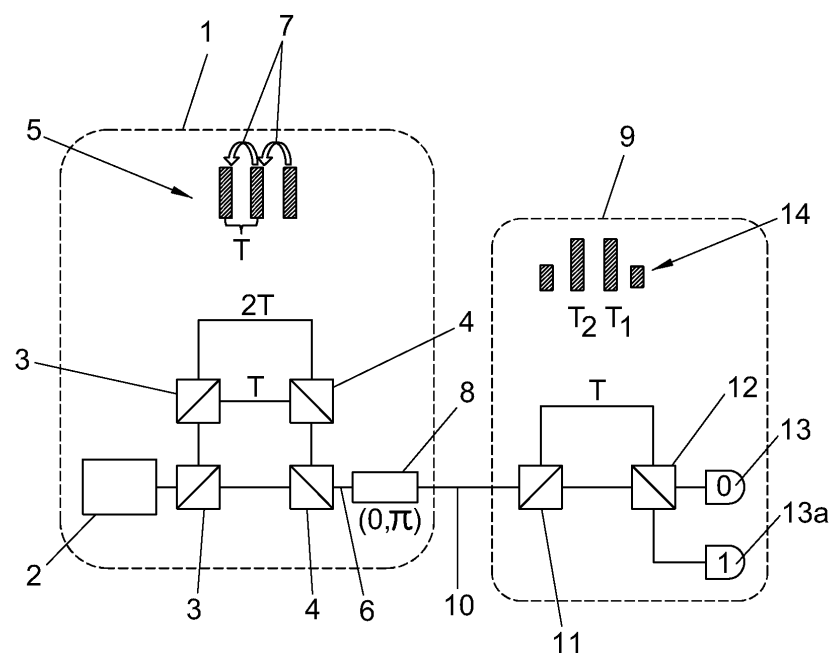


FIG. 1

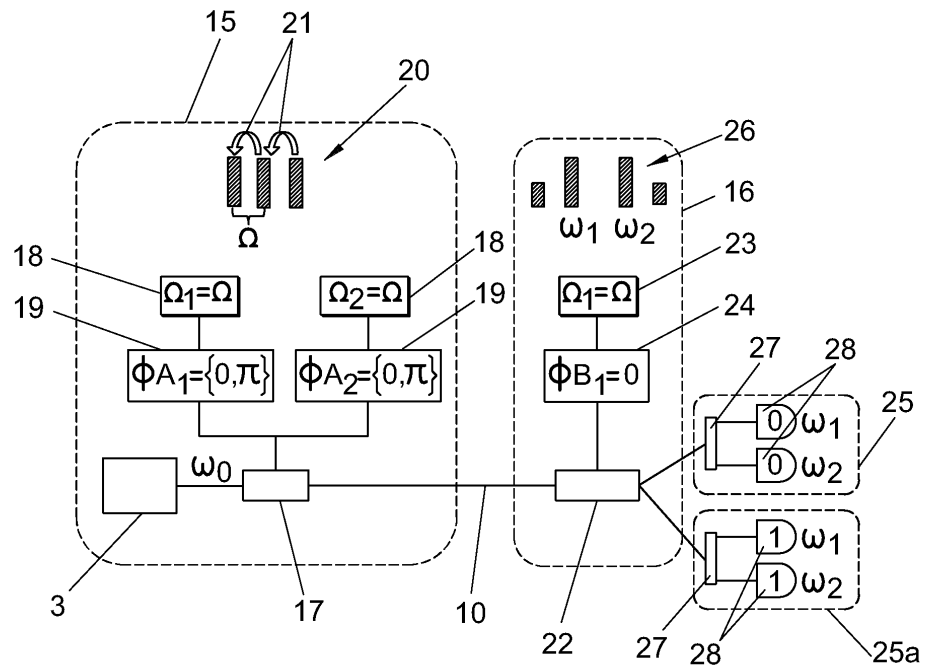


FIG. 2

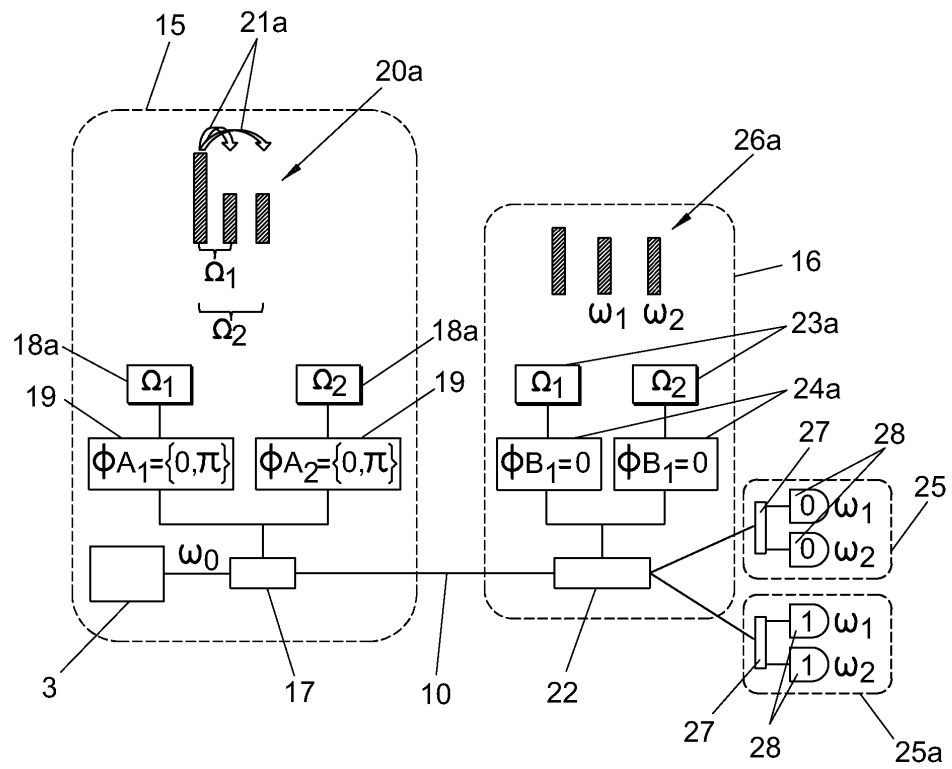


FIG. 3

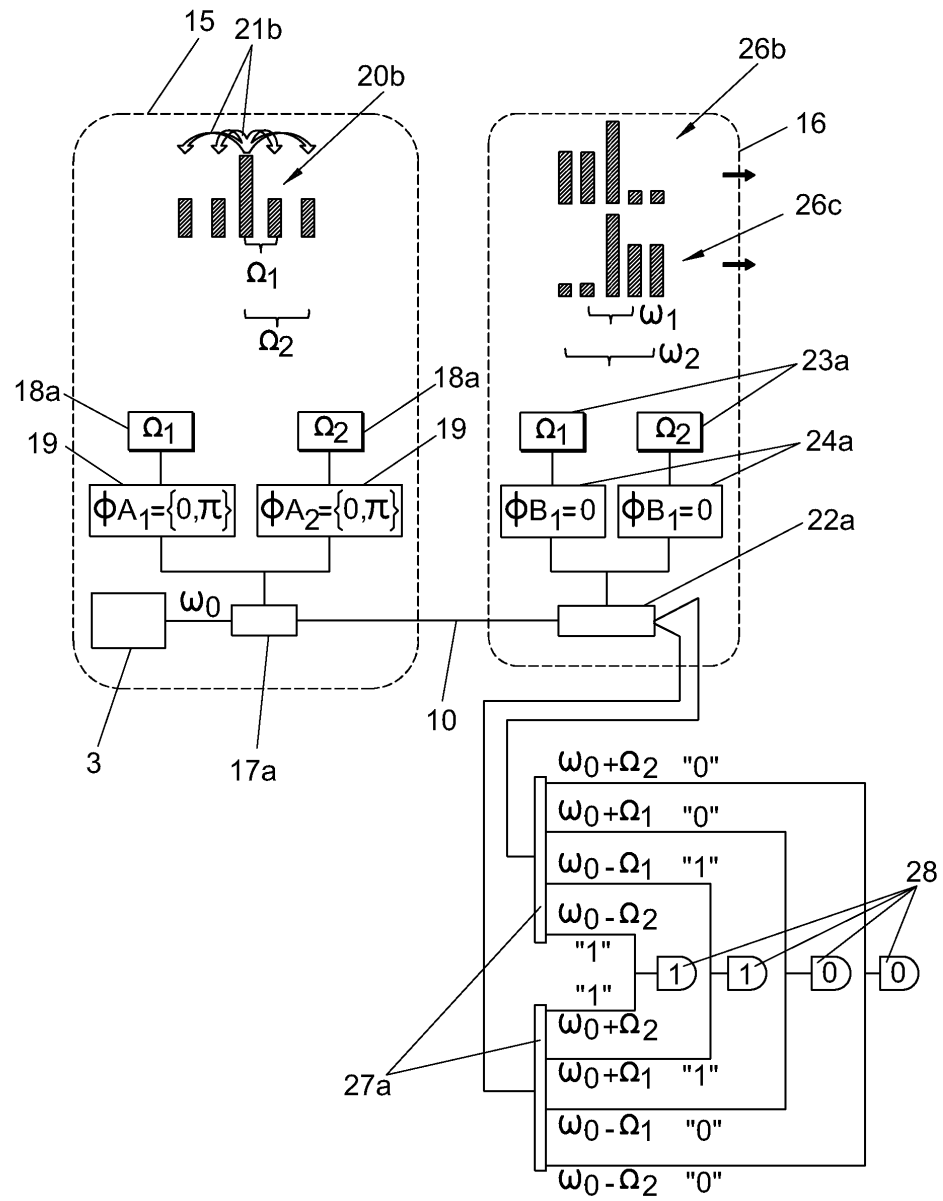


FIG. 4