(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 992 489**

(51) Int. Cl.:

***H04L 9/08*** (2006.01)
***H04B 10/70*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.07.2020 PCT/EP2020/070955**

(87) Fecha y número de publicación internacional: **28.01.2021 WO21013990**

(96) Fecha de presentación y número de la solicitud europea: **24.07.2020 E 20742765 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2024 EP 4005145**

(54) Título: **Procedimiento para proporcionar un marco de referencia común entre dos receptores**

(30) Prioridad:

**24.07.2019 EP 19188171**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**13.12.2024**

(73) Titular/es:

**ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN (100.0%)**
**Dr. Ignaz Seipel-Platz 2**
**1010 Wien, AT**

(72) Inventor/es:

**HANDSTEINER, JOHANNES;**
**SCHEIDL, THOMAS y**
**ZEILINGER, ANTON**

(74) Agente/Representante:

**PONTI & PARTNERS, S.L.P.**

## DESCRIPCIÓN

Procedimiento para proporcionar un marco de referencia común entre dos receptores

**[0001]** La invención se refiere a un procedimiento para alinear una fuente de fotones entrelazados y una fuente de fotones entrelazados que comprende dos receptores, útil para la distribución cuántica de claves. El primer receptor está conectado a través de un primer canal de transmisión a una fuente de fotones entrelazados, y el segundo receptor está conectado a través de un segundo canal de transmisión a la fuente de fotones entrelazados. La fuente de fotones entrelazados produce pares de fotones entrelazados, preferentemente entrelazados en la polarización o el intervalo de tiempo o el momento angular orbital o la trayectoria, donde el primer fotón de cada par de fotones entrelazados se envía a través del primer canal de transmisión al primer receptor y el segundo fotón de cada par de fotones entrelazados se envía a través del segundo canal de transmisión al segundo receptor.

**[0002]** La distribución cuántica de claves (DCC) es un procedimiento de comunicación seguro. Con DCC, se puede generar una clave para criptografía entre dos partes, en lo sucesivo denominado dos receptores (Alice y Bob). Esta clave se puede usar para cifrar y descifrar un mensaje. Para algunos procedimientos de DCC, como los propuestos por Bennett y Brassard en "Quantum cryptography: Public Key Distribution and coin-lossing.", en "Proceedings of IEEE International Conference a Computers, Systems and Signal Processing", Bangalore, India, 175-179 (1984), o por Bennet, Brassard y Mermin en "Quantum Cryptography without Bell's Theorem" en Phys. Rev. Lett. 68, 557,1992, se necesita una fuente de fotones entrelazados. Las fuentes de fotones entrelazados son bien conocidas, por ejemplo, como una fuente de BBO del documento US 6 424 665 B1 o como una configuración de fibra Sagnac del documento US 6 897 434 B1. Para generar la clave, ambos receptores tienen que asegurarse de que coinciden en las mismas bases de medición, es decir, los dos receptores deben establecer un marco de referencia de polarización común con la fuente de fotones entrelazados. Esto se realizaba antes mediante una alineación iterativa de dos bases de medición mutuamente imparciales entre la fuente y el primer receptor, y a continuación mediante una alineación iterativa de dos bases de medición mutuamente imparciales entre la fuente y el segundo receptor. Sin embargo, este procedimiento iterativo de alineación lleva mucho tiempo, pero la alineación es de crucial importancia para la generación de la clave.

**[0003]** En "Fully automated entanglement-base quantum cryptography system for telecom fiber networks" arXiv: 0901.2725v2 se propone un sistema de alineación automatizado. Alice envía fotones activador con polarización conocida a Bob para alinear el sistema con dos controladores de polarización.

**[0004]** Del documento GB 2 405 294 A se conoce una fuente de fotones entrelazados en el intervalo de tiempo con una fuente de fotones y dos módulos de detección. Cada módulo de detección comprende un interferómetro desequilibrado y dos detectores. Para tener franjas de interferencia casi perfectas y para reducir la tasa de error de bit cuántico del sistema, se proporcionan filtros de polarización antes de cada detector para eliminar cualquier componente ortogonal erróneo de la polarización.

**[0005]** Un objetivo de la presente invención es proporcionar un aparato y un procedimiento mejorado para establecer un marco de referencia común entre dos receptores.

**[0006]** El procedimiento para proporcionar un marco de referencia común entre dos receptores, preferentemente para la distribución cuántica de claves, se logra según la reivindicación 1.

**[0007]** El primer receptor está conectado a través de un primer canal de transmisión a una fuente de fotones entrelazados, y el segundo receptor está conectado a través de un segundo canal de transmisión a la fuente de fotones entrelazados. La fuente de fotones entrelazados produce pares de fotones entrelazados, preferentemente entrelazados en la polarización o el intervalo de tiempo o el momento angular orbital o la trayectoria, donde el primer fotón de cada par de fotones entrelazados se envía a través del primer canal de transmisión al primer receptor y el segundo fotón de cada par de fotones entrelazados se envía a través del segundo canal de transmisión al segundo receptor. El primer receptor comprende un primer y un segundo medio de medición para medir los fotones en dos bases de medición mutuamente imparciales, donde el segundo receptor comprende un tercer y un cuarto medio de medición para medir los fotones en dos bases de medición mutuamente imparciales. Cada medio de medición puede medir los fotones en al menos dos estados ortogonales. Los cuatro medios de medición pueden comunicar el tiempo de la detección de un fotón de los pares de fotones entrelazados para detectar coincidencias entre los dos receptores de un par de fotones entrelazados y para calcular la visibilidad y/o la tasa de error de bit cuántico (TBEC). Tres de los cuatro medios de medición comprenden cada uno un medio de corrección para establecer el marco de referencia común.

**[0008]** El procedimiento comprende las etapas de:

i) minimización de la TEBC o maximización de la visibilidad de los fotones detectados en los medios de medición primero (M1) y tercero (M3) mediante el ajuste del primer medio de corrección (C1) con el fin de establecer las mismas bases de medición entre el primer medio de medición (M1) y el tercer medio de medición (M3),

ii) maximización de la TEBC o minimización de la visibilidad de los fotones detectados en los medios de medición primero (M1) y cuarto (M4) mediante el ajuste del segundo medio de corrección (C2) con el fin de establecer bases de medición mutuamente imparciales entre el primer medio de medición (M1) y el cuarto medio de medición (M4),
iii) minimización de la TEBC o maximización de la visibilidad de los fotones detectados en los medios de medición cuarto (M4) y segundo (M2) mediante el ajuste del tercer medio de corrección (C3) con el fin de establecer las mismas bases de medición entre el cuarto medio de medición (M4) y el segundo medio de medición (M2).

**[0009]** En la etapa i), se establecen las mismas bases de medición entre el primer medio de medición (M1) y el tercer medio de medición (M3). En la etapa ii), se establecen las bases de medición mutuamente imparciales entre el primer medio de medición (M1) y el cuarto medio de medición (M4) y, debido a eso y a la etapa i), se establecen las bases de medición mutuamente imparciales entre el tercer medio de medición (M3) y el cuarto medio de medición (M4). En la etapa iii), se establecen las mismas bases de medición entre el cuarto medio de medición (M4) y el segundo medio de medición (M2) y, debido a eso y a la etapa i) y a la etapa ii), se establecen las bases de medición mutuamente imparciales entre el primer medio de medición (M1) y el segundo medio de medición (M2).

**[0010]** Las etapas i), ii) y iii) se pueden realizar en paralelo o en secuencia.

**[0011]** Las etapas i), ii) y iii) se pueden realizar en cualquier otro orden. Por ejemplo, al principio se pueden establecer las bases de medición mutuamente imparciales entre el primer medio de medición y el cuarto medio de medición y, a continuación, se pueden establecer las mismas bases de medición entre el primer medio de medición y el tercer medio de medición y las mismas bases de medición entre el cuarto medio de medición y el segundo medio de medición. En otro ejemplo, al principio se pueden establecer las mismas bases de medición entre el primer medio de medición y el tercer medio de medición y las mismas bases de medición entre el cuarto medio de medición y el segundo medio de medición. En una tercera etapa, se pueden establecer las bases de medición mutuamente imparciales entre el primer medio de medición y el cuarto medio de medición.

**[0012]** Establecer las mismas bases de medición entre dos medios de medición cualesquiera, por ejemplo, el primer (M1) y el tercer medios de medición (M3), significa aquí establecer en el primer medio de medición (M1) la base y establecer en el tercer medio de medición (M3) esta base.

**[0013]** El objeto de la invención se logra además mediante un aparato para proporcionar un marco de referencia común entre dos receptores según la reivindicación 12, donde el aparato comprende una fuente de fotones entrelazados, un primer receptor y un segundo receptor y un primer canal de transmisión y un segundo canal de transmisión. El primer receptor está conectado a través del primer canal de transmisión a una fuente de fotones entrelazados, y el segundo receptor está conectado a través del segundo canal de transmisión a la fuente de fotones entrelazados. La fuente de fotones entrelazados produce pares de fotones entrelazados, preferentemente entrelazados en la polarización o el intervalo de tiempo o el momento angular orbital o la trayectoria, donde el primer fotón de cada par de fotones entrelazados se envía a través del primer canal de transmisión al primer receptor y el segundo fotón de cada par de fotones entrelazados se envía a través del segundo canal de transmisión al segundo receptor. El primer receptor comprende un primer y un segundo medio de medición para medir los fotones en dos bases de medición mutuamente imparciales, donde el segundo receptor comprende un tercer y un cuarto medio de medición para medir los fotones en dos bases de medición mutuamente imparciales. Cada medio de medición puede medir los fotones en al menos dos estados ortogonales. Los cuatro medios de medición pueden comunicar el tiempo de la detección de un fotón de los pares de fotones entrelazados para detectar coincidencias entre los dos receptores de un par de fotones entrelazados y para calcular la visibilidad y/o la tasa de error de bit cuántico (TBEC). Tres de los cuatro medios de medición comprenden cada uno un medio de corrección para establecer el marco de referencia común.

**[0014]** Los medios de corrección también corrigen cualquier transformación unitaria de la propiedad de entrelazamiento del fotón causada por el primer o el segundo canal de transmisión con el fin de establecer la relación entre las bases de medición en las etapas i) a iii).

**[0015]** La propiedad de entrelazamiento significa aquí la calidad donde se entrelazan los fotones. Por ejemplo, para pares de fotones entrelazados en el grado de libertad de polarización, la propiedad de entrelazamiento es la polarización de los fotones.

**[0016]** Para generar la clave de la distribución cuántica de claves (DCC), ambos receptores (Alice y Bob) deben asegurarse de que coinciden en las mismas bases de medición. En esta invención, el marco de referencia común entre ambos receptores se puede establecer sin el conocimiento de las bases de medición reales en el primer y el segundo receptor. Con esta invención ya no es necesario corregir la transformación unitaria de la propiedad de entrelazamiento del fotón causada por el primer y/o el segundo canal de transmisión para cada canal de transmisión por separado. En esta invención, solamente se ajusta la relación entre las bases de medición de los medios de medición en ambos receptores. La invención se basa en el conocimiento de la relación entre las bases de medición, que tiene que ser de una manera específica para permitir la generación de una clave segura para la distribución cuántica de claves entre los dos receptores. Para un protocolo de distribución cuántica de claves, es necesario que

ambos receptores coincidan con las mismas dos bases de medición mutuamente imparciales para generar la clave. Esto se realiza en esta invención utilizando la detección de coincidencias y usando las tasas de recuento de coincidencias entre los dos receptores y calculando la visibilidad y/o la tasa de error de bit cuántico (TEBC) de los fotones y coincidencias detectados.

**[0017]** El valor deseado para la visibilidad (maximización) es 1 o -1 para la combinación de bases de medición coincidentes (por ejemplo, entre el primer medio de medición y el tercer medio de medición y también entre el cuarto medio de medición y el segundo medio de medición) y visibilidad 0 (minimización) para la combinación de bases de medición mutuamente imparciales (por ejemplo, entre el primer medio de medición y el cuarto medio de medición). Sin embargo, las imperfecciones técnicas generalmente no permiten lograr estos valores de inmediato, pero deben abordarse lo mejor posible porque garantizan el máximo rendimiento del sistema DCC. Una visibilidad de 1 o -1 corresponde a una TBEC de 0 o 1 para la combinación de bases de medición coincidentes (M1-M3 y M4-M2), y una visibilidad de 0 corresponde a una TBEC de 0,5 para la combinación de bases de medición mutuamente imparciales (M1-M4).

**[0018]** En una realización preferida de la invención del procedimiento y el aparato, los valores de la visibilidad para la combinación de bases de medición coincidentes están comprendidos entre 1 y 0,7 o entre -1 y -0,7. Más preferentemente, los valores de la visibilidad para la combinación de bases de medición coincidentes están entre 1 y 0,8 o entre - 1 y -0,8. Lo más preferentemente, los valores de la visibilidad para la combinación de bases de medición coincidentes están entre 1 y 0,9 o entre -1 y - 0,9. La TBEC se puede calcular según la ecuación que se describe a continuación.

**[0019]** En una realización preferida de la invención del procedimiento y el aparato, los valores de la visibilidad para la combinación de bases de medición mutuamente imparciales están entre 0,3 y 0 o entre -0,3 y 0. Más preferentemente, los valores de la visibilidad para la combinación de bases de medición mutuamente imparciales están entre 0,2 y 0 o entre -0,2 y 0. Lo más preferentemente, los valores de la visibilidad para la combinación de bases de medición mutuamente imparciales están entre 0,1 y 0 o entre -0,1 y 0. La TBEC se puede calcular según la ecuación que se describe a continuación.

**[0020]** Con los medios de corrección primero, segundo y tercero, el marco de referencia común entre ambos receptores se puede establecer sin el conocimiento de las bases de medición reales en el primer y el segundo receptor. Esto se realiza alterando la propiedad de los fotones entrelazados donde están entrelazados. Por ejemplo, alterando o influyendo (pero no midiendo) la polarización de los fotones. Esto se puede realizar, por ejemplo, con un controlador de polarización (es decir, birrefringencia inducida por tensión) en una fibra para pares de fotones entrelazados en la polarización o un modulador espacial de luz (MEL) para pares de fotones entrelazados en el momento angular óptico o un trombón o una línea de retardo para pares de fotones entrelazados en el intervalo de tiempo o para pares de fotones entrelazados en la trayectoria.

**[0021]** En una realización preferida de la invención del procedimiento y el aparato, los medios de corrección primero, segundo y tercero pueden alterar la propiedad de los fotones entrelazados donde están entrelazados.

**[0022]** En una realización preferida de la invención del procedimiento y el aparato, los dos receptores pueden estar en una red de más receptores, donde preferentemente la red con más receptores se construye mediante multiplexación por división de espacio, multiplexación por división de tiempo o multiplexación por división de frecuencia de los pares de fotones entrelazados.

**[0023]** Para proporcionar el marco de referencia común entre los dos receptores, esta invención se basa en la utilización de detección de coincidencia y en el uso de las tasas de recuento de coincidencias entre los dos receptores. Una tasa de recuento de coincidencias $CC_{Mij,Mij}$ es una medida para la detección simultánea de los dos fotones del par de fotones entrelazados en ambos receptores, teniendo en cuenta las distancias y las diferentes longitudes de cable, mientras que $M_{ij}$ es el medio de medición con $i$ = 1, 2, 3 *o* 4 correspondiente a uno de los cuatro medios de medición, *y* $j$ = a *o* $b$ correspondiente a uno de los dos estados ortogonales de ese medio de medición. Dicha detección simultánea también se denomina coincidencia. El tiempo de detección de una coincidencia puede estar influenciado por la fluctuación del detector, la sincronización entre los dos relojes de los dos receptores y/o el tiempo de correlación de los fotones del par de fotones entrelazados.

**[0024]** Como ejemplo, la visibilidad (V) para los fotones detectados en los medios de medición primero y tercero M1 y M3 se define como:

$$V_{M1,M3} = \frac{CC_{M1a,M3a} + CC_{M1b,M3b} - CC_{M1a,M3b} - CC_{M1b,M3a}}{CC_{M1a,M3a} + CC_{M1b,M3b} + CC_{M1a,M3b} + CC_{M1b,M3a}}$$

**[0025]** La tasa de error de bit cuántico (TEBC) para los fotones detectados en los medios de medición primero y tercero M1 y M3 se define como:

$$TEBC_{M1,M3} = \frac{1 - V_{M1,M3}}{2}$$

**[0026]** La TEBC o la visibilidad de los fotones detectados en cualquiera de los dos medios de medición, significa aquí la TEBC o la visibilidad entre estos medios de medición.

**[0027]** La visibilidad y la TEBC para los fotones detectados entre todos los demás medios de medición se pueden calcular de la misma manera.

**[0028]** En una realización preferida de la invención del procedimiento después de la etapa iii), se genera una clave de seguridad entre los dos receptores mediante una distribución cuántica de claves. Los pares de fotones detectados y usados para las etapas de ajuste i) a iii) no se usan para generar la clave segura. Para el ajuste, el resultado de la medición debe comunicarse entre los dos receptores, mientras que para la generación de la clave segura, el resultado de la medición en cada receptor se mantiene en secreto. Por tanto, los fotones detectados para establecer el marco de referencia común no forman parte de la clave segura.

**[0029]** Como ejemplo, el procedimiento para proporcionar el marco de referencia común que comprende las etapas i) a iii) se puede establecer antes de la generación de la clave segura. Como otro ejemplo, el procedimiento para proporcionar el marco de referencia común que comprende las etapas i) a iii) se puede aplicar en una secuencia. Por ejemplo, en una primera ventana temporal, por ejemplo, de 10 segundos, se aplica el procedimiento para proporcionar el marco de referencia común que comprende las etapas i) a iii). A continuación, en una segunda ventana temporal, por ejemplo, de 50 segundos, se genera una clave segura. Después de eso, el marco de referencia común se establece nuevamente, por ejemplo, en una ventana temporal de 10 segundos aplicando las etapas i) a iii), seguido de la generación de claves, por ejemplo, en una ventana temporal de 50 segundos. Preferentemente, las ventanas temporales dentro de las cuales se establece el marco de referencia común y la ventana temporal dentro de la cual se genera la clave segura pueden ser más cortas o más largas y también la relación entre las ventanas temporales puede diferir.

**[0030]** En una realización preferida de la invención del procedimiento, el procedimiento para proporcionar el marco de referencia común que comprende las etapas i) a iii) se aplica para corregir la rotación de polarización causada por una transmisión por satélite en una comunicación de satélite a tierra.

**[0031]** En una realización preferida de la invención del procedimiento y el aparato, la fuente de fotones entrelazados produce pares de fotones entrelazados en la polarización en un estado de entrelazamiento máximo. Preferentemente, el estado puede ser $|\Phi\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle + e^{i\varphi}|V\rangle|V\rangle)$ o $|\Psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle + e^{i\varphi}|H\rangle|V\rangle)$, con $|\Phi\rangle$ y $|\Psi\rangle$ como los estados de los pares de fotones entrelazados, $|H\rangle$ como polarizado lineal horizontal y $|V\rangle$ como polarizado lineal vertical, y $e^{i\varphi}$ como una fase aleatoria.

**[0032]** En una realización preferida de la invención del procedimiento y el aparato, el primer medio de corrección se asigna a los medios de medición primero o tercero, y donde el segundo medio de corrección se asigna a los medios de medición primero o cuarto, y donde el tercer medio de corrección se asigna a los medios de medición cuarto o segundo. En una realización preferida de la invención, los tres medios de corrección también pueden estar en cualquier otra configuración en los medios de medición. Por ejemplo, los tres medios de corrección también pueden estar en los medios de medición primero, tercero y cuarto, o en los medios de medición primero, segundo y cuarto, o en los medios de medición primero, segundo y tercero. Asignado a significa en este caso que solamente la propiedad de entrelazamiento de los fotones detectados en los medios de medición asignados es corregida por los medios de corrección relacionados.

**[0033]** En una realización preferida de la invención del procedimiento y el aparato, el primer medio de corrección (C1) está dispuesto en el primer canal de transmisión (10) o en o antes del primer medio de medición (M1), o en el segundo canal de transmisión (11) o en o antes del tercer medio de medición (M3), y/o

donde el segundo medio de corrección (C2) está dispuesto en el primer canal de transmisión (10) o en o antes del primer medio de medición (M1), o en el segundo canal de transmisión (11) o en o antes del cuarto medio de medición (M4), y/o
donde el tercer medio de corrección (C3) está dispuesto en el segundo canal de transmisión (11) o en o antes del cuarto medio de medición (M4), o en el primer canal de transmisión (10) o en o antes del segundo medio de medición (M2).

**[0034]** En una realización preferida de la invención del procedimiento y el aparato, los pares de fotones entrelazados pueden estar entrelazados en la polarización o el intervalo de tiempo o el momento angular orbital o el grado de libertad de trayectoria. Preferentemente, la propiedad de entrelazamiento puede ser la polarización o el intervalo de tiempo o el momento angular orbital o la trayectoria.

**[0035]** En una realización preferida de la invención del procedimiento y el aparato, el canal de transmisión primero y/o segundo es/son un canal de espacio libre o una guía de ondas, preferentemente una fibra.

**[0036]** En una realización preferida de la invención del procedimiento y el aparato, el medio de corrección primero, segundo y/o tercero es/son un conjunto de placas de cuarto de onda, semionda y cuarto de onda, y/o una placa de onda variable, y/o una placa de onda inclinada, y/o un elemento birrefringente, y/o un trombón, y/o un controlador de fibra, o un modulador espacial de luz (MEL), y/o una línea de retardo.

**[0037]** En una realización preferida de la invención del procedimiento y el aparato, el fotón de un par de fotones en el primer canal de transmisión se guía aleatoriamente a los medios de medición primero o segundo mediante un primer componente de separación, preferentemente un divisor de haz o un divisor de haz de fibra o se enruta aleatoriamente mediante un conmutador de fibra, y/o donde el fotón de un par de fotones en el segundo canal de transmisión se guía aleatoriamente a los medios de medición tercero o cuarto mediante un segundo componente de separación, preferentemente mediante un divisor de haz o un divisor de haz de fibra o se enruta aleatoriamente mediante un conmutador de fibra.

**[0038]** En una realización preferida de la invención del procedimiento y el aparato, en el primer canal de transmisión, un primer componente de separación, preferentemente un divisor de haz o un divisor de haz de fibra o un conmutador de fibra, está dispuesto para guiar aleatoriamente un fotón a los medios de medición primero o segundo, y/o donde en el segundo canal de transmisión un segundo componente de separación, preferentemente un divisor de haz o un divisor de haz de fibra o un conmutador de fibra, está dispuesto para guiar aleatoriamente un fotón a los medios de medición tercero o cuarto.

**[0039]** En una realización preferida de la invención del procedimiento y el aparato, el primer medio de corrección está dispuesto después o detrás del primer componente de separación en el primer medio de medición o está dispuesto después o detrás del segundo componente de separación en el tercer medio de medición, y donde el segundo medio de corrección está dispuesto después o detrás del segundo componente de separación en el tercer medio de medición o está dispuesto después o detrás del segundo componente de separación en el cuarto medio de medición, y donde el tercer medio de corrección está dispuesto después o detrás del segundo componente de separación en el cuarto medio de medición o está dispuesto después o detrás del primer componente de separación en el segundo medio de medición.

**[0040]** La invención también puede lograrse mediante un dispositivo de control, preferentemente un ordenador, capaz de proporcionar un procedimiento según una de las realizaciones descritas anteriormente, donde el dispositivo de control está conectado con los medios de detección primero, segundo, tercero y cuarto para registrar los fotones detectados y las coincidencias y para calcular la visibilidad y/o la tasa de error de bit cuántico de los fotones detectados, y con los medios de corrección primero, segundo y tercero para establecer el marco de referencia común entre los dos receptores.

**[0041]** La invención también puede lograrse mediante un dispositivo informático con un microprocesador con una memoria no volátil, donde la memoria no volátil comprende un programa ejecutable con el fin de proporcionar un procedimiento según una de las realizaciones descritas anteriormente, preferentemente donde el dispositivo informático es el dispositivo de control.

**[0042]** La invención también puede lograrse mediante el aparato para proporcionar un procedimiento según una de las realizaciones descritas anteriormente.

**[0043]** A continuación, se explicará la invención mediante realizaciones preferidas ilustradas en los dibujos, pero sin limitarse a las mismas. En el dibujo:

Fig. 1: configuración esquemática de un aparato para proporcionar un marco de referencia común entre dos receptores;
Fig. 2: configuración de un aparato para proporcionar y establecer un marco de referencia de polarización común entre dos receptores con pares de fotones entrelazados en la polarización;

**[0044]** La Fig. 1 muestra una configuración esquemática para proporcionar y establecer un marco de referencia común entre los dos receptores 2 y 3. La fuente de fotones entrelazados 1 está conectada a través de dos canales de transmisión 10 y 11 con los dos receptores 2 y 3.

**[0045]** Cada receptor 2 y 3 comprende dos medios de medición. El receptor 2 comprende los medios de medición M1 y M2 y el receptor 3 comprende los medios de medición M3 y M4. Cada medio de medición puede medir los fotones de la fuente de fotones entrelazados en una base de medición específica, mientras que las bases de la configuración configurada del receptor 2 son dos bases de medición mutuamente imparciales B1 y B2, y las bases de medición del receptor 3 son dos bases de medición mutuamente imparciales B3 y B4. Los fotones en el primer canal de transmisión 10 son guiados aleatoriamente por un primer componente de separación S1 a los medios de medición primero y segundo M1 y M2. Los fotones en el segundo canal de transmisión 11 son guiados aleatoriamente por un segundo componente de separación S2 a los medios de medición tercero y cuarto M3 y M4. Para configurar la configuración y establecer un marco de referencia común en ambos receptores 2 y 3, se disponen tres medios de corrección C1, C2 y C3 en tres de los cuatro medios de medición. En el ejemplo de la Fig. 1, los medios de corrección C1, C2 y C3 están dispuestos en los medios de medición M2, M3 y M4. En una realización preferida de la invención, los medios de corrección C1, C2 y C3 también pueden estar en cualquier otra configuración en los medios de medición. Por ejemplo, los medios de corrección C1, C2 y C3 también pueden estar en los medios de medición M1, M3 y M4, o en los medios de medición M1, M2 y M4, o en los medios de medición M1, M2 y M3. En los medios de medición M1, M2, M3 y M4, se detectan los fotones de la fuente de fotones entrelazados 1 y la señal se envía a través de cables a una lógica de coincidencia 4. El tiempo de llegada de cada señal queda registrado en la lógica de coincidencia 4, teniendo en cuenta las distancias y diferentes longitudes de cable. A partir de estas señales, se puede calcular la visibilidad (V) y/o la tasa de error de bit cuántico (TEBC).

**[0046]** La Fig. 2 muestra como un ejemplo de la invención una configuración de un aparato para proporcionar y establecer un marco de referencia de polarización común entre dos receptores con pares de fotones entrelazados en la polarización. Cada medio de medición M1, M2, M3 y M4 puede medir los fotones en al menos dos estados ortogonales. La fuente de fotones entrelazados 1 produce pares de fotones entrelazados en la polarización. El estado del par de fotones entrelazados producido es en este ejemplo

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle|H\rangle + e^{i\varphi}|V\rangle|V\rangle\right) o \quad |\Psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle|V\rangle + e^{i\varphi}|H\rangle|V\rangle\right)$$

con $|\Phi\rangle$ y $|\Psi\rangle$ como los estados de los pares de fotones entrelazados, $|H\rangle$ como base horizontal y $|V\rangle$ como base vertical, y $e^{i\varphi}$ como una fase aleatoria.

**[0047]** Un fotón de cada par es enviado al receptor 2 por la primera línea de transmisión 10, y el otro fotón de cada par es enviado al receptor 3 por la segunda línea de transmisión 11. Los fotones son guiados aleatoriamente por el componente de separación primero y segundo S1 y S2 a los medios de medición M1 o M2, y a los medios de medición M3 o M4. En el ejemplo de la Fig. 2, los componentes de separación S1 y S2 son divisores de haz 50/50 o son divisores de haz variables para equilibrar la eficiencia de detección de los detectores 13. En el ejemplo de la Fig. 2, cada medio de medición M1, M2, M3 y M4 es un divisor de haz de polarización 12 y dos detectores 13. Con eso, cada medio de medición M1, M2, M3 y M4 puede medir los fotones en al menos dos estados ortogonales.

**[0048]** Frente al divisor de haz de polarización 12 en los medios de medición M2, M3 y M4, se disponen los medios de corrección primero, segundo y tercero C1, C2 y C3. En el ejemplo de la Fig. 2, los medios de corrección C1, C2 comprenden una placa de cuarto de onda, semionda y cuarto de onda, y/o una placa de onda variable, y/o una placa de onda inclinada, y/o un elemento birrefringente, y/o un controlador de fibra para alterar la polarización sin medir la polarización de los fotones y, por tanto, para ajustar las bases de medición entre los medios de medición M1, M2, M3 y M4.

**[0049]** Cada detector 13 registra un único fotón y genera una señal eléctrica, que se envía a través de un cable 14 a la lógica de coincidencia 4. Con el divisor de haz de polarización 12 y los dos detectores 13 en cada medio de medición M1, M2, M3 y M4, los fotones se pueden medir en dos estados ortogonales a en el primer detector 13 y b en el segundo detector 13.

**[0050]** Como ejemplo para los pares de fotones entrelazados en la polarización, la visibilidad (V) y la tasa de error de bit cuántico TEBC se calculan en este caso para los fotones detectados en los medios de medición M1 y M3, donde $CC_{M1a,M3a}$ indica la tasa de recuento de coincidencias entre el primer detector 13 para el estado a en el medio de medición M1, y el primer detector 13 para el estado a en el medio de medición M3. La visibilidad (V) para los fotones detectados en los medios de medición M1 y M3 se define como:

$$V_{M1,M3} = \frac{CC_{M1a,M3a} + CC_{M1b,M3b} - CC_{M1a,M3b} - CC_{M1b,M3a}}{CC_{M1a,M3a} + CC_{M1b,M3b} + CC_{M1a,M3b} + CC_{M1b,M3a}}$$

**[0051]** La tasa de error de bit cuántico (TEBC) para los fotones detectados en los medios de medición M1 y

M3 se define como:

$$TEBC_{M1,M3} = \frac{1 - V_{M1,M3}}{2}$$

**[0052]** Preferentemente, la lógica de coincidencia 4 se puede conectar a los medios de corrección primero, segundo y tercero S1, S2 y S3 (la conexión no se muestra en las Fig. 1 y 2) para ajustar el marco de referencia de polarización común para una distribución segura de claves para la criptografía cuántica.

**[0053]** Para la distribución segura de claves, las bases de medición de los medios de medición M1 y M2 deben ser mutuamente imparciales. Los medios de medición M3 y M4 deben tener las mismas bases de medición que los medios de medición en M1 y M2. Según la invención, no es necesario que ambos receptores 2 y 3 conozcan las bases de medición exactas donde medirán los fotones. Para las configuraciones de las Fig. 1 y 2, las etapas para configurar la configuración y establecer un marco de referencia de polarización común son:

En primer lugar, la TEBC debe minimizarse o la visibilidad debe maximizarse para los fotones detectados en el primer medio de medición M1 y el tercer medio de medición M3. Esto puede realizarse ajustando el primer medio de corrección C1, que está dispuesto en el medio de medición M3, pero también puede estar dispuesto en el medio de medición M1. La TEBC o la visibilidad de los fotones detectados en los medios de medición M1 y M3 debe ajustarse para establecer la misma base de polarización entre el primer medio de medición M1 y el tercer medio de medición M3.
En una segunda etapa, se deben establecer las bases de polarización mutuamente imparciales entre el primer medio de medición M1 y el cuarto medio de medición M4. Esto se puede realizar mediante la maximización de la TEBC o la minimización de la visibilidad de los fotones detectados en el tercer medio de medición M3 y cuarto medio de medición M4 mediante el ajuste del segundo medio de corrección C2, que está dispuesto en el medio de medición M4, pero también puede estar dispuesto en el medio de medición M3.
En una tercera etapa, se debe establecer la misma base de polarización entre el cuarto medio de medición M4 y el segundo medio de medición M2. Esto se realiza mediante la minimización de la TEBC o la maximización de la visibilidad de los fotones detectados en el cuarto medio de medición M4 y el segundo medio de medición M2 mediante el ajuste del tercer medio de corrección C3, que está dispuesto en el medio de medición M2, pero también puede estar dispuesto en el medio de medición M4.

**[0054]** Las etapas descritas anteriormente se pueden realizar en cualquier otro orden. Por ejemplo, al principio se pueden establecer las bases de polarización mutuamente imparciales entre el primer medio de medición M1 y el cuarto medio de medición M4 y, a continuación, las mismas bases de polarización entre el primer medio de medición M1 y el tercer medio de medición M3 y las mismas bases de polarización entre el cuarto medio de medición M4 y el segundo medio de medición M2.

Signos de referencia

**[0055]**

| | |
|---|---|
| 1 | fuente de fotones entrelazados |
| 2 | primer receptor |
| 3 | segundo receptor |
| 4 | lógica de coincidencia |
| 10 | primer canal de transmisión |
| 11 | segundo canal de transmisión |
| 12 | divisor de haz de polarización |
| 13 | detector |
| 14 | cable |
| M1 | primer medio de medición |
| M2 | segundo medio de medición |
| M3 | tercer medio de medición |
| M4 | cuarto medio de medición |
| C1 | primer medio de corrección |
| C2 | segundo medio de corrección |
| C3 | tercer medio de corrección |
| S1 | primer componente de separación |

S2 segundo componente de separación

## REIVINDICACIONES

1. Un procedimiento para proporcionar un marco de referencia común entre dos receptores, preferentemente para la distribución cuántica de claves,

donde el primer receptor (2) está conectado a través de un primer canal de transmisión (10) a una fuente de fotones entrelazados (1) y el segundo receptor (3) está conectado a través de un segundo canal de transmisión (11) a la fuente de fotones entrelazados (1),
donde la fuente de fotones entrelazados (1) produce pares de fotones entrelazados, preferentemente entrelazados en la polarización o el intervalo de tiempo, el momento angular orbital o la trayectoria,
donde el primer fotón de cada par de fotones entrelazados se envía a través del primer canal de transmisión (10) al primer receptor (2) y el segundo fotón de cada par de fotones entrelazados se envía a través del segundo canal de transmisión (11) al segundo receptor (3),
donde el primer receptor (2) comprende un primer (M1) y un segundo (M2) medios de medición para medir los fotones en dos bases de medición mutuamente imparciales,
donde el segundo receptor (3) comprende un tercer (M3) y un cuarto (M4) medios de medición para medir los fotones en dos bases de medición mutuamente imparciales,
donde cada medio de medición puede medir los fotones en al menos dos estados ortogonales,
donde los cuatro medios de medición (M1, M2, M3, M4) pueden comunicar el momento de la detección de un fotón de los pares de fotones entrelazados para detectar las coincidencias entre los dos receptores de un par de fotones entrelazados y para calcular la visibilidad y/o la tasa de error de bit cuántico (TEBC),
- donde tres de los cuatro medios de medición comprenden cada uno un medio de corrección (C1, C2, C3) para establecer el marco de referencia común,
- donde el procedimiento comprende las etapas de
i) minimización de la TEBC o maximización de la visibilidad de los fotones detectados en los medios de medición primero (M1) y tercero (M3) mediante el ajuste del primer medio de corrección (C1) con el fin de establecer las mismas bases de medición entre el primer medio de medición (M1) y el tercer medio de medición (M3),
ii) maximización de la TEBC o minimización de la visibilidad de los fotones detectados en los medios de medición primero (M1) y cuarto (M4) mediante el ajuste del segundo medio de corrección (C2) con el fin de establecer dos bases de medición mutuamente imparciales entre el primer medio de medición (M1) y el cuarto medio de medición (M4),
iii) minimización de la TEBC o maximización de la visibilidad de los fotones detectados en los medios de medición cuarto (M4) y segundo (M2) mediante el ajuste del tercer medio de corrección (C3) con el fin de establecer las mismas bases de medición entre el cuarto medio de medición (M4) y el segundo medio de medición (M2).

2. Procedimiento según la reivindicación 1,
donde, después de la etapa iii), se genera una clave segura entre los dos receptores mediante distribución cuántica de claves.

3. Procedimiento según una de las reivindicaciones 1 o 2,

donde el primer medio de corrección (C1) está asignado a los medios de medición primero (M1) o tercero (M3), y
donde el segundo medio de corrección (C2) está asignado a los medios de medición tercero (M3) o cuarto (M4), y
donde el tercer medio de corrección (C3) está asignado a los medios de medición cuarto (M4) o segundo (M2).

4. Procedimiento según una de las reivindicaciones 1 a 3,

donde el primer medio de corrección (C1) está dispuesto en el primer canal de transmisión (10) o en o antes del primer medio de medición (M1), o en el segundo canal de transmisión (11) o en o antes del tercer medio de medición (M3), y/o
donde el segundo medio de corrección (C2) está dispuesto en el primer canal de transmisión (10) o en o antes del primer medio de medición (M1), o en el segundo canal de transmisión (11) o en o antes del cuarto medio de medición (M4), y/o
donde el tercer medio de corrección (C3) está dispuesto en el segundo canal de transmisión (11) o en o antes del cuarto medio de medición (M4), o en el primer canal de transmisión (10) o en o antes del segundo medio de medición (M2).

5. Procedimiento según una de las reivindicaciones 1 a 4,
donde los pares de fotones entrelazados pueden estar entrelazados en la polarización, el intervalo de tiempo, el momento angular orbital o la trayectoria.

6. Procedimiento según una de las reivindicaciones 1 a 5,
donde el canal de transmisión primero (10) y/o segundo (11) es/son un canal de espacio libre o una guía de ondas, preferentemente una fibra.

7. Procedimiento según una de las reivindicaciones 1 a 6,
donde el medio de corrección primero (C1), segundo (C2) y/o tercero (C3) es/son un conjunto de placas de cuarto de onda, semionda y cuarto de onda, y/o una placa de onda variable, y/o una placa de onda inclinada, y/o un elemento birrefringente, y/o un trombón y/o un controlador de fibra, o un modulador espacial de luz (MEL), y/o una línea de retardo.

8. Procedimiento según una de las reivindicaciones 1 a 7,

donde el fotón de un par de fotones en el primer canal de transmisión (10) se guía aleatoriamente a los medios de medición primero (M1) o segundo (M2) mediante un primer componente de separación (S1), preferentemente un divisor de haz o un divisor de haz de fibra o se enruta aleatoriamente mediante un conmutador de fibra,
y/o donde el fotón de un par de fotones en el segundo canal de transmisión (11) se guía aleatoriamente a los medios de medición tercero (M3) o cuarto (M4) mediante un segundo componente de separación (S2), preferentemente mediante un divisor de haz o un divisor de haz de fibra o se enruta aleatoriamente mediante un conmutador de fibra.

9. Procedimiento según la reivindicación 8,

donde el primer medio de corrección (C1) está dispuesto después o detrás del primer componente de separación (S1) en el primer medio de medición (M1) o está dispuesto después o detrás del segundo componente de separación (S2) en el tercer medio de medición (M3), y
donde el segundo medio de corrección (C2) está dispuesto después o detrás del segundo componente de separación (S2) en el tercer medio de medición (M3) o está dispuesto después o detrás del segundo componente de separación (S2) en el cuarto medio de medición (M4), y
donde el tercer medio de corrección (C3) está dispuesto después o detrás del segundo componente de separación (S2) en el cuarto medio de medición (M4) o está dispuesto después o detrás del primer componente de separación (S1) en el segundo medio de medición (M2).

10. El dispositivo de control (4), preferentemente un ordenador, capaz de proporcionar un procedimiento según una de las reivindicaciones 1 a 9,
donde el dispositivo de control está conectado

con los medios de detección primero (M1), segundo (M2), tercero (M3) y cuarto (M4) con el fin de registrar los fotones detectados y las coincidencias de los pares de fotones entrelazados y para calcular la visibilidad y/o la tasa de error de bit cuántico de los fotones detectados, y
con los medios de corrección primero (C1), segundo (C2) y tercero (C3) para establecer el marco de referencia común entre los dos receptores (2, 3).

11. Dispositivo informático como dispositivo de control según la reivindicación 10 con un microprocesador con una memoria no volátil, donde la memoria no volátil comprende un programa ejecutable con el fin de proporcionar un procedimiento según una de las reivindicaciones 1 a 9.

12. Un sistema para proporcionar un marco de referencia común entre dos receptores, preferentemente para la distribución cuántica de claves,

donde el sistema comprende una fuente de fotones entrelazados (1), un primer receptor (2) y un segundo receptor (3) y un primer canal de transmisión (10) y un segundo canal de transmisión (20),
donde el primer receptor (2) está conectado a través del primer canal de transmisión (10) a una fuente de fotones entrelazados (1) y el segundo receptor (3) está conectado a través del segundo canal de transmisión (11) a la fuente de fotones entrelazados (1),
donde la fuente de fotones entrelazados (1) produce pares de fotones entrelazados, preferentemente entrelazados en la polarización o el intervalo de tiempo, el momento angular orbital o la trayectoria,
donde el primer fotón de cada par de fotones entrelazados se envía a través del primer canal de transmisión (10) al primer receptor (2) y el segundo fotón de cada par de fotones entrelazados se envía a través del segundo canal de transmisión (11) al segundo receptor (3),
donde el primer receptor (2) comprende un primer (M1) y un segundo (M2) medios de medición para medir los fotones en dos bases de medición mutuamente imparciales,
donde el segundo receptor (3) comprende un tercer (M3) y un cuarto (M4) medios de medición para medir los fotones en dos bases de medición mutuamente imparciales,
donde cada medio de medición puede medir los fotones en al menos dos estados ortogonales,
donde los cuatro medios de medición (M1, M2, M3, M4) pueden comunicar el momento de la detección de un fotón de los pares de fotones entrelazados para detectar las coincidencias entre los dos receptores de un par de fotones entrelazados y para calcular la visibilidad y/o la tasa de error de bit cuántico (TEBC),
**caracterizado porque** tres de los cuatro medios de medición comprenden cada uno un medio de corrección (C1, C2, C3) para establecer el marco de referencia común adaptado para realizar las etapas i) a iii) según una de las

reivindicaciones 1 a 11.

13. Sistema según la reivindicación 12,

donde, en el primer canal de transmisión (10), un primer componente de separación (S1), preferentemente un divisor de haz o un divisor de haz de fibra, está dispuesto para guiar aleatoriamente un fotón a los medios de medición primero (M1) o segundo (M2), y/o
donde, en el segundo canal de transmisión (11), un segundo componente de separación (S2), preferentemente un divisor de haz o un divisor de haz de fibra está dispuesto para guiar aleatoriamente un fotón a los medios de medición tercero (M3) o cuarto (M4).

14. Sistema según la reivindicación 13,

donde el primer medio de corrección (C1) está dispuesto después o detrás del primer componente de separación (S1) en el primer medio de medición (M1) o está dispuesto después o detrás del segundo componente de separación (S2) en el tercer medio de medición (M3), y
donde el segundo medio de corrección (C2) está dispuesto después o detrás del segundo componente de separación (S2) en el tercer medio de medición (M3) o está dispuesto después o detrás del segundo componente de separación (S2) en el cuarto medio de medición (M4), y
donde el tercer medio de corrección (C3) está dispuesto después o detrás del segundo componente de separación (S2) en el cuarto medio de medición (M4) o está dispuesto después o detrás del primer componente de separación (S1) en el segundo medio de medición (M2).

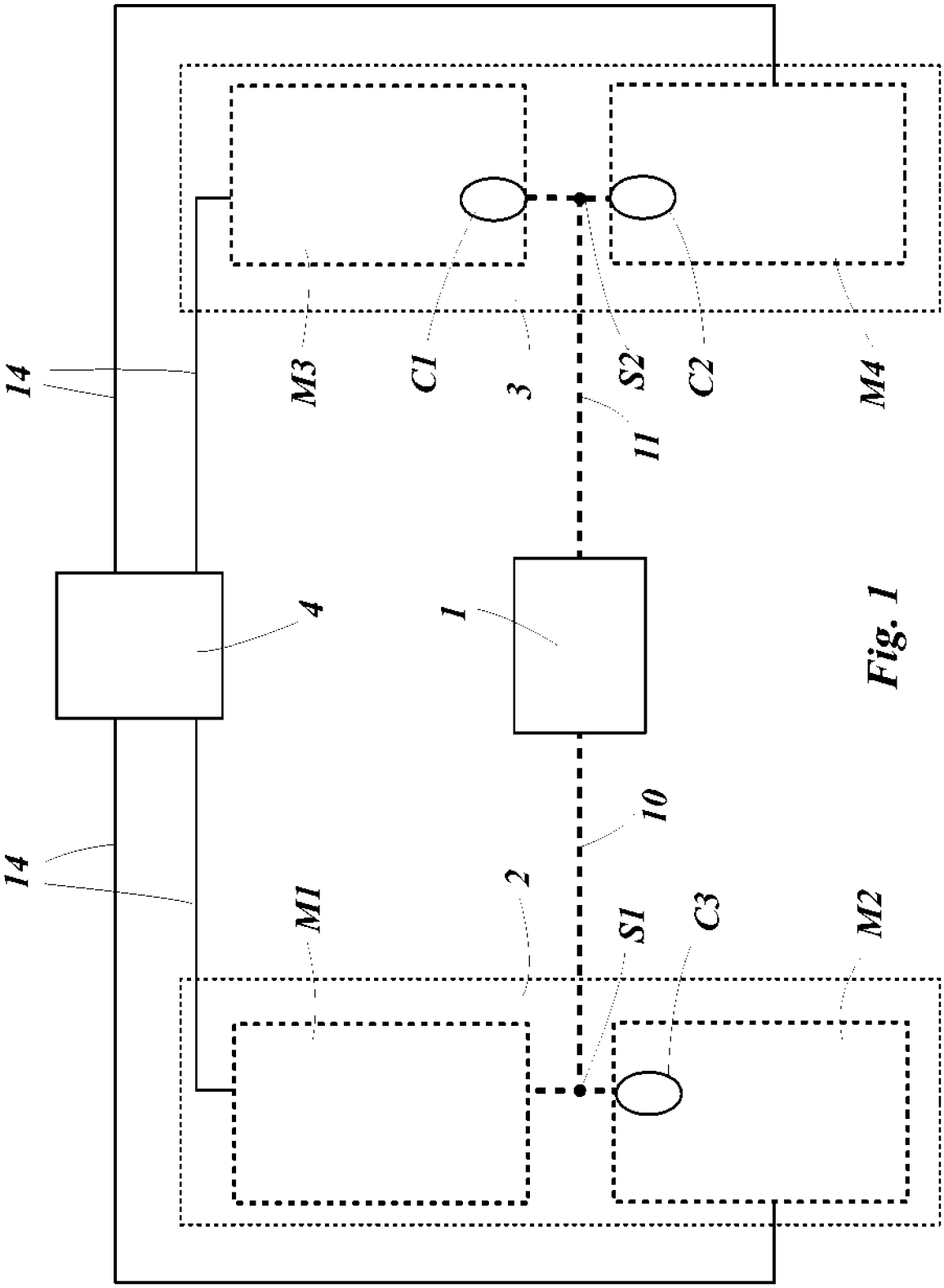


Fig. 1

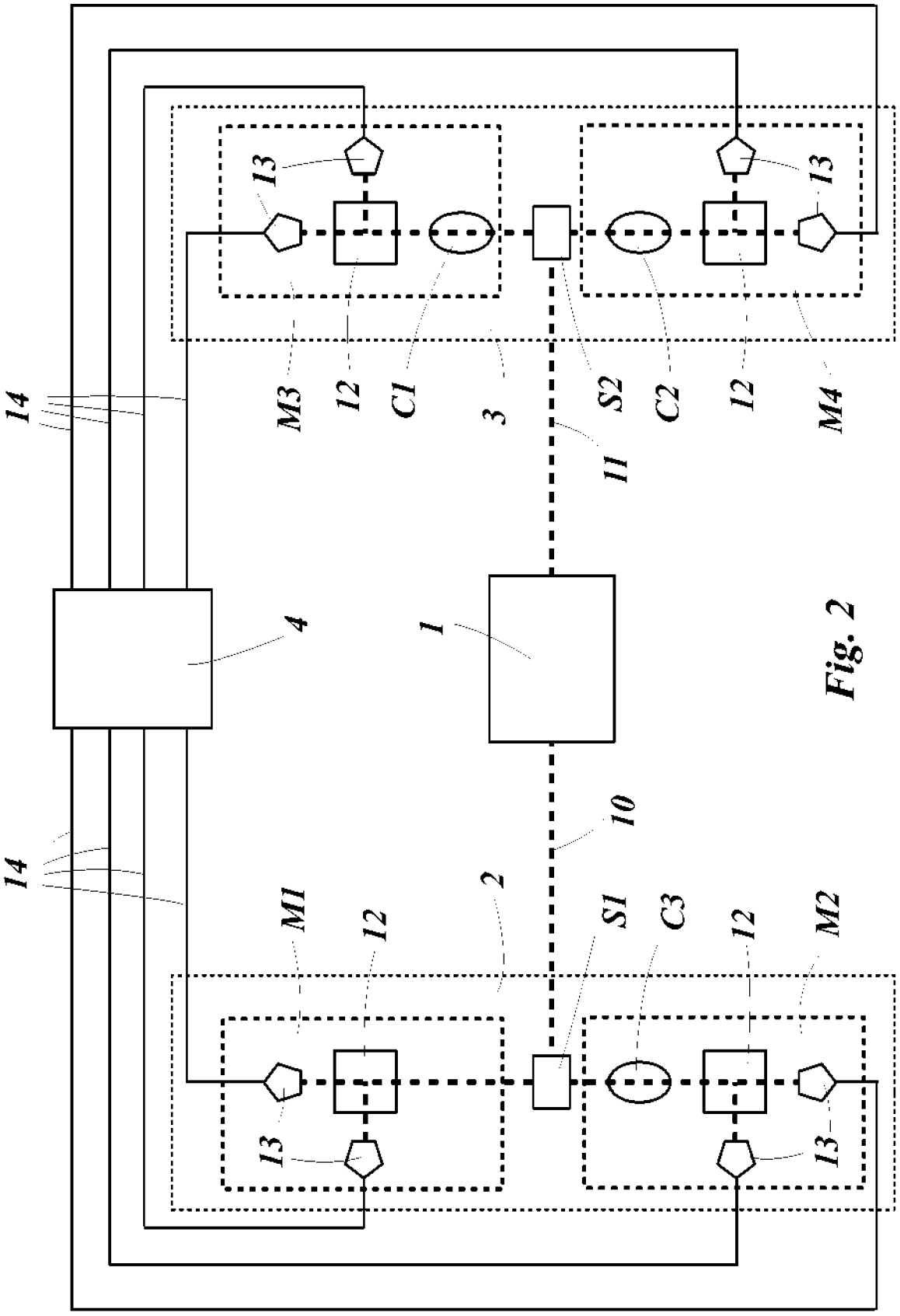


Fig. 2