(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 382 086**

(51) Int. CI.:
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05708730 .6**
(96) Fecha de presentación: **11.03.2005**
(97) Número de publicación de la solicitud: **1730879**
(97) Fecha de publicación de la solicitud: **13.12.2006**

(54) Título: **Método y dispositivo para sincronizar y adquirir fotones gemelos para un procedimiento de criptografía cuántica**

(30) Prioridad:
12.03.2004 IT TO20040165

(45) Fecha de publicación de la mención BOPI:
05.06.2012

(45) Fecha de la publicación del folleto de la patente:
05.06.2012

(73) Titular/es:
Selex Sistemi Integrati S.p.A.
Via Tiburtina, 1231
Roma, IT

(72) Inventor/es:
BOVINO, Fabio, Antonio;
VARISCO, Pietro y
DE NICOLO, Paolo

(74) Agente/Representante:
Carvajal y Urquijo, Isabel

DESCRIPCIÓN

Método y dispositivo para sincronizar y adquirir fotones gemelos para un procedimiento de criptografía cuántica

Campo técnico

La presente invención se refiere a un método de sincronización y adquisición de fotones gemelos para un procedimiento de criptografía cuántica.

La presente invención también se refiere a un dispositivo para sincronizar y adquirir fotones gemelos, que puede usarse en un sistema de criptografía cuántica.

Técnica anterior

Tal como se conoce, la criptografía cuántica emplea principios de física cuántica para generar, transmitir y decodificar información a un nivel de seguridad extremadamente alto.

Un ejemplo de estos procedimientos se da a conocer en BOVINO F A *ET AL*: “Demonstration of secure quantum key distribution” PROCEEDINGS OF THE SPIE - THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING SPIEINT. SOC. OPT. ENG USA, vol. 5105,2003, páginas 1-10, XP002337235 ISSN: 0277-786X.

Tales procedimientos se basan en varias etapas, que incluyen:

a) Crear un par de fotones entrelazados. Esto se realiza excitando un cristal lineal birrefringente (por ejemplo, borato de bario beta) usando un haz de láser (en particular un haz de láser pulsante) para crear un par de fotones de la misma frecuencia y polarización opuesta (vertical/horizontal).

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

c) Adquisición aleatoria. Cada usuario compara el único fotón recibido con una primera base de referencia (base A) y una segunda base de referencia (base B). Cada base de referencia comprende dos ejes perpendiculares, y las dos bases están separadas angularmente en un ángulo predeterminado (por ejemplo, 45º). Puesto que la polarización del fotón adquirido puede ser paralela o no a un eje de la base, la comparación facilita un resultado binario (0, 1).

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

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

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

En pruebas de laboratorio de sistemas de criptografía cuántica, los fotones en el par se adquieren por coincidencia, es decir, cuando un primer usuario detecta la llegada de un primer fotón en el par, se abre una ventana de tiempo en la que el segundo usuario espera la llegada del segundo fotón en el par. Puesto que las pruebas permiten controlar las trayectorias de los fotones y la propagación de las señales eléctricas entre usuarios, los problemas de

sincronización se resuelven fácilmente.

En el uso real, sin embargo, los canales de transmisión por los que se transmiten los fotones individuales en el par son mucho más largos (pueden tener incluso muchos kilometres de longitud), de modo que los fotones en el par alcanzan al usuario primero y segundo en instantes ampliamente diferentes, debido a los retardos de transmisión introducidos por cada canal de comunicación.

En tal caso, resulta impensable la adquisición de pares de fotones basándose en la coincidencia, como en las pruebas de laboratorio.

Descripción de la invención

Un objeto de la presente invención es proporcionar un método de sincronización para un procedimiento de criptografía cuántica, que puede implementarse y usarse para obtener ventajas con respecto a los sistemas de sincronización que funcionan actualmente.

Según la presente invención, se proporciona un método de sincronización y adquisición de fotones gemelos para un procedimiento de criptografía cuántica que comprende las etapas de: generar pares de fotones entrelazados, en que los fotones en cada par son de polarización opuesta; suministrar un primer fotón en el par para un primer canal de comunicación a una primera estación de recepción que tiene un primer reloj que genera una referencia de tiempo para la primera estación de recepción; suministrar un segundo fotón en el par para un segundo canal de comunicación a una segunda estación de recepción que tiene un segundo reloj que genera una referencia de tiempo para la segunda estación de recepción; comparar, en cada estación de recepción, la polarización de cada fotón recibido con una primera base de referencia o segunda base de referencia seleccionadas aleatoriamente, comprendiendo cada base de referencia dos ejes perpendiculares, y estando separadas angularmente la base de referencia primera y segunda por un ángulo dado; generar una señal de sincronización para activar el primer reloj y el segundo reloj; y buscar pares de fotones gemelos recibidos en las dos estaciones de recepción sustancialmente en el mismo instante medido partiendo de la base de la información proporcionada por los relojes respectivos; caracterizado porque la etapa de buscar pares de fotones gemelos comprende las etapas de: medir, en cada estación de recepción, la diferencia de tiempo ΔT entre el instante de adquisición t_n de un fotón y el instante de adquisición t_{n-1} del fotón recibido precedente: $\Delta T = t_n - t_{n-1}$; reconocer un par de fotones gemelos cuando la diferencia de tiempo ΔT_a medida en una primera estación de recepción y la diferencia de tiempo correspondiente ΔT_b medida en una segunda estación de recepción coinciden sustancialmente, y en particular cuando el valor absoluto de la diferencia entre ΔT_a y ΔT_b es menor que una ventana de tiempo de coincidencia: $|\Delta T_a - \Delta T_b| < w$; y repetir las etapas de medición y reconocimiento.

La presente invención también se refiere a un dispositivo para sincronizar y adquirir fotones gemelos para un procedimiento de criptografía cuántica que comprende: una fuente de fotones para generar pares de fotones entrelazados de polarización opuesta; un primer canal de comunicación para transmitir un primer fotón en el par; un segundo canal de comunicación para transmitir un segundo fotón en el par; una primera estación de recepción para recibir los fotones procedentes del primer canal de comunicación; y una segunda estación de recepción para recibir los fotones procedentes del segundo canal de comunicación; teniendo dicha estación de recepción primera y segunda un reloj primero y segundo, respectivamente, para generar referencias de tiempo respectivas para las estaciones de recepción; comprendiendo cada estación de recepción medios de referencia para comparar la polarización de cada fotón recibido con una primera base de referencia o segunda base de referencia seleccionadas aleatoriamente; comprendiendo cada base de referencia dos ejes perpendiculares, y estando separadas angularmente la base de referencia primera y segunda por un ángulo dado; recibiendo dicha estación de recepción primera y segunda una señal de sincronización para activar el primer reloj y el segundo reloj; y teniendo cada estación de recepción medios de búsqueda para buscar pares de fotones gemelos recibidos en las dos estaciones de recepción sustancialmente en el mismo instante medido partiendo de la base de la información proporcionada por los relojes respectivos; caracterizado porque dichos medios de búsqueda comprenden: medios de comparación para medir, en cada estación de recepción, la diferencia de tiempo ΔT entre el instante de adquisición t_n de un fotón y el instante de adquisición t_{n-1} del fotón recibido precedente: $\Delta T = t_n - t_{n-1}$; medios de detección para reconocer un par de fotones gemelos cuando la diferencia de tiempo ΔT_a medida en una primera estación de recepción y la diferencia de tiempo correspondiente ΔT_b medida en una segunda estación de recepción coinciden sustancialmente, y en particular cuando el valor absoluto de la diferencia entre ΔT_a y ΔT_b es menor que una ventana de tiempo de coincidencia: $|\Delta T_a - \Delta T_b| < w$; y medios de nueva selección para volver a seleccionar dichos medios de comparación y dichos medios de detección y repetir las operaciones de medición y reconocimiento.

Breve descripción de los dibujos

Ahora se describirá la invención con referencia particular a los dibujos adjuntos, en los que:

La figura 1 muestra, esquemáticamente, un sistema de criptografía cuántica que implementa el método según la

presente invención;

la figura 2 muestra un diagrama de bloques del método según la presente invención;

la figura 3 muestra datos de prueba obtenidos según la presente invención.

Mejor modo para llevar a cabo la invención

El número 1 en la figura 1 indica en conjunto un sistema de criptografía cuántica que comprende una fuente 2 de fotones entrelazados, y una estación 4, 5 de recepción primera y segunda que comunica con la fuente 2 por canales 7, 8 de comunicación respectivos estrictamente privados (fibra óptica).

Más específicamente, la fuente 2 comprende un cristal 10 no lineal, birrefringente, con forma de paralelepípedo (en particular, un cristal de borato de bario beta) de espesor constante L. El cristal 10 está conectado en un primer lado a una fuente 12 de haces de láser para generar un haz 14 de láser de excitación (haz de bomba) para excitar el cristal 10 y generar pares de fotones entrelazados de polarización.

Más específicamente, la fuente 12 de haces de láser comprende un primer láser 16 de potencia conocida, que genera un haz 18 de láser a un segundo láser 20 que, en respuesta, emite un haz 14 de láser de bomba en una dirección recta D formando un ángulo dado con el eje óptico del cristal 10.

El segundo láser 20 está conectado a un dispositivo 25 de conversión de frecuencia conocido, y a un sistema 26 de enfoque de entrada (mostrado esquemáticamente mediante una lente ubicada a lo largo de D entre el segundo láser 20 y el cristal 10) para estrechar el haz de láser de modo que el haz 14 de láser de bomba tenga una parte central de haz predeterminada r_p dentro del cristal 10.

Tal como se conoce, los fotones emitidos se desplazan en el espacio a lo largo de trayectorias que se disponen en regiones cónicas primera y segunda que tienen vértices tangentes al cristal y ejes simétricos con respecto al haz de bomba. Las trayectorias de fotón pueden representarse en un plano perpendicular al haz de bomba mediante anillos primero y segundo, que representan las ubicaciones más probables de las trayectorias de fotones primero y segundo en el par, respectivamente. La probabilidad de que un fotón esté ubicado hacia el interior del anillo es escasa, aunque menor que cero.

Más específicamente, los fotones generados mediante la interacción del haz 14 de láser de bomba y el cristal 10 se desplazan desde un segundo lado del cristal 10 a lo largo de trayectorias que se disponen en una primera región cónica C1 y una segunda región cónica C2, que son simétricas con respecto a la dirección de propagación D, están ubicadas en lados opuestos de la dirección D, y corresponden a la parte de intersección del anillo.

La fuente 2 comprende un primer sistema 27 de enfoque de salida separado una distancia de la dirección D en el segundo lado del cristal 10, y que enfoca los fotones de la región C1 en una región de enfoque correspondiente a la entrada de una primera fibra óptica que forma el primer canal 7 de comunicación.

La fuente 2 también comprende un segundo sistema 32 de enfoque de salida separado una distancia de la dirección D en el segundo lado del cristal 10, y que enfoca los fotones de la región C2 en una región de enfoque correspondiente a la entrada de una segunda fibra óptica que forma el segundo canal 8 de comunicación.

Fibras 7, 8 ópticas se extienden desde la fuente 2 hasta estaciones 4, 5 respectivas a lo largo de diferentes trayectorias, de modo que las fibras 7 y 8 ópticas son de longitudes diferentes.

Según el sistema 1, el haz de láser producido por el láser 20 también puede suministrarse directamente, en instantes predeterminados, a cada fibra 7, 8 óptica, tal como se muestra mediante las partes 35, 36 de fibra óptica, que, por medio de un divisor de haz B (no mostrado), recogen partes respectivas del haz del láser 20 y las enfocas en las entradas de las fibras 7, 8 ópticas. El divisor de haz B puede insertarse/excluirse selectivamente a lo largo de/desde la trayectoria del haz de láser saliente para alimentar el haz de láser a las partes 35, 36 de fibra óptica en instantes predeterminados.

Cada estación 4, 5 de recepción comprende un primer divisor 38 de haz que recibe los fotones de la fibra 7, 8 óptica, y que suministra a un segundo divisor 42 de haz y a un tercer divisor 44 de haz.

El divisor 38 de haz suministra el 50% de los fotones entrantes al segundo divisor 42 de haz, y el otro 50% al tercer divisor 44 de haz.

El segundo divisor 42 de haz actúa conjuntamente con un primer detector 50 de fotones y un segundo detector 51

de fotones, definidos preferiblemente por detectores de avalancha conocidos.

El tercer divisor 44 de haz actúa conjuntamente con un tercer detector 53 de fotones y un cuarto detector 54 de fotones, definidos preferiblemente por detectores de avalancha conocidos.

El segundo divisor 42 de haz (de tipo PBS, divisor de haz polarizado) alimenta los fotones entrantes al primer detector 50 de fotones o al segundo detector 51 de fotones, dependiendo de su polarización.

El tercer divisor 44 de haz (de tipo PBS, divisor de haz polarizado) alimenta los fotones entrantes al tercer detector 53 de fotones o al cuarto detector 54 de fotones, dependiendo de su polarización.

Más específicamente, el primer detector 50 de fotones adopta un estado de salida alto S_0 (activador de detector) durante un tiempo dado en la detección de un fotón con un eje de polarización paralelo a un eje de referencia inclinado en un ángulo de 0º con respecto a un eje de referencia; y el segundo detector 51 de fotones adopta un estado de salida alto S_{90} durante un tiempo dado en presencia de fotones con un eje de polarización paralelo a un eje de referencia inclinado en un ángulo de 90º con respecto a un eje de referencia.

El tercer detector 53 de fotones genera un primer estado lógico alto S_{45} durante un tiempo dado en la detección de un fotón con un eje de polarización paralelo a un eje de referencia inclinado en un ángulo de +45º con respecto a la referencia; y el cuarto detector 54 de fotones genera un estado lógico alto S_{-45} durante un tiempo dado en la detección de un fotón con un eje de polarización paralelo a un eje inclinado en un ángulo de -45º con respecto a la referencia.

Las señales de salida de los detectores 50, 51, 53, 54 se suministran a una unidad 60 de procesamiento electrónico que comprende, entre otras cosas, un reloj 62a, 62b para producir una referencia de tiempo para la estación 4, 5.

Por tanto, cada fotón entrante tiene la misma probabilidad de dirigirse al divisor 42 ó 44 de haz, y por tanto a los detectores 50, 51 o a los detectores 53, 54.

Cada fotón se dirige por el divisor 42 ó 44 de haz a los detectores 50, 51 o a los detectores 53, 54 partiendo de la base de su polarización.

La estación 4 de recepción compara la polarización de cada fotón recibido con una primera base de referencia seleccionada aleatoriamente (base A - detectores 50 y 51) o con la segunda base de referencia (base B - detectores 53 y 54). Cada base de referencia comprende dos ejes perpendiculares (0º, 90º y +45º, -45º respectivamente), y las dos bases están separadas angularmente 45º.

Puesto que la polarización del fotón puede ser paralela o no a un eje de la base, el resultado de la comparación es binario.

Por tanto, los detectores 50, 51, 53, 54 suministran a la unidad 60 electrónica información relativa a la base usada para la comparación (la base asociada con los dos detectores 50, 51 o 53, 54 que reciben un fotón), e información relativa al resultado de la comparación; ambos se usan de manera conocida para un procedimiento de criptografía cuántica mediante el cual las estaciones 4 y 5 comunican a través de un canal 65 de información público.

Una señal de sincronización también puede producirse suministrando fibras 7, 8 ópticas, por ejemplo, durante un tiempo dado (por ejemplo, aproximadamente algunos picosegundos) con un haz de láser de polarización conocido (por ejemplo, horizontal), de modo que un gran número de fotones alcanzan las estaciones 4 y 5. En este caso, lo más probable es que todos (o al menos tres) los detectores 50, 51, 53, 54 reciban al menos un fotón cuya polarización coincide con la de su eje de referencia, activando así los detectores. Por tanto, la recepción de la señal de sincronización se detecta cuando todos (o al menos tres) los detectores 50, 51, 53, 54 se activan simultáneamente.

Con la recepción de la señal de sincronización, se activa el reloj 62a, 62b (instante To).

Dados los diferentes retardos de transmisión de las fibras 7, 8 ópticas, la señal de sincronización llega en diferentes instantes a las estaciones 4 y 5, por lo que los relojes 62a, 62b de las estaciones 4 y 5 se activan en diferentes instantes de sincronización To. Los mismos retardos se aplican a la transmisión de los fotones individuales.

Desde el instante de sincronización To (que actúa como referencia y activa los relojes 62a, 62b), se realiza una búsqueda para pares de fotones “gemelos”, es decir fotones recibidos en las dos estaciones 4, 5 sustancialmente en el mismo instante con respecto a To, y que se usan para extraer la clave cuántica.

Teóricamente, los fotones “gemelos” pueden detectarse usando un criterio de comparación de tiempo absoluto denominado instante de sincronización To, es decir cuando la diferencia entre los instantes de llegada t_a y t_b (ambos calculados con respecto al instante de sincronización To) de dos fotones en diferentes estaciones 4, 5 coincide (o es inferior a un umbral, por ejemplo, dos nanosegundos, o a una denominada ventana de tiempo de coincidencia), entonces los dos fotones se reconocen como “gemelos”.

El criterio anterior sería válido si ambos relojes 62a, 62b tuvieran exactamente la misma frecuencia.

En realidad, por razones obvias físicas inevitables (diferencias de temperatura y componente), las frecuencias de oscilación de los dos relojes 62a, 62b nunca pueden ser exactamente iguales, limitando de ese modo el periodo en que pueden adquirirse pares de fotones “gemelos” usando el criterio teórico anterior.

De hecho, si t_n es el tiempo de llegada absoluto (es decir calculado con respecto a To) del par de fotones de orden n, $(1+\alpha)t_n$ el tiempo de llegada medido en la estación 4 basándose en el reloj 62a, y $(1+\beta)t_n$ el tiempo de llegada medido en la estación 5 basándose en el reloj 62b, los parámetros α y β tienen en cuenta el grado en que difiere la frecuencia del reloj 62a, 62b de la frecuencia nominal.

Usando el criterio de comparación de tiempo absoluto, se determina la coincidencia siempre que se aplica la siguiente condición:

$$|(1+\alpha) - (1+\beta)|\, t_n < w \qquad (1)$$

donde w representa la ventana de tiempo de coincidencia.

Dada la diferencia en frecuencia de los dos relojes 62a, 62b, sin embargo, la condición anterior (1) se aplica cuando:

$$t_n < w/|(\alpha - \beta)| \qquad (2)$$

Es decir, existe un tiempo de adquisición máximo t_n sobre y por encima del cual falla el método de comparación de tiempo absoluto, que las pruebas realizadas por el solicitante han demostrado que es extremadamente bajo (menor que una fracción de segundo). En otras palabras, el reconocimiento del par de fotones gemelos termina sólo tras algunas fracciones de segundo.

La presente invención emplea un método diferente de adquisición de fotones gemelos diseñado para resolver el problema técnico principal anterior.

El método según la presente invención se muestra en la figura 2.

En primer lugar (bloque 100), se genera una señal de sincronización suministrando el haz de láser desde la fuente 20 directamente a las fibras 7, 8 ópticas. El haz de sincronización se recibe por las estaciones 4 y 5, donde la señal de sincronización entrante activa los detectores 50, 51, 53, 54 (o al menos tres de ellos) e inicia los relojes 62a, 62b; este instante marca el origen de tiempo local de las estaciones 4 y 5.

El siguiente bloque (bloque 110) calcula el tiempo relativo ΔT_a del fotón adquirido en una primera estación (por ejemplo, la estación 4) con respecto al origen de tiempo local, y el tiempo relativo ΔT_b del fotón adquirido en una segunda estación (por ejemplo, la estación 5) con respecto al origen de tiempo local.

El siguiente bloque (bloque 120) reconoce un par de fotones gemelos cuando la diferencia de tiempo ΔT_a medida en una primera estación (por ejemplo, la estación 4) y la diferencia de tiempo correspondiente ΔT_b medida en una segunda estación (por ejemplo, la estación 5) coinciden sustancialmente, es decir cuando el valor absoluto de la diferencia entre ΔT_a y ΔT_b es inferior a la ventana de tiempo de coincidencia:

$$|\Delta T_a - \Delta T_b| < w \qquad (4)$$

Si esto es así, el origen de tiempo local de ambas estaciones se desplaza hacia el instante de coincidencia determinado (bloque 130); de otro modo, continúa la exploración de datos.

Cualquiera que sea el caso, ambos bloques 120 y 130 vuelven al bloque 110 para repetir las operaciones anteriores y buscar otros pares de fotones gemelos.

En otras palabras, la diferencia de tiempo ΔT entre el instante de adquisición t_n de un fotón y el instante de adquisición t_{n-1} del fotón recibido anteriormente en un par: $\Delta T = t_n - t_{n-1}$, se mide (bloque 110) en cada estación 4, 5, y

se reconoce un par de fotones gemelos cuando el tiempo relativo ΔT_a medido en una primera estación (4) y el tiempo relativo correspondiente ΔT_b medido en una segunda estación (5) coinciden sustancialmente (bloque 120).

Entonces se repiten las operaciones de medición y reconocimiento anteriores.

El método de sincronización según la presente invención resuelve el problema técnico al que se hizo referencia anteriormente permitiendo que el tiempo de adquisición se prolongue indefinidamente.

Es decir, dada la ecuación (1), a la luz de la descripción anterior con referencia al diagrama de bloques de la figura 2:

$$|(1+\alpha) – (1+\beta)| (t_n – t_{n-1}) < w \quad (5)$$

En cuyo caso, si $\Delta T = t_n - t_{n-1}$, la ecuación (5) da:

$$\Delta T < w / (\alpha - \beta) \quad (6)$$

Por tanto, siempre que los datos lleguen a una frecuencia

$$\nu = 1/\Delta T = (\alpha - \beta)/w \quad (7)$$

el tiempo de adquisición de los relojes 62a, 62b puede prolongarse indefinidamente.

La figura 3 muestra un gráfico del resultado de la prueba, en que el eje x muestra el índice de coincidencia resultante (es decir, el número de fotones gemelos extraídos), y el eje y, el valor de tiempo de uno de los relojes 62a, 62b. La curva sombreada densamente indica el resultado del método de comparación absoluto, que se interrumpe bruscamente en un punto de interrupción PR; mientras que la curva sombreada densamente muestra el resultado del método descrito con referencia a la figura 2, y que como puede observarse, no tiene punto de interrupción.

Por medio de software, el método según la presente invención resuelve el problema planteado por la diferencia en la frecuencia de oscilación (desfase) de los dos relojes 62a, 62b; el método es extremadamente “robusto” e independiente de la frecuencia de oscilación de los relojes (que, tal como se conoce, tiende a variar con el tiempo); y no es necesario conocer de antemano la desviación de los relojes 62a, 62b con respecto al rendimiento nominal, de modo que no se requiere calibración preliminar de los relojes 62a, 62b.

Si la fuente de fotones genera fotones con una frecuencia distinta a la de la ecuación (7), podrían no reconocerse los pares de fotones gemelos. Este problema se resuelve de antemano superponiendo sobre la señal de fluorescencia paramétrica una señal adicional conocida fácilmente reconocible, por ejemplo, un tren de impulsos clásico, para aumentar la frecuencia total de la señal recibida por las estaciones 4, 5 primera y segunda, y por tanto satisfacer todavía la ecuación (7). La señal adicional se reconoce y se elimina posteriormente. Usando un tren de impulsos clásico, es decir con un número muy grande de fotones, la señal adicional se reconoce cuando se activan los cuatro fotodetectores.

REIVINDICACIONES

1. Método de sincronización y adquisición de fotones gemelos para un procedimiento de criptografía cuántica, que comprende las etapas de:

- generar pares de fotones entrelazados, en que los fotones en cada par son de polarización opuesta;

- suministrar un primer fotón en el par a través de un primer canal (7) de comunicación a una primera estación (4) de recepción que tiene un primer reloj (62a) que genera una referencia de tiempo para la primera estación de recepción;

- suministrar un segundo fotón en el par a través de un segundo canal (8) de comunicación a una segunda estación (5) de recepción que tiene un segundo reloj (62b) que genera una referencia de tiempo para la segunda estación de recepción;

- comparar, en cada estación de recepción, la polarización de cada fotón recibido con una primera base de referencia o segunda base de referencia seleccionadas aleatoriamente; comprendiendo cada base de referencia dos ejes perpendiculares, y estando separadas angularmente las bases de referencia primera y segunda por un ángulo dado;

- generar una señal de sincronización para activar el primer reloj y el segundo reloj; y

- buscar pares de fotones gemelos recibidos en las dos estaciones (4, 5) de recepción en el mismo instante medido partiendo de la base de la información proporcionada por los relojes respectivos;

caracterizado porque la etapa de buscar pares de fotones gemelos comprende las etapas de:

- medir, en cada estación (4, 5) de recepción, la diferencia de tiempo ΔT entre el instante de adquisición t_n de un fotón y el instante de adquisición t_{n-1} del fotón recibido precedente:

$$\Delta T = t_n - t_{n-1}$$

- reconocer un par de fotones gemelos cuando el valor absoluto de la diferencia entre la diferencia de tiempo ΔT_a medida en una primera estación (4) de recepción y la diferencia de tiempo correspondiente ΔT_b medida en una segunda estación (5) de recepción es menor que una ventana de tiempo de coincidencia: $|\Delta T_a - \Delta T| <$w: y

- repetir las etapas de medición y reconocimiento.

2. Método según la reivindicación 1, en el que los fotones se generan con una frecuencia v de $(\alpha-\beta)/w$ o superior, donde α y β son parámetros que tienen en cuenta el grado en que se desvía la frecuencia del reloj primero/segundo de la frecuencia nominal, y w representa la ventana de tiempo de coincidencia.

3. Método según la reivindicación 1, en el que la etapa de generar una señal de sincronización comprende las etapas de:

- suministrar un haz óptico de sincronización a las entradas del canal de comunicación primero y segundo;

- determinar la recepción del haz óptico de sincronización en la estación de recepción primera y segunda; y

- sincronizar el reloj respectivo en cada estación de recepción con la recepción de dicho haz óptico de sincronización.

4. Método según la reivindicación 3, en el que dicha etapa de comparación se realiza suministrando los fotones recibidos, con la misma probabilidad, a un primer par de detectores (50, 51) asociados con la primera base de referencia, o a un segundo par de detectores (53, 54) asociados con la segunda base de referencia; estando asociado cada detector en el par con un eje de referencia respectivo perpendicular al otro eje de referencia; activándose cada detector cuando el fotón recibido por él adopta una relación predeterminada y comprendiendo dicha etapa de medición la etapa de determinar la activación de ambos detectores de una estación de recepción con la recepción de dicho haz óptico de sincronización.

5. Método según la reivindicación 1, y que comprende las etapas de suministrar sobre ambos canales de comunicación una señal adicional conocida reconocible para aumentar la frecuencia total de la señal recibida por la

estación (4, 5) de recepción primera y segunda; y reconocer y eliminar la señal adicional en dichas estaciones (4, 5) de recepción.

6. Dispositivo para sincronizar y adquirir fotones gemelos para un procedimiento de criptografía cuántica que comprende:

- una fuente (2) de fotones para generar pares de fotones entrelazados de polarización opuesta;

- un primer canal (7) de comunicación para transmitir un primer fotón en el par;

- un segundo canal (8) de comunicación para transmitir un segundo fotón en el par;

- una primera estación (4) de recepción para recibir los fotones procedentes del primer canal (7) de comunicación; y

- una segunda estación (5) de recepción para recibir los fotones procedentes del segundo canal (8) de comunicación;

teniendo dicha estación de recepción primera y segunda un reloj (62a, 62b) primero y segundo, respectivamente, para generar referencias de tiempo respectivas para las estaciones de recepción;

comprendiendo cada estación de recepción medios de referencia para comparar la polarización de cada fotón recibido con una primera base de referencia o segunda base de referencia seleccionadas aleatoriamente; comprendiendo cada base de referencia dos ejes perpendiculares, y estando separadas angularmente la base de referencia primera y segunda por un ángulo dado;

recibiendo dicha estación de recepción primera y segunda una señal de sincronización para activar el primer reloj y el segundo reloj;

y teniendo cada estación de recepción medios de búsqueda para buscar pares de fotones gemelos recibidos en las dos estaciones (4, 5) de recepción en el mismo instante medido partiendo de la base de la información proporcionada por los relojes respectivos;

caracterizado porque dichos medios de búsqueda comprenden:

- medios (110) de comparación para medir, en cada estación (4, 5) de recepción, la diferencia de tiempo ΔT entre el instante de adquisición t_n de un fotón y el instante de adquisición t_{n-1} del fotón recibido precedente

$$\Delta T = t_n - t_{n-1}$$

- medios (120) de detección para reconocer un par de fotones gemelos cuando el valor absoluto de la diferencia entre la diferencia de tiempo ΔT_a medida en una primera estación (4) de recepción y la diferencia de tiempo correspondiente ΔT_b medida en una segunda estación (5) de recepción es menor que una ventana de tiempo de coincidencia: $|\Delta T_a - \Delta T_b| < w$; y

- medios (120) de nueva selección para volver a seleccionar dichos medios de comparación y dichos medios de detección y repetir las operaciones de medición y reconocimiento.

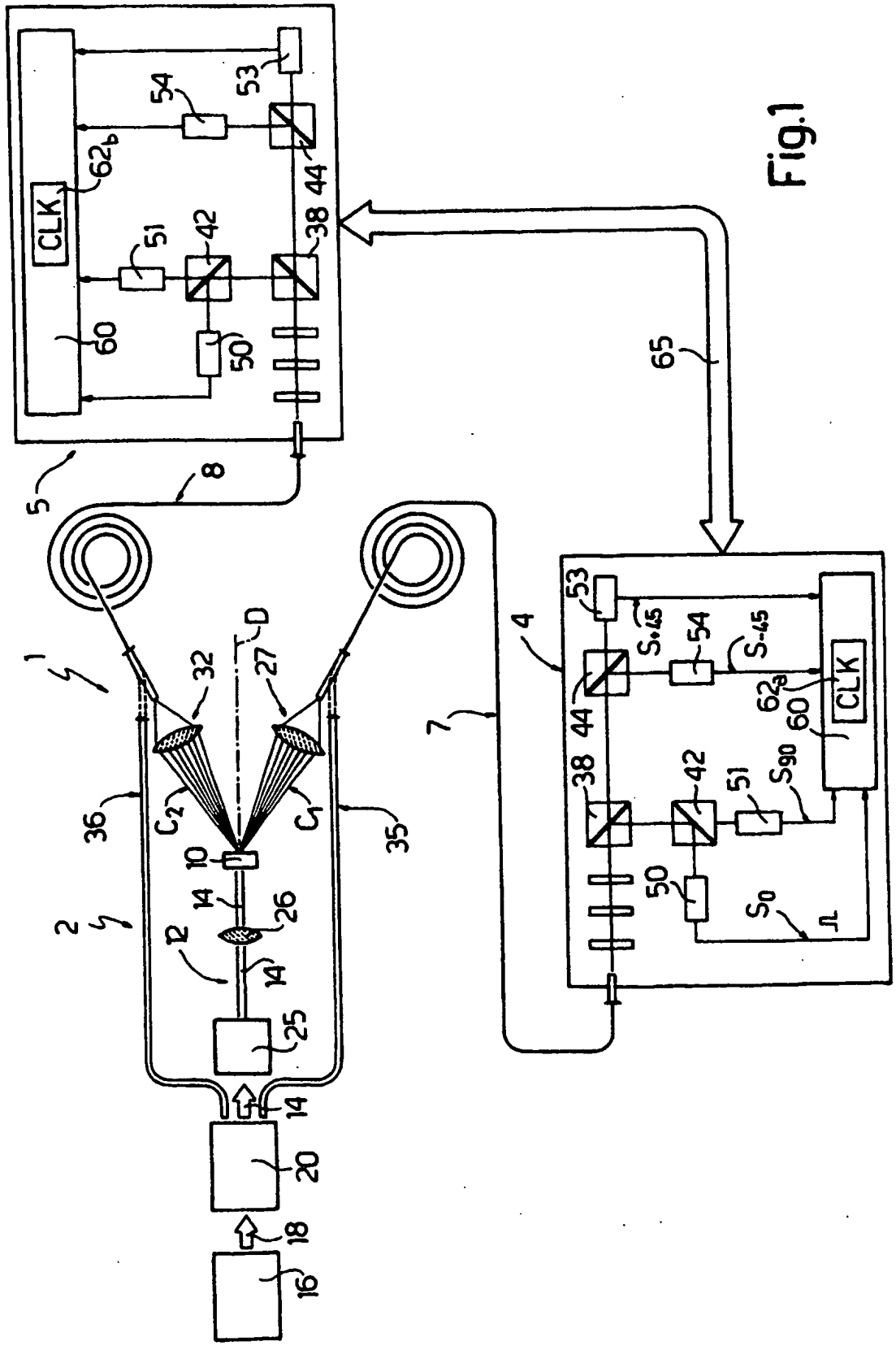

CLK
53
54
62b
44
38
42
51
60
50
65
5
8
1
32
27
D
C2
C1
36
35
10
14
26
12
25
20
18
16
7
4
S45
S90
S0
62a

Fig.1

Fig.2

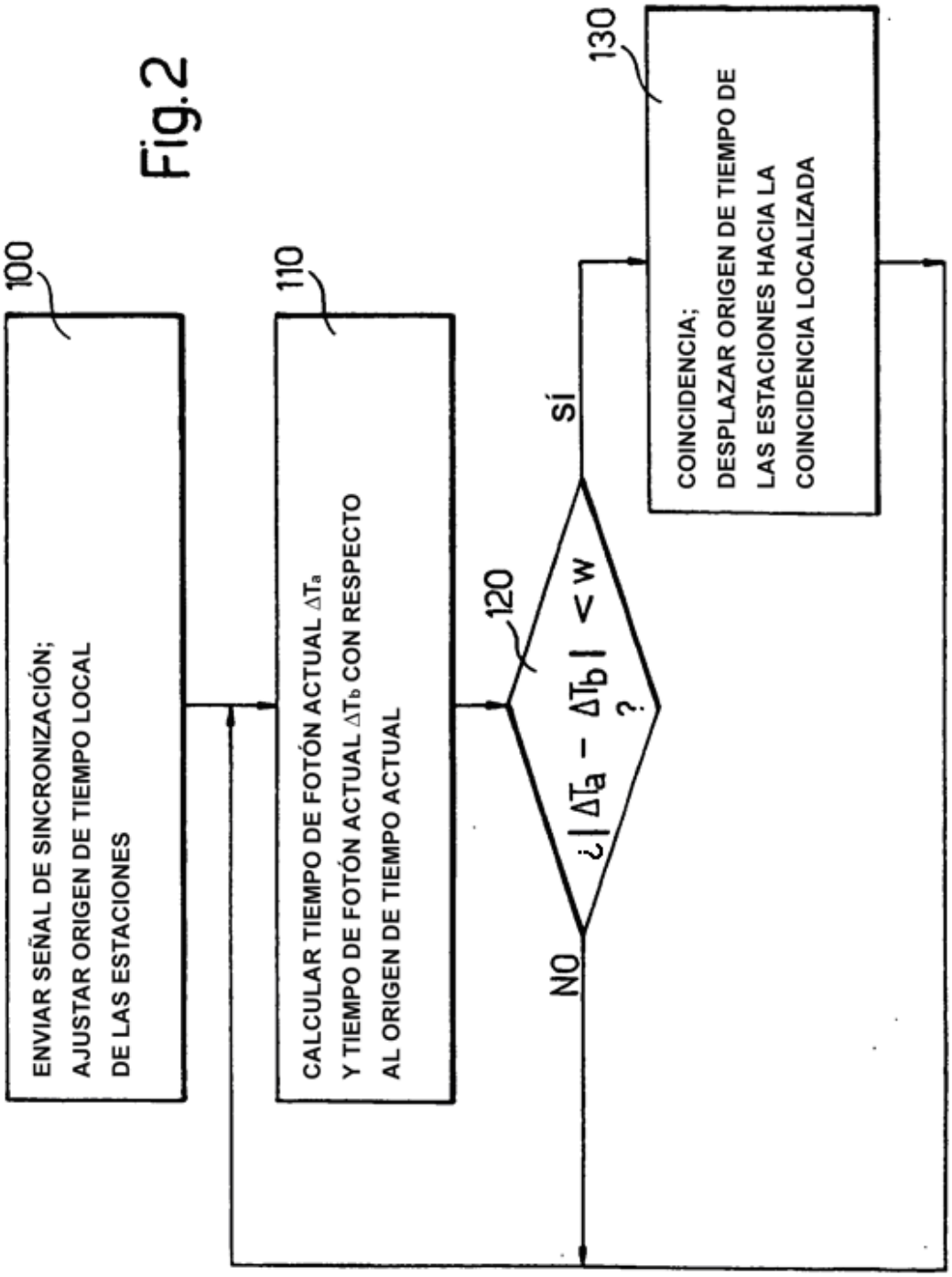
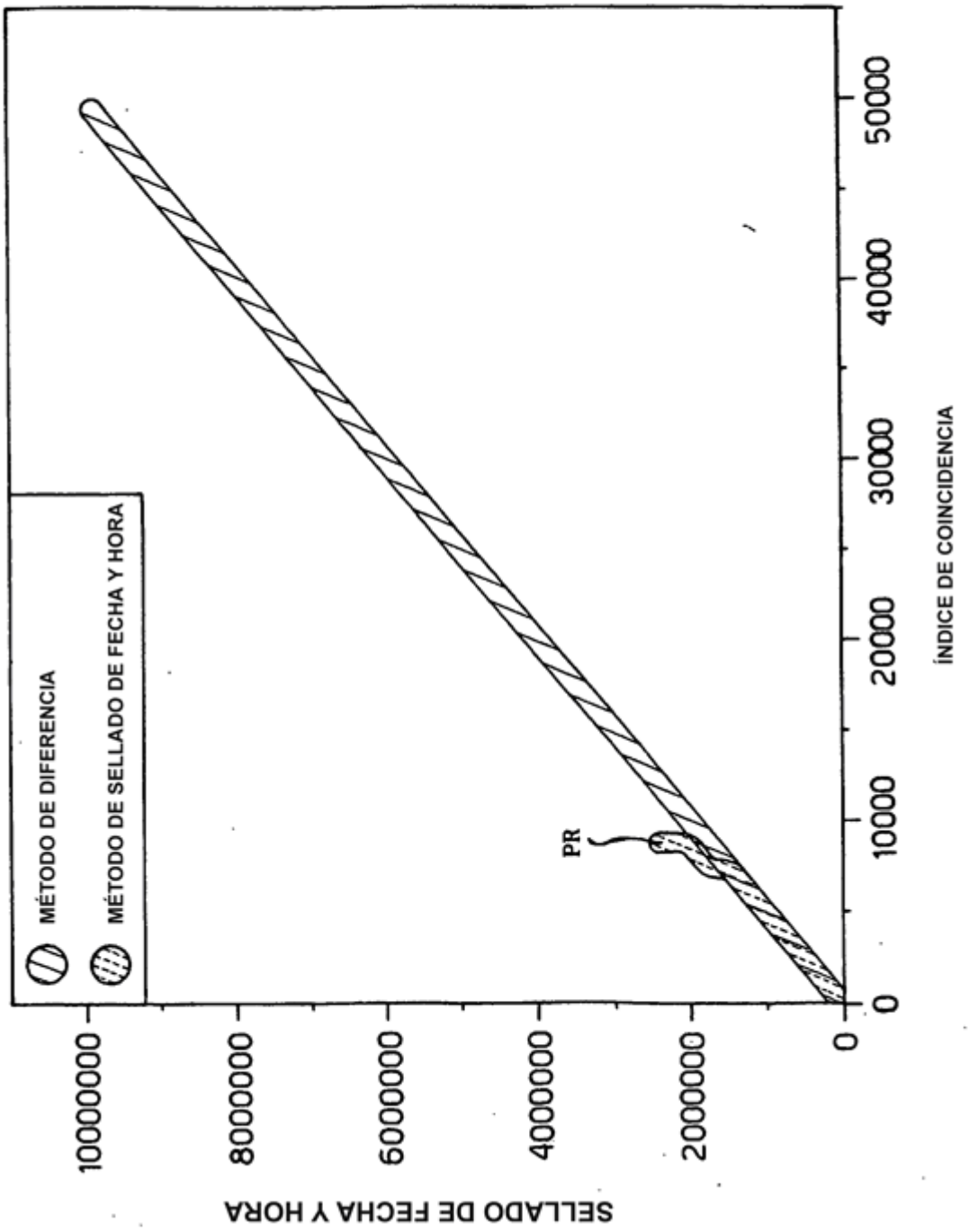

100
ENVIAR SEÑAL DE SINCRONIZACIÓN;
AJUSTAR ORIGEN DE TIEMPO LOCAL
DE LAS ESTACIONES
110
CALCULAR TIEMPO DE FOTÓN ACTUAL ΔTa
Y TIEMPO DE FOTÓN ACTUAL ΔTb CON RESPECTO
AL ORIGEN DE TIEMPO ACTUAL
120
¿| ΔTa − ΔTb | < w ?
SÍ
NO
130
COINCIDENCIA;
DESPLAZAR ORIGEN DE TIEMPO DE
LAS ESTACIONES HACIA LA
COINCIDENCIA LOCALIZADA

Fig.3


MÉTODO DE DIFERENCIA
MÉTODO DE SELLADO DE FECHA Y HORA
PR
SELLADO DE FECHA Y HORA
ÍNDICE DE COINCIDENCIA
0
2000000
4000000
6000000
8000000
10000000
0
10000
20000
30000
40000
50000