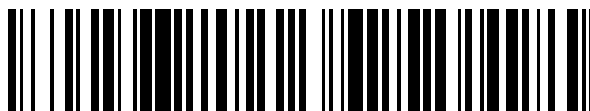


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 632 784**

51 Int. Cl.:

H04L 9/08

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **24.01.2014** **PCT/IB2014/058532**

87 Fecha y número de publicación internacional: **31.07.2014** **WO14115118**

96 Fecha de presentación y número de la solicitud europea: **24.01.2014** **E 14712035 (6)**

97 Fecha y número de publicación de la concesión europea: **12.04.2017** **EP 2949072**

54 Título: **Sistema de distribución de clave criptográfica cuántica que incluye dos dispositivos periféricos y una fuente óptica**

30 Prioridad:

25.01.2013 EP 13425014

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

15.09.2017

73 Titular/es:

**LEONARDO S.P.A (100.0%)
Piazza Monte Grappa 4
00195 Roma, IT**

72 Inventor/es:

BOVINO, FABIO, ANTONIO

74 Agente/Representante:

IGARTUA IRIZAR, Ismael

ES 2 632 784 T3

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

DESCRIPCIÓN

Sistema de distribución de clave criptográfica cuántica que incluye dos dispositivos periféricos y una fuente óptica

5 **Campo técnico**

La presente invención se refiere a un sistema de distribución de clave criptográfica cuántica que incluye dos dispositivos periféricos y una fuente óptica.

10 **Técnica anterior**

Tal como se conoce, actualmente hay numerosos protocolos de distribución de clave cuántica (QKD) disponibles que garantizan niveles particularmente altos de seguridad a nivel teórico.

15 Por ejemplo, se conoce el denominado protocolo BB84, que se describió por primera vez por C. H. Bennett y G. Brassard en "Quantum cryptography: Public key distribution and coin tossing", Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing, Bangalore, India, 10-12 de diciembre de 1984, págs. 175-179.

20 En la figura 1 se muestra otro ejemplo de un sistema de distribución de clave cuántica; en particular, la figura 1 muestra un sistema de distribución de clave cuántica (indicado mediante el número de referencia 1) del tipo independiente del dispositivo de medición (distribución de clave cuántica independiente del dispositivo de medición, MDI-QKD), que, por motivos de brevedad, se denominará a continuación en el presente documento sistema 1 de distribución.

25 El sistema 1 de distribución incluye un primer, un segundo y un tercer dispositivo de comunicaciones A, B y C.

El primer dispositivo de comunicaciones A comprende una primera fuente óptica 2, un primer modulador de polarización 4, un primer atenuador óptico variable 6 (VOA) y un primer generador de estados de polarización 8.

30 En uso, la primera fuente óptica 2 genera una pluralidad de pulsos ópticos, también denominados pulsos de primera fuente, que se reciben por el primer modulador de polarización 4, que a su vez se controla mediante el primer generador de estados de polarización 8. En la práctica, cada pulso de primera fuente emitido desde el primer modulador de polarización 4 tiene un estado de polarización que depende del primer modulador de polarización 4; además, cada pulso de primera fuente se atenúa entonces de una manera controlable mediante el primer atenuador óptico variable 6.

El segundo dispositivo de comunicaciones B comprende una segunda fuente óptica 12, un segundo modulador de polarización 14, un segundo atenuador óptico variable 16 (VOA) y un segundo generador de estados de polarización 18.

40 En uso, la segunda fuente óptica 12 genera una pluralidad de pulsos ópticos, también denominados pulsos de segunda fuente, que se reciben por el segundo modulador de polarización 14, que a su vez se controla mediante el segundo generador de estados de polarización 18. En la práctica, cada pulso de segunda fuente emitido desde el segundo modulador de polarización 14 tiene un estado de polarización que depende del segundo modulador de polarización 14; además, cada pulso de segunda fuente se atenúa entonces de una manera controlable mediante el segundo atenuador óptico variable 16.

50 Los pulsos de primera y segunda fuente emitidos desde el primer y segundo atenuadores ópticos variables 6 y 16, se reciben por el tercer dispositivo de comunicaciones C. Para ello, el primer y segundo dispositivos de comunicaciones A y B están conectados de manera óptica al tercer dispositivo de comunicaciones C mediante, respectivamente, un primer y un segundo canal de comunicaciones 20 y 22, también conocidos como canales cuánticos. Además, un canal público 30 está presente entre el primer, segundo y tercero dispositivos de comunicaciones A, B y C.

55 Los pulsos de primera y segunda fuente son pulsos coherentes débiles (WCP) y se generan respectivamente mediante la primera y segunda fuentes ópticas 2 y 12, que están formadas por diodos láser correspondientes.

60 En más detalle, el primer y segundo generadores de estados de polarización 8 y 18 funcionan de manera aleatoria y por tanto los pulsos de primera y segunda fuente se codifican por polarización de manera aleatoria. Más en particular, cada primer y segundo generador de estados de polarización 8 y 18 conmuta aleatoriamente entre un primer y un segundo sistema de bases de polarización del espacio de Hilbert, generalmente conocido como sistema de bases rectilíneas (por motivos de brevedad, también conocido como base rectilínea) y sistema de bases diagonales (por motivos de brevedad, también conocido como base diagonal). El sistema de bases rectilíneas está formado por el estado de polarización vertical $|V\rangle$ (también conocido como la base vertical) y el estado de polarización horizontal $|H\rangle$ (también conocido como la base horizontal), mientras que el sistema de bases diagonales está formado por los estados de polarización $+45^\circ$ y -45° , también conocido como la base $+45^\circ$

y la base -45° .

En la práctica, cada pulso óptico emitido por la primera y segunda fuentes ópticas 2 y 12 se modula por polarización en función del sistema de bases elegido por el generador de estados de polarización correspondiente, así como mediante el bit correspondiente generado por este último; además, el atenuador óptico variable correspondiente establece el número promedio de fotones de cada pulso óptico.

El primer y segundo canales de comunicaciones 20 y 22 están formados, por ejemplo, por tramos de fibra óptica correspondientes y son de tal manera que los pulsos de primera fuente y los pulsos de segunda fuente alcanzan el tercer dispositivo de comunicaciones C de una manera sustancialmente sincronizada.

El tercer dispositivo de comunicaciones C puede realizar una denominada medición de Bell con los fotones recibidos y anunciar públicamente los resultados de la medición. En otras palabras, el tercer dispositivo de comunicaciones C es un analizador de estado de Bell (BSA). Para ello, tal como se muestra en la figura 2, el tercer dispositivo de comunicaciones C comprende un primer, un segundo y un tercer divisor de haz óptico 31, 32 y 34.

El primer divisor de haz óptico 31 es del tipo sin polarización y también del denominado tipo 50/50; además, el primer divisor de haz óptico 31 tiene dos entradas y puede recibir pares de pulsos, estando cada par de pulsos formado por un pulso de primera fuente respectivo, recibido en una primera entrada, y un pulso de segunda fuente respectivo, recibido en una segunda entrada.

El primer divisor de haz óptico 32 tiene una primera y una segunda salida, que están conectadas de manera óptica a las entradas del segundo y tercer divisores de haz ópticos 32 y 34, respectivamente, que son del tipo de divisor de haz por polarización (PBS), que tienen, cada uno, un par de salidas respectivo. En particular, una primera y una segunda salida del segundo divisor de haz óptico 32 están conectadas de manera óptica a un primer y un segundo detector óptico 40 y 42, respectivamente, mientras que una primera y una segunda salida del tercer divisor de haz óptico 34 están conectadas de manera óptica a un tercer y un cuarto detector óptico 44 y 46, respectivamente. Cada primer, segundo, tercer y cuarto detector 40-46 óptico es un denominado detector de fotones individuales, tal como un fotodiodo de avalancha de fotones individuales (SPAD) por ejemplo.

Los estados de polarización, y en particular los ángulos correspondientes, se refieren a los ejes ópticos del segundo y tercer divisores de haz ópticos 32 y 34.

Habiendo mencionado esto, las medidas de Bell del tercer dispositivo de comunicaciones C pueden deberse a detecciones individuales de uno o más fotones que solo alcanzan uno de entre el primer, segundo, tercer y cuarto detectores 40-46 ópticos, en cuyo caso las medidas de Bell no pueden usarse, o a detecciones coincidentes, por dos de entre el primer, segundo, tercer y cuarto detectores 40-46 ópticos, en cuyo caso se usan las medidas de Bell. Con respecto a esto, las detecciones individuales no pueden usarse porque los tipos conocidos de detectores no pueden distinguir el número de fotones por unidad de tiempo; a la inversa, las detecciones coincidentes son útiles para los fines de implementación de protocolo, porque cada una de ellas indica una proyección de fotones sobre el subespacio simétrico o antisimétrico. Por estos motivos, excepto cuando se especifique lo contrario, el término "medición de Bell" implica generalmente una referencia a una detección coincidente; además, las detecciones coincidentes también se conocen como recuentos de coincidencia, lo que implica que las detecciones se refieren a una ventana de tiempo de observación, que puede tomarse como la unidad de tiempo.

Todavía más particularmente, el tercer dispositivo de comunicaciones C permite distinguir entre los estados de

Bell $|\Psi^-\rangle$ y $|\Psi^+\rangle$, es decir entre el estado de polarización singlete $(|eo\rangle - |oe\rangle)/\sqrt{2}$ y el estado de polarización

tripleto $(|eo\rangle + |oe\rangle)/\sqrt{2}$. En particular, un recuento de coincidencia cle2o o c2elo significa que la proyección tuvo lugar en el subespacio antisimétrico de singlete; además, un recuento de coincidencia clelo o c2e2o significa que la proyección tuvo lugar en el subespacio simétrico de tripleto. Para fines prácticos, el estado de Bell $|\Psi^+\rangle$ se detecta en el caso de un recuento de coincidencia que implica al primer y cuarto detectores ópticos 40 y 46, o al segundo y tercer detectores ópticos 42 y 44; a la inversa, el estado de Bell $|\Psi^-\rangle$ se detecta en el caso de un recuento de coincidencia que implica al primer y segundo detectores ópticos 40 y 42, o al tercer y cuarto detectores ópticos 44 y 46. Los resultados de las mediciones de Bell realizadas mediante el tercer dispositivo de comunicaciones C, dependiendo de los estados de polarización en la entrada del mismo dispositivo de comunicaciones, se indican en la tabla mostrada en la figura 3, que se refiere tanto al caso ideal de fotones entrelazados como al caso real de pulsos coherentes débiles.

En detalle, si el primer y segundo dispositivos de comunicaciones A y B transmiten polarizaciones ortogonales en la base rectilínea, el tercer dispositivo de comunicaciones C detecta el estado $|\Psi^-\rangle$ o $|\Psi^+\rangle$; en consecuencia, el primer y segundo dispositivos de comunicaciones A y B realizan una denominada "manipulación de bits" para

correlacionar sus bits, en asociación con las polarizaciones transmitidas. A la inversa, si el primer y segundo dispositivos de comunicaciones A y B usan la base diagonal, la operación de manipulación de bits solo se realiza si el tercer dispositivo de comunicaciones C detecta el estado $|\Psi^-\rangle$.

5 En más detalle, el primer y segundo dispositivos de comunicaciones A y B se comunican los sistemas de bases que usan entre sí sobre el canal público 30. A su vez, tal como se mencionó anteriormente, el tercer dispositivo de comunicaciones C comunica las medidas de Bell que ha obtenido al primer y segundo dispositivos de comunicaciones A y B sobre el canal público 30.

10 En el procedimiento de generación de la clave, el primer y segundo dispositivos de comunicaciones A y B desechan mediciones realizadas con señales codificadas con estados de polarización discordantes y solo mantienen mediciones realizadas con señales codificadas con estados de polarización concordantes; además, los bits conservados y obtenidos con la base rectilínea se usan para la generación de la clave, mientras que los bits conservados y obtenidos con la base diagonal se usan, por ejemplo, para evaluar la denominada tasa de error de bits cuántica (QBER) y la denominada ganancia de canal.

15 En la práctica, dado un conjunto de bits determinados mediante uno de entre el primer y segundo dispositivos de comunicaciones A y B, el conjunto de bits obtenidos con las bases rectilíneas y los mismos estados de polarización define una clave en bruto correspondiente, también conocida como "clave filtrada". Además, las claves en bruto generadas por el primer y segundo dispositivos de comunicaciones A y B deben ser una negación mutua entre sí, y por tanto iguales, aparte del procedimiento de manipulación de bits mencionado anteriormente, que es un procedimiento de negación lógica. Dado que se considera que este procedimiento de negación lógica está implícito, en el lenguaje técnico se dice que, de manera ideal, las claves en bruto generadas por el primer y segundo dispositivos de comunicaciones A y B deben coincidir.

20 En realidad, las dos claves en bruto no coinciden, debido a que el sistema 1 de distribución no es ideal, y también como resultado de posibles escuchas realizadas por un tercero no autorizado. Por tanto, tras haber generado las claves en bruto, el primer y segundo dispositivos de comunicaciones A y B realizan dos etapas adicionales, que dan como resultado la generación de una única clave criptográfica. Estas etapas adicionales del protocolo BB84 se conocen respectivamente como reconciliación de claves y amplificación de privacidad, y se describieron por primera vez por C. H. Bennett, F. Bessette, G. Brassard, L. Salvail y J. Smolin en "Experimental Quantum Cryptography", Journal of Cryptology, vol. 5, n.º 1, 1992, págs. 3-28.

25 En particular, en la etapa de reconciliación de claves (también conocida como la etapa de corrección de errores), el primer y segundo dispositivos de comunicaciones A y B corrigen los errores presentes en las dos claves en bruto, para generar una clave reconciliada, idéntica para ambos.

30 En detalle, en la etapa de reconciliación de claves, el primer y segundo dispositivos de comunicaciones A y B intercambian información útil para corregir los errores presentes en las claves en bruto sobre el canal público 30, minimizando la información transmitida con respecto a cada clave en bruto.

Al final de la etapa de reconciliación de información, el primer y segundo dispositivos de comunicaciones A y B tienen una misma clave reconciliada.

35 Posteriormente, en la etapa de amplificación de privacidad, y basándose en la clave reconciliada, el primer y segundo dispositivos de comunicaciones A y B generan una clave segura, que puede usarse al menos por el primer y segundo dispositivos de comunicaciones A y B, o por los usuarios respectivos, para iniciar una sesión de comunicación segura, por ejemplo a través del canal público 30. Entonces se repiten las operaciones descritas, por ejemplo periódicamente, para determinar nuevas claves seguras, para nuevas sesiones de comunicación.

En general, las etapas de reconciliación de claves y de amplificación de privacidad reducen la eficacia de la generación de clave segura y, en particular, la denominada tasa de generación de claves por pulso.

40 Con respecto a esto, habitualmente se adopta la notación $Q_{rect}^{n,m}$, $Q_{diag}^{n,m}$, $e_{rect}^{n,m}$ y $e_{diag}^{n,m}$ para indicar, respectivamente, las ganancias y las QBER de los estados de señal enviados por el primer y segundo dispositivos de comunicaciones A y B; según esta notación, n y m indican los números promedio de fotones transmitidos respectivamente por el primer y segundo dispositivos de comunicaciones A y B, mientras que rect y diag identifican respectivamente la base rectilínea y la base diagonal. Independientemente de la notación, en el caso de estados de polarización rectilínea mutuamente iguales, un error corresponde a la detección por el tercer dispositivo de comunicaciones C del estado $|\Psi^-\rangle$ o $|\Psi^+\rangle$. Además, de manera ideal, $e_{rect}^{n,m}$ es nulo para todos los valores de n y m; por tanto, de manera ideal, la etapa de corrección de errores no es necesaria.

En realidad, tal como se mencionó anteriormente, sí se producen errores, y por tanto se realizan las etapas de

corrección de errores y de amplificación de privacidad. En particular, las medidas obtenidas por el tercer dispositivo de comunicaciones C con bases diagonales se usan para determinar las características y el grado de las operaciones de amplificación de privacidad. En este caso, un error corresponde a la proyección en el estado de singlete, si el primer y segundo dispositivos de comunicaciones A y B han generado el mismo estado de polarización, o en el estado de triplete, si el primer y segundo dispositivos de comunicaciones A y B han generado estados de polarización ortogonales. De manera ideal, se encuentra $e_{diag}^{1,1} = 0$, porque, cuando dos fotones idénticos alcanzan el primer divisor de haz óptico 31, el efecto de Hong-Ou-Mandel garantiza que ambos fotones salen por la misma salida.

A la vista de lo anterior, la tasa de generación de claves es, de manera ideal, igual a $Q_{rect}^{1,1}$, en el límite asintótico de una clave infinitamente larga. En realidad, considerando las situaciones no ideales, la tasa de generación de claves es igual a:

$$R = Q_{rect}^{1,1} \left[1 - H(e_{diag}^{1,1}) \right] - Q_{rect} f(E_{rect}) H(E_{rect})$$

donde Q_{rect} y E_{rect} indican respectivamente la ganancia y la QBER cuando el primer y segundo dispositivos de comunicaciones A y B usan ambos la base rectilínea, concretamente:

$$Q_{rect} = \sum_{n,m} Q_{rect}^{n,m}$$

y

$$E_{rect} = \sum_{n,m} Q_{rect}^{n,m} e_{rect}^{n,m} / Q_{rect}$$

mientras que $f(E_{rect}) > 1$ es una función que tiene en cuenta la ineficacia del procedimiento de corrección de errores; finalmente, $H(x) = -x \log(x) - (1-x) \log(1-x)$, que es la función de entropía de Shannon binaria. También se ha supuesto de manera implícita que el denominado método de estados señuelo puede usarse para determinar los valores de ganancia $Q_{rect}^{1,1}$ y de error $e_{diag}^{1,1}$.

Con respecto a esto, a continuación en el presente documento se supone que el primer, segundo, tercer y cuarto detectores 40-46 ópticos tienen el mismo nivel de ruido, o más bien que tienen el mismo recuento de oscuros y la misma eficacia de detección. También se supone que las cuentas de oscuros son independientes de los pulsos ópticos recibidos y también que el primer y segundo canales de comunicaciones 20 y 22 están formados por tramos de fibra óptica correspondientes con atenuación, a la longitud de onda de los pulsos de primera y segunda fuente, de 0,2 dB/km. También se supone lo siguiente:

- $f(E_{rect}) = 1,16$;
- tasa de error intrínseca debida a desalineación e inestabilidad del sistema de distribución igual al 1,5%;
- eficacia de detección de los detectores ópticos y transmitancia de componentes ópticos igual al 15%;
- tasa de recuento de fondo, incluyendo la denominada cuenta de oscuros y contribuciones debidas a la denominada luz parásita, igual a $6,02 \cdot 10^{-6}$.

Habiendo dicho esto, la figura 4 muestra, con una línea discontinua, el límite inferior de la tasa de generación de claves R que caracteriza al sistema 1 de distribución en el caso de pulsos coherentes débiles. Además, la figura 4 muestra, con una línea continua, el límite inferior de la tasa de generación de claves R que caracteriza al sistema 1 de distribución en el caso en el que el primer y segundo dispositivos de comunicaciones A y B generan pares de estados entrelazados de dos fotones, tal como en el caso, por ejemplo, en el que los pares de fotones se generan mediante conversión paramétrica descendente espontánea (SPDC) de una fuente interpuesta entre el primer y segundo dispositivos de comunicaciones A y B. En la práctica, las fuentes de SPDC todavía están tecnológicamente limitadas en la actualidad, y por tanto el valor efectivo de la tasa de generación de claves R es inferior al mostrado por la línea continua en la figura 4.

Con fines prácticos, la figura 4 muestra que la tasa de generación de claves R que puede obtenerse en el caso de pulsos coherentes débiles es comparable a la obtenida mediante la generación de estados entrelazados. Además, el sistema 1 de distribución puede tolerar altas pérdidas ópticas, del orden de 40 dB (correspondiente a una distancia de aproximadamente 200 km) cuando el tercer dispositivo de comunicaciones C está colocado en

el centro entre el primer y segundo dispositivos de comunicaciones A y B.

Basándose en lo que se ha descrito, resulta evidente cómo la implementación práctica de un esquema de distribución de clave criptográfica conlleva determinadas limitaciones con respecto a la teoría, incluso en ausencia de escuchas. En particular, el hecho de que las señales emitidas por las fuentes no sean estados de fotón individual, sino pulsos coherentes débiles con un número promedio de fotones normalmente superior o igual a 0,1, conlleva un riesgo para la seguridad del protocolo y una reducción en la tasa de generación de claves R y la distancia útil para la generación de clave, prevista como la suma de las distancias del primer y segundo canales de comunicaciones 20 y 22. De hecho, dado que algunos pulsos contienen múltiples fotones con un mismo estado de polarización, es posible que un tercero que desee interceptar la clave criptográfica pueda actuar sin las limitaciones impuestas por el teorema de la no clonación, ya que algunos pulsos contienen múltiples copias de un mismo elemento de información. En particular, un tercero, conocido en el lenguaje técnico como Eve, puede implementar un denominado ataque por división del número de fotones (PNS) en los pulsos de múltiples fotones. Por tanto, Eve puede bloquear los pulsos de fotón individual y dividir los pulsos de múltiples fotones, manteniendo una copia para sí misma y enviando la parte restante al tercer dispositivo de comunicaciones C. Este ataque permite a Eve obtener toda la información referente a la parte de la clave generada con pulsos de múltiples fotones, sin introducir ninguna alteración de la polarización.

Además, tal como se mencionó anteriormente, causas adicionales que dan como resultado una reducción en la tasa de generación de claves R o, para la misma tasa de generación de claves R, en la distancia máxima alcanzable, se originan a partir de las situaciones no ideales de los detectores ópticos, así como de la diferencia que existe entre la alineación entre el primer y tercer dispositivos de comunicaciones A y C, y la alineación entre el segundo y tercer dispositivos de comunicaciones B y C.

El razonamiento anterior referente a la reducción en la tasa de generación de claves R también se aplica a sistemas de distribución de clave criptográfica en los que los pulsos ópticos se codifican en fase en lugar de codificarse en polarización, tal como se describe, por ejemplo, en Physical Review A 86, 062319 (2012), "Alternative schemes for measurement-device-independent quantum key distribution", de Xiongfeng Ma *et al.*, y en Physical Review Letters 108, 130503 (2012), "Measurement-Device-Independent Quantum Key Distribution", de Hoi-Kwong Lo *et al.*, o en sistemas que prevén la conversión de la codificación en fase a la codificación en polarización.

El documento de F. Bovino *et al.*, "Practical Quantum Cryptography: the Q-KeyMaker", 13 de abril de 2011, recuperado de Internet en <http://arxiv.org/abs/1104.2475> da a conocer una red de distribución de clave cuántica en la que un servidor está conectado de manera controlable a uno de una pluralidad de clientes. Un documento adicional que trata de la distribución de clave cuántica es el de F. Bovino *et al.*, "Quantum Correlation Bounds for Quantum Information Experiments Optimization: the Wigner Inequality Case", del 15 de febrero de 2008, recuperado de Internet en <http://arxiv.org/abs/0802.2256>.

Descripción de la invención

Por tanto, el objeto de la presente invención es proporcionar un sistema de distribución de clave criptográfica cuántica que supere al menos parcialmente las limitaciones de la técnica conocida.

Según la presente invención, se proporcionan un sistema y un método de distribución de clave criptográfica tal como se definen en las reivindicaciones adjuntas.

Breve descripción de los dibujos

Para entender mejor la invención, ahora se describirán algunas realizaciones, meramente a modo de ejemplo no limitativo, y con referencia a los dibujos adjuntos, en los que:

- la figura 1 muestra un diagrama de bloques de un sistema de distribución de clave criptográfica de tipo conocido;
- la figura 2 muestra un diagrama de bloques de un componente del sistema de distribución de clave criptográfica mostrado en la figura 1;
- la figura 3 muestra una tabla que indica las probabilidades de dos tipos diferentes de recuento de coincidencia ($|\Psi^-\rangle$ y $|\Psi^+\rangle$), basándose en dos tipos diferentes de estado de entrada (estados entrelazados o pulsos coherentes débiles), así como los estados de polarización de dos señales procedentes de dos dispositivos de comunicaciones;
- la figura 4 muestra la tendencia de la tasa de generación de claves que caracteriza al sistema de distribución mostrado en la figura 1, en función de la distancia, y en los casos de i) pulsos coherentes débiles y ii) estados entrelazados de dos fotones;
- la figura 5 muestra un diagrama de bloques del presente sistema de distribución de clave criptográfica;
- la figura 6 muestra cualitativamente una sucesión de pulsos ópticos de un primer y un segundo tipo, según se reciben en el tiempo por un componente del sistema mostrado en la figura 5;

- la figura 7 muestra una tabla que indica las detecciones realizadas de manera ideal dentro del sistema mostrado en la figura 5, a medida que varían los desplazamientos de fase introducidos por el sistema;
- la figura 8 muestra la tendencia de una estimación de un valor óptimo para un número promedio de fotones μ , en función de la probabilidad e_{detector} de detección errónea dentro del sistema mostrado en la figura 5; y
- las figuras 9-12 muestran tendencias de cantidades características del sistema mostrado en la figura 5.

Mejor modo de llevar a cabo la invención

La figura 5 muestra un sistema de distribución de clave criptográfica, que se denominará a continuación en el presente documento sistema criptográfico 49, que comprende un primer, un segundo y un tercer dispositivo de comunicaciones 50, 52 y 54, que se denominarán a continuación en el presente documento respectivamente primer y segundo dispositivos periféricos 50 y 52 y dispositivo central 54.

El dispositivo central 54 comprende una primera unidad de procesamiento 60, una fuente óptica 62, una unidad de sincronización 64, un circulador óptico 66, una tarjeta de marca de tiempo 68 y una primera y una segunda unidad de detección óptica 70 y 72. Además, el dispositivo central 54 comprende un primer, un segundo y un tercer divisor de haz óptico 80, 82 y 84.

En detalle, la unidad de sincronización 64 está conectada a la fuente óptica 62, a la que le suministra una señal de control eléctrica, para controlar la generación a lo largo del tiempo de pulsos ópticos por la fuente óptica 62, que es una fuente de láser de tipo conocido y genera pulsos coherentes débiles en su salida óptica. Además, la unidad de sincronización 64 también está conectada eléctricamente a la primera unidad de procesamiento 60 y proporciona a esta última una señal indicativa de la señal de control eléctrica.

El circulador óptico 66 tiene tres puertos. El primer puerto está conectado a la salida de la fuente óptica 62, para recibir los pulsos ópticos generados por esta última. El segundo puerto está conectado a un primer puerto del primer divisor de haz óptico 80. Finalmente, el tercer puerto está conectado a una primera entrada de la primera unidad de detección óptica 70. Debe observarse que, en la presente descripción, cuando se hace referencia a un enlace óptico, se pretende generalmente que este enlace esté formado por una longitud correspondiente de fibra óptica, excepto cuando se especifique lo contrario. Además, excepto cuando se especifique lo contrario, se pretende que las partes de fibra óptica empleadas sean de tipo conocido y del tipo que mantienen la polarización. En cualquier caso, son posibles unas realizaciones en las que al menos parte de los enlaces ópticos que forman el sistema criptográfico 49 son de tipos diferentes, tales como enlaces por espacio libre por ejemplo.

En más detalle, cada primera y segunda unidad de detección óptica 70 y 72 es de tipo conocido y está formada por un denominado módulo contador de fotones individuales (SCPM) que incluye, por ejemplo, un fotodiodo de avalancha respectivo que funciona en modo de Geiger. Además, cada primera y segunda unidad de detección óptica 70 y 72 tiene una primera entrada, de un tipo óptico, y una segunda entrada, de un tipo eléctrico, estando la segunda entrada conectada a la unidad de sincronización 64, para recibir una señal desde esta última indicativa de la señal de control eléctrica. Además, mientras que, tal como se mencionó, la primera entrada de la primera unidad de detección óptica 70 está conectada de manera óptica al tercer puerto del circulador óptico 66, la primera entrada de la segunda unidad de detección óptica 72 está conectada a un segundo puerto del primer divisor de haz óptico 80. Además, cada primera y segunda unidad de detección óptica 70 y 72 tiene una salida respectiva, de un tipo eléctrico, que está conectada a una entrada correspondiente de la tarjeta de marca de tiempo 68; con respecto a esto, la tarjeta de marca de tiempo 68 tiene una entrada adicional, conectada a una salida eléctrica de la fuente óptica 62, y está configurada además para comunicarse eléctricamente de una manera bidireccional con la primera unidad de procesamiento 60. En particular, la tarjeta de marca de tiempo 68 recibe una señal eléctrica de la fuente óptica 62 indicativa de los tiempos de generación de los pulsos ópticos y comunica esta información a la primera unidad de procesamiento 60.

En más detalle, el primer divisor de haz óptico 80 es un dispositivo de cuatro puertos y por tanto, además del primer y segundo puertos ya mencionados, comprende un tercer y un cuarto puerto. Además, el primer divisor de haz óptico 80 es del tipo 50/50 y por tanto cada pulso óptico que se recibe en el primer puerto se divide en partes iguales en el tercer y cuarto puertos, sin alterar su polarización. En otras palabras, el primer divisor de haz óptico 80 es del tipo sin polarización.

Cada segundo y tercer divisor de haz óptico 84 y 82 es un divisor de haz de polarización de tres puertos. En particular, un primer puerto del segundo divisor de haz óptico 82 está conectado de manera óptica al tercer puerto del primer divisor de haz óptico 80, mientras que un primer puerto del tercer divisor de haz óptico 84 está conectado de manera óptica al cuarto puerto del primer divisor de haz óptico 80.

En más detalle, un segundo puerto del segundo divisor de haz óptico 82 está conectado de manera óptica, a través de un primer tramo de fibra óptica 90, al primer dispositivo periférico 50, mientras que un segundo puerto del tercer divisor de haz óptico 84 está conectado de manera óptica, a través de un segundo tramo de fibra óptica 92, al segundo dispositivo periférico 52. Además, los terceros puertos del segundo y tercer divisores de haz óptico 82 y 84 están conectados de manera óptica entre sí.

El primer dispositivo periférico 50 comprende un primer divisor óptico variable 94, un primer modulador de fase 96, un primer espejo de Faraday 98, un primer fotodiodo de avalancha 100, un primer generador de pulsos arbitrarios 102 (APG) y una segunda unidad de procesamiento 104.

En detalle, el primer divisor óptico variable 94 funciona como atenuador variable y tiene un primer, un segundo y un tercer puerto de un tipo óptico, estando el primer puerto conectado al primer tramo de fibra óptica 90, que tiene una longitud igual a L_A . Además, el primer divisor óptico variable 94 tiene una entrada de control, de un tipo eléctrico, en la que recibe una primera señal de control de fase, generada por el primer generador de pulsos arbitrarios 102 en una primera salida respectiva de tipo eléctrico.

El primer modulador de fase 96 tiene un primer y un segundo puerto, estando el primer puerto conectado al segundo puerto del primer divisor óptico variable 94. En vez de eso, el segundo puerto está conectado al primer espejo de Faraday 98. Además, el primer modulador de fase 96 tiene una entrada de control respectiva, de un tipo eléctrico, en la que recibe una primera señal de control de amplitud, generada por el primer generador de pulsos arbitrarios 102 en una segunda salida respectiva de un tipo eléctrico.

El primer fotodiodo de avalancha 100 tiene una entrada óptica, que está conectada al tercer puerto del primer divisor óptico variable 94. Además, el primer fotodiodo de avalancha 100 tiene una salida eléctrica, que está conectada a una primera entrada eléctrica del primer generador de pulsos arbitrarios 102.

Con respecto al primer generador de pulsos arbitrarios 102, este también tiene una segunda entrada eléctrica, que está conectada eléctricamente a la segunda unidad de procesamiento 104.

El segundo dispositivo periférico 52 comprende un segundo divisor óptico variable 114, un segundo modulador de fase 116, un segundo espejo de Faraday 118, un segundo fotodiodo de avalancha 120, un segundo generador de pulsos arbitrarios 122 y una tercera unidad de procesamiento 124.

En detalle, el segundo divisor óptico variable 114 tiene un primer, un segundo y un tercer puerto, de un tipo óptico, estando el primer puerto conectado al segundo tramo de fibra óptica 92, que tiene una longitud igual a L_B . Además, el segundo divisor óptico variable 114 tiene una entrada de control, de un tipo eléctrico, en la que recibe una segunda señal de control de fase, generada por el segundo generador de pulsos arbitrarios 122 en una primera salida respectiva de un tipo eléctrico.

El segundo modulador de fase 116 tiene un primer y un segundo puerto, estando el primer puerto conectado al segundo puerto del segundo divisor óptico variable 114. En vez de eso, el segundo puerto está conectado al segundo espejo de Faraday 118. Además, el segundo modulador de fase 116 tiene una entrada de control respectiva, de un tipo eléctrico, en la que recibe una segunda señal de control de amplitud, generada por el segundo generador de pulsos arbitrarios 122 en una segunda salida respectiva de un tipo eléctrico.

El segundo fotodiodo de avalancha 120 tiene una entrada óptica, que está conectada al tercer puerto del segundo divisor óptico variable 114. Además, el segundo fotodiodo de avalancha 120 tiene una salida eléctrica, que está conectada a una primera entrada, de un tipo eléctrico, del segundo generador de pulsos arbitrarios 122.

Con respecto al segundo generador de pulsos arbitrarios 122, este también tiene una segunda entrada eléctrica, que está conectada eléctricamente a la tercera unidad de procesamiento 124.

En cuanto al funcionamiento, dado un pulso óptico que llega al primer puerto del primer divisor de haz óptico 80 con una primera polarización, la mitad del mismo alcanza el primer dispositivo periférico 50, tras haber atravesado el segundo divisor de haz óptico 82 y el primer tramo de fibra óptica 90, mientras que una segunda mitad del mismo alcanza el segundo dispositivo periférico 52, tras haber atravesado el tercer divisor de haz óptico 84 y el segundo tramo de fibra óptica 92. Por motivos de claridad, a continuación en el presente documento la primera y segunda mitades de pulso óptico mencionadas anteriormente se denominarán respectivamente primer y segundo subpulsos ópticos. En la práctica, el primer y segundo subpulsos ópticos se generan respectivamente en el tercer y cuarto puertos del primer divisor de haz óptico 80. Además, se supone, sin ninguna pérdida de generalidad, que la primera polarización mencionada anteriormente es una denominada polarización horizontal.

Dentro del primer dispositivo periférico 50, el primer subpulso óptico pasa a través del primer divisor óptico variable 94 y el primer modulador de fase 96 una primera vez, manteniéndose este último inactivo durante el pase, hasta que incide sobre el primer espejo de Faraday 98, que tiene una matriz de transferencia ortogonal y lo refleja, invirtiendo la polarización. El primer subpulso pasa entonces una segunda vez, en sentido opuesto, a través del primer modulador de fase 96, que también se mantiene inactivo durante este pase adicional, y el primer divisor óptico variable 94.

Tras el segundo pase a través del primer divisor óptico variable 94, parte del primer subpulso óptico, que por

motivos de claridad todavía se denominará primer subpulso óptico, se dirige de nuevo hacia el primer tramo de fibra óptica 90, mientras que una parte se dirige hacia el primer fotodiodo de avalancha 100. En consecuencia, el primer fotodiodo de avalancha 100 envía una señal eléctrica al primer generador de pulsos arbitrarios 102 indicativa del tiempo de tránsito del primer subpulso óptico a través del primer divisor óptico variable 94, y por tanto el tiempo en el primer dispositivo periférico 50, así como la potencia del primer subpulso óptico, o más bien la potencia de la señal enviada desde el dispositivo central 54.

Después de eso, el primer subpulso óptico pasa de nuevo a través del primer tramo de fibra óptica 90, hasta que incide sobre el segundo puerto del segundo divisor de haz óptico 82, con polarización vertical, debido a la polarización realizada por el primer espejo de Faraday 98. Por tanto, el primer subpulso óptico se refleja por el segundo divisor de haz óptico 82 y se dirige al tercer puerto del segundo divisor de haz óptico 82, y por tanto al tercer puerto del tercer divisor de haz óptico 84.

Después de eso, el primer subpulso óptico se refleja por el tercer divisor de haz óptico 84, que lo dirige hacia su segundo puerto. Por tanto, el primer subpulso óptico pasa a través del segundo tramo de fibra óptica 92 y alcanza el segundo dispositivo periférico 52.

Dentro del segundo dispositivo periférico 52, el primer subpulso óptico pasa a través del segundo divisor óptico variable 114 y el segundo modulador de fase 116 una primera vez, hasta que incide sobre el segundo espejo de Faraday 118, que lo refleja, invirtiendo la polarización. Entonces, el primer subpulso pasa una segunda vez, en sentido opuesto, a través del segundo modulador de fase 116 y el segundo divisor óptico variable 114.

Tras el segundo pase a través del segundo divisor óptico variable 114, parte del primer subpulso óptico, que por motivos de claridad todavía se denominará primer subpulso óptico, se dirige de nuevo hacia el segundo tramo de fibra óptica 92, mientras que una parte se dirige hacia el segundo fotodiodo de avalancha 120. En consecuencia, el segundo fotodiodo de avalancha 120 envía una señal eléctrica al segundo generador de pulsos arbitrarios 122 indicativa del tiempo de tránsito del primer subpulso óptico a través del segundo divisor óptico variable 114, y por tanto el tiempo en el segundo dispositivo periférico 52, así como la potencia del primer subpulso óptico, o más bien la potencia de la señal enviada desde el primer dispositivo periférico 50.

En más detalle, la tercera unidad de procesamiento 124 controla el segundo generador de pulsos arbitrarios 122 de una manera tal que controla el segundo modulador de fase 116 de modo que el doble pase del primer subpulso óptico a través del mismo da como resultado una modulación de fase, es decir codificación de fase, del primer subpulso óptico. Además, el segundo divisor óptico variable 114 atenúa el primer subpulso óptico con una atenuación, prevista como la diferencia entre la potencia con la que incide el primer pulso óptico sobre el segundo dispositivo periférico 52 y la potencia con la que se redirige por este último hacia el segundo tramo de fibra óptica 92, que es mayor que la atenuación introducida por el primer divisor óptico variable 94 en el primer pulso óptico.

Después de eso, el primer subpulso óptico pasa de nuevo a través del segundo tramo de fibra óptica 92, hasta que incide sobre el segundo puerto del tercer divisor de haz óptico 84.

Dado que el primer subpulso óptico, debido a la inversión de polarización realizada por el segundo espejo de Faraday 118, incide sobre el segundo puerto del tercer divisor de haz óptico 84 con polarización ordinaria, pasa a través del tercer divisor de haz óptico 84 y alcanza el cuarto puerto del primer divisor de haz óptico 80.

En vez de eso, con respecto al segundo subpulso óptico mencionado anteriormente generado en el cuarto puerto del primer divisor de haz óptico 80, éste atraviesa una trayectoria óptica idéntica a la seguida por el primer pulso óptico, pero en sentido opuesto.

En más detalle, dentro del segundo dispositivo periférico 52, el segundo subpulso óptico pasa a través del segundo divisor óptico variable 114 y el segundo modulador de fase 116 una primera vez, manteniéndose este último inactivo durante el pase, hasta que incide sobre el segundo espejo de Faraday 118, que lo refleja, invirtiendo la polarización. Entonces, el segundo subpulso pasa una segunda vez, en sentido opuesto, a través del segundo modulador de fase 116, que también se mantiene inactivo durante este pase adicional, y el segundo divisor óptico variable 114.

Tras el segundo pase a través del segundo divisor óptico variable 114, parte del segundo subpulso óptico, que por motivos de claridad todavía se denominará segundo subpulso óptico, se dirige de nuevo hacia el segundo tramo de fibra óptica 92, mientras que una segunda parte se dirige hacia el segundo fotodiodo de avalancha 120. En consecuencia, el segundo fotodiodo de avalancha 120 envía una señal eléctrica al segundo generador de pulsos arbitrarios 122 indicativa del tiempo de tránsito del segundo subpulso óptico a través del segundo divisor óptico variable 114, y por tanto el tiempo en el segundo dispositivo periférico 52, así como la potencia del segundo subpulso óptico, o más bien la potencia de la señal enviada desde el dispositivo central 54.

Después de eso, el segundo subpulso óptico pasa de nuevo a través del segundo tramo de fibra óptica 92, hasta

que impacta en el segundo puerto del tercer divisor de haz óptico 84, con polarización extraordinaria, debido a la inversión de polarización realizada por el segundo espejo de Faraday 118. Por tanto, el segundo subpulso óptico se refleja por el tercer divisor de haz óptico 84 y se dirige hacia el tercer puerto del tercer divisor de haz óptico 84, y por tanto hacia el tercer puerto del segundo divisor de haz óptico 82.

5

Entonces, se refleja el segundo subpulso óptico por el segundo divisor de haz óptico 82, que lo dirige hacia su segundo puerto. Por tanto, el segundo subpulso óptico pasa a través del primer tramo de fibra óptica 90 y alcanza el primer dispositivo periférico 50.

10

Dentro del primer dispositivo periférico 50, el segundo subpulso óptico pasa a través del primer divisor óptico variable 94 y el primer modulador de fase 96 una primera vez, hasta que incide sobre el primer espejo de Faraday 98, que lo refleja, invirtiendo la polarización.

15

Entonces, el segundo subpulso óptico pasa una segunda vez, en sentido opuesto, a través del primer modulador de fase 96 y el primer divisor óptico variable 94. En particular, tras el segundo pase a través del primer divisor óptico variable 94, parte del segundo subpulso óptico, que por motivos de claridad todavía se denominará segundo subpulso óptico, se dirige de nuevo hacia el primer tramo de fibra óptica 90, mientras que una parte se dirige hacia el primer fotodiodo de avalancha 100. En consecuencia, el primer fotodiodo de avalancha 100 envía una señal eléctrica al primer generador de pulsos arbitrarios 102 indicativa del tiempo de tránsito del segundo subpulso óptico a través del primer divisor óptico variable 94, y por tanto el tiempo en el primer dispositivo periférico 50, así como la potencia del segundo subpulso óptico, o más bien la potencia de la señal enviada desde el segundo dispositivo periférico 52.

20

25

En más detalle, la segunda unidad de procesamiento 104 controla el primer generador de pulsos arbitrarios 102 de una manera tal que controla el primer modulador de fase 96 de modo que el doble pase del segundo subpulso óptico a través del mismo da como resultado una modulación de fase, es decir codificación de fase, del segundo subpulso óptico. Además, el primer divisor óptico variable 94 atenúa el segundo subpulso óptico con una atenuación, prevista como la diferencia entre la potencia con la que el segundo pulso óptico incide sobre el primer dispositivo periférico 50 y la potencia con la que se redirige por este último hacia el primer tramo de fibra óptica 90, que es mayor que la atenuación introducida por el segundo divisor óptico variable 114 en el segundo pulso óptico.

30

Después de eso, el segundo subpulso óptico pasa de nuevo a través del primer tramo de fibra óptica 90, hasta que incide sobre el segundo puerto del segundo divisor de haz óptico 82.

35

Dado que el segundo subpulso óptico, debido a la inversión de polarización realizada por el primer espejo de Faraday 98, incide sobre el segundo puerto del segundo divisor de haz óptico 82 con polarización ordinaria, pasa a través del segundo divisor de haz óptico 82 y alcanza el tercer puerto del primer divisor de haz óptico 80.

40

En detalle, con respecto a la codificación de fase realizada por el primer y segundo moduladores de fase 96 y 116 en el primer y segundo subpulsos ópticos, respectivamente, el primer modulador de fase 96 somete el segundo subpulso óptico a desplazamiento de fase una fase φ_A ; además, el segundo modulador de fase 116 somete el primer subpulso óptico a desplazamiento de fase una fase φ_B .

45

En más detalle, con el fin de determinar la fase φ_A , el primer modulador de fase 96 aleatoriamente selecciona un sistema de bases de un primer sistema de bases, formado por los ángulos $\{0, \pi\}$, y un segundo sistema de bases,

formado por los ángulos $\left\{ \frac{\pi}{2}, \frac{3\pi}{2} \right\}$. Además, tras haber seleccionado un sistema de bases, el primer modulador de fase 96 selecciona aleatoriamente uno de los dos ángulos que forman el sistema de bases seleccionado y establece la fase φ_A igual al ángulo seleccionado.

50

De manera similar, con el fin de determinar la fase φ_B , el segundo modulador de fase 96 aleatoriamente selecciona un sistema de bases de entre el primer y segundo sistemas de bases. Después de eso, el segundo modulador de fase 96 selecciona aleatoriamente uno de los dos ángulos que forman el sistema de bases seleccionado y establece fase φ_B igual al ángulo seleccionado.

55

Tal como se muestra en más detalle en la figura 6, dada una secuencia de un número NUM (en la figura 6, NUM=5) de pulsos ópticos generados por la fuente óptica 62, el sistema criptográfico 49 es de tal manera que el primer dispositivo periférico 50 experimenta el pase de NUM primeros subpulsos ópticos (indicados por la línea continua), y solo después de eso el pase de NUM segundos subpulsos ópticos (indicados por la línea discontinua). A la inversa, aunque no se muestra, el segundo dispositivo periférico 52 experimenta el pase de NUM segundos subpulsos ópticos, y solo después de eso el pase de NUM primeros subpulsos ópticos. Además, la fuente óptica 62 no transmite ningún pulso óptico adicional hasta que la totalidad de los NUM pares de primer y segundos subpulsos ópticos han alcanzado el primer divisor de haz óptico 80. Además, con referencia, por

60

ejemplo, al primer dispositivo periférico 50, este mantiene el primer divisor óptico variable 94 y el primer modulador de fase 96 inactivos durante el tránsito de los primeros subpulsos ópticos, mientras que controla aleatoriamente, tal como se explicó anteriormente, el primer modulador de fase 96 durante el tránsito de cada uno de los segundos subpulsos ópticos.

Habiendo dicho esto, dado que el primer y segundo subpulsos ópticos inciden respectivamente sobre el cuarto y tercer puertos del primer divisor de haz óptico 80 tras haber atravesado una trayectoria óptica idéntica, están temporalmente alineados; además, esta trayectoria óptica, cuyos dos extremos están conectados respectivamente al tercer y cuarto puertos del primer divisor de haz óptico 80, presenta autoestabilización de fase.

En la práctica, el primer y segundo subpulsos ópticos inciden respectivamente sobre el cuarto y tercer puertos del primer divisor de haz óptico 80 simultáneamente, y también con una misma polarización. Por tanto, el primer y segundo subpulsos ópticos, que también son mutuamente coherentes, pueden interferir y el primer divisor de haz óptico 80 se comporta como un denominado interferómetro de Sagnac. Además, en el caso en el que el primer y segundo subpulsos ópticos forman estados de señal correspondientes (a continuación en el presente documento se proporciona una descripción de los estados de señal), la atenuación introducida por el primer y segundo divisores ópticos variables 94 y 114 en el primer y segundo subpulsos ópticos es tal que el estado de entrada en el tercer y cuarto puertos del primer divisor de haz óptico 80 (que se denomina precisamente estado de señal) tiene un número promedio de fotones μ sustancialmente igual a uno, es decir es un denominado estado de fotón individual. Debe observarse que, en general, el término "estado de señal" también se usa para indicar los estados de fase generados individualmente por el primer y segundo dispositivos periféricos 50 y 52, cuando estos estados de fase contribuyen a formar un estado de señal correspondiente en el tercer y cuarto puertos del primer divisor de haz óptico 80.

En la práctica, las detecciones realizadas por la primera y segunda unidades de detección óptica 70 y 72 dependen de las fases φ_A y φ_B introducidas por el primer y segundo moduladores de fase 96 y 116. Más en particular, si el primer y segundo dispositivos periféricos 50 y 52 han seleccionado un mismo sistema de bases y los valores de las fases φ_A y φ_B son los mismos, la segunda unidad de detección óptica 72 detectará una señal óptica, de lo contrario la detección de señal óptica se produce en la primera unidad de detección óptica 70. A la inversa, si el primer y segundo dispositivos periféricos 50 y 52 han seleccionado dos sistemas de bases diferentes, las detecciones de señal correspondientes no son deterministas y deben descartarse. Más en particular, las instancias de detección de señal por la primera o por la segunda unidad de detección óptica 70 y 72 (indicadas respectivamente como SPCM 1 y SPCM 2), dependiendo de las fases φ_A y φ_B , se indican en la tabla mostrada en la figura 7. En esta tabla también se indican el bit de clave correspondiente obtenido y la oportunidad de realizar una operación de manipulación de bits.

En la práctica, el primer y segundo subpulsos ópticos interfieren en el primer divisor de haz óptico 80 de tal manera que, si las fases φ_A y φ_B son iguales a ángulos que pertenecen a un mismo sistema de bases, la interferencia genera una señal óptica dirigida de manera determinista a la primera o a la segunda unidad de detección óptica 70 ó 72, dependiendo de si las fases φ_A y φ_B son iguales o no.

La primera y segunda unidades de detección óptica 70 y 72 envían señales eléctricas a la tarjeta de marca de tiempo 68 indicativas de las detecciones respectivas y de los tiempos de detección correspondientes; esta información se comunica entonces por la tarjeta de marca de tiempo 68 a la primera unidad de procesamiento 60, que a su vez la transmite, junto con información referente a los tiempos de generación de los pulsos ópticos, a las segunda y tercera unidades de procesamiento 104 y 124, sobre el canal público.

Desde un punto de vista analítico, el sistema criptográfico 49 puede describirse modelando la fuente óptica 62 como un estado coherente atenuado. En particular, suponiendo que la fase de cada pulso óptico es completamente aleatoria, el número de fotones para cada pulso óptico sigue una distribución de Poisson con un número promedio de fotones igual a $|\alpha|^2$. El estado emitido desde la fuente óptica 62 viene dado por:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} a_1^{\dagger n} |0\rangle$$

El primer divisor de haz óptico 80 introduce la transformación:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} \left(\frac{a_A^{\dagger} - a_B^{\dagger}}{\sqrt{2}} \right)^n |0\rangle$$

donde los subíndices A y B se refieren a modos identificados respectivamente por el primer y segundo tramos de

fibra óptica 90 y 92, es decir por los canales de comunicaciones de fibra óptica que discurren respectivamente hacia el primer y segundo dispositivos periféricos 50 y 52. El estado puede volver a escribirse de la forma:

$$\begin{aligned} |\alpha\rangle &= e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \left(\frac{\alpha}{\sqrt{2}} \right)^n \sum_{k=0}^{\infty} \binom{n}{k} \frac{a_A^{\dagger k} a_B^{\dagger(n-k)}}{n!} |0\rangle \\ &= e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \left(\frac{\alpha}{\sqrt{2}} \right)^n \frac{a_B^{\dagger(n-k)}}{(n-k)!} |0\rangle \sum_{k=0}^{\infty} \left(-\frac{\alpha}{\sqrt{2}} \right)^k \frac{a_A^{\dagger k}}{k!} |0\rangle \\ &= \left| \alpha / \sqrt{2} \right\rangle_A \left| -\alpha / \sqrt{2} \right\rangle_B \end{aligned}$$

5

donde $\left| \alpha / \sqrt{2} \right\rangle_A$ y $\left| \alpha / \sqrt{2} \right\rangle_B$ todavía son dos estados coherentes con un número promedio de fotones igual a la mitad del número promedio de fotones iniciales. Los dos estados discurren respectivamente a lo largo del primer y segundo tramos de fibra óptica 90 y 92.

10 La evolución de los dos estados coherentes da como resultado el estado:

$$\left| \alpha e^{-\alpha L_A} e^{-\nu_{A1}} / \sqrt{2} \right\rangle_A \left| -\alpha e^{-\alpha L_B} e^{-\nu_{B1}} / \sqrt{2} \right\rangle_B$$

15 donde $\exp(-\alpha L_A)$ y $\exp(-\alpha L_B)$ representan la atenuación debida a la propagación en el primer y segundo tramos de fibra óptica 90 y 92, y donde $\exp(-\nu_{A1})$ y $\exp(-\nu_{B1})$ indican la atenuación introducida por el primer y segundo dispositivos periféricos 50 y 52, respectivamente en el primer y segundo subpulsos ópticos. Los dos estados coherentes se propagan desde el primer dispositivo periférico 50 hasta el segundo dispositivo periférico 52, y desde el segundo dispositivo periférico 52 hasta el primer dispositivo periférico 50:

$$\left| \alpha e^{-a(2L_A+L_B)} e^{-\nu_{A1}} / \sqrt{2} \right\rangle_B \left| -\alpha e^{-a(L_A+2L_B)} e^{-\nu_{B1}} / \sqrt{2} \right\rangle_A$$

20

Una atenuación adicional da como resultado el estado:

$$\left| \alpha e^{-a(2L_A+L_B)} e^{-(\nu_{A1}+\nu_{B2})} / \sqrt{2} \right\rangle_B \left| -\alpha e^{-a(L_A+2L_B)} e^{-(\nu_{A2}+\nu_{B1})} / \sqrt{2} \right\rangle_A$$

25

que se propaga hacia el primer divisor de haz óptico 80 tras haberse sometido a desplazamiento de fase de φ_B y φ_A .

Entonces se obtiene lo siguiente:

30

$$\left| \alpha e^{i\varphi_B} \alpha e^{-2a(L_A+L_B)} e^{-(\nu_{A1}+\nu_{B2})} / \sqrt{2} \right\rangle_B \otimes \left| -\alpha e^{i\varphi_A} \alpha e^{-2a(L_A+L_B)} e^{-(\nu_{A2}+\nu_{B1})} / \sqrt{2} \right\rangle_A$$

El estado de salida del primer divisor de haz óptico 80, es decir en la salida del primer y segundo puertos, viene dado por:

35

$$\begin{aligned} &\left| \alpha e^{-2a(L_A+L_B)} \left(e^{i\varphi_B} e^{-(\nu_{A1}+\nu_{B2})} - e^{i\varphi_A} e^{-(\nu_{A2}+\nu_{B1})} \right) / 2 \right\rangle_1 \\ &\otimes \left| \alpha e^{-2a(L_A+L_B)} \left(e^{i\varphi_B} e^{-(\nu_{A1}+\nu_{B2})} + e^{i\varphi_A} e^{-(\nu_{A2}+\nu_{B1})} \right) / 2 \right\rangle_2 \end{aligned}$$

a partir de lo cual puede deducirse que la visibilidad de interferencia máxima se obtiene con:

40

$$v_{A1} + v_{B2} = v_{A2} + v_{B1}$$

es decir, si la atenuación global introducida por el primer y segundo dispositivos periféricos 50 y 52 en el primer subpulso óptico es igual a la atenuación global introducida por el primer y segundo dispositivos periféricos 50 y 52 en el segundo subpulso óptico.

Por tanto, el estado final viene dado por:

$$\left| \alpha e^{-2a(L_A+L_B)} e^{-(v_A+v_B)} \left(e^{i\varphi_B} - e^{i\varphi_A} \right) \right\rangle_1 \left| \alpha e^{-2a(L_A+L_B)} e^{-(v_A+v_B)} \left(e^{i\varphi_B} + e^{i\varphi_A} \right) / 2 \right\rangle_2$$

De nuevo con referencia al primer y segundo dispositivos periféricos 50 y 52, estos se comunican entre sí sobre el canal público, pasando los sistemas de bases seleccionados anteriormente, pero no los valores de fase seleccionados. De esta manera, el primer y segundo dispositivos periféricos 50 y 52 determinan una clave filtrada, basándose en las detecciones realizadas por la primera y segunda unidades de detección óptica 70 y 72 con sistemas de bases concordantes; en este caso, es posible, por ejemplo, asociar el bit "0" con los ángulos 0 y $\pi/2$, y el bit "1" con los ángulos " π " y " $3/2\pi$ ", antes de una posible inversión.

Con el fin de aumentar la tasa de generación de claves R y/o aumentar la distancia, el primer y segundo dispositivos periféricos 50 y 52 implementan un esquema de distribución de clave cuántica con estados señuelo. En particular, cada primer y segundo dispositivo periférico 50 y 52 varía aleatoriamente la atenuación que introduce respectivamente en algunos de los segundos subpulsos ópticos (en el caso del primer dispositivo periférico 50), o en algunos de los primeros subpulsos ópticos (en el caso del segundo dispositivo periférico 52); en particular, se aumenta la atenuación con respecto a la atenuación introducida por el mismo dispositivo periférico en el caso de los estados de señal mencionados anteriormente. Además, la selección de los primeros/segundos subpulsos ópticos que van a usarse para la generación de los estados señuelo tiene lugar de manera aleatoria.

Se comunica información referente a la transmisión, al tiempo de transmisión y al tipo (número promedio de fotones) de cada estado señuelo por el generador de pulsos arbitrarios del dispositivo periférico que ha generado el estado señuelo a la unidad de procesamiento correspondiente, que a su vez comunica esta información a la unidad de procesamiento del otro dispositivo periférico sobre el canal público.

El primer y segundo dispositivos periféricos 50 y 52, y en particular la segunda y tercera unidades de procesamiento 104 y 124, pueden estimar entonces la tasa de generación de claves R, combinando el enfoque basado en la "destilación de entrelazado" de Gottesman-Lo-Lutknhaus-Preskill (GLLP) con los estados señuelo y obteniendo:

$$R \geq q \left\{ -Q_\mu f(E_\mu) H(E_\mu) + Q_1 [1 - H(e_1)] \right\}$$

donde: el parámetro q depende de la implementación (en particular, las probabilidades con las que se generan los estados señuelo y los estados de señal; por ejemplo, si estas probabilidades son iguales, $q=1/2$); μ es indicativo de la potencia del estado de señal; Q_μ es la ganancia del estado de señal; E_μ es el QBER total; Q_1 es la ganancia del estado de fotón individual; e_1 representa el error del estado de fotón individual; $f(E_\mu)$ representa la eficacia de corrección de errores con un límite de Shannon dado por 1; y $H(x)$ representa la entropía de Shannon binaria.

Considerando el caso de medición realizada con bases concordantes y fases iguales, y suponiendo que la fase de cada pulso óptico es completamente aleatoria, el número de fotones sigue una distribución de Poisson con un parámetro μ que es precisamente el número promedio de fotones emitidos conjuntamente por el primer y segundo dispositivos periféricos 50 y 52. La matriz de densidad del estado de entrada en el tercer y cuarto puertos del primer divisor de haz óptico 80 viene dada por:

$$\rho_{AB} = \sum_{i=0}^{\infty} \frac{\mu e^{-\mu}}{i!} |i\rangle \langle i|$$

Para sistemas de QKD basados en fibra óptica, las pérdidas de canal cuántico pueden derivarse a partir del coeficiente de atenuación medido en dB/Km y la longitud de la fibra óptica. La transmitancia total del canal cuántico puede expresarse como:

$$t_{Ch} = 10^{-\frac{A}{10}(L_{Ch})}$$

donde A indica la atenuación en dB/Km de la fibra óptica y donde L_{Ch} es alternativamente igual a L_A o L_B ; sin ninguna pérdida de generalidad, a continuación en el presente documento se supone $L_{Ch}=L_A$.

Es posible indicar la transmitancia del dispositivo central 54 (Charlie) como $\eta_{Charlie}$, que incluye tanto la transmitancia óptica $t_{Charlie}$ del dispositivo central 54, como la eficacia η_D de la primera y segunda unidades de detección óptica 70 y 72; esto da:

$$\eta_{Charlie} = t_{Charlie} \eta_D$$

Por tanto, la eficacia total de transmisión y detección entre el primer dispositivo periférico 50 (Alice), el segundo dispositivo periférico 52 (Bob) y el dispositivo central 54 (Charlie) viene dada por:

$$\eta = t_{Ch} \eta_{Charlie}$$

Tal como se mencionó anteriormente, se supone que la primera y segunda unidades de detección óptica 70 y 72 comprenden fotodiodos de avalancha que funcionan en modo de Geiger, y por tanto que el dispositivo central 54 puede distinguir un estado vacío de un estado con un determinado número de fotones, pero no puede distinguir el número de fotones. Además, resulta razonable suponer que hay independencia estadística entre los fotones en los estados con i fotones. Por tanto, la transmitancia del estado de fotón i viene dada por:

$$\eta_i = 1 - (1 - \eta)^i \quad \text{por } i = 0, 1, 2, \dots$$

También es posible definir la probabilidad de detección por el dispositivo central 54 (y por tanto, por al menos una de entre la primera y segunda unidades de detección óptica 70 y 72) cuando el estado de entrada en el tercer y cuarto puertos del primer divisor de haz óptico 80 es un estado de fotón i, como Y_i . En este caso, Y_0 es la tasa de fondo; además, Y_i comprende tanto la tasa de fondo como las contribuciones debidas a los estados de señal. Suponiendo que los recuentos de fondo son independientes de la detección de los estados de señal, Y_i viene dada por:

$$Y_i = Y_0 + \eta_i - \eta_i Y_0 \cong Y_0 + \eta_i$$

La ganancia Q_i del estado de fotón i viene dada por:

$$Q_i = Y_i \frac{\mu e^{-\mu}}{i!}$$

Con respecto a esto, la ganancia es el producto de la probabilidad de que el primer y segundo dispositivos periféricos 50 y 52 generen conjuntamente un estado de fotón i en la entrada en el tercer y cuarto puertos del primer divisor de haz óptico 80, y la probabilidad condicional de que el dispositivo central 54 detecte un acontecimiento, es decir que una de entre la primera y segunda unidades de detección óptica 70 y 72 realice una detección.

La tasa de error e_i del estado de fotón i viene dada por:

$$E_i = \frac{e_0 Y_0 + e_{detector} \eta_i}{Y_i}$$

donde $e_{detector}$ es la probabilidad de que se detecte un fotón por la unidad equivocada de entre la primera y segunda unidades de detección óptica 70 y 72, es decir provocando violación de la tabla mostrada en la figura 7.

Es posible suponer que $e_{detector}$ no depende de la longitud de los tramos de fibra óptica y que la tasa de error de fondo es estadísticamente independiente, es decir $e_0=1/2$. En este caso, la ganancia total viene dada por:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu e^{-\mu}}{i!} = Y_0 + 1 - e^{-\eta\mu}$$

mientras que QBER total viene dada por:

$$E_\mu = \frac{1}{Q_\mu} \sum_{i=0}^{\infty} \frac{e_0 Y_0 + e_{\text{detector}} \eta Y_i}{Y_i} \frac{\mu e^{-\mu}}{i!} = \frac{e_0 Y_0 + e_{\text{detector}} (1 - e^{-\eta\mu})}{Y_0 + 1 - e^{-\eta\mu}}$$

Habiendo dicho esto, es posible intentar optimizar el número promedio μ de fotones emitidos conjuntamente por el primer y segundo dispositivos periféricos 50 y 52, dado que el estado de fotón individual es el único que garantiza la seguridad de la clave. Por tanto, por un lado es posible maximizar la probabilidad de que el primer y segundo dispositivos periféricos 50 y 52 generen conjuntamente un estado de fotón individual, siendo esta probabilidad máxima, con estadística de Poisson, para $\mu=1$; por otro lado, es posible reducir la ganancia en muchos fotones Q_μ , de modo que se garantiza la seguridad. Por tanto, con fines prácticos, es posible maximizar la razón Q_1/Q_μ ; intuitivamente, resulta oportuno que $\mu \in (0, 1]$.

En la práctica, suponiendo que el primer y segundo dispositivos periféricos 50 y 52 pueden estimar e_1 e Y_1 , y suponiendo que la tasa de fondo es baja ($Y_0 \ll \eta$) y que la transmitancia es baja ($\eta \ll 1$), se obtiene:

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \approx \eta\mu$$

$$Q_1 = (Y_0 + \eta) \mu e^{-\mu} \approx \eta \mu e^{-\mu}$$

$$e_1 = \frac{e_0 Y_0 + e_{\text{detector}} \eta}{(Y_0 + \eta)} \approx e_{\text{detector}}$$

$$E_\mu = \frac{e_0 Y_0 + e_{\text{detector}} (1 - e^{-\eta\mu})}{Y_0 + 1 - e^{-\eta\mu}} \approx e_{\text{detector}}$$

En este caso, la tasa de generación de claves es igual a:

$$R \approx q \left\{ -\eta\mu f(e_{\text{detector}}) H(e_{\text{detector}}) + \eta\mu e^{-\mu} [1 - H(e_{\text{detector}})] \right\}$$

y se optimiza para el valor $\mu = \mu_{\text{opt}}$ que verifica la relación:

$$(1 - \mu) e^{-\mu} = \frac{f(e_{\text{detector}}) H(e_{\text{detector}})}{[1 - H(e_{\text{detector}})]}$$

a partir de lo cual es posible obtener la tendencia de μ_{opt} en función de e_{detector} , tal como se muestra en la figura 8. Este valor es aproximado ya que no depende del ruido de fondo.

En general, si el primer y segundo dispositivos periféricos 50 y 52 generan conjuntamente estados de señal con un número promedio de fotones μ y estados señuelo con números promedio de fotones iguales a $v_1, v_2, \dots, v_m$, entonces:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i e^{-\mu}}{i!}$$

$$E_{\mu} Q_{\mu} = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i e^{-\mu}}{i!}$$

$$Q_{\nu_1} = \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i e^{-\nu_1}}{i!}$$

$$E_{\nu_1} Q_{\nu_1} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_1^i e^{-\nu_1}}{i!}$$

$$Q_{\nu_2} = \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i e^{-\nu_2}}{i!}$$

$$E_{\nu_2} Q_{\nu_2} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_2^i e^{-\nu_2}}{i!}$$

$$Q_{\nu_m} = \sum_{i=0}^{\infty} Y_i \frac{\nu_m^i e^{-\nu_m}}{i!}$$

$$E_{\nu_m} Q_{\nu_m} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_m^i e^{-\nu_m}}{i!}$$

- 15 Dado que m tiende a infinito, el primer y segundo dispositivos periféricos 50 y 52 determinan con precisión tanto el conjunto $\{Y_i\}$ como el conjunto $\{e_i\}$ y obtienen un nuevo límite inferior de Y_0 :

$$Y_1 [1 - H(e_1)]$$

- 20 Desde un punto de vista práctico, no es posible usar un número infinito de estados señuelo, sin embargo es posible demostrar que un número finito y limitado de estados señuelo es suficiente para obtener una estimación precisa de la ganancia y el error debido a estados de fotón individual.

- 25 Por ejemplo, es posible suponer que el primer y segundo dispositivos periféricos 50 y 52 generan conjuntamente dos estados señuelo, con números promedio de fotones dados por ν_1 y ν_2 , respectivamente, lo que satisface las condiciones:

$$0 \leq \nu_2 < \nu_1$$

$$\nu_1 + \nu_2 < \mu$$

30

En este caso, el primer y segundo dispositivos periféricos 50 y 52 pueden estimar el límite inferior de fondo Y_0 , basándose en:

$$\begin{aligned} & \nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1} \\ &= \nu_1 \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!} - \nu_2 \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!} \\ &= (\nu_1 - \nu_2) Y_0 - \nu_1 \nu_2 \left(Y_2 \frac{\nu_1 - \nu_2}{2!} + Y_3 \frac{\nu_1^2 - \nu_2^2}{3!} + \dots \right) \\ &\leq (\nu_1 - \nu_2) Y_0 \end{aligned}$$

35

Por tanto, un límite inferior de Y_0 viene dado por:

$$Y_0 \geq Y_0^L = \max \left\{ \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{(\nu_1 - \nu_2)}, 0 \right\}$$

donde el signo de igualdad es cierto para $\nu_2=0$, es decir cuando uno de los dos estados señuelo está vacío.

5

La contribución de múltiples fotones (con un número de fotones superior o igual a dos) en el estado de señal puede expresarse de la forma:

$$Q_\mu - Y_0 e^{-\mu} - Y_1 \mu e^{-\mu} = \sum_{i=2}^{\infty} Y_i \frac{\mu^i e^{-\mu}}{i!}$$

10

Esto da:

$$\begin{aligned} Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} &= (\nu_1 - \nu_2) Y_1 + \sum_{i=2}^{\infty} Y_i \frac{(\nu_1^i - \nu_2^i)}{i!} \\ &\leq (\nu_1 - \nu_2) Y_1 + \frac{(\nu_1^2 - \nu_2^2)}{\mu^2} \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} \\ &= (\nu_1 - \nu_2) Y_1 + \frac{(\nu_1^2 - \nu_2^2)}{\mu^2} (Q_\mu e^\mu - Y_0 - Y_1 \mu) \\ &\leq (\nu_1 - \nu_2) Y_1 + \frac{(\nu_1^2 - \nu_2^2)}{\mu^2} (Q_\mu e^\mu - Y_0^L - Y_1 \mu) \end{aligned}$$

15

donde se ha usado la desigualdad $(a^i - b^i) \leq (a^2 - b^2)$ cada vez que $0 < a + b < 1$ e $i \geq 2$. El límite inferior de ganancia Y_1 debido al estado de fotón individual viene dado por:

$$\begin{aligned} Y_1 &\geq Y_1^{L, \nu_1, \nu_2} \\ &= \frac{\mu}{\mu \nu_1 - \mu \nu_2 - \nu_1^2 + \nu_2^2} \left[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{(\nu_1^2 - \nu_2^2)}{\mu^2} (Q_\mu e^\mu - Y_0^L) \right] \end{aligned}$$

20

y la ganancia del estado de fotón individual tiene un límite inferior dado por:

$$\begin{aligned} Q_1 &\geq Q_1^{L, \nu_1, \nu_2} = \mu e^{-\mu} Y_1^{L, \nu_1, \nu_2} \\ &= \frac{\mu^2 e^{-\mu}}{\mu \nu_1 - \mu \nu_2 - \nu_1^2 + \nu_2^2} \left[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{(\nu_1^2 - \nu_2^2)}{\mu^2} (Q_\mu e^\mu - Y_0^L) \right] \end{aligned}$$

La QBER de los estados señuelo viene dada por:

25

$$E_{\nu_1} Q_{\nu_1} e^{\nu_1} = e_0 Y_0 + e_1 \nu_1 Y_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_1^i}{i!}$$

$$E_{\nu_2} Q_{\nu_2} e^{\nu_2} = e_0 Y_0 + e_1 \nu_2 Y_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_2^i}{i!}$$

a partir de lo cual puede obtenerse el límite superior de e_1 , dado por:

$$e_1 \leq e_1^{U, \nu_1, \nu_2} = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^{L, \nu_1, \nu_2}}$$

En el caso en el que ν_1 y ν_2 tienden a cero, se obtiene lo siguiente:

$$Y_1^{L, 0} = Y_0 + \eta$$

$$e_1^{U, 0} = \frac{e_0 Y_0 + e_{\text{detector}} \eta}{Y_1},$$

siendo éstos los valores teóricos calculados anteriormente. La desviación relativa del valor teórico de Y_1 viene dada por:

$$\beta_{Y_1} = \frac{Y_1^{L, 0} - Y_1^{L, \nu_1, \nu_2}}{Y_1^{L, 0}}$$

Mientras que la desviación relativa de e_1 viene dada por:

$$\beta_{e_1} = \frac{e_1^{U, \nu_1, \nu_2} - e_1^{U, 0}}{e_1^{U, 0}}$$

Con fines prácticos, el rendimiento del sistema criptográfico 49 puede apreciarse observando que el estado presente en el primer y segundo puertos del primer divisor de haz 80 es, tal como se especificó anteriormente, igual a:

$$\left| \alpha e^{-2a(L_A + L_B)} e^{-(\nu_{A1} + \nu_{B2})} (e^{i\varphi_B} - e^{i\varphi_A}) / 2 \right\rangle_1 \otimes \left| \alpha e^{-2a(L_A + L_B)} e^{-(\nu_{A1} + \nu_{B2})} (e^{i\varphi_B} + e^{i\varphi_A}) / 2 \right\rangle_2$$

y puede volver a escribirse como:

$$\left| \frac{\alpha_{Bob}}{\sqrt{2}} e^{-aL_B} (e^{i\varphi_B} - e^{i\varphi_A}) \right\rangle_1 \otimes \left| \frac{\alpha_{Bob}}{\sqrt{2}} e^{-aL_B} (e^{i\varphi_B} + e^{i\varphi_A}) \right\rangle_2$$

donde:

$$\alpha_{Bob} = \frac{\alpha}{\sqrt{2}} e^{-a(2L_A + L_B)} e^{-(\nu_A + \nu_B)}$$

En otras palabras, es como si el segundo dispositivo periférico 52 tuviera una fuente con un número promedio de fotones dado por:

$$\mu_{Bob} = |\alpha_{Bob}|^2 = \frac{|\alpha|^2}{2} e^{-2a(2L_A + L_B)} e^{-2(\nu_A + \nu_B)}$$

y el primer dispositivo periférico 50 tuviera una fuente con un número promedio de fotones dado por:

$$\mu_{Alice} = \frac{|\alpha|^2}{2} e^{-2a(L_A+2L_B)} e^{-2(v_A+v_B)} = \mu_{Bob} e^{2a(L_A-L_B)}$$

Considerando una medida útil, es decir, haciendo referencia al caso en el que el primer y segundo dispositivos periféricos 50 y 52 seleccionan valores de fase pertenecientes a la misma base e iguales entre sí, la matriz de densidad viene dada por:

$$\rho_{AB} = \sum_{i=0}^{\infty} \frac{2\mu_{Bob} e^{-2\mu_{Bob}}}{i!} |i\rangle\langle i|$$

donde la transmitancia t_{Ch} del canal se expresa por:

$$t_{Ch} = e^{-2aL_B} = 10^{-\frac{A}{10}L_B}$$

Por tanto, la elección óptima de μ_{Bob} viene dada por:

$$\mu_{Bob} = \frac{\mu_{opt}}{2}$$

en el caso en el que la longitud L_B del segundo tramo de fibra óptica 92 es mayor que longitud L_A del primer tramo de fibra óptica 90; en este caso, la fuente del primer dispositivo periférico 50 tiene un número promedio de fotones igual a:

$$\mu_{Alice} = \frac{\mu_{opt}}{2} 10^{-\frac{A}{10}(L_B-L_A)} \leq \mu_{Bob}$$

La siguiente relación también es cierta:

$$\mu_{Alice} + \mu_{Bob} \leq \mu_{opt}$$

Debe observarse que el signo de igualdad es cierto cuando $L_B=L_A$, es decir cuando el dispositivo central 54 está a medio camino entre el primer y segundo dispositivos periféricos 50 y 52. En este caso, en las mismas condiciones, la distancia máxima entre el primer y segundo dispositivos periféricos 50 y 52 alcanza aquella de un sistema de QKD basado en estados entrelazados; además, el dispositivo central 54 funciona como un repetidor cuántico.

Las consideraciones anteriores referentes a la relación entre μ_{Alice} y μ_{Bob} también se aplican al par v_{Alice1} y v_{Bob1} y al par v_{Alice2} y v_{Bob2} , que indican los números promedio de fotones emitidos por el primer y segundo dispositivos periféricos 50 y 52 cuando se generan respectivamente los estados señuelo primero y segundo.

Desde un punto de vista cuantitativo, la figura 9 muestra un ejemplo de las tendencias en la tasa de generación de claves R (por pulso), en función de la posición del dispositivo central 54 con respecto al enlace óptico entre el primer y segundo dispositivos periféricos 50 y 52. En este caso, se supone $e_{detector}=1\%$ e $Y_0=25 \cdot 10^{-6}$; además, la posición del dispositivo central 54 viene indicada por medio de un parámetro que tiene valores de 1 y 0,5, respectivamente cuando la posición del dispositivo central 54 coincide con la posición del primer dispositivo periférico 50 y cuando el dispositivo central 54 está colocado a medio camino entre el primer y segundo dispositivos periféricos 50 y 52.

En vez de eso, la figura 10 muestra la tendencia del valor óptimo de μ a medida que varía la distancia (prevista como L_A+L_B) y para las mismas suposiciones especificadas para la figura 9.

La figura 11 muestra un ejemplo de la tendencia de la tasa de generación de claves R (por pulso), en función de la distancia mencionada anteriormente, suponiendo $Y_0=25 \cdot 10^{-6}$ y teniendo el dispositivo central 54 ubicado a medio camino entre el primer y segundo dispositivos periféricos 50 y 52.

Finalmente, la figura 12 muestra la tendencia del valor óptimo de μ a medida que varía la distancia mencionada anteriormente, suponiendo $Y_0=25 \cdot 10^{-6}$ y teniendo el dispositivo central 54 ubicado a medio camino entre el primer y segundo dispositivos periféricos 50 y 52.

- 5 Las ventajas que pueden obtenerse con el presente sistema criptográfico surgen claramente de la descripción anterior. De hecho, el presente sistema criptográfico implementa un esquema interferométrico que, partiendo de un pulso óptico, permite generar un primer y un segundo subpulso óptico, que, antes de interferir, atraviesan una misma trayectoria óptica en sentidos opuestos. De esta manera, se garantiza una alineación temporal así como una alta estabilidad de fase. Además, al contrario que tipos conocidos de sistemas criptográficos, el dispositivo
- 10 central 54 también tiene la fuente óptica 62, además de los detectores ópticos; en cualquier caso, esto no implica que el dispositivo central 54 tenga control de la fuente óptica 62, ya que el primer y segundo dispositivos periféricos 50 y 52 pueden, por medio del primer y segundo divisores ópticos variables 94 y 114, atenuar los subpulsos ópticos hasta el nivel deseado, así como monitorizar fluctuaciones de potencia provocadas por el dispositivo central 54.
- 15 Finalmente, queda claro que pueden realizarse modificaciones y variaciones del presente sistema criptográfico sin apartarse del alcance de la presente invención, según se define en las reivindicaciones adjuntas.
- 20 Por ejemplo, el primer y segundo tramos de fibra óptica 90 y 92 pueden no ser de los que mantienen la polarización, al igual que: los enlaces ópticos entre el circulador 66 y i) la fuente óptica, ii) la primera unidad de detección óptica 70 y iii) el primer divisor de haz óptico 80; el enlace óptico entre el primer divisor de haz óptico 80 y la segunda unidad de detección óptica 72; las trayectorias ópticas dentro del primer y segundo dispositivos periféricos 50 y 52.
- 25 Adicionalmente, además del dispositivo central 54 que actúa como servidor, el sistema puede comprender un número de terminales periféricos mayor de dos. En este caso, es posible, por ejemplo, insertar un tipo controlable electrónicamente de conmutador óptico entre el tercer divisor de haz óptico 84, por un lado, y una pluralidad de dispositivos periféricos por el otro, que incluyen el segundo dispositivo periférico 52. Además, cada uno de los dispositivos de la pluralidad mencionada anteriormente de dispositivos periféricos está conectado al conmutador óptico por medio de un tramo de fibra óptica correspondiente. De esta manera, el dispositivo central
- 30 54 está conectado de manera óptica al primer dispositivo periférico 50 y a cualquiera de los dispositivos periféricos conectados al conmutador óptico.
- 35 Finalmente, son posibles unas realizaciones en las que la codificación de fase del primer y segundo subpulsos ópticos tiene lugar usando un número de sistemas de bases mayor de dos y/o un número de sistemas de bases formados por ángulos diferentes y/o por un número de ángulos mayor de dos.

REIVINDICACIONES

1. Sistema de distribución de clave criptográfica cuántica que comprende:

- una fuente óptica (62) configurada para generar una pluralidad de pulsos ópticos;
- un primer divisor de haz óptico (80) que tiene un primer, un segundo, un tercer y un cuarto puerto y configurado para generar, a partir de cada pulso óptico, un primer y un segundo subpulso óptico, respectivamente en el tercer y cuarto puertos;
- un primer y un segundo dispositivo periférico (50, 52); y
- una trayectoria óptica (50, 52, 82, 84, 90, 92) que tiene un primer y un segundo extremo que están conectados respectivamente al tercer y cuarto puertos del primer divisor de haz óptico, extendiéndose dicha trayectoria óptica a través del primer y segundo dispositivos periféricos y estando también configurada para atravesarse en un primer y un segundo sentido, respectivamente por el primer y segundo subpulsos ópticos, siendo dichos primer y segundo sentidos opuestos entre sí, de modo que el primer y segundo subpulsos ópticos inciden respectivamente sobre el cuarto y tercer puertos del primer divisor de haz óptico;

en el que el primer dispositivo periférico está configurado para someter el segundo subpulso óptico a un desplazamiento de fase aleatorio en una primera fase (ϕ_A), y el segundo dispositivo periférico está configurado para someter el primer subpulso óptico a un desplazamiento de fase aleatorio en una segunda fase (ϕ_B); y en el que, en uso, el primer y segundo subpulsos ópticos inciden simultáneamente sobre el primer divisor de haz óptico, provocando así una interferencia en el primer divisor de haz óptico entre el primer y segundo subpulsos ópticos, generando dicha interferencia una señal óptica de una manera determinista en el primer o el segundo puerto del primer divisor de haz óptico, o de una manera no determinista, en función de una relación entre la primera y segunda fases; y en el que cada primer y segundo dispositivo periférico está configurado para generar una clave criptográfica basándose en si dicha señal óptica, cuando se genera de una manera determinista, se genera en el primer o el segundo puerto del primer divisor de haz óptico.

2. Sistema según la reivindicación 1, en el que el primer dispositivo periférico (50) está configurado para seleccionar la primera fase (ϕ_A) de entre los ángulos de al menos un primer y un segundo sistema de bases, y el segundo dispositivo periférico (52) está configurado para seleccionar la segunda fase (ϕ_B) de entre los ángulos de dicho al menos un primer y un segundo sistema de bases; y en el que, en uso, si la primera y segunda fases son iguales a ángulos que pertenecen a un mismo sistema de bases, la interferencia genera dicha señal óptica de una manera determinista en el primer o el segundo puerto del primer divisor de haz óptico, en función de la relación entre la primera y segunda fases.

3. Sistema según la reivindicación 2, que comprende un dispositivo central (54), que incluye el primer divisor de haz óptico (80) y una primera y una segunda unidad de detección óptica (70, 72) conectadas de manera óptica, respectivamente, al primer y segundo puertos del primer divisor de haz óptico; en el que el dispositivo central está configurado para comunicar las detecciones de la primera y segunda unidades de detección óptica al primer y segundo dispositivos periféricos (50, 52); y en el que el primer sistema de bases está formado por una respectiva pluralidad de ángulos y el segundo sistema de bases está formado por una respectiva pluralidad de ángulos; y en el que cada primer y segundo dispositivo periférico está configurado para:

- seleccionar aleatoriamente un sistema de bases de entre dicho al menos un primer y un segundo sistema de bases;
- seleccionar aleatoriamente uno de los ángulos de entre los ángulos de la pluralidad de ángulos del sistema de bases seleccionado;
- comunicar el sistema de bases seleccionado al otro dispositivo periférico; y
- generar dicha clave criptográfica, basándose en las detecciones de la primera y segunda unidades de detección óptica y los sistemas de bases seleccionados por dicho dispositivo periférico y por el otro dispositivo periférico.

4. Sistema según la reivindicación 2 ó 3, en el que, en uso, el primer y segundo subpulsos ópticos inciden sobre el cuarto y tercer puertos del primer divisor de haz óptico (80) con una misma polarización.

5. Sistema según la reivindicación 4, en el que la trayectoria óptica (50, 52, 82, 84, 90, 92) comprende un segundo y un tercer divisor de haz óptico (82, 84), cada uno de los cuales es de tipo polarizador y tiene un primer, un segundo y un tercer puerto; y en el que el primer, segundo y tercer puertos del segundo divisor de haz óptico están conectados respectivamente al tercer puerto del primer divisor de haz óptico (80), al primer dispositivo periférico (50) y al tercer puerto del tercer divisor de haz óptico, estando el primer y segundo puertos del tercer divisor de haz óptico conectados respectivamente al cuarto puerto del primer divisor de haz óptico y al segundo dispositivo periférico (52).

6. Sistema según la reivindicación 5, en el que cada primer y segundo dispositivo periférico (50, 52) comprende un elemento reflectante (98, 118) respectivo configurado para reflejar el primer y segundo subpulsos ópticos, invirtiendo la polarización del primer y segundo subpulsos ópticos.
- 5 7. Sistema según cualquiera de las reivindicaciones anteriores, en el que, durante la propagación a lo largo de la trayectoria óptica, el primer subpulso óptico pasa en primer lugar a través del primer dispositivo periférico (50) y después a través del segundo dispositivo periférico (52), y el segundo subpulso óptico pasa en primer lugar a través del segundo dispositivo periférico y después a través del primer dispositivo periférico.
- 10 8. Sistema según cualquiera de las reivindicaciones anteriores, en el que cada primer y segundo dispositivo periférico (50, 52) comprende detectores (100, 102; 120, 122) respectivos configurados para detectar la potencia del primer y segundo subpulsos ópticos.
- 15 9. Sistema según cualquiera de las reivindicaciones anteriores, en el que cada primer y segundo dispositivo periférico (50, 52) está configurado para funcionar en un primer modo de funcionamiento; y en el que, cuando el primer y segundo dispositivos periféricos funcionan ambos en el primer modo de funcionamiento, el primer y segundo subpulsos ópticos experimentan una misma atenuación a lo largo de la trayectoria óptica (50, 52, 82, 84, 90, 92).
- 20 10. Sistema según la reivindicación 9, en el que, cuando el primer y segundo dispositivos periféricos (50, 52) funcionan ambos en el primer modo de funcionamiento, el primer y segundo subpulsos forman en conjunto, cuando inciden sobre el primer divisor de haz óptico (80), un estado óptico que tiene un número promedio de fotones que no supera uno.
- 25 11. Sistema según la reivindicación 10, que comprende además un primer tramo de fibra óptica (90), que conecta el primer dispositivo periférico (50) con el primer divisor de haz óptico (80), y un segundo tramo de fibra óptica (92), que conecta el segundo dispositivo periférico (52) con el primer divisor de haz óptico; y en el que, cuando el primer y segundo dispositivos periféricos funcionan ambos en el primer modo de funcionamiento, el primer subpulso sale del segundo dispositivo periférico con un número promedio de fotones μ_{Bob} y el segundo subpulso sale del primer dispositivo periférico con un número promedio de fotones μ_{Alice} , siendo la razón μ_{Alice}/μ_{Bob} una función de la diferencia entre las longitudes de los tramos primero y segundo de fibra óptica.
- 30 12. Sistema según cualquiera de las reivindicaciones 9 a 11, en el que cada primer y segundo dispositivo periférico (50, 52) está configurado para conmutar aleatoriamente entre el primer modo de funcionamiento y al menos un segundo modo de funcionamiento; y en el que, cuando funcionan en el segundo modo de funcionamiento, el primer y segundo dispositivos periféricos atenúan respectivamente el segundo y primer subpulsos ópticos en mayor medida que con respecto al primer modo de funcionamiento.
- 35 40 13. Método de distribución de clave criptográfica, que comprende las etapas de:
 - generar una pluralidad de pulsos ópticos;
 - 45 - generar un primer y un segundo subpulso óptico, a partir de cada pulso óptico y por medio de un primer divisor de haz óptico (80) que tiene un primer, un segundo, un tercer y un cuarto puerto, generándose el primer y segundo subpulsos ópticos respectivamente en el tercer y cuarto puertos;
 - provocar la propagación del primer y segundo subpulsos ópticos a través de una trayectoria óptica (50, 52, 82, 84, 90, 92) que tiene un primer y un segundo extremo que están conectados respectivamente al
 - 50 tercer y cuarto puertos del primer divisor de haz óptico y que se extiende a través de un primer y un segundo dispositivo periférico (50, 52), siendo dicha etapa de provocar la propagación tal que el primer y segundo subpulsos ópticos se propagan respectivamente a lo largo de la trayectoria óptica en un primer y un segundo sentido, siendo dichos primer y segundo sentidos opuestos entre sí, de modo que el primer y segundo subpulsos ópticos inciden respectivamente sobre el cuarto y tercer puertos del primer divisor de haz óptico;
 - 55 - someter el segundo subpulso óptico a un desplazamiento de fase aleatorio en una primera fase (ϕ_A);
 - someter el primer subpulso óptico a un desplazamiento de fase aleatorio en una segunda fase (ϕ_B);
 - hacer que el primer y segundo subpulsos ópticos incidan simultáneamente sobre el primer divisor de haz óptico, provocando así una interferencia en el primer divisor de haz óptico entre el primer y segundo subpulsos ópticos, generando dicha interferencia una señal óptica de una manera determinista en el primer o el segundo puerto del primer divisor de haz óptico, o de una manera no determinista, en función de una relación entre la primera y segunda fases; y
 - 60 - generar una clave criptográfica basándose en si dicha señal óptica, cuando se genera de una manera determinista, se genera en el primer o el segundo puerto del primer divisor de haz óptico.
 - 65
14. Método según la reivindicación 13, en el que dicha etapa de someter el segundo subpulso óptico a un

- desplazamiento de fase comprende seleccionar la primera fase (φ_A) de entre los ángulos de al menos un primer y un segundo sistema de bases; y en el que dicha etapa de someter el primer subpulso óptico a un desplazamiento de fase comprende seleccionar la segunda fase (φ_B) de entre los ángulos de dicho al menos un primer y un segundo sistema de bases; y en el que, si la primera y segunda fases son iguales a ángulos que pertenecen a un mismo sistema de bases, la interferencia genera dicha señal óptica de una manera determinista en el primer o el segundo puerto del primer divisor de haz óptico, en función de la relación entre la primera y segunda fases.
- 5
- 10 15. Método según la reivindicación 13 ó 14, en el que, durante la propagación a lo largo de la trayectoria óptica (50, 52, 82, 84, 90, 92), el primer subpulso óptico pasa en primer lugar a través del primer dispositivo periférico (50) y después a través del segundo dispositivo periférico (52), y el segundo subpulso óptico pasa en primer lugar a través del segundo dispositivo periférico y después a través del primer dispositivo periférico.
- 15 16. Método según cualquiera de las reivindicaciones 13 a 15, que comprende además:
- 20 - una primera etapa de atenuación del segundo subpulso óptico mediante el primer dispositivo periférico (50); y
 - una segunda etapa de atenuación del primer subpulso óptico mediante el segundo dispositivo periférico (52);
 y en el que el primer y segundo subpulsos ópticos experimentan una misma atenuación a lo largo de la trayectoria óptica (50, 52, 82, 84, 90, 92).
- 25 17. Método según la reivindicación 16, en el que el primer y segundo subpulsos forman en conjunto, cuando inciden sobre el primer divisor de haz óptico (80), un estado óptico que tiene un número promedio de fotones que no supera uno.
- 30 18. Método según la reivindicación 16 ó 17, que comprende además:
- una tercera etapa de atenuación del segundo subpulso óptico mediante el primer dispositivo periférico (50), comprendiendo dicha tercera etapa de atenuación una atenuación mayor del segundo subpulso óptico con respecto a la primera etapa de atenuación; y
 - una cuarta etapa de atenuación el primer subpulso óptico mediante el segundo dispositivo periférico (52), comprendiendo dicha cuarta etapa de atenuación una atenuación mayor del primer subpulso óptico con respecto a la segunda etapa de atenuación;
- 35 comprendiendo dicho método además las etapas de:
- 40 - conmutar aleatoriamente entre la primera y tercera etapas de atenuación; y
 - conmutar aleatoriamente entre la segunda y cuarta etapas de atenuación.

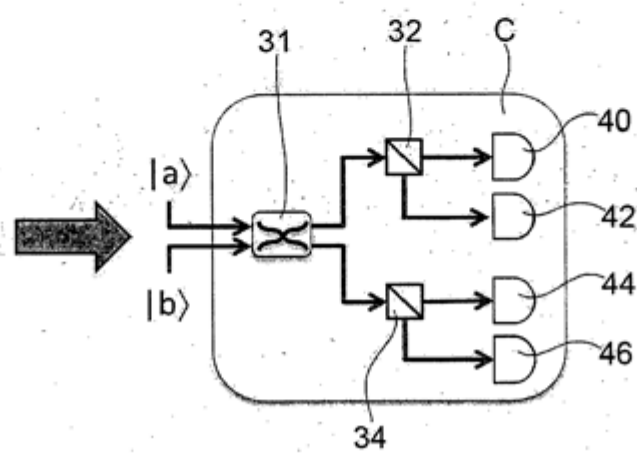
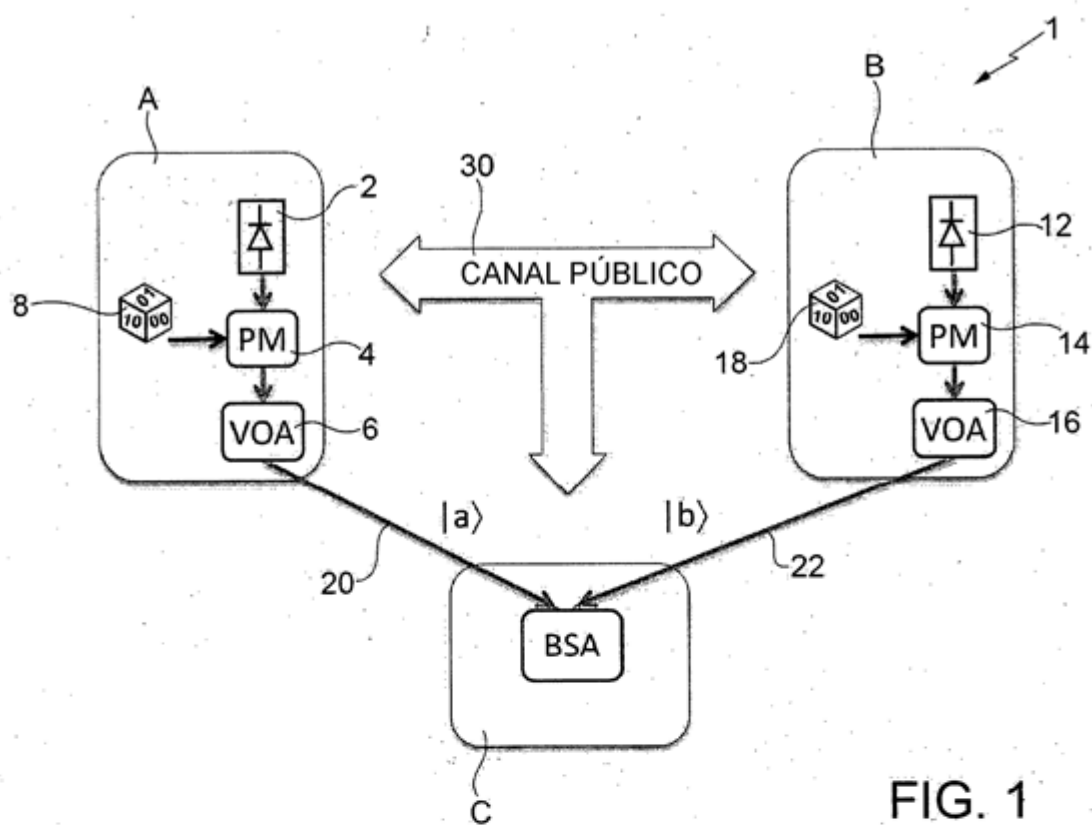


FIG. 2

Base rectilínea		Salida de BSA			Base diagonal		Salida de BSA		
Estados de polarización		Fotones individuales		WCP	Estados de polarización		Fotones individuales		WCP
A	B	$ \psi^+\rangle$	$ \psi^-\rangle$	$ \psi\rangle$	A	B	$ \psi^+\rangle$	$ \psi^-\rangle$	$ \psi\rangle$
$ H\rangle$	$ H\rangle$	0	0	0	$ +45\rangle$	$ +45\rangle$	1	0	0.75 0.25
$ V\rangle$	$ V\rangle$	0	0	0	$ +45\rangle$	$ +45\rangle$	1	0	0.75 0.25
$ H\rangle$	$ V\rangle$	0.5	0.5	0.5	$ +45\rangle$	$ +45\rangle$	0	1	0.25 0.75
$ V\rangle$	$ H\rangle$	0.5	0.5	0.5	$ +45\rangle$	$ +45\rangle$	0	1	0.25 0.75

FIG. 3

ϕ_A	ϕ_B	SPCM que detecta una señal	Manipulación de bits	Bit de clave
0	0	2	no	0
0	π	1	sí	1
π	0	1	sí	
π	π	2	no	0
$\pi/2$	$\pi/2$	2	no	
$\pi/2$	$3\pi/2$	1	sí	1
$3\pi/2$	$\pi/2$	1	sí	
$3\pi/2$	$3\pi/2$	2	no	

FIG. 7

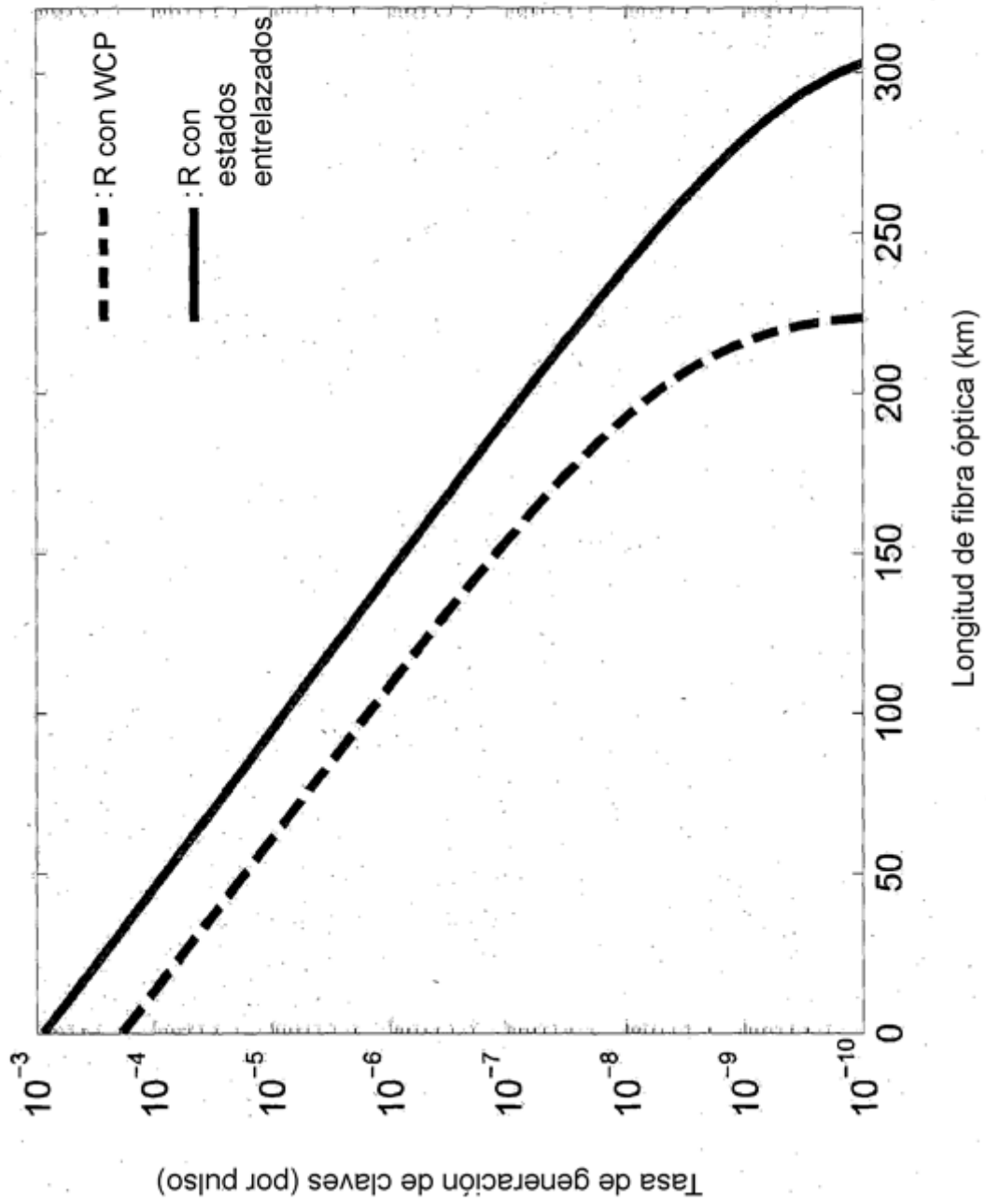


FIG. 4

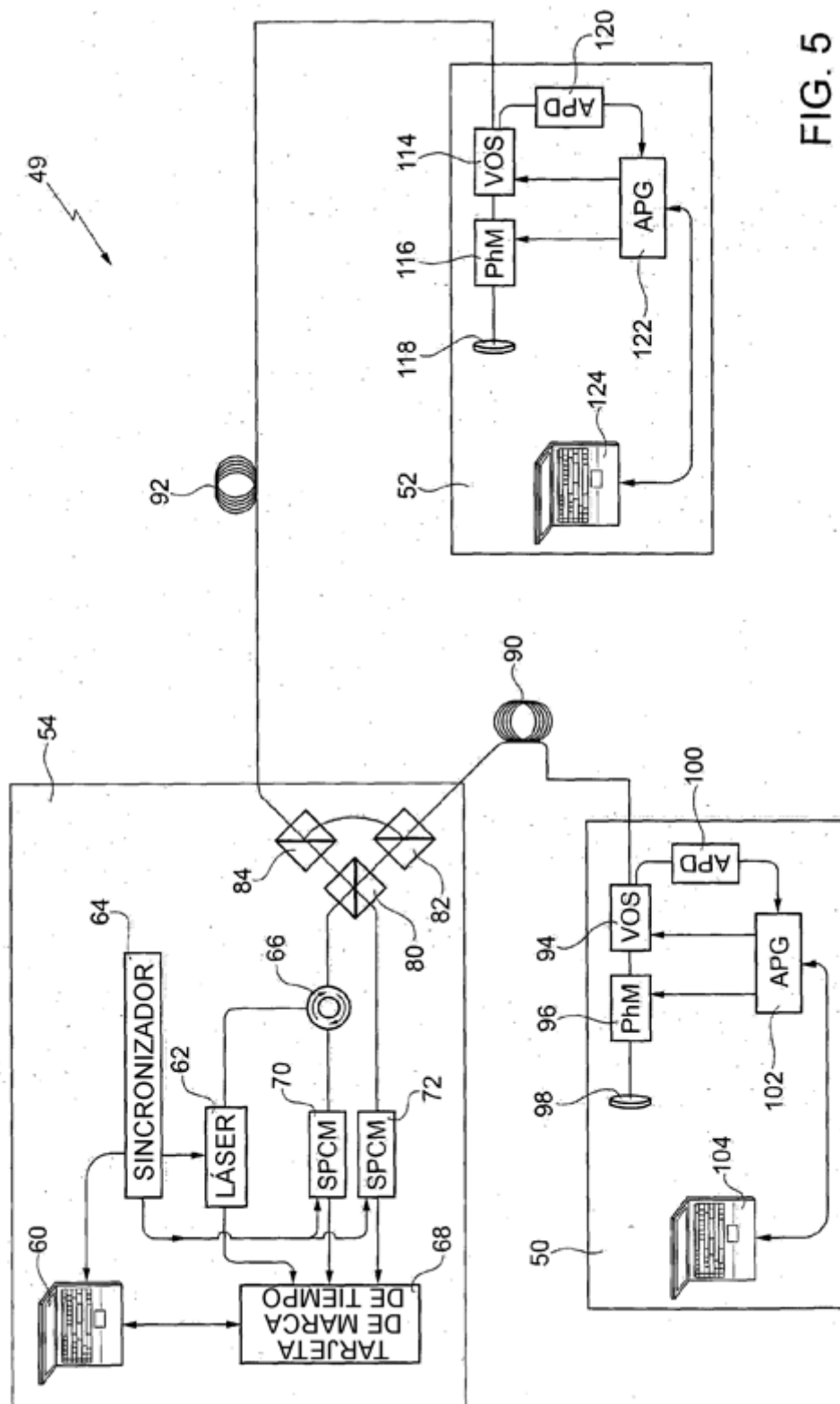


FIG. 5

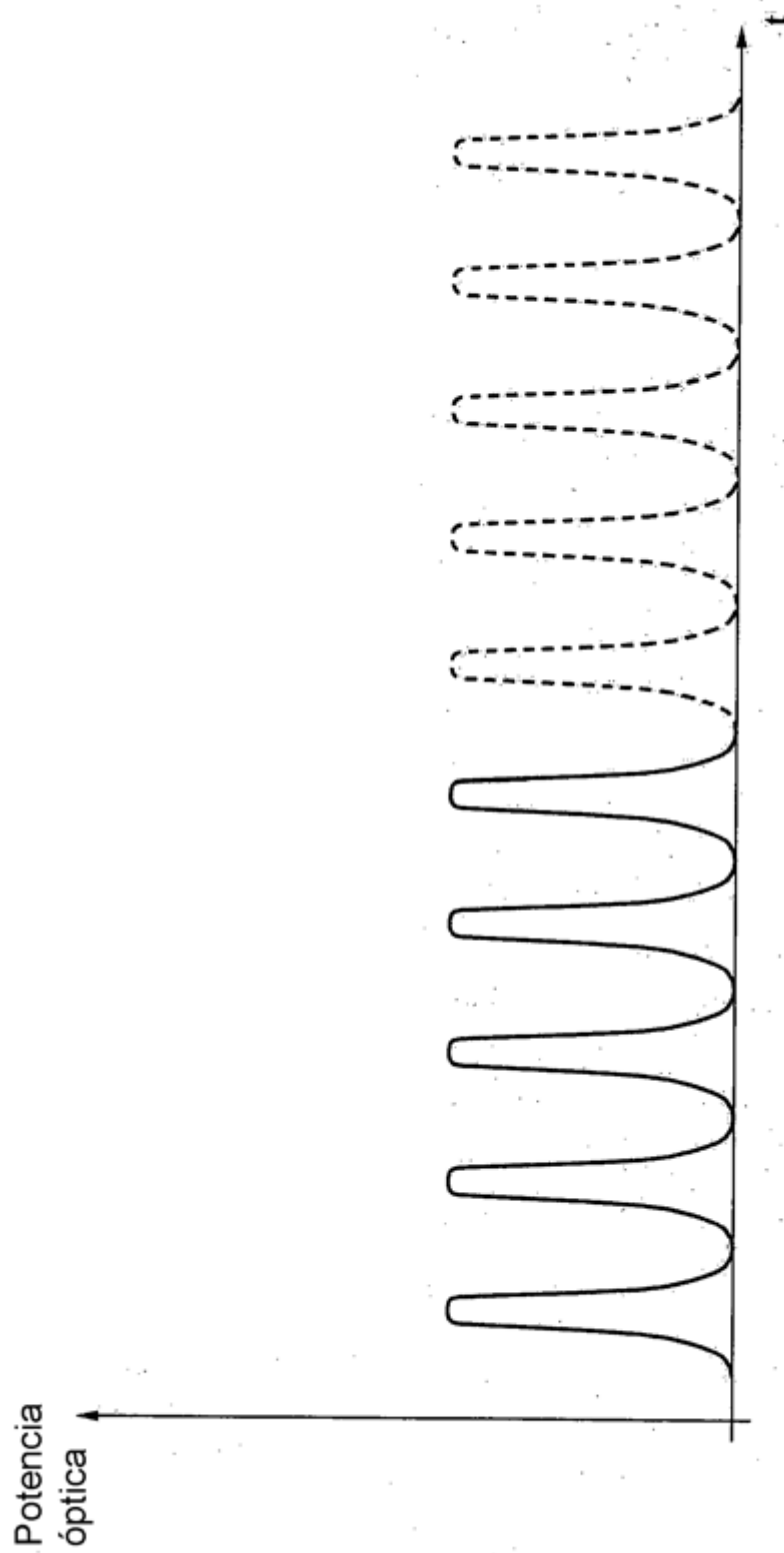


FIG. 6

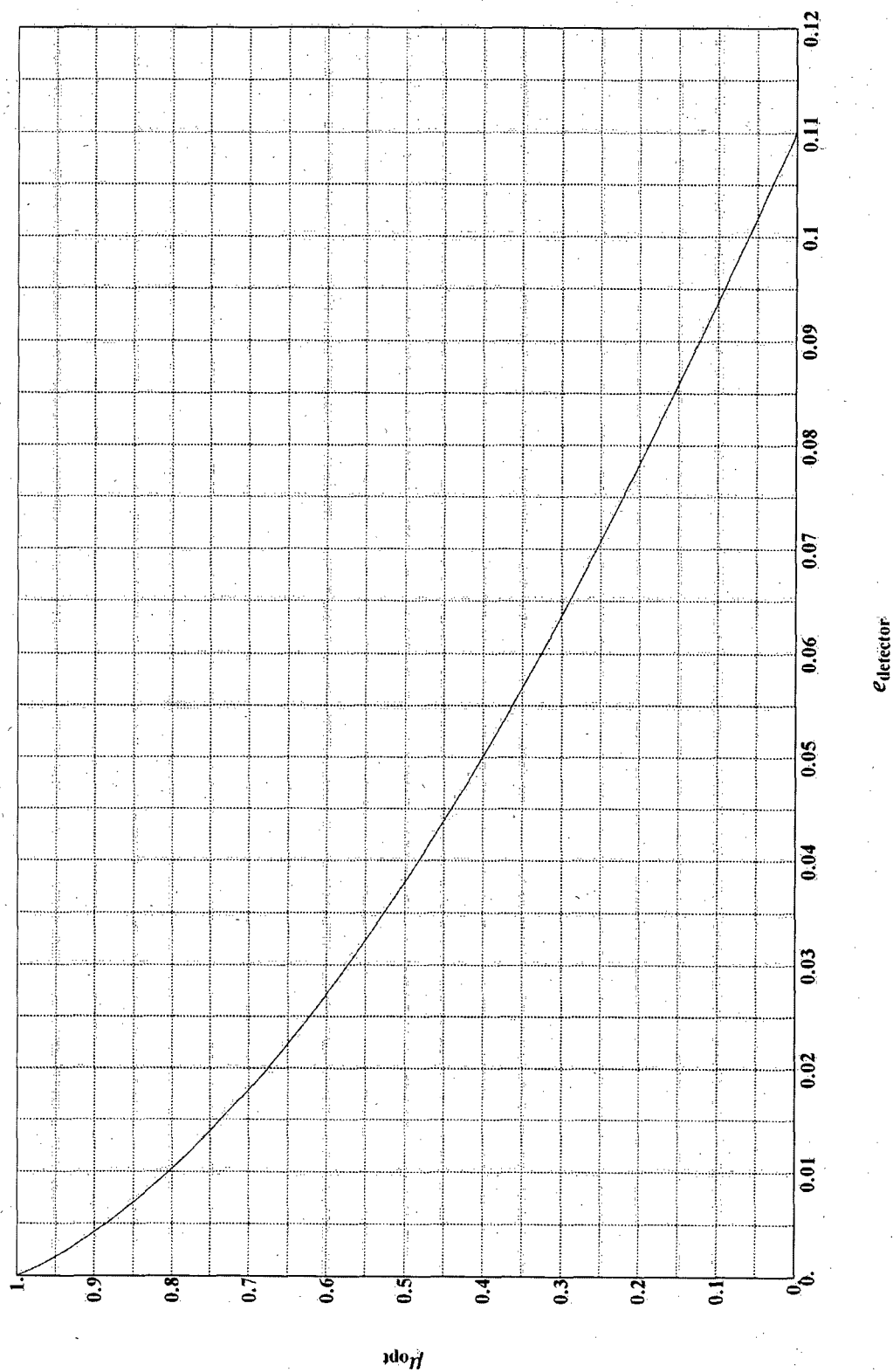


FIG. 8

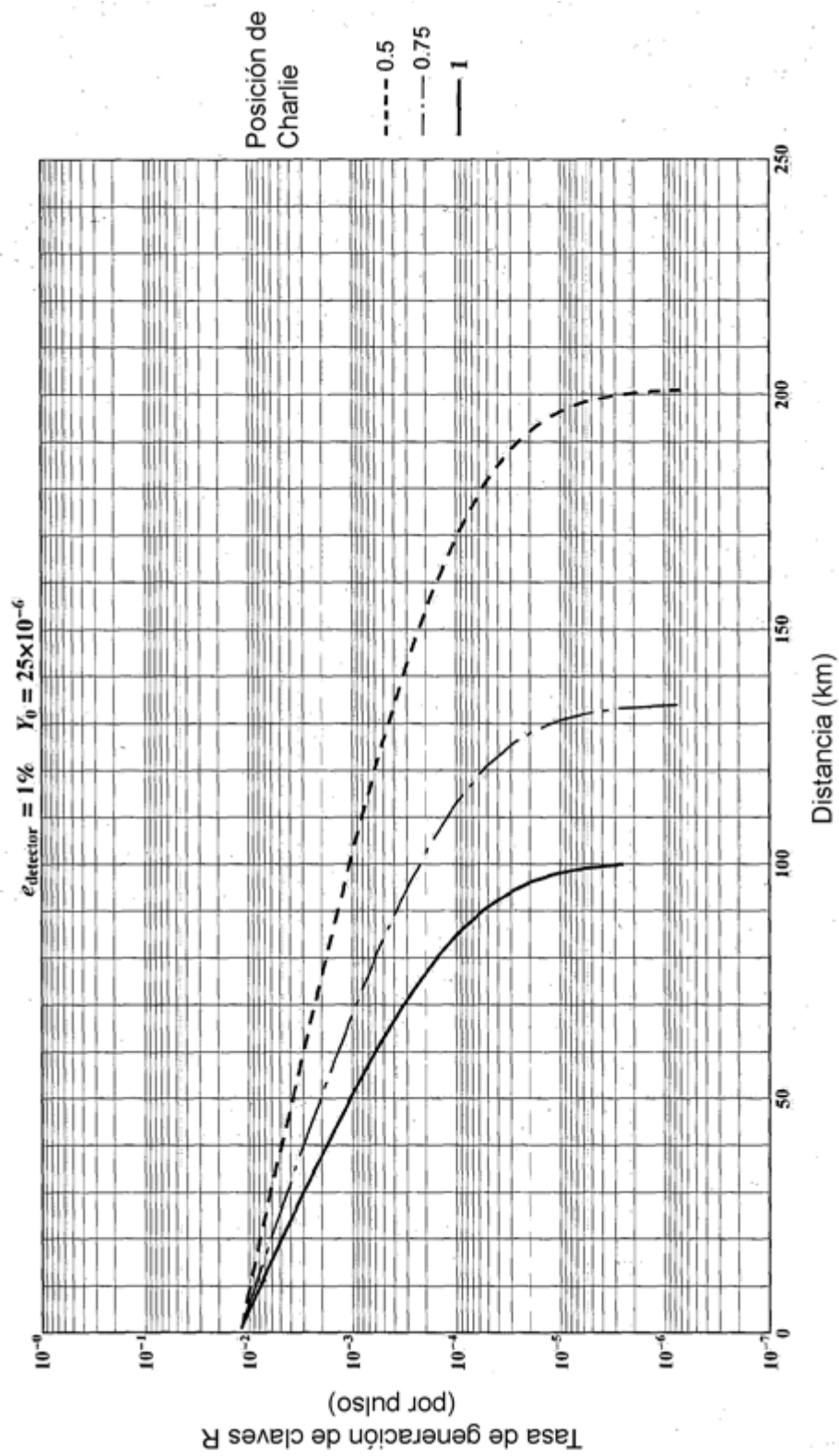


FIG. 9

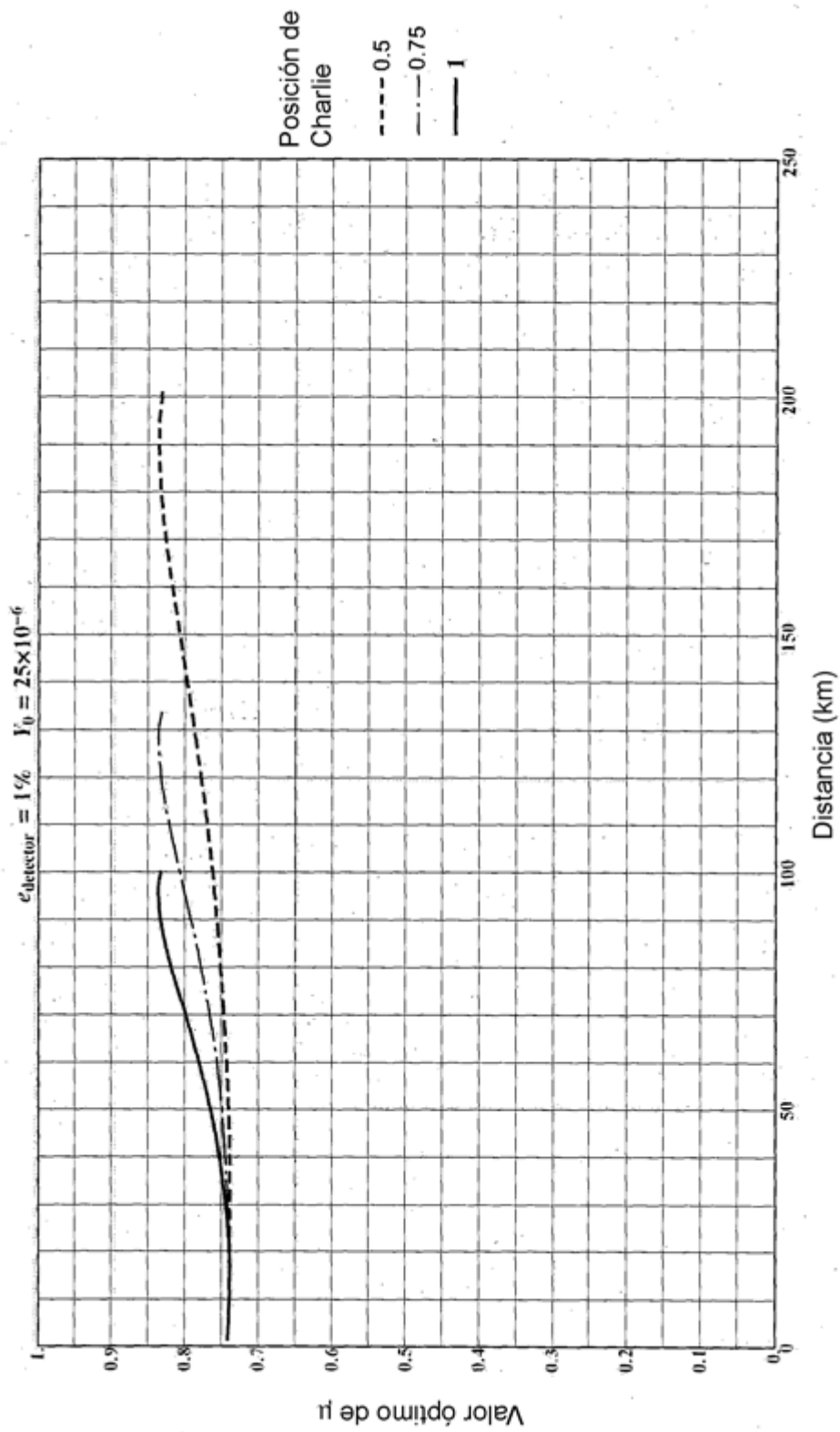


FIG. 10

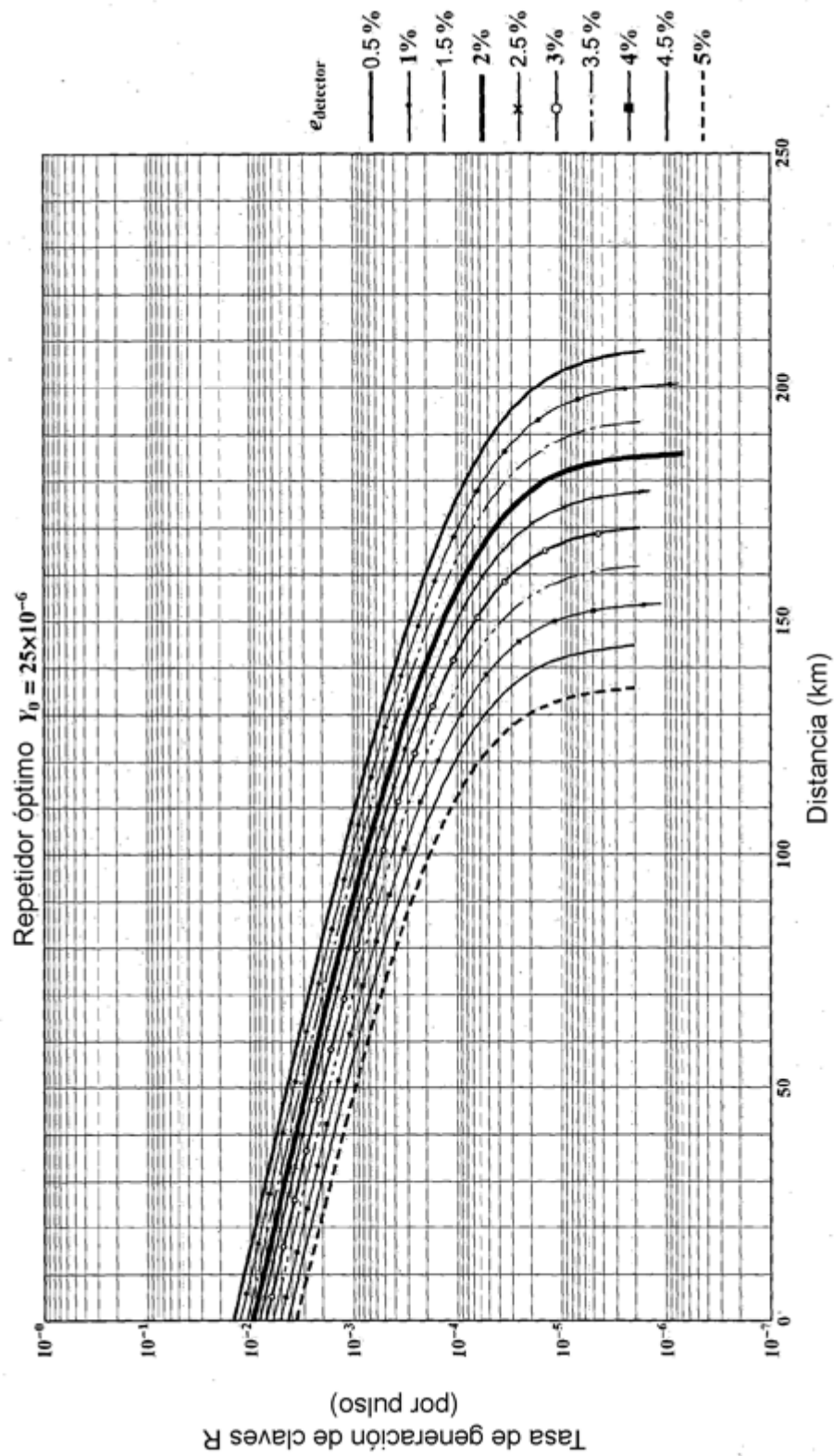


FIG. 11

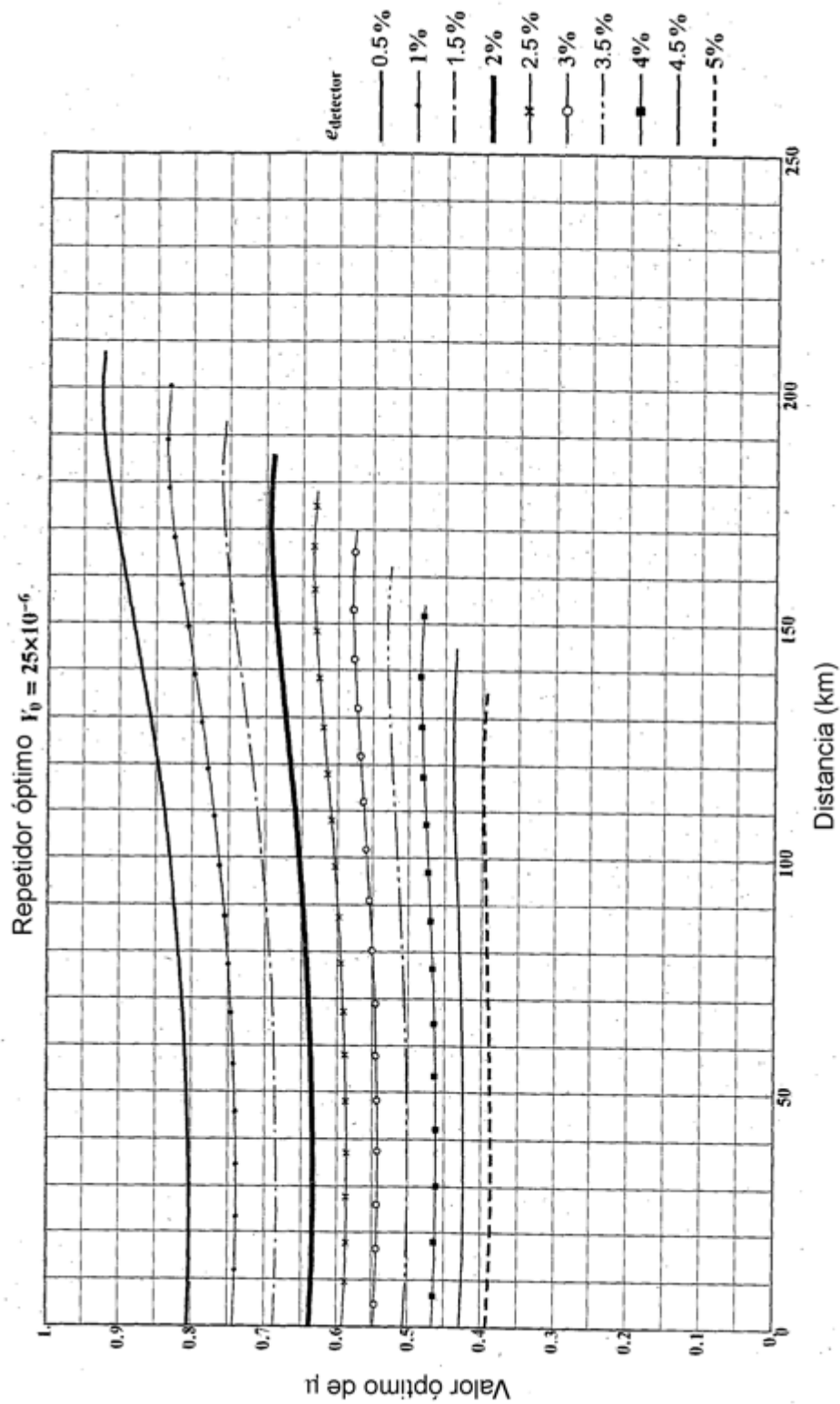


FIG. 12