(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 750 300**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2015 E 15020257 (0)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 3185463**

(54) Título: **Aparato y método para distribución de clave cuántica con seguridad mejorada y requisitos de confianza reducidos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.03.2020

(73) Titular/es:

ID QUANTIQUE S.A. (100.0%)
Chemin De La Marbrerie 3
1227 Carouge, CH

(72) Inventor/es:

RIBORDY, GRÉGOIRE

(74) Agente/Representante:

ZUAZO ARALUZE, Alexander

DESCRIPCIÓN

Aparato y método para distribución de clave cuántica con seguridad mejorada y requisitos de confianza reducidos

Campo técnico

La presente invención se refiere en general al campo de la distribución de clave cuántica y, más precisamente, a un aparato y un método que mejoran la seguridad de un sistema de distribución de clave cuántica (QKD, *quantum key distribution*).

Antecedentes y técnica anterior

El objetivo principal de la criptografía cuántica o la distribución de clave cuántica (QKD) es poder compartir entre un emisor y un receptor una secuencia de bits cuya privacidad puede demostrarse con un conjunto limitado de suposiciones.

Si dos usuarios disponen de información secreta aleatoria compartida (denominada a continuación en el presente documento la “clave”), pueden conseguir, con seguridad demostrable, dos de los objetivos de la criptografía: 1) hacer que sus mensajes sean ininteligibles para una persona que realiza una escucha clandestina y 2) distinguir mensajes legítimos de falsificados o alterados. Un algoritmo criptográfico de libreta de un solo uso logra el primer objetivo, mientras que la autenticación de Wegman-Carter logra el segundo. Desafortunadamente, estos dos esquemas criptográficos consumen material de clave y hacen que no sea apto para uso adicional. Por tanto, es necesario que las dos partes que desean proteger los mensajes que intercambian con cualquiera o ambas de estas técnicas criptográficas ideen un modo de intercambiar material de clave nuevo. La primera posibilidad es que una parte genere la clave y la inscriba en un medio físico (disco, CD-ROM, ROM) antes de hacerla pasar a la segunda parte. El problema de este enfoque es que la seguridad de la clave depende del hecho de si se ha protegido durante toda su vida, desde su generación hasta su uso, hasta que se descarta finalmente. Además, es poco práctico y muy tedioso.

Debido a estas dificultades, en muchas aplicaciones se recurre en lugar de ello a métodos puramente matemáticos que permiten que las dos partes se pongan de acuerdo sobre un secreto compartido por un canal de comunicación inseguro. Desafortunadamente, todos los métodos matemáticos de este tipo para el acuerdo de claves se basan en requisitos no demostrados, tales como la dificultad de factorizar números enteros grandes. Por tanto, su seguridad es solo condicional y cuestionable. El desarrollo matemático futuro puede demostrar que son totalmente inseguros.

La criptografía cuántica o la distribución de clave cuántica (QKD) es un método que permite la distribución de una clave secreta entre dos partes distantes, el emisor y el receptor, con una seguridad demostrable. Una explicación del método puede encontrarse en Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel y Hugo Zbinden, “Quantum Cryptography”, Rev. of Mod. Phys. 74, (2002), cuyo contenido se supone que lo conoce un experto en la técnica. Las dos partes codifican la clave en sistemas cuánticos elementales, tales como fotones, que intercambian por un canal cuántico, tal como una fibra óptica. La seguridad de este método procede del hecho bien conocido de que la medición del estado cuántico de un sistema cuántico desconocido modifica el sistema en sí mismo. Dicho de otro modo, un espía que escucha de manera clandestina el canal de comunicación cuántico no puede obtener información sobre la clave sin introducir errores en la clave intercambiada entre el emisor y el receptor.

De manera equivalente, la QKD es segura debido al teorema de no clonación de la mecánica cuántica, que garantiza que un espía no puede duplicar el sistema cuántico transmitido y reenviar una copia perfecta al receptor.

• Principio

Existen varios protocolos de QKD. Estos protocolos describen dos partes:

1- cómo se codifican los valores de bit en sistemas cuánticos usando conjuntos de estados cuánticos y

2- cómo el emisor y el receptor actúan conjuntamente para producir una clave secreta a partir de la medición de cúbits. El protocolo usado más habitualmente de estos protocolos, que también fue el primero en inventarse, se conoce como el protocolo de Bennett-Brassard 84 (BB84), dado a conocer por Charles Bennett y Gilles Brassard en Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, Nueva York, 1984), págs. 175-179), cuyo contenido también se supone que lo conoce el experto en la técnica. Este ejemplo puede usarse para ilustrar las dos partes citadas anteriormente.

1- Por ejemplo, usando estados de polarización, el emisor codifica cada bit en un sistema cuántico de dos niveles o bien como un autoestado de la base horizontal-vertical (base “+”) o bien como un autoestado de la base diagonal (base “x”). Se dice que los bits están codificados en dos bases incompatibles. Antes de intercambiar sistemas cuánticos, el emisor y el receptor se ponen de acuerdo sobre una asignación lógica de valores de bit con estados base. En un ejemplo de una asignación lógica de bits, deciden que el valor de bit de “1” se codifica como un estado

vertical ¦I> (base horizontal-vertical) y como un estado de +45° ¦/> (base diagonal). En este caso, el valor de bit de "0" se codifica como un estado horizontal ¦-> (base horizontal-vertical) o un estado de -45° ¦\> (base diagonal).

2- Para cada bit, el emisor usa un generador de números aleatorios apropiado para generar dos bits aleatorios de información, que se usan para determinar el valor de bit (un bit aleatorio) y la información de base (un bit aleatorio). El sistema cuántico se envía al receptor, que lo analiza en una de las dos bases. El receptor usa un generador de números aleatorios apropiado para producir un bit aleatorio de información usado para determinar la base de medición (la información de base). La base de medición se selecciona aleatoriamente para cada sistema cuántico. Después del intercambio de un gran número de sistemas cuánticos, el emisor y el receptor llevan a cabo un procedimiento denominado reconciliación de bases o también conocido como tamizado. En una primera etapa, el emisor anuncia al receptor, a través de un canal de comunicación convencional y público, que se denomina canal de servicio, la base + o x en la que se preparó cada sistema cuántico. En una segunda etapa, el receptor considera la compatibilidad de bases para cada cúbit. Cuando el receptor ha usado la misma base que el emisor para su medición, sabe que el valor de bit que ha medido debe ser el que se envió por el emisor. El mismo indica públicamente (a través del canal de servicio) para qué sistemas cuánticos se satisface esta condición. Las mediciones para las que se ha usado la base errónea simplemente se descartan. En ausencia de un espía, la secuencia de bits compartida no tiene errores. Aunque un espía que quiere obtener cierta información sobre la secuencia de bits que está intercambiándose puede elegir entre varios ataques, las leyes de la física cuántica garantizan que no será capaz de hacerlo sin introducir una perturbación perceptible en la clave.

Sin embargo en un entorno práctico, también pueden generarse errores por imperfecciones experimentales. Por tanto, todos los protocolos se complementan con un protocolo de destilación de claves que se ejecuta por el canal de servicio, que consiste normalmente en una etapa de corrección de errores y una etapa de amplificación de privacidad, y en las que se autentican comunicaciones clásicas.

Existen varios protocolos de QKD (véase Gisin *et al.* para una buena visión general) y estos protocolos de QKD pueden agruparse en familias, en las que todos los protocolos en una familia pueden implementarse con el mismo hardware. Como ejemplo, todos los protocolos basados en cuatro estados de cúbit, que son los autoestados de dos bases conjugadas, forman una familia de protocolos. Una ilustración de este ejemplo se proporciona en los protocolos BB84 y SARG (véase Valerio Scarani, Antonio Acín, Grégoire Ribordy y Nicolas Gisin (2004). "Quantum Cryptography Protocolos Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations"), que pertenecen a la misma familia descrita previamente. En este caso, solo la etapa de reconciliación de bases (o tamizado) cambia de un protocolo a otro. Tal como se explicó anteriormente, en el caso del protocolo BB84, el receptor anuncia el valor de bit aleatorio usado para la elección de la base de medición, mientras que el valor de bit del cúbit medido se mantiene secreto. Cuando el emisor anuncia la compatibilidad de la base, el emisor y el receptor saben que sus valores de bit respectivos usados para la definición u obtenidos con la medición del cúbit son idénticos. En el caso del protocolo SARG, el tamizado es diferente. El receptor anuncia el valor de bit del cúbit medido y el valor de bit usado para la elección de la base de medición se mantiene secreto. El emisor anuncia cuando puede adivinar el valor de bit secreto del receptor con sus dos valores de bit (uno es el valor de bit portado por el cúbit; el otro define la base de este cúbit).

A diferencia de otros enfoques para la distribución de claves, la QKD ofrece seguridad demostrable basándose en las leyes de la física cuántica. Aunque esto es cierto para sistemas de QKD ideales, el hardware práctico puede incluir imperfecciones que pueden conducir a fugas de información. Tales imperfecciones podrían introducirse incluso por un fabricante malintencionado, que pretende engañar a los usuarios de sus productos.

Confiar en el fabricante de un sistema puede no ser apropiado en todas las situaciones. Este problema también se conoce bien en el campo de la criptografía convencional. Como ejemplo, en el caso del Estándar de cifrado avanzado por ejemplo, puede conseguirse este objetivo modificando la caja de sustitución (caja S, *S-box*) usada en su etapa de *SubBytes*. Haciendo esto, es posible obtener una pluralidad de algoritmos que comparten la estructura de AES pero que son diferentes. Después de la modificación de las cajas S, el usuario es la única parte que sabe el algoritmo de cifrado real usado. No obstante, no se ha desarrollado la misma clase de solución para la criptografía cuántica.

Sería deseable reducir en la distribución de clave cuántica la posibilidad de introducir debilidades en el sistema tales como puertas traseras. Además, otro problema es que la mayoría de los ataques en sistemas de QKD definidos en pirateo cuántico se definen de manera óptima para un protocolo de QKD específico. Un modo de abordar estos problemas es que el fabricante incluya en sus productos la posibilidad de modificar algunos de los parámetros relevantes para la seguridad. Esta modificación la realiza normalmente el usuario después de que el equipo haya abandonado las instalaciones del fabricante, de manera que los parámetros modificados solo los conoce el usuario.

Sin embargo, este enfoque no es compatible con el concepto de QKD tal como se considera en la técnica anterior. De hecho, una de las suposiciones principales en las pruebas de QKD es que el protocolo se conoce completamente por cualquier persona (por ejemplo, un espía). Una vez que el protocolo se ha elegido, cualquier persona conoce todos los valores de parámetro excepto los valores de los bits aleatorios que se usarán para la elección de la generación o el análisis de estados de cúbit. Puede ser necesario introducir variables desconocidas extra debido a

las diferencias que pueden aparecer entre el principio de QKD y su implementación. Un enfoque de este tipo se ha considerado en la patente relacionada con la supresión de puertas EP 2625817 que da a conocer una solución que impide que una persona que realice una escucha clandestina tome el control del único fotón de un aparato de QKD. En este caso, se introducen valores aleatorios, desconocidos por el cliente pero quizá conocidos por el fabricante de QKD, para cambiar aleatoriamente el valor de eficiencia de este detector. Este tipo de solución permite mejorar la seguridad de QKD frente a intentos de escucha clandestina introduciendo parámetros aleatorios que son desconocidos para la persona que realiza una escucha clandestina. No obstante, este tipo de solución que permite mejorar la seguridad frente a intentos de escucha clandestina no aborda ciertos problemas de seguridad desde el punto de vista del cliente. Un cliente que quiere estar seguro respecto a su fabricante de QKD podría pedir la posibilidad de cambiar algunos de los parámetros relevantes para la seguridad de su aparato de QKD de tal manera que el fabricante no pueda saberlo con antelación. La técnica anterior no permite que los usuarios de QKD modifiquen parámetros del sistema de QKD para que sean desconocidos para el fabricante de QKD con antelación.

La invención definida pretende superar este problema.

La bibliografía no de patente incluye:

- Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel y Hugo Zbinden, (2002) “Quantum Cryptography”, Rev. of Mod. Phys. 74,
- C. H. Bennett y G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. En Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volumen 175, página 8. Nueva York, 1984.
- Valerio Scarani, Antonio Acín, Grégoire Ribordy y Nicolas Gisin (2004). “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”

Sumario de la invención y definición del problema técnico

Un modo de abordar el problema descrito anteriormente es incluir, en productos de QKD, la posibilidad de modificar algunos de los parámetros relevantes para la seguridad. Esta modificación la realiza habitualmente el usuario después de que el equipo haya abandonado las instalaciones del fabricante, de modo que los parámetros modificados solo los conoce el usuario. Se ofrece un ejemplo de tal modificación de parámetros en el campo de la criptografía convencional mediante el uso de un algoritmo de cifrado personalizado. En este caso de criptografía convencional, la idea es modificar algunos parámetros del algoritmo de cifrado, mientras se mantiene su estructura general tal como se presenta en la sección de antecedentes.

El objeto de esta invención es aplicar el mismo principio a QKD modificando algunos parámetros usados para definir el protocolo implementado. Al hacerlo así, se vuelve más difícil que un adversario prepare un ataque de implementación y extraiga información útil. También permite que el usuario modifique su sistema de modo desconocido para el fabricante del producto y aumente de ese modo su protección frente a ataques basándose en características de producto.

Por tanto, la invención se refiere a un aparato de distribución de clave cuántica para intercambiar al menos una clave cuántica, que comprende un emisor que incluye un controlador de QKD y un transmisor de QKD, un receptor que incluye un controlador de QKD y un receptor de QKD, un canal de servicio para la sincronización del emisor y el receptor y la realización una de etapa de tamizado, un canal cuántico para intercambiar cúbits, en el que el emisor y el receptor están adaptados para recibir parámetros de personalización y parámetro de , respectivamente, en el que el sistema de QKD está adaptado para soportar al menos dos protocolos P1 y P2, en el que el sistema de QKD está adaptado para conmutar de un primer protocolo P1 a un segundo protocolo P2.

Preferiblemente, el controlador de QKD incluye al menos dos subcontroladores, el controlador 1, el controlador 2 y un conmutador (113).

Preferiblemente, la elección del protocolo puede definirse gracias a valores digitales almacenados en los parámetros de fabricante del equipo o en los parámetros de personalización.

Preferiblemente, las secuencias de protocolos Pi se definen mediante bloques de longitud L_i de cúbits.

Preferiblemente, la conmutación de protocolo se realiza durante la operación de QKD.

Preferiblemente, la diferencia entre protocolos soportados se define en la etapa de tamizado.

Un segundo aspecto de la invención se refiere a un método de uso de parámetros de personalización en el aparato de QKD y que comprende las etapas de definir valores de parámetros de personalización en el controlador de QKD y leer y almacenar parámetros de personalización para un cúbit, usar parámetros de personalización para el

tamizado de dicho cúbit y almacenar la nueva clave tamizada, analizar si la clave tamizada es suficientemente grande, realizar la destilación de la clave tamizada almacenada si la clave tamizada es suficientemente grande.

Breve descripción de los dibujos

Se describen a continuación realizaciones preferidas de la invención con referencia a los dibujos, que ilustran realizaciones preferidas de la invención sin limitar la misma. En los dibujos,

Figura 1: Aparato de la invención basado en el sistema de QKD con parámetro adicional

Figura 2: Aparato de la invención con bloques de protocolos diferentes

Figura 3: Caso específico de bloques de protocolo con asignación de valores de bit lógicos diferentes

Figure 4: Método asociado a la implementación del aparato de la invención

Descripción de realizaciones preferidas

La descripción de la invención se basa en varias figuras.

El objeto principal de la invención es mejorar la seguridad ofrecida por un sistema de QKD y reducir los requisitos de confianza de un usuario de QKD hacia el fabricante del equipo.

Tal como se muestra en la figura 1, esta invención puede usarse para intercambiar de manera segura claves de cifrado entre un emisor (100) y un receptor (200). Se basa en un sistema de QKD tradicional modificado para aceptar un parámetro de personalización adicional. El hardware del sistema de QKD consiste en un transmisor (120) de QKD y un receptor (220) de QKD conectados a través de un canal cuántico, un canal (500) cuántico. El transmisor (120) y el receptor (220) de QKD consisten normalmente en componentes ópticos y electrónicos adaptados para producir y detectar un flujo de cúbits (520). El transmisor (120) y el receptor (220) de QKD se controlan por controladores (110 y 210) de QKD a través de líneas (115 y 215) de comunicación. Estos controladores consisten, por ejemplo, en uno o varios microprocesadores u ordenadores así como software. Los controladores (110 y 210) de QKD se conectan a través de un canal (400) de servicio. El canal de servicio es un canal de comunicación que permite que los controladores intercambien una serie de mensajes. Por ejemplo, pueden consistir en una conexión de Internet o un enlace óptico directo.

Los controladores (110 y 210) de QKD controlan el funcionamiento del transmisor (120) y el receptor (220) de QKD para iniciar el intercambio de la secuencia de cúbits (520).

El controlador (110) de QKD en el emisor (100) comprende una serie de subcontroladores que pueden hacer funcionar el aparato de QKD con protocolos diferentes. En la figura 1, se muestra el caso de un aparato que ejecuta dos protocolos diferentes. Sin embargo, este caso puede extenderse a cualquier valor entero. En la figura 1, el controlador (110) de QKD comprende un controlador (111) 1 que permite que el sistema de QKD funcione con el protocolo 1, un controlador (112) 2 que permite que el sistema de QKD funcione con el protocolo 2 y un conmutador (113) que controla la transición del protocolo 1 al protocolo 2. De manera similar, el controlador (120) de QKD en el receptor (200) comprende un controlador (211) 1 que permite que el sistema de QKD funcione con el protocolo 1, un controlador (212) 2 que permite que el sistema de QKD funcione con el protocolo 2 y un conmutador (213) que controla la transición del protocolo 1 al protocolo 2.

El controlador (110) de QKD registra la lista de cúbits (520) transmitidos. De manera similar, el controlador (210) de QKD registra la base de medición y el resultado de detección, si lo hubiera, para cada cúbit (520). Los controladores (110 y 210) de QKD ejecutan entonces un protocolo conocido como el tamizado intercambiando mensajes en el canal (400) de servicio para producir la clave tamizada. Este protocolo implica normalmente la comparación cúbit a cúbit de la base de preparación y medición para la secuencia de cúbits (520). En ausencia de escucha clandestina e imperfecciones experimentales, la clave tamizada del emisor (100) y el receptor (200) son exactamente idénticas.

Suponiendo que la tasa de errores en la clave tamizada es menor que un valor umbral, los controladores (110 y 210) de QKD pueden destilar entonces este material (150 y 250) de clave tamizada para dar uno compartido. Esta fase de destilación incluye normalmente una etapa de corrección de errores y una etapa de amplificación de privacidad, pero pueden usarse otras etapas. El material (150 y 250) de clave consiste en una secuencia de bits, que se emite por los controladores (110 y 220) de QKD, a través de líneas (151 y 251) de comunicación. La línea (151) de comunicación puede implementarse, por ejemplo, con un enlace de comunicación en serie portado por hilos de cobre que enlazan el controlador (110) de QKD y un aparato del cliente a través del que se definen los parámetros (160) de personalización. La cantidad de información que una persona que realiza una escucha clandestina puede haber obtenido sobre este material (150 y 250) de clave puede vincularse a un valor arbitrariamente pequeño, siempre que la persona que realiza una escucha clandestina cumpla con las leyes de la física.

Este sistema de QKD, que consiste en un emisor (100) y un receptor (200), puede implementar una pluralidad de protocolos de QKD que forman una familia de protocolos. En una primera realización de esta invención, se modifica para aceptar la introducción de un parámetro (160) de personalización a través de la línea (161) de comunicación en el controlador (110) de QKD del emisor (100). El parámetro (160) de personalización puede implementarse, por ejemplo, como un valor digital que define el protocolo que el aparato de QKD deber usar para el intercambio de claves secretas. De manera similar, se introduce un parámetro (260) de personalización en el controlador (210) de QKD del controlador (210) de QKD del receptor (200) a través de la línea (261) de comunicación. Los parámetros (260) de personalización y la línea (261) de comunicación pueden implementarse como los parámetros (160) de personalización y la línea (161) de comunicación. Dependiendo de la realización, los parámetros (160 y 260) de personalización serán idénticos o diferentes. En el ejemplo anterior, el parámetro (160) de personalización permite que un usuario accione un conmutador (113). El conmutador (113) activa alternativamente o bien controlador (111) 1 activando de este modo el protocolo 1 o bien el controlador (112) 2 activando de este modo el protocolo 2 en el sistema de QKD.

En cada controlador (110) y (120) de QKD, un conjunto de parámetros por defecto se almacena en una memoria. Si al menos uno de los dos controladores (110) o (120) de QKD no recibe ningún parámetro (160) o (260) de personalización, se usan los parámetros por defecto para ajustar los conmutadores (113) y (213) a una configuración por defecto que permite que funcione el dispositivo de QKD, aunque no se haya definido ningún parámetro de personalización. Por ejemplo, los aparatos (100) y (200) de QKD funcionan con los controladores (111) y (211) 1 de manera continua.

La figura 2 ilustra un primer uso posible de los parámetros (160 y 260) de personalización. Los cúbits (520) intercambiados por el canal (500) cuántico se agrupan en bloques (510) que consisten en al menos un cúbit y cuya longitud L_i (511), donde 'i' representa el índice del bloque, especificado en número de cúbits, puede ser idéntica o diferente. Esta agrupación puede predefinirse en el emisor (100) y el transmisor (200) por el fabricante del equipo. Alternativamente, puede especificarse en los parámetros (160 y 260) de personalización. Para cada bloque (510) de cúbits (520), se usa un protocolo (530) de QKD seleccionado de la familia de protocolos que pueden implementarse usando el emisor (100) y el transmisor (200). La lista de protocolos (530) usados para los diferentes bloques puede predefinirse en el emisor (100) y el transmisor (200) por el fabricante del equipo. Alternativamente, puede especificarse en los parámetros (160 y 260) de personalización. La implementación de esta invención requiere la posibilidad de usar al menos dos protocolos (530). Una posible realización se basa en el uso de los protocolos BB84 y SARG. Estos dos protocolos pueden implementarse usando el mismo hardware del transmisor (120) y el receptor (220) de QKD. La única diferencia reside en la implementación de la etapa de tamizado en los controladores (110) y (210) de QKD, lo que hace que estos protocolos sean particularmente adecuados para la implementación de la invención.

Dependiendo de los protocolos (530) seleccionados de la familia de protocolos que puede implementarse usando el transmisor (120) y el receptor (220) de QKD, algunos parámetros físicos de los cúbits (520) pueden ser diferentes para cada protocolo. En este caso, estos parámetros pueden ajustarse bloque a bloque. Alternativamente, puede usarse un único conjunto de valores, que es adecuado aunque no óptimo, para todos los protocolos.

Un ejemplo de tal ajuste es, cuando se selecciona entre los protocolos BB84 y SARG, suponiendo que se usan pulsos de láser débiles como cúbits (520), el número medio de fotones de dichos cúbits (520). El número de fotones promedio óptimo difiere para los protocolos BB84 y SARG. Es posible que el emisor (100) ajuste el número medio de fotones para un bloque particular de los bloques (510) según el protocolo asociado a este protocolo. Alternativamente, el emisor (100) también podría ajustar el número medio de fotones de los cúbits (520) al valor correspondiente al peor caso de los protocolos que están usándose.

Tras la producción de la clave tamizada para cada uno de los bloques (510) usando los controladores (110 y 210) de QKD, este material de clave debe destilarse. Normalmente, prefieren usarse bloques grandes de bits para esta destilación para optimizar el rendimiento. Un primer enfoque para la destilación de claves es reunir todos los bloques de clave tamizada correspondientes a un protocolo particular en un bloque mayor que luego se destila. Este enfoque ofrece la posibilidad de optimizar los parámetros de destilación para el material de clave producido usando cada uno de los protocolos. Otro enfoque es combinar los bloques de clave tamizada correspondientes a al menos dos protocolos en un bloque mayor, que luego se destila. Con este enfoque, los parámetros de destilación deben ajustarse a un valor que sea adecuado para todos los protocolos, aunque puede no ser óptimo para uno o varios de los protocolos. Después de la destilación de clave, el material (150) y (250) de clave se pone, igual que en el caso de QKD tradicional, a disposición de aplicaciones externas tales como, por ejemplo, cifrado de enlace, usando las líneas (151) y (251) de comunicación. La ventaja de esta invención es que el usuario tiene la capacidad de modificar el funcionamiento del emisor (100) y el receptor (200) después de que haya abandonado las instalaciones del fabricante, y reducir de ese modo los requisitos de confianza hacia el fabricante del equipo. La invención también puede hacer que sea más difícil que un atacante externo prepare un ataque de implementación, dado que no sabría, para un cúbit particular, frente a qué protocolo debe prepararse el ataque.

En una segunda realización de la invención, se implementan los protocolos (520) usados para los bloques (510) usando diferentes asignaciones de valores de cúbit a bit. Dos ejemplos de tales asignaciones se muestran en la

figura 3, para el caso en el que se usan variaciones del protocolo BB84. El protocolo BB84 se basa en dos conjuntos de dos estados. Se asigna un valor de bit binario a cada estado de estos conjuntos y es posible cambiar esta asignación. En la figura 3, la principal diferencia entre las posibilidades (550) n.º 1 (540) y n.º 2 de correspondencia de valor de cúbit a bit es para la base diagonal. Esta asignación puede predefinirse en el emisor (100) y el transmisor (200) por el fabricante del equipo. Alternativamente, puede especificarse en los parámetros (160 y 260) de personalización. Para cada bloque (510) de cúbits (520), se especifica una asignación de valor de bit particular. La lista de asignaciones de valores de bit usada para los diferentes bloques puede predefinirse en el emisor (100) y el transmisor (200) por el fabricante del equipo. Alternativamente, puede especificarse en los parámetros (160 y 260) de personalización. La elección de la asignación de valor de bit puede definirse gracias a un valor digital almacenado en el fabricante (100 y 200) del equipo o en los parámetros (160 y 260) de personalización. Los otros aspectos de esta segunda realización son idénticos a los de la primera realización. En esta segunda realización de la invención, la asignación de valor de bit es el parámetro usado para cambiar el protocolo.

Una tercera realización consiste en una combinación de las realizaciones primera y segunda, en las que tanto el protocolo como la asignación de valores de bit se modifican bloque a bloque.

La figura 4 muestra un método (600) de uso de los parámetros de personalización con el aparato (100) y (200) de QKD. En una primera etapa (610), los controladores (110) y (210) de QKD reciben los parámetros de personalización del cliente. Esta recepción puede realizarse bloque a bloque o de manera continua. El rendimiento de recepción debe ser suficiente en comparación con la necesidad de rendimiento del aparato de QKD. En paralelo con esta etapa (610), los controladores (110) y (210) de QKD empiezan un proceso en bucle. En una primera etapa (620) de este proceso en bucle, se vacían todas las memorias intermedias usadas en los controladores de QKD. En una segunda etapa (630), los controladores de QKD leen y almacenan el valor de los parámetros de personalización para un cúbit. Por ejemplo, los parámetros de personalización definen que el protocolo usado para dicho cúbit es BB84 o SARG. En una tercera etapa (640), se usan estos parámetros de personalización por los controladores de QKD para enviar los valores de parámetro adecuados a los transmisores (120) y (220) de QKD. Esto lo realiza el subcontrolador (111) o (112) apropiado seleccionado por el conmutador (113). Por ejemplo, la generación y el análisis del cúbit se realizarán con respecto al protocolo BB84 o SARG elegido. En una cuarta etapa (650), se usan los parámetros de personalización por los controladores (110) y (210) de QKD definen cómo realizar el tamizado de dicho cúbit. Esto lo realiza el subcontrolador (111) o (112) apropiado seleccionado por el conmutador (113). Por ejemplo, el tamizado puede llevarse a cabo tal como se define en el protocolo BB84 o SARG. Este nuevo valor de bit tamizado se almacena en los controladores (110) y (210) de QKD. En una quinta etapa (660), los controladores de QKD verifican si el número de bits tamizados almacenados es suficientemente grande para iniciar la destilación. Si no es el caso, el método retrocede a la etapa (630) para preparar el intercambio de otro cúbit. Si el número de bits tamizados almacenados es suficientemente grande, se inicia la destilación. En una sexta etapa (670), se usan los parámetros de personalización por los controladores (110) y (210) de QKD para llevar a cabo la destilación de clave de modo apropiado. Esto lo realiza el subcontrolador (111) o (112) apropiado seleccionado por el conmutador (113). Por ejemplo, los bits tamizados se reparten en dos grupos, uno correspondiente al uso de BB84 para el proceso de intercambio y tamizado de cúbits, otro correspondiente al uso de SARG. Y entonces, los dos grupos de bit se destilan con respecto a su protocolo de grupo. Entonces, el método (600) retrocede en bucle a la etapa (620) en la que inició la generación de claves y se vacían todas las memorias intermedias.

Uno de los aspectos que no forma parte de la invención, pero que es esencial para su funcionamiento es la sincronización de dos listas de parámetros de personalización. En efecto, para el funcionamiento apropiado de esta invención, es necesario que el emisor (100) y el receptor (200) conmuten en el mismo subcontrolador en su controlador (110) o (120) de QKD respectivo para cada cúbit. Los siguientes párrafos describen algunas técnicas que pueden usarse para llevar a cabo esta tarea.

El valor correspondiente de los parámetros (160) y (260) de personalización debe estar disponible para el emisor (100) y el receptor (200) y existen dos enfoques para garantizar esta disponibilidad. En un primer enfoque, los parámetros se distribuyen manualmente entre el emisor (100) y (200). La implementación de QKD tradicional requiere la distribución de un secreto compartido previamente usado para la autenticación de las comunicaciones que tienen lugar por el canal (400) de servicio durante la primera sesión de QKD. Es posible adjuntar los parámetros (160) y (260) de personalización a este secreto compartido previamente y distribuir manualmente esta información al emisor (100) y el receptor (200).

Un segundo enfoque para garantizar la disponibilidad de los parámetros (160) y (260) de personalización al emisor (100) y el receptor (200) es asignar la selección local de la personalización a una de las partes (100 o 200) y hacer que esta parte transfiera esta información a su pareja. Esta transmisión puede tener lugar en formato cifrado usando una clave de cifrado, para impedir la intercepción de esta información por una parte malintencionada. Esta transmisión puede tener lugar antes del intercambio de cúbits (520) o después de esta transmisión. En este segundo caso, una parte malintencionada no tendrá acceso a los parámetros (160 y 260) de personalización durante el intercambio de los cúbits (520) y no podrá usar esta información para seleccionar qué información preparar. Esta asincronía puede usarse para aliviar los requisitos para la transmisión de dichos parámetros (160 y 260) de personalización en formato cifrado.

Dichos parámetros (160 y 260) de personalización pueden usarse directamente para definir la personalización exacta del sistema de QKD tal como, por ejemplo la agrupación de cúbits (520) en bloques (510) así como el protocolo asignado a cada bloque. Alternativamente, estos parámetros (160 y 260) de personalización pueden posprocesarse y expandirse usando un proceso algorítmico para producir la personalización exacta. Un ejemplo de tal expansión algorítmica consiste en un generador de números pseudoaleatorios en el que los parámetros (160 y 260) de personalización se usan como semillas.

Finalmente, los parámetros (160 y 260) de personalización pueden renovarse durante el funcionamiento del sistema de QKD usando parte del material (150 y 250) de clave producido por el sistema. Este material de clave puede usarse o bien como nuevos parámetros de personalización o bien usarse para cifrar la transmisión de nuevos valores de los parámetros de personalización.

Aunque se describió anteriormente la presente invención en relación con realizaciones preferidas, se entenderá que no está limitada de ese modo a las realizaciones descritas o ilustradas, sino por el alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Aparato de distribución de clave cuántica para intercambiar al menos una clave cuántica, que comprende

un emisor (100) que incluye un controlador (110) de QKD y un transmisor (120) de QKD

un receptor (200) que incluye un controlador (120) de QKD y un receptor (220) de QKD

un canal (400) de servicio para la sincronización del emisor (100) y el receptor (200) y la realización de una etapa de tamizado,

un canal (500) cuántico para intercambiar bloques de al menos un cúbit entre el emisor y el receptor,

en el que el aparato de QKD está adaptado para soportar al menos dos protocolos P1 y P2 diferentes y comprende un conmutador para conmutar entre dichos al menos dos protocolos diferentes, y el emisor (100) y el receptor (200) están adaptados para recibir parámetros (160) de personalización y parámetros (260) de personalización que definen, respectivamente, una elección de protocolo entre los al menos dos protocolos P1 y P2,

en el que la diferencia entre los protocolos soportados se define en la etapa de destilación, y

caracterizado porque la conmutación de protocolo se realiza durante la operación de QKD.

2. Aparato según la reivindicación 1, en el que secuencias de cúbits intercambiadas según los al menos dos protocolos P1 y P2 diferentes se definen mediante bloques de longitud L_i de cúbits.

3. Aparato según la reivindicación 1, en el que una asignación de valor de cúbit a bit depende de bloques de cúbit.

4. Aparato según la reivindicación 1, en el que la elección del protocolo puede definirse gracias a parámetros por defecto almacenados en los parámetros (100 y 200) de fabricante de equipo o en los parámetros (160 y 260) de personalización.

5. Aparato según la reivindicación 1, en el que los protocolos P1 y P2 implementados difieren en la asignación lógica de valores de bit.

6. Aparato según la reivindicación 1, en el que la diferencia entre protocolos soportados se define en la etapa de destilación

7. Método de hacer funcionar el aparato de QKD según la reivindicación 1, que comprende las etapas de:

- una etapa de inicio que comprende ejecutar una operación de QKD entre un emisor (100) y un receptor (200) según un protocolo elegido entre al menos dos protocolos P1 y P2 diferentes, comprendiendo dicha operación de QKD
    - intercambiar bloques de al menos un cúbit entre el emisor y el receptor,
    - realizar una sincronización del emisor (100) y el receptor (200) y
    - realizar una etapa de tamizado;
- una etapa de recepción en la que el emisor (100) y el receptor (200) reciben valores de parámetros de personalización que definen una elección de protocolo entre al menos dos protocolos P1 y P2,
- una etapa de conmutación que comprende conmutar entre dichos al menos dos protocolos P1 y P2 diferentes según los valores de parámetros de personalización,

caracterizado porque la conmutación de protocolo se realiza durante la operación de QKD.

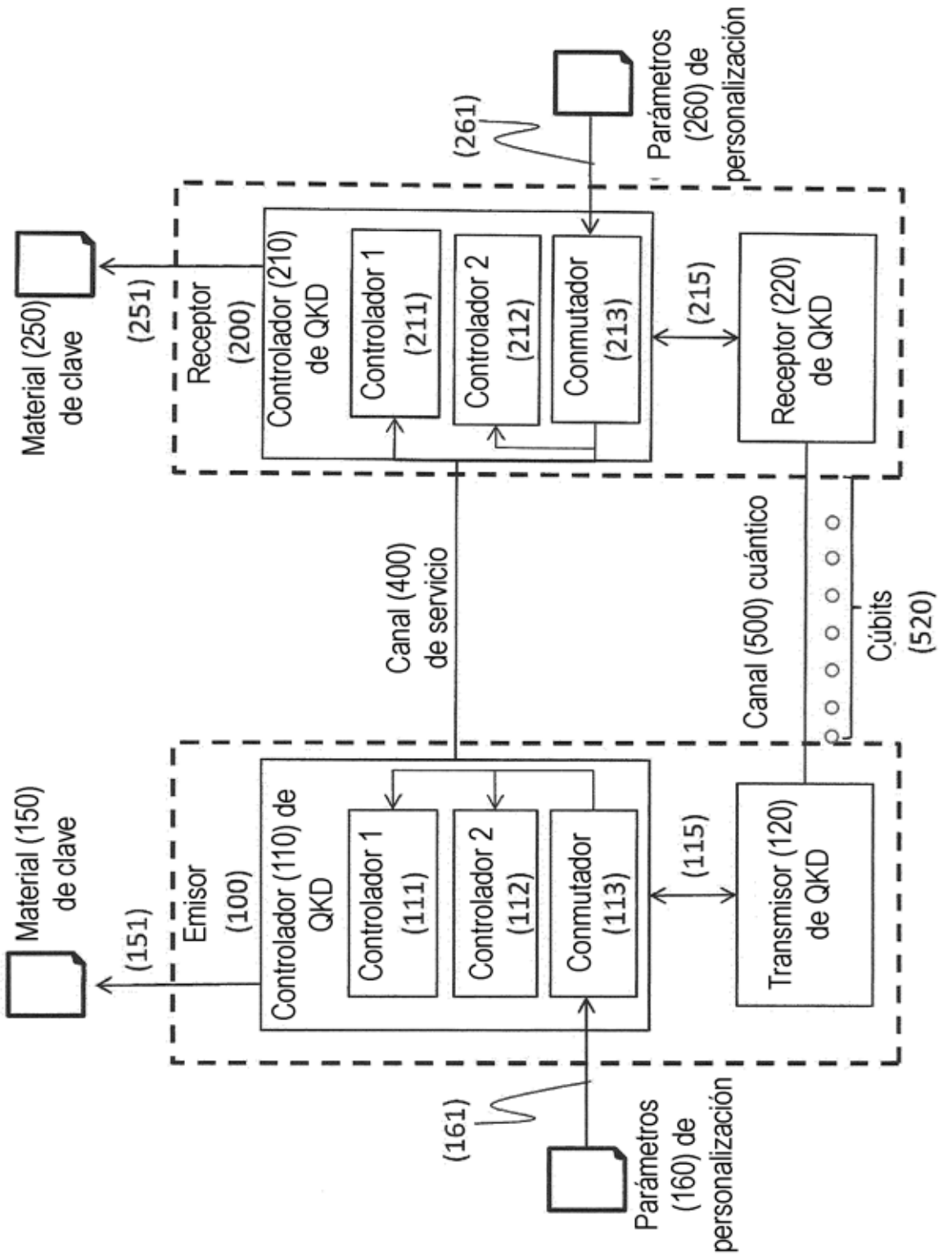
Material (250) de clave
(251)
Receptor (200)
Controlador (210) de QKD
Controlador 1 (211)
Controlador 2 (212)
Conmutador (213)
(215)
Receptor (220) de QKD
(261)
Parámetros (260) de personalización
Canal (400) de servicio
Canal (500) cuántico
Cúbits (520)
Material (150) de clave
(151)
Emisor (100)
Controlador (110) de QKD
Controlador 1 (111)
Controlador 2 (112)
Conmutador (113)
(115)
Transmisor (120) de QKD
(161)
Parámetros (160) de personalización

Figura 1

Bloque (510)	1	2	3	…	n
Longitud (511)	L_1	L_2	L_3	…	L_n
Cúbits (520)	$Q(1;1) - Q(L_1;1)$	$Q(1;2) - Q(L_2;2)$	$Q(1;3) - Q(L_3;3)$	…	$Q(1;n) - Q(L_n;n)$
Protocolo (530)	P_1	P_2	P_3	…	P_n
Parámetros (160) de personalización	$L_1 – P_1$	$L_2 – P_2$	$L_3 – P_3$	…	$L_n – P_n$
Parámetros (260) de personalización	$L_1 – P_1$	$L_2 – P_2$	$L_3 – P_3$	…	$L_n – P_n$

Figura 2

Posibilidad nº. 1 (540) de correspondencia de valor de cúbit a bit

Base	Horizontal-Vertical (+)		Diagonal (x)	
Estado	I	-	/	\
Valor	0	1	0	1

Posibilidad nº. 2 (550) de correspondencia de valor de cúbit a bit

Base	Horizontal-Vertical (+)		Diagonal (x)	
Estado	I	-	/	\
Valor	0	1	1	0

Figura 3

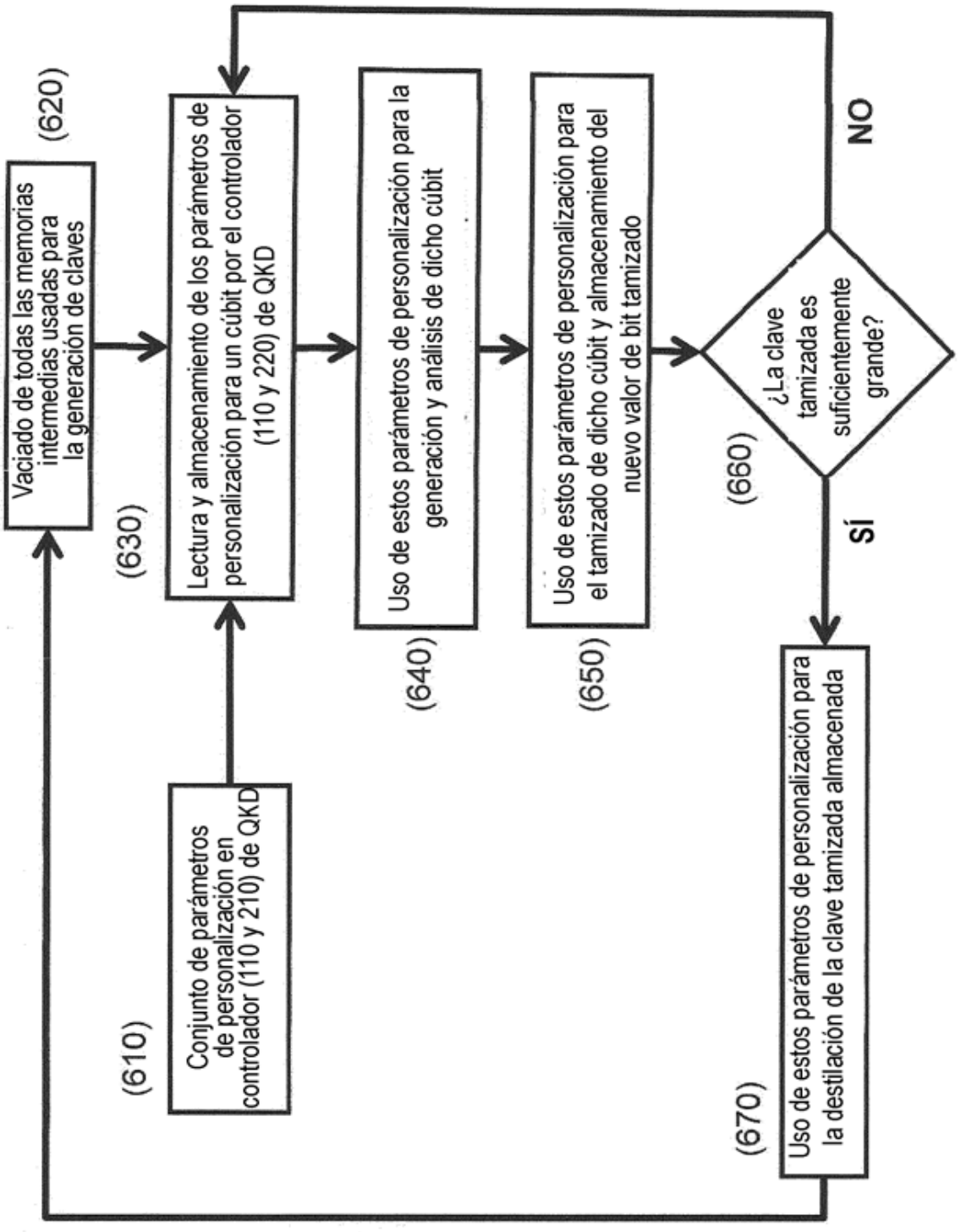
Vaciado de todas las memorias intermedias usadas para la generación de claves
(620)
Lectura y almacenamiento de los parámetros de personalización para un cúbit por el controlador (110 y 220) de QKD
(630)
Conjunto de parámetros de personalización en controlador (110 y 210) de QKD
(610)
Uso de estos parámetros de personalización para la generación y análisis de dicho cúbit
(640)
Uso de estos parámetros de personalización para el tamizado de dicho cúbit y almacenamiento del nuevo valor de bit tamizado
(650)
¿La clave tamizada es suficientemente grande?
(660)
NO
SÍ
Uso de estos parámetros de personalización para la destilación de la clave tamizada almacenada
(670)

Figura 4