(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 615 455**

(51) Int. CI.:

H04L 9/08 (2006.01)
G02F 1/39 (2006.01)
G02F 3/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.07.2004 PCT/IB2004/002344**

(87) Fecha y número de publicación internacional: **27.01.2005 WO05008952**

(96) Fecha de presentación y número de la solicitud europea: **21.07.2004 E 04744004 (5)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2016 EP 1649632**

(54) Título: **Generador de pares de fotones usando fluorescencia paramétrica**

(30) Prioridad:

22.07.2003 IT TO20030562

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.06.2017

(73) Titular/es:

LEONARDO S.P.A. (100.0%)
Piazza Monte Grappa 4
Roma, IT

(72) Inventor/es:

BOVINO, FABIO, ANTONIO

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Generador de pares de fotones usando fluorescencia paramétrica

Campo técnico

La presente invención se refiere a un generador de alta eficiencia para generar pares de fotones, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica. La presente invención también se refiere a un método de generación de pares de fotones de alta eficiencia, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica.

Técnica anterior

Tal como se sabe, una aplicación de procedimientos de fluorescencia paramétrica es la criptografía cuántica, que emplea principios de física cuántica para generar, transmitir y decodificar información a un nivel de seguridad extremadamente alto.

Tales procedimientos comprenden un número de etapas, que incluyen:

a) Crear un par de fotones entrelazados. Esto se realiza excitando un cristal no lineal birrefringente (por ejemplo beta-borato de bario) usando un haz láser, en particular un haz láser pulsado, para crear un par de fotones de la misma frecuencia y polarización opuesta (vertical/horizontal).

b) Transmisión cuántica aproximada. Los pares de fotones generados se transmiten mediante respectivos canales de transmisión privados (por ejemplo fibras ópticas o vacío) a un primer y segundo usuario.

c) Adquisición aleatoria. Cada usuario compara el único fotón recibido con una primera base de referencia (base A) y una segunda base de referencia (base B). Cada base de referencia comprende dos ejes perpendiculares, y las dos bases están separadas de manera angular mediante un ángulo predeterminado (por ejemplo 45°). La primera base (base A) y la segunda base (base B) se seleccionan aleatoriamente e independientemente por los dos usuarios. Como la polarización del fotón adquirido puede ser paralela a un primer y segundo eje de la base, la comparación da un resultado binario (0, 1).

d) Discusión pública. Por un canal público, los dos usuarios comparan el tipo de base (base A, base B) usado para realizar la comparación, pero sin intercambiar los resultados de la comparación entre el fotón y la base. Cuando las bases usadas para la correspondencia de la comparación, los resultados de la comparación por los dos usuarios son comparables. Los resultados de la comparación realizada por los dos usuarios en relación con el mismo par de fotones pero con bases de diferencia (bases A, B y B, A respectivamente) se descartan para reducir el conjunto de datos y formar un conjunto de datos “cribados” relacionados solamente con los resultados de la comparación realizada del mismo par de fotones con la misma base. Debido al principio cuántico mencionado anteriormente (cada par de fotones tiene polarizaciones opuestas), cada resultado (0, 1) adquirido por un primer usuario debe corresponder a un resultado (1, 0) opuesto adquirido por el segundo usuario con la misma base. Por consiguiente, los datos cribados adquiridos por el primer usuario deben ser opuestos (en el sentido binario) a los datos adquiridos por el segundo usuario.

e) Prueba de espionaje. Los dos usuarios intercambian subconjuntos de datos cribados por el canal público para garantizar que los datos están realmente correlacionados tal como se describió anteriormente. Si es así, se reconoce la seguridad absoluta de los datos recibidos. Si no es así, se indica el posible espionaje de la transmisión de datos por el canal privado. De hecho, cualquier intento de medir y/o copiar datos transmitidos por el canal privado afecta a la relación de polarización (vertical/horizontal) del par, proporcionando por tanto a los usuarios con una clara alerta de espionaje. Debido a la imposibilidad de clonar o extraer información de estado cuántico, la criptografía cuántica proporciona la generación de una clave de usuario de seguridad prácticamente máxima.

f) Corrección de errores. Ambos usuarios evalúan la seguridad de sus claves de código realizando una comprobación de paridad de ciertos subconjuntos de datos cribados por el canal público. Por motivos de seguridad, esto se realiza usando conjuntos muy limitados de datos.

En relación con la generación de pares de fotones entrelazados, esto se realiza habitualmente mediante un primer láser de potencia (por ejemplo de 10 W) que excita un segundo láser de potencia inferior (por ejemplo de 2,2 W), que a su vez genera un haz láser (bomba) que golpea el cristal no lineal birrefringente.

Un cristal birrefringente de tipo dos, sin embargo, no es particularmente eficaz en la generación de pares de fotones entrelazados, de modo que los generadores conocidos no son adecuados para la mayoría de aplicaciones prácticas.

La patente US 6.430.345 da a conocer un método y un dispositivo para generar una elección de fotones individuales o pares de fotones en un canal óptico. La generación de esta elección implica generar un estado de dos fotones que corresponde a un par de fotones y separar espacialmente el par de fotones mientras se conserva la correlación cuántico-mecánica, en el caso de que los fotones se emitan de manera colineal. Un fotón está acoplado en un canal óptico cada uno, conteniendo el un canal un interferómetro con diferencia de longitud de camino óptico variable, e

incluyendo el otro canal una sección de retraso óptico que tiene un camino óptico. Los canales se unen de nuevo espacialmente a través de un divisor de haz, y sucede un ajuste de la diferencia de longitud de camino óptico y de la longitud óptica de modo que la probabilidad K para coincidencias entre las salidas del divisor de haz es una elección de aproximadamente K=0 o aproximadamente K=1, o aproximadamente un valor intermedio predeterminado, correspondiendo K=0 a un par de fotones en uno de los canales de salida del divisor de haz, y correspondiendo K=1 a dos fotones individuales en ambos canales de salida del divisor de haz. Con esta generación de elección, puede implementarse un filtro o puerta de separación óptica para una elección de estados de un fotón o dos fotones, que puede usarse en criptografía cuántica y como un elemento básico de una máquina de computación cuántico-óptica.

Divulgación de la invención

Es un objeto de la presente invención proporcionar un dispositivo de alta eficiencia para generar pares de fotones, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica.

Según la presente invención, se proporciona un generador de alta eficiencia para generar pares de fotones, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica, que comprende: un cristal de tipo uno que recibe un haz de bomba láser en la entrada y que genera pares de fotones de polarización similar en la salida; un primer y un segundo rotador de polarización, que respectivamente recibe los fotones en cada par generado, realizando dichos rotadores de polarización cada uno una rotación de 45°; un divisor de haz, que refleja una polarización en sus entradas, y transmite la otra polarización; medios de transporte para dirigir los fotones desde el primer y segundo rotador de polarización a las entradas de dicho divisor de haz; comprendiendo el estado de los fotones en las salidas de dicho divisor de haz que comprende un estado de Bell $\Phi^{(-)}$ que puede usarse, por ejemplo, en un procedimiento de criptografía cuántica.

La presente invención también se refiere a un método de generación de pares de fotones de alta eficiencia, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica, que comprende las etapas de: dirigir un haz de bomba láser sobre un cristal de tipo uno para generar pares de fotones de polarización similar en la salida del cristal; dirigir los fotones en cada par generado respectivamente a un primer y segundo rotador de polarización, realizando cada uno una rotación de 45°; y dirigir los fotones desde el primer y segundo rotador de polarización a las entradas de un divisor de haz, que refleja una polarización y transmite la otra polarización; el estado de los fotones en las salidas de dicho divisor de haz que comprende un estado de Bell $\Phi^{(-)}$ que puede usarse, por ejemplo, en un procedimiento de criptografía cuántica.

Breve descripción del dibujo

La invención se describirá ahora con referencia al dibujo adjunto con referencia al dibujo adjunto que muestra, esquemáticamente, un generador, según las enseñanzas de la presente invención, para generar pares de fotones, y que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica.

Mejor modo de llevar a cabo la invención

El número 1 en el dibujo adjunto indica de manera global un generador de alta eficiencia para generar pares de fotones, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica, en particular un procedimiento de criptografía cuántica.

El generador 1 comprende un cristal de tipo uno 3, en particular un cristal de yodato de litio en forma de paralelepípedo de espesor constante L.

El cristal 3 está conectado en un primer lado 3a a una conocida fuente de haz láser 5 para generar un haz láser de excitación (haz de bomba) 12 que golpea el cristal 3 para producir pares de fotones f que se emiten desde un segundo lado 3b de cristal 3.

Los pares de fotones generados en la salida tienen la misma polarización (es decir ambos fotones tienen polarización vertical (e) u horizontal (o).

El haz láser 12 viaja en una dirección de propagación D recta que se cruza con el cristal 3.

Tal como se conoce, los fotones generados por la interacción entre el haz de bomba láser 12 y el cristal de tipo uno 3 viajan a lo largo de caminos situados dentro de una zona cónica simétrica con respecto a la dirección de propagación D. Más específicamente, la intersección de la zona de propagación cónica y un plano perpendicular a la dirección D define un anillo que representa la zona en el espacio en el que están situados de manera más probable los pares de fotones generados están situados.

El generador 1 comprende un primer y un segundo elemento reflectante 14a, 14b (de manera conveniente definido por espejos de metal plano) situados en lados opuestos de, y separados de manera equivalente con respecto a la dirección D.

El generador 1 también comprende un divisor de haz 17 situado a lo largo de la dirección de propagación D, sobre el

lado opuesto de los elementos reflectantes 14a, 14b al cristal 3.

Un primer y un segundo fotón en cada par generado viajan a lo largo de caminos a, b, que respectivamente comprenden:

- una primera parte a1, b1 que se extiende entre el segundo lado 3b del cristal 3 y el primer y segundo elemento reflectante 14a, 14b respectivamente; y
- una segunda parte a2, b2 que se extiende respectivamente desde el primer y el segundo elemento reflectante 14a, 14b hasta el divisor de haz 17, a través del que se extienden los caminos a y b.

El divisor de haz 17, por ejemplo un tipo cúbico, refleja una de las polarizaciones en la entrada (por ejemplo la polarización vertical), y permite que pase la otra polarización (por ejemplo la polarización horizontal).

Las caras de plano adyacentes primera y segunda 17a, 17b del divisor de haz 17 definen las entradas primera y segunda del divisor de haz 17, y están inclinadas a 45° con respecto a la dirección de propagación D: y las caras de plano tercera y cuarta 17c, 17d, opuestas a las caras 17a, 17b, definen las salidas primera y segunda del divisor de haz 17.

Según la presente invención, un primer y un segundo rotador de polarización 20a, 20b están situados a lo largo de los caminos a y b, entre el cristal 3 y el primer y segundo elemento reflectante 14a, 14b, y se cruzan con los fotones que viajan a lo largo de la primera y segunda parte de camino a1, b1. Los rotadores de polarización 20a, 20b (conocidos) realizan una rotación de 45° rotación, y están definidos por placas planas perpendiculares a la primera y segunda pate del camino a1, b1.

Los rotadores de polarización 20a, 20b están de manera conveniente dotados de unos iris 21a, 21b que están orientados hacia el cristal 3 y que tienen aberturas del orden de un milímetro.

En el uso real, el par de fotones generado por la interacción entre el haz láser 12 y el cristal tiene, por ejemplo, el siguiente estado:

$$|1\rangle_{ao}\ |1\rangle_{bo} \qquad (1)$$

Más específicamente, la notación anterior (mecánica cuántica estándar) significa que, en cada par, un primer fotón (notación |1) viaja a lo largo del camino a (subíndice a) y tiene polarización horizontal (subíndice o), y un segundo fotón (notación |1) viaja a lo largo del camino b (subíndice b) y también tiene polarización horizontal (subíndice o).

El estado del par de fotones que golpea los rotadores de polarización 20a, 20b es por tanto:

$$|1\rangle_{ao}\ |1\rangle_{bo} \qquad (2)$$

El estado de los fotones en la salida de los rotadores de polarización, por otro lado, se expresa mediante la notación:

$$\tfrac{1}{2}(|1\rangle_{ae}\ |1\rangle_{be} + |1\rangle_{ao}\ |1\rangle_{bo} - |1\rangle_{ae}\ |1\rangle_{bo} - |1\rangle_{ao}\ |1\rangle_{be}) \qquad (3)$$

Es decir, los pares de fotones en la salida de los rotadores de polarización pueden definirse mediante fotones verticales ($|1\rangle_{ae}\ |1\rangle_{be}$), mediante fotones horizontales ($|1\rangle_{ao}\ |1\rangle_{bo}$), o mediante un fotón vertical y un fotón horizontal ($|1\rangle_{ae}\ |1\rangle_{bo}$ y $|1\rangle_{ao}\ |1\rangle_{be}$).

Los fotones del estado de la notación (3) golpean espejos 14a, 14b, que no alteran su estado, y que los dirigen a entradas 17a, 17b respectivas del divisor de haz 17.

El estado de los fotones en las salidas 17c, 17d del divisor de haz 17 se expresa mediante la siguiente notación:

$$\tfrac{1}{2}(|1\rangle_{ao}\ |1\rangle_{bo} - |1\rangle_{ae}\ |1\rangle_{be}) - i/2(|1\rangle_{be}\ |1\rangle_{bo} + |1\rangle_{ae}\ |1\rangle_{ao}) \qquad (4)$$

En la que el primer término:

$$½(|1>_{ao}|1>_{bo} - |1>_{ae}|1>_{be}) \quad (5)$$

de la notación (4) representa un estado de Bell $\Phi^{(-)}$ que, como se sabe, puede usarse en un procedimiento de criptografía cuántica.

El segundo término:

$$-i/2(|1>_{be}|1>_{bo}+|1>_{ae}|1>_{ao}) \quad (6)$$

de la notación (4) muestra cómo los fotones en el par tienen polarizaciones opuestas (e y o), pero ambos viajan a lo largo del mismo camino (a o b), es decir no pueden detectarse simultáneamente mediante dos detectores (no mostrados) que se comunican con las salidas de los caminos respectivos. La notación (6) por tanto simplemente constituye un término de ruido, que puede descartarse fácilmente durante el procedimiento de criptografía cuántica.

La notación (4) puede, por tanto, reescribirse como:

$$\Phi^{(-)} + \text{ruido} \quad (7)$$

Aunque estén generados originalmente por un cristal de tipo uno, los fotones en la salida del divisor de haz 17 pueden por tanto ventajosamente usarse en un procedimiento de criptografía cuántica.

Se aplica lo mismo también sustancialmente cuando se comienza con dos fotones de polarización vertical, es decir:

$$|1>ae\ |1>be \quad (1a)$$

Como la eficacia de generación de un cristal de tipo uno es superior a la de un cristal de tipo dos en al menos un orden de magnitud, el uso de un cristal de tipo uno proporciona la obtención de un generador de alta eficiencia.

En comparación con generadores conocidos que emplean un cristal de tipo dos birrefringente, puede usarse por tanto un haz de bomba láser de potencia inferior, con sustancialmente la misma eficacia de generación de pares de fotones.

Las salidas primera y segunda del divisor de haz 17 pueden conectarse a los prismas primero y segundo 23a, 23b para dirigir los fotones en sus salidas a lo largo de caminos inclinados, con respecto a los prismas, en un ángulo α que depende de la longitud de onda de los fotones. Las salidas de los prismas 23a, 23b pueden por tanto suministrar diferentes canales de comunicación (por ejemplo diferentes fibras ópticas FO) que tienen entradas en diferentes posiciones angulares con respecto a los prismas 23a, 23b para recibir fotones de diferentes longitudes de onda. Así modificado, el generador 1 puede suministrar numerosos canales.

REIVINDICACIONES

1. Generador de alta eficiencia para generar pares de fotones, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica, que comprende:

- un cristal de tipo uno (3) que recibe un haz de bomba láser (12) en la entrada y que genera pares de fotones (f) de polarización similar (e, o) en la salida (3b):

- un primer y un segundo rotador de polarización (20a, 20b), que respectivamente reciben los fotones en cada par generado, dichos rotadores de polarización realizando cada uno una rotación de 45°;

- un divisor de haz (17), que refleja una polarización en sus entradas (17a, 17b), y transmite la otra polarización;

- medios de transporte (14a, 14b) para dirigir los fotones desde el primer y segundo rotador de polarización (20a, 20b) a las entradas (17a, 17b) de dicho divisor de haz (17);

comprendiendo el estado de los fotones en las salidas (17c, 17d) de dicho divisor de haz (17) un estado de Bell $\Phi^{(-)}$ que puede usarse, por ejemplo, en un procedimiento de criptografía cuántica.

2. Generador según la reivindicación 1, en el que dichos medios de transporte comprenden espejos primero y segundo (14a, 14b) para reflejar los fotones sobre dicho divisor de haz (17).

3. Generador según la reivindicación 1 ó 2, en el que iris primero y segundo (21a, 21b) están conectados a dichos rotadores de polarización (20a, 20b).

4. Generador según una cualquiera de las reivindicaciones anteriores, en el que el divisor de haz tiene salidas primera y segunda (17a, 17d) conectadas a unos prismas primero y segundo (23a, 23b) para dirigir los fotones en sus salidas a lo largo de caminos inclinados, con respecto a los prismas, en un ángulo α que depende de la longitud de onda de los fotones; suministrando las salidas de los prismas diferentes canales de comunicación que tienen entradas en diferentes posiciones angulares con respecto a los prismas para recibir fotones de diferentes longitudes de onda.

5. Método de generación de pares de fotones de alta eficiencia, que puede usarse en un procedimiento cuántico que emplea procedimientos de fluorescencia paramétrica, que comprende las etapas de:

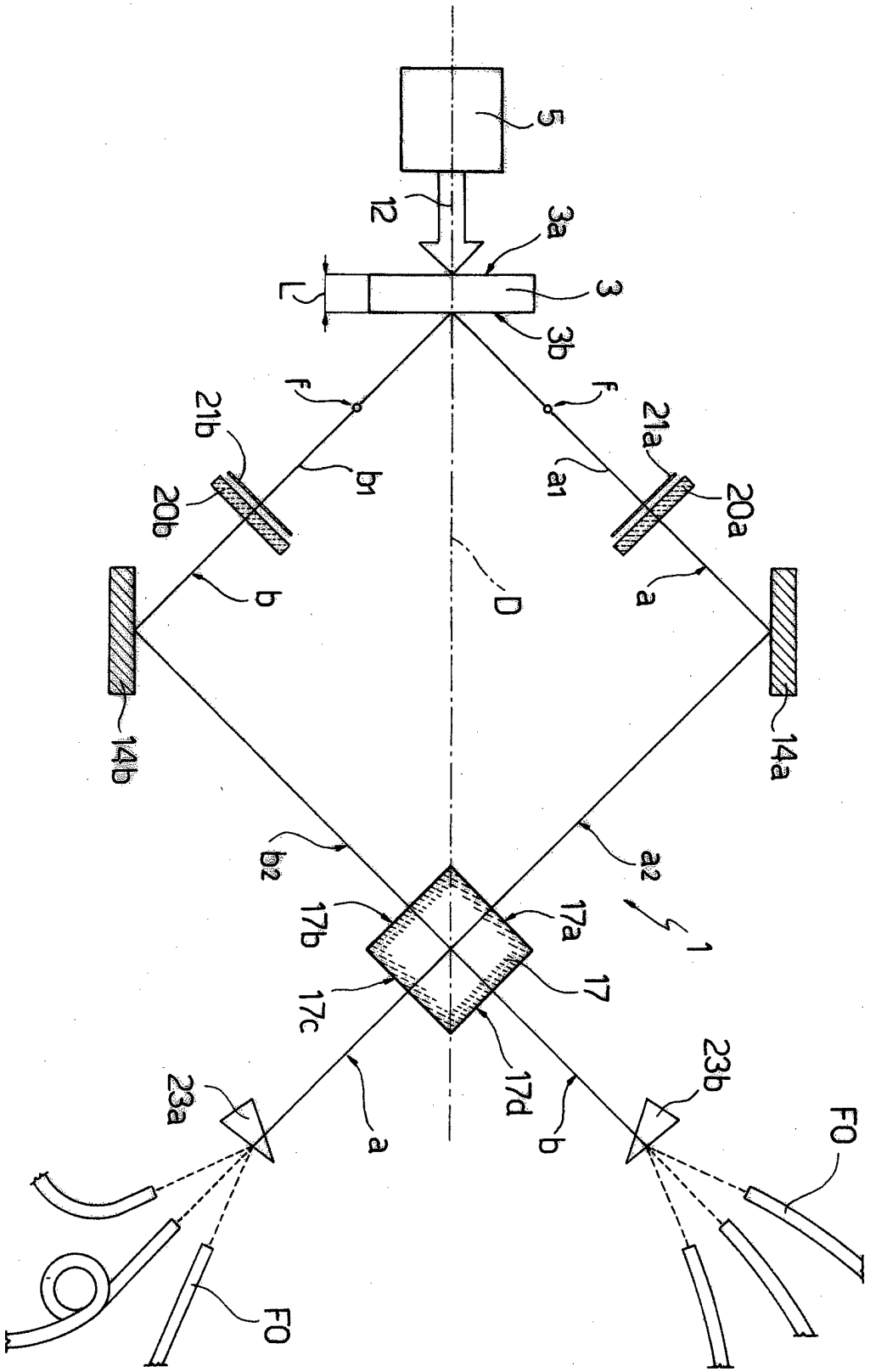
- dirigir un haz de bomba láser (12) sobre un cristal de tipo uno (3) para generar pares de fotones (f) de polarización similar (e, o) en la salida (3b) del cristal;

- dirigir los fotones en cada par generado respectivamente a un primer y segundo rotador de polarización (20a, 20b), realizando cada uno una rotación de 45°;

- dirigir (14a, 14b) los fotones desde el primer y segundo rotador de polarización (20a, 20b) a las entradas (17a, 17b) de un divisor de haz (17), que refleja una polarización y transmite la otra polarización;

comprendiendo el estado de los fotones en las salidas de dicho divisor de haz (17) un estado de Bell $\Phi^{(-)}$ que puede usarse, por ejemplo, en un procedimiento de criptografía cuántica.

6. Método según la reivindicación 5, en el que dicha etapa de dirigir los fotones desde el primer y segundo rotador de polarización (20a, 20b) comprende la etapa de reflejar (14a, 14b) los fotones sobre dicho divisor de haz (17).


5
12
3a
3
L
3b
F
f
21b
20b
b1
a1
21a
20a
b
D
a
14b
14a
b2
a2
17b
17a
1
17c
17
17d
23a
23b
a
b
FO
FO