(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 509 816**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.08.2012 E 12179118 (0)**

(97) Fecha y número de publicación de la concesión europea: **02.07.2014 EP 2555466**

(54) Título: **Sistema para la distribución de claves criptográficas**

(30) Prioridad:

05.08.2011 IT TO20110733

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2014

(73) Titular/es:

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

(72) Inventor/es:

BOVINO, FABIO ANTONIO

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema para la distribución de claves criptográficas.

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención se refiere, en general, a un sistema de distribución de claves criptográficas y, en particular, a un sistema de distribución de claves criptográficas basado en la distribución de clave cuántica.

ESTADO DE LA TÉCNICA

Como es conocido, la Distribución de clave cuántica (DCC) (QKD por sus siglas en inglés) es una técnica basada en los principios de la mecánica cuántica que permite a dos dispositivos de comunicación conectados entre sí por medio de un canal cuántico generar una clave criptográfica aleatoria, llamada clave cuántica, la cual puede ser utilizada por dichos dispositivos de comunicación o por los usuarios de dichos dispositivos de comunicación, para comunicarse entre sí de una manera segura por un canal público o más bien por un canal de interceptación, por ejemplo una conexión a través de Internet.

En general, el canal cuántico comprende un enlace cuántico, por ejemplo un enlace a través de fibra óptica o en espacio libre, y un enlace convencional, o más bien no cuántico, tal como una conexión a través de Internet.

La QKD dispone que una serie de estados cuánticos, usualmente en forma de fotones, se transmita en el canal cuántico, en particular por el enlace cuántico del canal cuántico, con el fin de generar una clave cuántica común a los dos dispositivos de comunicación.

En particular, la QKD dispone que los dos dispositivos de comunicación realicen las siguientes operaciones:

- midan propiedades específicas, por ejemplo el plano de polarización, de los fotones transmitidos por el enlace cuántico del canal cuántico;
- intercambien, por el enlace convencional del canal cuántico, información relacionada con las medidas realizadas; y
- generen una y la misma clave cuántica sobre la base de las medidas realizadas y de la información intercambiada por el enlace convencional del canal cuántico.

Como es conocido, los protocolos de distribución de claves criptográficas tradicionales no permiten detectar si las claves criptográficas distribuidas han sido interceptadas. En particular, los protocolos de distribución de claves criptográficas tradicionales no permiten descubrir si una clave criptográfica distribuida antes de iniciar una comunicación encriptada basada en dicha clave criptográfica ha sido interceptada, por ejemplo por medio de un ataque de intermediarios (man in the middle).

Por el contrario, la QKD permite detectar si alguien ha intentado interceptar de manera abusiva la clave cuántica. En particular, la QKD no solo permite detectar si alguien ha interceptado o no de manera abusiva cualquier información intercambiada y/o cualquier fotón transmitido por el canal cuántico durante la generación de la clave cuántica, sino que también permite evitar que la información interceptada se pueda utilizar para rastrear la clave cuántica.

El protocolo BB84 es un algoritmo de QKD conocido que fue descrito por primera vez por C.H. Bennett y G. Brassard en “Criptografía cuántica: distribución de clave pública y el lanzamiento de moneda”, Proc. de la Conf. Int. del IEEE sobre el procesamiento de señales, sistemas y ordenadores, Bangalore, India, del 10-12 de diciembre de 1984, págs. 175-179.

En particular, el protocolo BB84 permite que dos dispositivos de comunicación conectados entre sí por medio de un canal cuántico que comprende un enlace cuántico y un enlace convencional, es decir, un enlace no cuántico, generen una clave cuántica binaria segura. Ninguno de los dos enlaces necesita ser una conexión segura; de hecho, el protocolo BB84 está diseñado también para tener en cuenta posibles interferencias, en cualquier forma, con ambos enlaces por un tercero no autorizado.

En lo sucesivo, los dos dispositivos de comunicación se denominarán dispositivo A y dispositivo B en beneficio de la simplicidad de la descripción.

En particular, de acuerdo con el protocolo BB84, el dispositivo A transmite una serie de estados cuánticos al dispositivo B por el canal cuántico, específicamente por el enlace cuántico del canal cuántico, en forma de fotones oportunamente polarizados para codificar información binaria. Las polarizaciones de los fotones transmitidos se pueden definir de acuerdo con dos bases distintas, por ejemplo una primera base + que comprende las polarizaciones ortogonales *0º* y *90º* y una segunda base x que comprende las polarizaciones ortogonales *45º* y *135º*.

En detalle, de acuerdo con el protocolo BB84, el dispositivo A realiza las siguientes operaciones:

● genera una secuencia aleatoria de bits; y

● para cada bit generado,

- selecciona aleatoriamente una base respectiva,

- transmite, por el canal cuántico, específicamente por el enlace cuántico del canal cuántico, un fotón polarizado respectivo de acuerdo con la base seleccionada respectiva para codificar dicho bit, y

- almacena dicho bit, la base seleccionada respectiva y el instante de tiempo cuando se transmite el fotón respectivo.

En la tabla que aparece a continuación se proporciona un ejemplo de cómo se pueden polarizar los fotones transmitidos por el canal cuántico para codificar *0* ó *1* en las dos bases + y x.

TABLA

BASE	*0*	*1*
+	*0º*	*90º*
x	*45º*	*135º*

Además, Para cada fotón recibido por el canal cuántico, específicamente por el enlace cuántico del canal cuántico, el dispositivo B realiza las siguientes operaciones:

● selecciona aleatoriamente una base respectiva;

● mide la polarización del fotón recibido utilizando la base seleccionada respectiva;

● determina el bit codificado por la polarización medida; y

● almacena el bit determinado, la base seleccionada respectiva y el instante de tiempo cuando se recibe dicho fotón.

Una vez que termina la transmisión de los fotones, el dispositivo A envía al dispositivo B, por el enlace convencional del canal cuántico, las bases utilizadas para polarizar los fotones transmitidos y el dispositivo B envía al dispositivo A, de nuevo por el enlace convencional del canal cuántico, las bases utilizadas para medir las polarizaciones de los fotones recibidos. Los dispositivos A y B descartan cualquier bit para el cual el dispositivo B ha utilizado una base para medir la polarización del fotón que es diferente de la utilizada por el dispositivo A para polarizar dicho fotón. Cada dispositivo obtiene de este modo una clave sin procesar respectiva constituida por los bits no descartados.

En beneficio de la simplicidad de la descripción, hasta ahora el protocolo BB84 se ha descrito asumiendo que el dispositivo A transmite fotones únicos al dispositivo B por el canal cuántico. No obstante, como es conocido, el protocolo BB84 se puede implementar también mediante el uso de pares de los así llamados fotones entrelazados, donde los fotones de cada par transportan la misma información cuántica. En particular, en el caso de un protocolo BB84 basado en pares de fotones entrelazados, un dispositivo cuántico acoplado al canal cuántico que conecta los dispositivos A y B se utiliza para transmitir pares de fotones entrelazados por dicho canal cuántico, específicamente por el enlace cuántico del canal cuántico, de tal forma que, para cada par transmitido, un primer fotón sea recibido por el dispositivo A y un segundo fotón sea recibido por el dispositivo B.

En detalle, en el caso de un protocolo BB84 basado en pares de fotones entrelazados, para cada fotón recibido por el canal cuántico, cada uno de los dispositivos A y B realiza las siguientes operaciones:

● cada dispositivo selecciona aleatoriamente una base respectiva;

● cada dispositivo mide la polarización del fotón recibido utilizando la base seleccionada respectiva;

● cada dispositivo determina el bit codificado por la polarización medida; y

● cada dispositivo almacena el bit determinado, la base seleccionada respectiva y el instante de tiempo cuando se recibe dicho fotón.

Una vez que termina la transmisión de los fotones, los dispositivos A y B intercambian las bases utilizadas para medir las polarizaciones de los fotones recibidos por el enlace convencional del canal cuántico y descartan los bits para los cuales utilizan diferentes bases. Cada dispositivo obtiene de este modo una clave sin procesar respectiva constituida por los bits no descartados.

De manera ideal, ambos en el caso de un protocolo BB84 basado en fotones únicos y en el caso de un protocolo BB84 basado en pares de fotones entrelazados, las claves sin procesar generadas por los dispositivos A y B deberían coincidir. Desafortunadamente, no obstante, en el mundo real las dos claves sin procesar no coinciden debido a una posible interceptación llevada a cabo por un tercero no autorizado y debido a la no idealidad del canal cuántico y los dispositivos de comunicación implicados en la QKD o más bien debido a errores (QBER) producidos inevitablemente en la generación de las claves sin procesar.

Por lo tanto, ambos en el caso de un protocolo BB84 basado en fotones únicos y en el caso de un protocolo BB84 basado en pares de fotones entrelazados, después de haber generado las claves sin procesar, los dispositivos A y B llevan a cabo dos pasos adicionales que resultan en la generación de una clave criptográfica única conocida solamente por dichos dispositivos A y B. Estos pasos adicionales del protocolo BB84 se conocen respectivamente como reconciliación de información y amplificación de privacidad y fueron descritos por primera vez por C. H. Bennett, F. Bessette, G. Brassard, L. Salvail y J. Smolin en "Criptografía cuántica experimental", diario de criptología, vol.5, n.º 1, 1992, págs. 3-28.

En particular, en el paso de reconciliación de información, los dispositivos A y B corrigen errores en las dos claves sin procesar de manera que se genere una clave reconciliada idéntica para ambos dispositivos A y B.

En detalle, en el paso de reconciliación de información, los dispositivos A y B intercambian información útil por el enlace convencional del canal cuántico para corregir los errores en las claves sin procesar, de manera que se minimice la información transmitida con respecto a cada clave sin procesar.

Al final del paso de reconciliación de información, los dispositivos A y B obtienen la misma clave reconciliada y también son capaces de reconocer:

● qué información sobre las claves sin procesar ha sido interceptada por un tercero no autorizado durante la generación de las claves sin procesar; y

● qué información sobre la clave reconciliada ha sido interceptada por un tercero no autorizado durante el paso de reconciliación de información.

Finalmente, en el paso de amplificación de privacidad, sobre la base de la clave reconciliada y por medio de un mecanismo de autenticación recíproco para los dispositivos A y B o, más bien, para los respectivos usuarios, los dispositivos A y B generan una y la misma clave segura que puede ser utilizada por dichos dispositivos A y B o más bien por los respectivos usuarios, para comunicarse entre sí de una manera segura por un canal público.

En particular, en el paso de amplificación de privacidad, por medio de un mecanismo de autenticación recíproco para los dispositivos A y B o, más bien, para los respectivos usuarios, los dispositivos A y B generan una y la misma clave segura que es más corta que la clave reconciliada de manera que se minimice la probabilidad de que un tercero no autorizado pueda rastrear dicha clave segura sobre la base de la información interceptada.

En detalle, cada uno de los dispositivos A y B realiza las siguientes operaciones en el paso de amplificación de privacidad:

● cada dispositivo determina una matriz hash sobre la base de una clave de autenticación actual respectiva; y

● cada dispositivo comprime la clave reconciliada por medio de la matriz hash respectiva, obteniendo de este modo una cadena de bits final respectiva que es más corta que la clave reconciliada.

Con mayor detalle, si ambos dispositivos A y B o, más bien, los respectivos usuarios, poseen una y la misma clave de autenticación actual, dichos dispositivos A y B determinan una y la misma matriz hash sobre la base de la misma clave de autenticación actual y, por lo tanto, cuando se comprime la clave reconciliada utilizando la misma matriz hash, generan una y la misma cadena de bits final que comprende:

● una y la misma clave cuántica que puede ser utilizada por dichos dispositivos A y B o más bien, por los respectivos usuarios, para comunicarse entre sí de una manera segura por un canal público; y

● una y la misma clave de autenticación nueva que se va a utilizar como la clave de autenticación actual en el paso de amplificación de privacidad de una QKD posterior.

En su lugar, si los dispositivos A y B o más bien los respectivos usuarios no tienen una misma clave de autenticación actual, al final del paso de amplificación de privacidad, dichos dispositivos A y B generan dos cadenas de bits finales diferentes y, por lo tanto, dos claves cuánticas diferentes y dos claves de autenticación nuevas diferentes, las cuales se vuelven inutilizables de este modo.

Un primer inconveniente de la QKD está relacionado con el hecho de que los dos dispositivos de comunicación implicados deben estar relativamente cerca porque el enlace cuántico del canal cuántico que los conecta solamente puede estar a pocos kilómetros como máximo.

Además, un segundo inconveniente está relacionado con el hecho de que, si se desea explotar la QKD para permitir que una serie de dispositivos de comunicación se comuniquen de manera segura, sí que es necesario que cada posible par de dispositivos de comunicación esté conectado por medio de un canal cuántico respectivo.

Por consiguiente, dado que el coste asociado con la implementación de un canal cuántico único es bastante elevado, la implementación de un canal cuántico respectivo para cada posible par de dispositivos de comunicación resulta muy cara.

Por último, la restricción de la existencia de un canal cuántico para cada posible par de nodos limita el tamaño físico de una red completamente conectada con la distancia máxima permitida para un enlace cuántico.

La solicitud PCT WO 2007/123869 A2 describe una administración de clave criptográfica y métodos y sistemas de autenticación de usuario para redes de criptografía cuántica que permiten a los usuarios comunicarse de manera segura por un canal de comunicación tradicional.

En particular, WO 2007/123869 A2 describe un método que incluye la conexión de una autoridad central de clave criptográfica QKCA a cada usuario de una manera segura por medio de enlaces cuánticos que permiten que se encripten y desencripten datos sobre la base de claves cuánticas. De acuerdo con el método descrito en WO 2007/123869 A2, cuando dos usuarios desean comunicarse entre sí de una manera segura, la autoridad central de clave criptográfica QKCA envía una secuencia de bits aleatoria a cada usuario por el enlace cuántico respectivo y, entonces, los dos usuarios utilizan dicha secuencia de bits aleatoria como una clave para codificar y descodificar los datos que intercambian por un canal de comunicación tradicional.

De acuerdo con una forma de realización específica de la invención descrita en WO 2007/123869 A2 (en particular, descrita en la página 8 e ilustrada en la figura 4 de WO 2007/123869 A2), un primer usuario A está conectado por medio de un primer canal cuántico QL-A a una primera autoridad central de clave criptográfica QKCA-A y un segundo usuario B está conectado por medio de un segundo canal cuántico QL-B a una segunda autoridad central de clave criptográfica QKCA-B que, a su vez, está conectada a la primera autoridad central de clave criptográfica QKCA-A por medio de un tercer canal cuántico QL-AB. Cuando el primer usuario A desea comunicarse con el segundo usuario B por un canal de comunicaciones tradicional, dicho primer usuario A envía una solicitud para la comunicación con dicho segundo usuario B por el primer canal cuántico QL-A a la primera autoridad central de clave criptográfica QKCA-A, la cual enruta dicha solicitud por el tercer canal cuántico QL-AB a la segunda autoridad central de clave criptográfica QKCA-B, la cual, a su vez, enruta dicha solicitud por el segundo canal cuántico QL-B al segundo usuario B. Si el segundo usuario B acepta la solicitud, la segunda autoridad central de clave criptográfica QKCA-B genera una secuencia de bits aleatoria y envía dicha secuencia de bits aleatoria al segundo usuario B por

el segundo canal cuántico QL-B y a la primera autoridad central de clave criptográfica QKCA-A por el tercer canal cuántico QL-AB. La primera autoridad central de clave criptográfica QKCA-A enruta entonces dicha secuencia de bits aleatoria al primer usuario A por el primer canal cuántico QL-A. En otras palabras, la primera autoridad central de clave criptográfica QKCA-A actúa como un enrutador entre el primer usuario A y la segunda autoridad central de clave criptográfica QKCA-B que genera la secuencia de bits aleatoria que se va a utilizar para volver las comunicaciones por el canal de comunicación tradicional entre los usuarios A y B seguras.

La forma de realización específica anteriormente mencionada de la invención descrita en WO 2007/123869 A2 tiene algunos problemas de seguridad intrínsecos, ya que la primera autoridad central de clave criptográfica QKCA-A conoce la secuencia de bits aleatoria que se va a utilizar para volver las comunicaciones entre los usuarios A y B seguras. Por lo tanto, si la primera autoridad central de clave criptográfica QKCA-A fuese de mala fe, podría distribuir también dicha secuencia de bits aleatoria a otros usuarios no autorizados, que serían capaces de descodificar por consiguiente los datos intercambiados por el canal de comunicación tradicional entre los usuarios A y B sin que ellos se den cuenta.

OBJETO Y RESUMEN DE LA INVENCIÓN

El objeto de la presente invención es, por lo tanto, el de proporcionar un sistema de distribución de clave criptográfica basado en la distribución de clave cuántica que es capaz de mitigar los inconvenientes descritos previamente.

El objeto indicado anteriormente se logra por la presente invención en lo que se refiere a un sistema de distribución de clave criptográfica, de acuerdo con lo que se define en las reivindicaciones adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para un mejor entendimiento de la presente invención, algunas formas de realización preferidas, proporcionadas a modo de ejemplo no limitativo, se ilustrarán ahora con referencia a los dibujos adjuntos (no a escala), donde:

- la figura 1 muestra de manera esquemática un sistema de distribución de clave criptográfica de acuerdo con un primer aspecto de la presente invención; y

- la figura 2 muestra de manera esquemática un sistema de distribución de clave criptográfica de acuerdo con un segundo aspecto de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN PREFERIDAS DE LA INVENCIÓN

La siguiente descripción se proporciona para permitir a un experto en el campo incorporar y utilizar la invención. Diversas modificaciones en las formas de realización descritas serán inmediatamente obvias para los expertos en el campo y los principios genéricos descritos en este documento se pueden aplicar a otras formas de realización y aplicaciones sin dejar el ámbito de protección de la presente invención.

En consecuencia, la presente invención no debería considerarse como limitada solo a las formas de realización descritas e ilustradas en este documento, sino que se le debería conceder el ámbito de protección más amplio en consonancia con los principios y características descritos en este documento y definidos en las reivindicaciones adjuntas.

La presente invención se refiere a un sistema de distribución de clave criptográfica basado en la Distribución de clave cuántica (QKD). De acuerdo con la presente invención, con el fin de implementar una QKD, tanto el protocolo BB84 basado en fotones únicos como el protocolo BB84 basado en pares de fotones entrelazados se pueden utilizar de manera conveniente.

Un sistema de distribución de clave criptográfica de acuerdo con un primer aspecto de la presente invención comprende:

- al menos un nodo de servidor; y

- uno o varios nodo(s) de cliente.

De acuerdo con dicho primer aspecto de la presente invención, cada nodo de cliente está conectado al nodo del servidor por medio de un canal cuántico correspondiente que comprende:

- un enlace cuántico respectivo, por ejemplo, en fibra óptica o en espacio libre; y
- un enlace público respectivo, es decir, un enlace de interceptación, tal como una conexión a través de Internet.

Además, siempre de acuerdo con dicho primer aspecto de la presente invención, el nodo del servidor se configura para implementar con cada nodo de cliente las QKD basadas en el protocolo BB84 respectivas en el canal cuántico correspondiente.

Con el fin de describir con detalle el primer aspecto de la presente invención, la figura 1 muestra de manera esquemática un ejemplo de un sistema de distribución de clave criptográfica de acuerdo con dicho primer aspecto de la presente invención.

En particular, el sistema de distribución de clave criptográfica mostrado en la figura 1 comprende:

- un nodo del servidor (S); y
- cuatro nodos de cliente, indicados respectivamente como (C1), (C2), (C3) y (C4), cada uno de los cuales está conectado al nodo del servidor (S) por medio de un canal cuántico correspondiente representado en la figura 1 por un segmento de línea sólido.

En la práctica, cada uno de los nodos de cliente (C1), (C2), (C3) y (C4) pueden ser utilizados por uno o varios suscriptores al sistema de distribución de clave criptográfica.

En particular, un suscriptor al sistema de distribución de clave criptográfica puede utilizar uno de los nodos de cliente (C1), (C2), (C3) y (C4) para recibir una o varias claves cuánticas de enlace respectivas. De hecho, el nodo del servidor (S) y cada uno de los nodos de cliente (C1), (C2), (C3) y (C4) están configurados para generar en cooperación claves cuánticas de enlace respectivas mediante la implementación de QKD basadas en el protocolo BB84 respectivas en el canal cuántico correspondiente.

Con detalle, si un suscriptor al sistema de distribución de clave criptográfica utiliza uno de los nodos de cliente (C1), (C2), (C3) y (C4) para recibir una clave cuántica de enlace respectiva, el nodo del servidor (S) y el nodo de cliente utilizado implementan una QKD basada en el protocolo BB84 en el canal cuántico correspondiente con el fin de generar una *clave* cuántica de enlace k_L asociada a dicho suscriptor.

Con mayor detalle, cuando un suscriptor al sistema de distribución de clave criptográfica utiliza uno de los nodos de cliente (C1), (C2), (C3) y (C4) para recibir una clave cuántica de enlace respectiva, se llevan a cabo las siguientes operaciones:

- el nodo de cliente utilizado recibe del suscriptor una clave de autenticación de QKD actual $k_{AUT\text{-}QKD}$ de *M* bits de dicho suscriptor con respecto al nodo del servidor (S);
- el nodo de cliente utilizado y el nodo del servidor (S), el cual almacena dicha clave de autenticación de QKD actual $k_{AUT\text{-}QKD}$ del suscriptor con respecto a dicho nodo del servidor (S), implementa una QKD basada en un protocolo BB84 en el canal cuántico correspondiente mediante el uso de dicha clave de autenticación de QKD actual $k_{AUT\text{-}QKD}$ del suscriptor con respecto al nodo del servidor (S) en el paso de amplificación de privacidad; de esta forma, el nodo del cliente y el nodo del servidor (S) utilizados generan una cadena de *L* bits que comprende una *clave* cuántica de enlace k_L de *N* bits asociada al suscriptor y una clave de autenticación de QKD nueva $k_{AUT-QKD}^{NUEVA}$ de *M* bits del suscriptor con respecto al nodo del servidor (S) (donde *L*=*N*+*M*);
- el nodo del servidor (S) almacena la *clave* cuántica de enlace k_L asociada a dicho suscriptor y la clave de autenticación de QKD nueva $k_{AUT-QKD}^{NUEVA}$ de dicho suscriptor con respecto a dicho nodo del servidor (S); y
- el nodo de cliente utilizado proporciona al suscriptor la clave cuántica de enlace k_L asociada a dicho suscriptor y la

clave de autenticación de QKD nueva $k_{AUT-QKD}^{NUEVA}$ de dicho suscriptor con respecto al nodo del servidor (S).

Cuando el suscriptor utiliza de nuevo uno de los nodos de cliente (C1), (C2), (C3) y (C4) para recibir una clave cuántica de enlace nueva, el nodo de cliente y el nodo del servidor (S) utilizados utilizarán la clave de autenticación de QKD nueva $k_{AUT-QKD}^{NUEVA}$ de dicho suscriptor con respecto al nodo del servidor (S) en el paso de amplificación de privacidad de la QKD nueva implementada para generar la clave cuántica de enlace nueva.

De manera conveniente, la clave de autenticación de QKD inicial con respecto al nodo del servidor (S) se puede proporcionar a cada suscriptor cuando se firma la suscripción al sistema de distribución de clave criptográfica.

Un suscriptor al sistema de distribución de clave criptográfica de acuerdo con el primer aspecto de la presente invención que utiliza un nodo de cliente para recibir una *clave* cuántica de enlace respectiva k_L puede proporcionar de manera conveniente dicho nodo de cliente con la QKD de clave de autenticación actual respectiva $k_{AUT-QKD}$ con respecto al nodo del servidor (S) de diversas formas, en particular:

- por medio de una interfaz de usuario de dicho nodo de cliente; o

- conectando localmente a dicho nodo de cliente, por ejemplo por medio de una conexión USB, un dispositivo electrónico portátil respectivo que almacena dicha QKD de clave de autenticación actual respectiva $k_{AUT-QKD}$ con respecto al nodo del servidor (S); en este caso, el nodo de cliente adquiere/recibe la QKD de clave de autenticación actual $k_{AUT-QKD}$ del dispositivo electrónico portátil conectado localmente.

De la misma manera, un nodo de cliente puede proporcionar de manera conveniente a un suscriptor la clave cuántica de enlace respectiva k_L y la QKD de clave de autenticación nueva $k_{AUT-QKD}^{NUEVA}$ de dicho suscriptor con respecto al nodo del servidor (S) de diversas formas, en particular:

- por medio de una interfaz de usuario de dicho nodo de cliente; o

- almacenando dichas claves en un dispositivo electrónico portátil de dicho suscriptor conectado localmente a dicho nodo de cliente por ejemplo por medio de una conexión USB.

El dispositivo electrónico portátil conectado localmente al nodo de cliente puede ser de manera conveniente un dispositivo de almacenamiento de datos portátil, tal como una unidad flash USB o una unidad de disco duro USB externa o un ordenador portátil, tal como un portátil o una tableta o un teléfono inteligente.

En este punto, con el fin de continuar describiendo con detalle el funcionamiento del sistema de distribución de clave criptográfica mostrado en la figura 1, se asume que:

- los suscriptores *P* (donde *P>1*) a dicho sistema de distribución de clave criptográfica han utilizado al menos uno de los nodos de cliente (C1), (C2), (C3) y (C4) para recibir cada una de las claves cuánticas de enlace respectivas;

- el nodo del servidor (S) almacena las claves cuánticas de enlace de dichos suscriptores *P*; y

- dichos suscriptores *P*, ya que tienen la intención de comunicarse entre sí de una manera segura, se conectan de manera remota cada uno utilizando un dispositivo de comunicación electrónico respectivo (tal como un ordenador de escritorio, un portátil, una tableta, un teléfono inteligente o incluso uno de los nodos de cliente (C1), (C2), (C3) y (C4)) al nodo del servidor (S) por medio de uno o varios canal(es) público(s) respectivo(s), por ejemplo a través de Internet, para solicitar una clave criptográfica común que se va a utilizar para crear una comunicación segura.

De manera conveniente, los mensajes, los cuales son enviados por los suscriptores *P* al nodo del servidor (S) y los cuales están relacionados con la solicitud para establecer una comunicación segura entre dichos suscriptores *P* y, por lo tanto, con la solicitud de una clave criptográfica correspondiente común a dichos suscriptores *P*, se encriptan con el fin de evitar que cualquier tercero no autorizado sea capaz de interceptar y desencriptar de manera

fraudulenta dichos mensajes y, entonces, ocupar el lugar de uno de dichos suscriptores autorizados *P* o unirse a dichos suscriptores autorizados.

Con el fin de permitir una comunicación segura entre dichos suscriptores *P*, el nodo del servidor (S) lleva a cabo las siguientes operaciones:

- genera una clave criptográfica de tráfico para dichos suscriptores *P*;

- para cada uno de dichos suscriptores *P*, encripta la clave criptográfica de tráfico sobre la base de la clave cuántica de enlace respectiva obteniendo de este modo un mensaje encriptado respectivo; y

- envía el mensaje encriptado respectivo a cada uno de dichos suscriptores *P* por el(los) canal(es) público(s) respectivo(s).

Cada uno de dichos suscriptores *P*, después de recibir el mensaje encriptado respectivo del nodo del servidor (S), lo desencripta utilizando la clave cuántica de enlace respectiva, obteniendo así la clave criptográfica de tráfico.

Preferiblemente, el nodo del servidor (S) está configurado para generar de manera aleatoria las claves criptográficas de tráfico.

Incluso más preferiblemente, el nodo del servidor (S) está configurado para funcionar como un Generador de números aleatorios cuántico (QRNG, por sus siglas en inglés). Por lo tanto, en la práctica, el nodo del servidor (S) genera las claves criptográficas de tráfico funcionando como un QRNG.

En una forma de realización alternativa, el nodo del servidor (S) no genera las claves criptográficas de tráfico, sino que está configurado para recibirlas de un generador de claves, por ejemplo un QRNG, independiente de dicho nodo del servidor S. En particular, el nodo del servidor (S) puede estar conectado de manera conveniente al generador de claves por medio de un canal intrínsecamente seguro, que es uno tal que garantice, o no comprometa, la seguridad de la conexión entre el nodo del servidor (S) y el generador de claves y, en consecuencia, el nodo del servidor (S) puede recibir de manera conveniente las claves criptográficas de tráfico de una manera absolutamente segura por dicho canal intrínsecamente seguro. Alternativamente, un administrador del nodo del servidor (S) podría llevar a cabo de manera conveniente el siguiente procedimiento con el fin de proporcionar las claves criptográficas de tráfico al nodo del servidor (S):

- causando que el generador de claves genere las claves criptográficas de tráfico;

- conectando localmente, por ejemplo por medio de una conexión USB, un dispositivo electrónico portátil, tal como una unidad flash USB, una unidad de disco duro USB externa, un portátil, una tableta o un teléfono inteligente a dicho generador de claves;

- almacenando las claves criptográficas de tráfico generadas por el generador de claves en dicho dispositivo electrónico portátil conectado localmente al generador de claves; y

- yendo al nodo del servidor (S) y conectando localmente, por ejemplo por medio de una conexión USB, dicho dispositivo electrónico portátil en el cual las claves criptográficas de tráfico se almacenan en dicho nodo del servidor (S); de esta forma el nodo del servidor (S) adquiere/recibe las claves criptográficas de tráfico desde el dispositivo electrónico portátil conectado localmente.

Entrando en más detalle con respecto al funcionamiento del sistema de distribución de clave criptográfica de acuerdo con el primer aspecto de la presente invención, las claves cuánticas de enlace son utilizadas por el nodo del servidor (S) para encriptar la clave criptográfica de tráfico de acuerdo con la metodología llamada “libreta de un solo uso” (One-Time Pad, OTP).

Por ejemplo, si un primer suscriptor asociado con una primera clave cuántica de enlace k_{L1} de *N* bits y un segundo suscriptor asociado con una segunda clave cuántica de enlace k_{L2} de *N* bits se conectan al nodo del servidor (S) para solicitar una clave criptográfica común que se va a utilizar para comunicarse entre sí de una manera segura (como se ha dicho previamente, mediante el envío al nodo del servidor (S) de mensajes encriptados respectivos), el nodo del servidor (S) realiza las siguientes operaciones:

● genera (o, en la forma de realización alternativa anteriormente indicada, recibe del generador de claves) y almacena una clave criptográfica de tráfico k_T de *N* bits;

● realiza una encriptación de OTP de la clave criptográfica de tráfico k_T utilizando la primera clave cuántica de enlace k_{L1} como la clave de encriptación obteniendo de este modo un primer mensaje encriptado $k_T \oplus k_{L1}$ de *N* bits, donde el símbolo $\oplus$ representa la operación lógica de OR exclusiva, es decir, la operación lógica de XOR;

● envía el primer mensaje encriptado $k_T \oplus k_{L1}$ al primer suscriptor;

● realiza una encriptación de OTP de la *clave* criptográfica de tráfico k_T mediante el uso de la segunda clave cuántica de enlace k_{L2} como la clave de encriptación obteniendo de este modo un segundo mensaje encriptado $k_T \oplus k_{L2}$ de *N* bits; y

● envía el segundo mensaje encriptado $k_T \oplus k_{L2}$ al segundo suscriptor.

El primer suscriptor desencripta el primer mensaje encriptado $k_T \oplus k_{L1}$ recibido del nodo del servidor (S) mediante el uso de la primera clave cuántica de enlace k_{L1} y obtiene de este modo la clave criptográfica de tráfico k_T.

De la misma forma, el segundo suscriptor desencripta el segundo mensaje encriptado $k_T \oplus k_{L2}$ recibido del nodo del servidor (S) mediante el uso de la segunda clave cuántica de enlace k_{L2} y obtiene de este modo la clave criptográfica de tráfico k_T.

A partir de la descripción anterior, se puede apreciar inmediatamente cómo, gracias a la encriptación de OTP, la distribución de la clave criptográfica de tráfico k_T a los dos suscriptores no conlleva prácticamente ningún riesgo de que dicha clave criptográfica de tráfico k_T sea interceptada por un tercero no autorizado.

En particular, el uso de la encriptación de OTP para la transferencia de la clave criptográfica de tráfico k_T garantiza la inviolabilidad de la *clave* criptográfica de tráfico k_T en sí misma, como demostró Claude Shannon en “Teoría de la comunicación de los sistemas de secreto”, diario técnico del sistema Bell, vol. 28(4), páginas 656-715, 1949. De hecho, si un tercero no autorizado intercepta de manera abusiva el primer mensaje encriptado $k_T \oplus k_{L1}$ y el segundo mensaje encriptado $k_T \oplus k_{L2}$, como máximo dicho tercero no autorizado obtendría:

$$k_T \oplus k_{L1} \oplus k_T k_{L2} = k_{L1} \oplus k_T \oplus k_T k_{L2} = k_{L1} \oplus k_{L2}$$

Por lo tanto, ya que todas las claves son aleatorias, el tercero no autorizado no obtiene información sobre la clave criptográfica de tráfico k_T y las claves cuánticas de enlace k_{L1} y k_{L2}.

En consecuencia, la distribución de una y la misma clave criptográfica de tráfico a los suscriptores *P* (donde *P>1*) permite a dichos suscriptores *P* comunicarse entre sí de una manera segura por uno o varios canal(es) público(s), por ejemplo a través de Internet.

De manera conveniente, la clave criptográfica de tráfico puede ser utilizada por dichos suscriptores *P* como una clave de encriptación, puede ser utilizada por dichos suscriptores *P* como una ayuda para los algoritmos de encriptación, puede ser utilizada por dichos suscriptores *P* directamente para una encriptación de OTP, puede ser almacenada en dispositivos electrónicos de dichos suscriptores *P* (por ejemplo en dispositivos de almacenamiento de datos portátiles, tales como unidades flash USB o unidades de disco duro USB externas o en ordenadores de escritorio o en ordenadores portátiles tales como portátiles o tabletas o en teléfonos inteligentes, etc.) para un uso posterior por dichos suscriptores *P* para comunicarse entre sí de una manera segura, etc.

Después de que se haya utilizado una clave cuántica de enlace para la encriptación de OTP de una clave criptográfica de tráfico, esta clave cuántica de enlace se descartará y se deberá utilizar una clave cuántica de enlace nueva para la distribución de una clave criptográfica de tráfico nueva.

Por lo tanto, con el sistema de distribución de clave criptográfica de acuerdo con el primer aspecto de la presente invención, se pueden adoptar las tres estrategias de distribución siguientes para las claves cuánticas de enlace y las

claves criptográficas de tráfico:

1) cada vez que los suscriptores *P* (donde *P>1*) al sistema de distribución de clave criptográfica necesitan comunicarse entre sí de una manera segura, dichos suscriptores *P* utilizan uno o varios nodo(s) de cliente para obtener, cada uno, una clave cuántica de enlace respectiva que utilizan entonces para obtener una y la misma clave criptográfica de tráfico desde el nodo del servidor (S);

2) un suscriptor al sistema de distribución de clave criptográfica utiliza un nodo de cliente para obtener una serie de claves cuánticas de enlace que él/ella almacena en un dispositivo electrónico respectivo (por ejemplo en dispositivos de almacenamiento de datos portátiles, tales como unidades flash USB o unidades de disco duro USB externas o en ordenadores de escritorio o en ordenadores portátiles tales como portátiles o tabletas o en teléfonos inteligentes, etc.) y entonces los utiliza de uno en uno cuando él/ella necesita obtener las claves criptográficas de tráfico desde el nodo del servidor (S); mediante el uso de las claves cuánticas de enlace almacenadas, dicho suscriptor puede obtener las claves criptográficas de tráfico por medio de un nodo de cliente o por medio de cualquier dispositivo de comunicación electrónico capaz de comunicarse con el nodo del servidor (S) por un canal público; una vez que dicho suscriptor se quede sin las claves cuánticas de enlace almacenadas, él/ella deberá utilizar un nodo de cliente de nuevo para obtener claves cuánticas de enlace adicionales;

3) los suscriptores *P* (donde *P>1*) al sistema de distribución de clave criptográfica utilizan dicho sistema de distribución de clave criptográfica para obtener una serie de claves criptográficas de tráfico que almacenan en dispositivos electrónicos respectivos (por ejemplo en dispositivos de almacenamiento de datos portátiles, tales como unidades flash USB o unidades de disco duro USB externas o en ordenadores de escritorio o en ordenadores portátiles tales como portátiles o tabletas o en teléfonos inteligentes, etc.) y los utilizan entonces cuando necesitan comunicarse entre sí de una manera segura.

El sistema de distribución de clave criptográfica de acuerdo con el primer aspecto de la presente invención es un sistema jerárquico en el cual el nodo del servidor (S) está en posesión de todas las claves criptográficas de tráfico, todas las claves cuánticas de enlace y todas las claves de autenticación de QKD, mientras que cada suscriptor solamente posee las claves cuánticas de enlace respectivas, las claves criptográficas de tráfico para las cuales él/ella está autorizado y la clave de autenticación de QKD actual respectiva con respecto al nodo del servidor (S).

En particular, el nodo del servidor (S) funciona como un administrador de clave o más bien:

- almacena/actualiza las claves criptográficas de tráfico generadas, las claves criptográficas de tráfico distribuidas, las claves cuánticas de enlace generadas, las claves cuánticas de enlace utilizadas, las claves de autenticación de QKD generadas y las claves de autenticación de QKD utilizadas en una base de datos, donde también almacena datos de tiempo sobre cuándo se generaron y distribuyeron/utilizaron las claves;

- responde a solicitudes globales y/o especiales para las claves criptográficas; y

- monitoriza la red cuántica o más bien la red formada por los canales cuánticos, en tiempo real de forma que se establezcan siempre en tiempo real, los parámetros óptimos necesarios para la comunicación cuántica.

El sistema de distribución de clave criptográfica de acuerdo con el primer aspecto de la presente invención puede comprender de manera conveniente un nodo del servidor de copia de seguridad configurado para sustituir el nodo del servidor principal (S) si el último no es capaz de funcionar, por ejemplo, en el caso de un simple error del nodo del servidor principal (S) o en el caso de recuperación de desastres.

En particular, el nodo del servidor de copia de seguridad puede estar configurado de manera conveniente para sincronizarse de forma periódica él mismo con el nodo del servidor principal (S) de tal forma que todas las claves criptográficas de tráfico, las claves cuánticas de enlace y las claves de autenticación de QKD almacenadas por dicho nodo del servidor principal (S) se almacenen/actualicen en una base de datos respectiva, de manera que estén siempre alineadas con el nodo del servidor principal (S) con respecto a las claves generadas y distribuidas/utilizadas.

Con el fin de incrementar el nivel de seguridad garantizado por el sistema de distribución de clave criptográfica, de acuerdo con una forma de realización preferida del primer aspecto de la presente invención, además de las claves cuánticas de enlace, las claves de autenticación de servicio de los suscriptores con respecto al nodo del servidor (S) se utilizan también para proteger la distribución de las claves criptográficas de tráfico a los suscriptores.

En particular, de acuerdo con dicha forma de realización preferida del primer aspecto de la presente invención, un primer suscriptor y un segundo suscriptor, después de haber recibido respectivamente la primera clave cuántica de enlace k_{L1} y la segunda clave cuántica de enlace k_{L2}, se conectan al nodo del servidor (S) para solicitar una clave criptográfica común que se va a utilizar para comunicarse entre sí de una manera segura (como se ha dicho previamente, mediante el envío al nodo del servidor (S) de mensajes encriptados respectivos) y el nodo del servidor (S), el cual almacena una clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}1}$ de D bits del primer suscriptor con respecto a dicho nodo del servidor (S) y una clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}2}$ de D bits del segundo suscriptor con respecto a dicho nodo del servidor (S), realiza las siguientes operaciones:

- genera (o, en la forma de realización alternativa mencionada anteriormente, recibe del generador de claves) y almacena una clave criptográfica de tráfico k_T de *N'* bits;

- genera (o, en la forma de realización alternativa mencionada anteriormente, recibe del generador de claves) y almacena una clave de autenticación de servicio nueva de $k_{AUT-S-1}^{NUEVA}$ de D bits del primer suscriptor con respecto a dicho nodo del servidor (S);

- realiza una encriptación de OTP de la clave criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-1}^{NUEVA}$ del primer suscriptor con respecto a dicho nodo del servidor (S) mediante

el uso de la primera clave cuántica de enlace k_{L1} como clave de encriptación y, de esta forma, obtiene un primer mensaje encriptado $(k_T + k_{AUT-S-1}^{NUEVA}) \oplus k_{L1}$ de *N bits* (donde *N=N'+D*);

- realiza una encriptación de no-OTP del primer mensaje encriptado $(k_T + k_{AUT-S-1}^{NUEVA}) \oplus k_{L1}$, por ejemplo basada en un algoritmo de encriptación de clave simétrica, mediante el uso de la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}1}$ del primer suscriptor con respecto a dicho nodo del servidor (S) como clave de encriptación y, de esta forma, obtiene un segundo mensaje encriptado;

- envía el segundo mensaje encriptado al primer suscriptor;

- genera (o, en la forma de realización alternativa mencionada anteriormente, recibe del generador de claves) y almacena una clave de autenticación de servicio nueva $k_{AUT-S-2}^{NUEVA}$ de D bits del segundo suscriptor con respecto a dicho nodo del servidor (S);

- realiza una encriptación de OTP de la *clave* criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-2}^{NUEVA}$ del segundo suscriptor con respecto a dicho nodo del servidor (S) mediante el uso de la segunda clave cuántica de enlace k_{L2} como clave de encriptación y, de esta forma, obtiene un tercer mensaje encriptado $(k_T + k_{AUT-S-2}^{NUEVO}) \oplus k_{L2}$ de N bits;

- realiza una encriptación de no-OTP del tercer mensaje encriptado $(k_T + k_{AUT-S-2}^{NUEVO}) \oplus k_{L2}$, por ejemplo basada en un algoritmo de encriptación de clave simétrica, mediante el uso de la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}2}$ del segundo suscriptor con respecto a dicho nodo del servidor (S) como clave de encriptación y, de esta forma, obtiene un cuarto mensaje encriptado; y

- envía el cuarto mensaje encriptado al segundo suscriptor.

El primer suscriptor desencripta el segundo mensaje encriptado recibido del nodo del servidor (S) utilizando, primeramente, la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}1}$ de dicho primer suscriptor con respecto a dicho nodo del servidor (S) y, a continuación, la primera clave cuántica de enlace k_{L1}, obteniendo de este modo la clave criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-1}^{NUEVA}$ de dicho primer suscriptor con respecto a dicho nodo del servidor (S).

De la misma forma, el segundo suscriptor desencripta el cuarto mensaje encriptado recibido del nodo del servidor (S)

utilizando, primeramente, la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}2}$ de dicho segundo suscriptor con respecto a dicho nodo del servidor (S) y, a continuación, la segunda clave cuántica de enlace k_{L2}, obteniendo de este modo la *clave* criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-2}^{NUEVA}$ de dicho segundo suscriptor con respecto a dicho nodo del servidor (S).

Las claves de autenticación de servicio nuevas del primer y el segundo suscriptor con respecto al nodo del servidor (S) se utilizarán entonces para la distribución de las claves de tráfico nuevas desde el nodo del servidor (S) al primer y segundo suscriptor.

Convenientemente, las claves de autenticación de servicio iniciales con respecto al nodo del servidor (S) se pueden suministrar a los suscriptores cuando el último se suscriba al sistema de distribución de clave criptográfica.

De acuerdo con el primer aspecto de la presente invención, cuando un suscriptor desea comunicarse con el nodo del servidor (S), por ejemplo para solicitar una clave criptográfica de tráfico con el fin de ser capaz de comunicarse de manera segura con otro suscriptor, él/ella puede llevar a cabo de forma conveniente el procedimiento completo descrito previamente en relación con la generación de una clave cuántica de enlace respectiva mediante el uso de un nodo de cliente y en relación con la distribución (con o sin el uso de la clave de autenticación de servicio respectiva al nodo del servidor (S)) de una clave criptográfica de tráfico, de manera que se obtenga una clave criptográfica de tráfico adicional que el suscriptor pueda utilizar de manera conveniente para comunicarse de una manera segura con el nodo del servidor (S).

El sistema de distribución de clave criptográfica de acuerdo con el primer aspecto de la presente invención tiene, con respecto a la red cuántica, una arquitectura en forma de estrella que se puede expandir de manera conveniente tanto para garantizar la generación y la distribución de claves criptográficas por distancias superiores a las metropolitanas (aproximadamente *90 Km*) como para garantizar la redundancia del sistema desde un punto de vista centrado en redes.

En particular, de acuerdo con un segundo aspecto de la presente invención, la arquitectura de la red cuántica del sistema de distribución de clave criptográfica se puede expandir de manera conveniente mediante el uso de uno o varios nodo(s) repetidor(es) que se configura(n) para funcionar tanto como nodo(s) del servidor como nodo(s) de cliente.

A este respecto, con el fin de describir el segundo aspecto de la presente invención, la figura 2 muestra un ejemplo de un sistema de distribución de clave criptográfica de acuerdo con dicho segundo aspecto de la presente invención.

En particular, el sistema de distribución de clave criptográfica mostrado en la figura 2 comprende:

- un nodo del servidor (S);
- un primer nodo de cliente (C1) conectado al nodo del servidor (S) por medio de un primer canal cuántico representado en la figura 2 por un segmento de línea sólida;
- un nodo repetidor (R) conectado al nodo del servidor (S) por medio de un segundo canal cuántico representado en la figura 2 por un segmento de línea sólida; y
- un segundo nodo de cliente (C2) que está conectado al nodo repetidor (R) por medio de un tercer canal cuántico representado en la figura 2 por un segmento de línea sólida.

En la práctica, los nodos de cliente (C1) y (C2) pueden ser utilizados, cada uno, por uno o varios suscriptor(es) del sistema de distribución de clave criptográfica para recibir una o varias clave(s) cuántica(s) de enlace respectiva(s).

En particular, si, por ejemplo, un primer suscriptor utiliza el primer nodo de cliente (C1) para recibir una clave cuántica de enlace respectiva, se llevan a cabo las siguientes operaciones:

- el primer nodo de cliente (C1) recibe del primer suscriptor una clave de autenticación de QKD actual $k_{AUT\text{-}QKD\text{-}1}$ de *M* bits de dicho primer suscriptor con respecto al nodo del servidor (S);
- el primer nodo de cliente (C1) y el nodo del servidor S, el cual almacena dicha clave de autenticación de QKD

actual $k_{AUT-QKD-1}$ del primer suscriptor con respecto a dicho nodo del servidor (S), implementan una QKD basada en el protocolo BB84 en el primer canal cuántico mediante el uso de dicha clave de autenticación de QKD actual $k_{AUT-QKD-1}$ del primer suscriptor con respecto a dicho nodo del servidor (S) en el paso de amplificación de privacidad; de esta forma, el primer nodo de cliente (C1) y el nodo del servidor (S) generan una cadena de *L* bits que comprende una primera clave cuántica de enlace k_{L1} de *N bits* asociada a dicho primer suscriptor y una clave de autenticación de QKD nueva $k_{AUT-QKD-1}^{NUEVA}$ de *M* bits de dicho primer suscriptor con respecto al nodo del servidor (S) (donde *L=N+M*);

- el nodo del servidor (S) almacena la primera clave cuántica de enlace k_{L1} asociada con dicho primer suscriptor y la clave de autenticación de QKD nueva $k_{AUT-QKD-1}^{NUEVA}$ de dicho primer suscriptor con respecto a dicho nodo del servidor (S); y

- el primer nodo de cliente (C1) proporciona al primer suscriptor la primera clave cuántica de enlace k_{L1} asociada con dicho primer suscriptor y la clave de autenticación de QKD nueva $k_{AUT-QKD-1}^{NUEVA}$ de dicho primer suscriptor con respecto al nodo del servidor (S).

Cuando el primer suscriptor utiliza de nuevo un nodo de cliente para recibir una clave cuántica de enlace nueva, dicho nodo de cliente y el nodo del servidor (S) utilizarán la clave de autenticación de QKD nueva $k_{AUT-QKD-1}^{NUEVA}$ de dicho primer suscriptor con respecto al nodo del servidor (S) en el paso de amplificación de privacidad de la QKD nueva implementada para generar la clave cuántica de enlace nueva.

Convenientemente, la clave de autenticación de QKD inicial con respecto al nodo del servidor (S) se puede proporcionar al primer suscriptor cuando el último se suscriba al sistema de distribución de clave criptográfica.

Además, si un segundo suscriptor utiliza el segundo nodo de cliente (C2) para recibir una clave cuántica de enlace respectiva, se llevan a cabo las siguientes operaciones:

- el nodo del servidor (S) y el nodo repetidor (R), el cual almacena una clave de autenticación de QKD actual $k_{AUT-QKD-R}$ de *M* bits de dicho nodo repetidor (R) con respecto a dicho nodo del servidor S, implementan una QKD basada en el protocolo BB84 en el segundo canal cuántico mediante el uso de la clave de autenticación de QKD actual $k_{AUT-QKD-R}$ de dicho nodo repetidor (R) con respecto a dicho nodo del servidor (S) en el paso de amplificación de privacidad; de esta forma, el nodo del servidor (S) y el nodo repetidor (R) generan una cadena de *L* bits que comprende una segunda clave cuántica de enlace k_{L2} de *N* bits asociada con dicho segundo suscriptor y una clave de autenticación de QKD nueva $k_{AUT-QKD-R}^{NUEVA}$ de M bits de dicho nodo repetidor (R) con respecto a dicho nodo del servidor (S) (donde *L=N+M*);

- el nodo del servidor (S) almacena dicha segunda clave cuántica de enlace k_{L2} asociada con dicho segundo suscriptor y la clave de autenticación de QKD nueva $k_{AUT-QKD-R}^{NUEVA}$ de dicho nodo repetidor (R) con respecto a dicho nodo del servidor (S);

- el nodo repetidor (R) almacena la clave de autenticación de QKD nueva $k_{AUT-QKD-R}^{NUEVA}$ de dicho nodo repetidor (R) con respecto a dicho nodo del servidor (S);

- el segundo nodo de cliente (C2) (el cual ha recibido del segundo suscriptor una clave de autenticación de QKD actual $k_{AUT-QKD-2}$ de *M* bits de dicho segundo suscriptor con respecto al nodo repetidor (R)) y el nodo repetidor (R) (el cual almacena dicha clave de autenticación de QKD actual $k_{AUT-QKD-2}$ de dicho segundo suscriptor con respecto a dicho nodo repetidor (R)) implementan una QKD basada en el protocolo BB84 en el tercer canal cuántico mediante el uso de dicha clave de autenticación de QKD actual $k_{AUT-QKD-2}$ de dicho segundo suscriptor con

respecto a dicho nodo repetidor (R) en el paso de amplificación de privacidad y, de esta forma, generan una cadena de *L* bits que comprende una clave cuántica de transferencia k_{R-2} de *N* bits y una clave de autenticación de QKD nueva $k_{AUT-QKD-2}^{NUEVA}$ de *M* bits de dicho segundo suscriptor con respecto al nodo repetidor (R);

● el segundo nodo de cliente (C2) proporciona al segundo suscriptor la clave cuántica de transferencia k_{R-2} y la clave de autenticación de QKD nueva $k_{AUT-QKD-2}^{NUEVA}$ de dicho segundo suscriptor con respecto al nodo repetidor (R);

● el nodo repetidor (R)

- almacena la clave de autenticación de QKD nueva $k_{AUT-QKD-2}^{NUEVA}$ de dicho segundo suscriptor con respecto a dicho nodo repetidor (R),

- realiza una encriptación de OTP de la segunda clave cuántica de enlace k_{L2} mediante el uso de la clave cuántica de transferencia k_{R-2} como clave de encriptación, obteniendo de ese modo un mensaje encriptado $k_{L2} \oplus k_{R-2}$ de *N* bits, y

- envía dicho mensaje encriptado $k_{L2} \oplus k_{R-2}$ por un canal público al segundo suscriptor, quien utiliza de manera conveniente un dispositivo de comunicación electrónico respectivo (tal como un ordenador de escritorio, un portátil, una tableta o incluso un nodo de cliente); y

● el segundo suscriptor desencripta el mensaje encriptado $k_{L2} \oplus k_{R-2}$ recibido del nodo repetidor (R) mediante el uso de la clave cuántica de transferencia k_{R-2} obteniendo de ese modo la segunda clave cuántica de enlace k_{L2}.

Cuando el segundo suscriptor utiliza un nodo de cliente conectado al nodo repetidor (R) para recibir una clave cuántica de enlace nueva, dicho nodo de cliente y el nodo repetidor (R) utilizarán la clave de autenticación de QKD nueva $k_{AUT-QKD-2}^{NUEVA}$ de dicho segundo suscriptor con respecto al nodo repetidor (R) en el paso de amplificación de privacidad de la nueva QKD implementada para generar la clave cuántica de transferencia nueva y el nodo repetidor (R) y el nodo del servidor (S) utilizarán la clave de autenticación de QKD nueva $k_{AUT-QKD-R}^{NUEVA}$ de dicho nodo repetidor (R) con respecto a dicho nodo del servidor (S) en el paso de amplificación de privacidad de la nueva QKD implementada para generar la clave cuántica de enlace nueva para el segundo suscriptor.

De manera conveniente, la clave de autenticación de QKD inicial con respecto al nodo del servidor (S) se puede suministrar al nodo repetidor (R) en el momento de la instalación, mientras que se puede suministrar al segundo suscriptor cuando el último se suscriba al sistema de distribución de clave criptográfica.

Un suscriptor al sistema de distribución de clave criptográfica de acuerdo con el segundo aspecto de la presente invención que utiliza un nodo de cliente (conectado directamente al nodo del servidor (S) o al nodo repetidor (R)) para recibir una clave cuántica de enlace/transferencia respectiva k_L/ k_R, puede proporcionar de manera conveniente a dicho nodo de cliente la clave de autenticación de QKD actual respectiva $k_{AUT-QKD}$ con respecto al nodo del servidor/repetidor (S/R) de diversas formas, en particular:

● por medio de una interfaz de usuario de dicho nodo de cliente; o

● conectando localmente, por ejemplo por medio de una conexión USB, un dispositivo electrónico portátil respectivo que almacena dicha QKD de clave de autenticación actual respectiva $k_{AUT-QKD}$ con respecto al nodo del servidor/repetidor S/R; en este caso, el nodo de cliente adquiere/ recibe la QKD de clave de autenticación actual $k_{AUT-QKD}$ del dispositivo electrónico portátil conectado localmente.

De la misma manera, un nodo de cliente puede proporcionar de manera conveniente a un suscriptor la clave cuántica de enlace/transferencia respectiva k_L/k_R y la clave de autenticación de QKD nueva $k_{AUT-QKD}^{NUEVA}$ de dicho

suscriptor con respecto al nodo del servidor/repetidor (S/R) de diversas formas, en particular:

● por medio de una interfaz de usuario de dicho nodo de cliente; o

● almacenando dichas claves en un dispositivo electrónico portátil de dicho suscriptor conectado localmente a dicho nodo de cliente, por ejemplo por medio de una conexión USB.

El dispositivo electrónico portátil conectado localmente al nodo de cliente puede ser de manera conveniente un dispositivo de almacenamiento de datos portátil, tal como una unidad flash USB o una unidad de disco duro USB externa o un ordenador portátil, tal como un portátil o una tableta o un teléfono inteligente.

En este punto, si el primer suscriptor y el segundo suscriptor, después de haber recibido respectivamente la primera clave cuántica de enlace k_{L1} y la segunda clave cuántica de enlace k_{L2}, se conectan al nodo del servidor (S), utilizando ambos un dispositivo de comunicación electrónico respectivo (por ejemplo un ordenador de escritorio, un portátil, una tableta o incluso un nodo de cliente), para solicitar una clave criptográfica común que se va a utilizar para comunicarse entre sí de una manera segura, el nodo del servidor (S), el cual almacena una clave de autenticación de servicio actual $k_{AUT-S-1}$ de D bits del primer suscriptor con respecto a dicho nodo del servidor (S) y una clave de autenticación de servicio actual $k_{AUT-S-2}$ de D bits del segundo suscriptor con respecto a dicho nodo del servidor S, realiza las siguientes operaciones:

● genera y almacena una *clave* criptográfica de tráfico k_T de N' bits;

● genera y almacena una clave de autenticación de servicio nueva $k_{AUT-S-1}$ de D bits del primer suscriptor con respecto a dicho nodo del servidor (S);

● realiza una encriptación de OTP de la clave criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-1}$ del primer suscriptor con respecto a dicho nodo del servidor (S) mediante el uso de la primera clave cuántica de enlace k_{L1} como clave de encriptación y, de esta forma, obtiene un primer mensaje encriptado $(k_T + k_{AUT-S-1}^{NUEVA}) \oplus k_{L1}$ de *N bits* (donde *N=N'+D*);

● realiza una encriptación de no-OTP del primer mensaje encriptado $(k_T + k_{AUT-S-1}^{NUEVA}) \oplus k_{L1}$, por ejemplo basada en un algoritmo de encriptación de clave simétrica, mediante el uso de la clave de autenticación de servicio actual $k_{AUT-S-1}$ del primer suscriptor con respecto a dicho nodo del servidor (S) como clave de encriptación y, de esta forma, obtiene un segundo mensaje encriptado;

● envía el segundo mensaje encriptado al primer suscriptor.

● genera y almacena una clave de autenticación de servicio nueva $k_{AUT-S-2}^{NUEVA}$ de D bits del segundo suscriptor con respecto a dicho nodo del servidor (S);

● realiza una encriptación de OTP de la *clave* criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-2}^{NUEVA}$ del segundo suscriptor con respecto a dicho nodo del servidor (S) mediante el uso de la segunda clave cuántica de enlace k_{L2} como clave de encriptación y, de esta forma, obtiene un tercer mensaje encriptado $(k_T + k_{AUT-S-2}^{NUEVA}) \oplus k_{L2}$ de *N* bits;

● realiza una encriptación de no-OTP del tercer mensaje encriptado $(k_T + k_{AUT-S-2}^{NUEVA}) \oplus k_{L2}$, por ejemplo basada en un algoritmo de encriptación de clave simétrica, mediante el uso de la clave de autenticación de servicio actual $k_{AUT-S-2}$ del segundo suscriptor con respecto a dicho nodo del servidor (S) como clave de encriptación y, de esta forma, obtiene un cuarto mensaje encriptado; y

● envía el cuarto mensaje encriptado al segundo suscriptor.

El primer suscriptor desencripta el segundo mensaje encriptado recibido del nodo del servidor (S) utilizando, primeramente, la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}1}$ de dicho primer suscriptor con respecto a dicho nodo del servidor (S) y, a continuación, la primera clave cuántica de enlace k_{L1}, obteniendo de este modo la *clave* criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-1}^{NUEVA}$ de dicho primer suscriptor con respecto a dicho nodo del servidor (S).

De la misma forma, el segundo suscriptor desencripta el cuarto mensaje encriptado recibido del nodo del servidor (S) utilizando, primeramente, la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}2}$ de dicho segundo suscriptor con respecto a dicho nodo del servidor (S) y, a continuación, la segunda clave cuántica de enlace k_{L2}, obteniendo de este modo la clave criptográfica de tráfico k_T y la clave de autenticación de servicio nueva $k_{AUT-S-2}^{NUEVA}$ de dicho segundo suscriptor con respecto a dicho nodo del servidor (S).

Las claves de autenticación de servicio nuevas del primer y el segundo suscriptor con respecto al nodo del servidor (S) se utilizarán entonces para la distribución de las claves criptográficas de tráfico nuevas desde el nodo del servidor (S) al primer y segundo suscriptor.

Convenientemente, las claves de autenticación de servicio iniciales con respecto al nodo del servidor (S) se pueden suministrar al primer suscriptor y al segundo suscriptor cuando se suscriban al sistema de distribución de clave criptográfica.

Como se ha descrito con respecto al primer aspecto de la presente invención, los mensajes, los cuales son enviados por el primer y el segundo suscriptor al nodo del servidor (S) y los cuales se refieren a la solicitud para establecer una comunicación segura entre dichos suscriptores y, por lo tanto, a la solicitud de una clave criptográfica correspondiente común a dichos suscriptores, se encriptan de manera conveniente con el fin de evitar que cualquier tercero no autorizado sea capaz de interceptar y desencriptar de forma fraudulenta dichos mensajes y, entonces, ocupe el lugar de uno de dichos suscriptores autorizados o se una a dichos suscriptores autorizados.

Preferiblemente, el nodo del servidor (S) está configurado para generar de manera aleatoria las claves criptográficas de tráfico y las claves de autenticación de servicio nuevas de los suscriptores con respecto a dicho nodo del servidor (S).

Incluso más preferiblemente, el nodo del servidor (S) está configurado para funcionar como un QRNG. Por lo tanto, en la práctica, el nodo del servidor (S) genera las claves criptográficas de tráfico y las claves de autenticación de servicio nuevas de los suscriptores con respecto a dicho nodo del servidor (S) funcionando como un QRNG.

En una forma de realización alternativa, el nodo del servidor (S) no genera las claves criptográficas de tráfico ni las claves de autenticación de servicio nuevas de los suscriptores con respecto a dicho nodo del servidor (S), sino que está configurado para recibirlas de un generador de claves, por ejemplo un QRNG, independiente de dicho nodo del servidor (S). En particular, el nodo del servidor (S) puede estar conectado de manera conveniente al generador de claves por medio de un canal intrínsecamente seguro, que es uno tal que garantice, o no comprometa, la seguridad de la conexión entre el nodo del servidor (S) y el generador de claves y, en consecuencia, el nodo del servidor (S) puede recibir de manera conveniente las claves criptográficas de tráfico y las claves de autenticación de servicio nuevas de los suscriptores con respecto a dicho nodo del servidor (S) de una manera absolutamente segura por dicho canal intrínsecamente seguro. Alternativamente, las claves criptográficas de tráfico y las claves de autenticación de servicio nuevas de los suscriptores con respecto al nodo del servidor (S) pueden ser suministradas de manera conveniente a dicho nodo del servidor (S) por un administrador de dicho nodo del servidor (S) que lleva a cabo el procedimiento descrito previamente en relación con el primer aspecto de la presente invención.

A partir de la descripción anterior, se puede apreciar inmediatamente cómo, gracias a la encriptación doble, la distribución de la *clave* criptográfica de tráfico k_T a los dos suscriptores, no conlleva prácticamente ningún riesgo de que dicha clave criptográfica de tráfico k_T sea interceptada por un tercero no autorizado.

En particular, gracias al uso de la encriptación de no-OTP basada en la clave de autenticación de servicio actual $k_{AUT\text{-}S\text{-}2}$ de dicho segundo suscriptor con respecto a dicho nodo del servidor (S) en la distribución de la clave criptográfica de tráfico k_T desde el nodo del servidor (S) al segundo suscriptor, ni siquiera el nodo repetidor (R), el cual conoce realmente la segunda clave cuántica de enlace k_{L2}, es capaz de rastrear la clave criptográfica de tráfico k_T. Por lo tanto, el sistema de distribución de clave criptográfica de acuerdo con el segundo aspecto de la presente

invención resuelve los problemas de seguridad que afectan a la invención descritos en WO 2007/123869 A2.

Con el fin de conectar nodos de cliente adicionales posicionados a distancias muy lejanas del nodo del servidor (S), la arquitectura de la red cuántica del sistema de distribución de clave criptográfica de acuerdo con el segundo aspecto de la presente invención se puede expandir además mediante el uso de una red de repetidor que comprende una serie de nodos repetidores. En cualquier caso, el funcionamiento del sistema expandido adicional sigue siendo conceptualmente el que se ha descrito previamente en relación con el sistema de distribución de clave criptográfica mostrado en la figura 2.

De acuerdo con el segundo aspecto de la presente invención, cuando un suscriptor desea comunicarse con el nodo del servidor (S), por ejemplo para solicitar una clave criptográfica de tráfico con el fin de ser capaz de comunicarse de una manera segura con otro suscriptor, él/ella puede llevar a cabo de forma conveniente el procedimiento completo descrito previamente en relación con la generación de una clave cuántica de enlace respectiva mediante el uso de un nodo de cliente (y posiblemente uno o varios nodos repetidores) y en relación con la distribución de una clave criptográfica de tráfico, de manera que se obtenga una clave criptográfica de tráfico adicional que el usuario pueda utilizar de manera conveniente para comunicarse de una manera segura con el nodo del servidor (S).

El sistema de distribución de clave criptográfica de acuerdo con el segundo aspecto de la presente invención es un sistema jerárquico donde:

● el nodo del servidor (S) almacena/actualiza en una base de datos las claves criptográficas de tráfico (generadas y distribuidas), las claves cuánticas de enlace (generadas y utilizadas) asociadas con los suscriptores, las claves de autenticación de QKD (generadas y utilizadas) asociadas con los suscriptores que utilizan nodos de cliente conectados a dicho nodo del servidor (S) por medio de los canales cuánticos respectivos, las claves de autenticación de QKD (generadas y utilizadas) asociadas con los nodos repetidores conectados a dicho nodo del servidor (S) por medio de los canales cuánticos respectivos y las claves de autenticación de servicio (generadas y utilizadas) de los suscriptores con respecto a dicho nodo del servidor (S);

● cada nodo repetidor (R) almacena las claves cuánticas de transferencia (generadas y utilizadas) asociadas con los suscriptores que utilizan los nodos conectados a dicho nodo repetidor (R) por medio de los canales cuánticos respectivos y las claves de autenticación de QKD (generadas y utilizadas) de dicho nodo repetidor (R) con respecto a los nodos conectados a dicho nodo repetidor (R) por medio de los canales cuánticos respectivos y de los suscriptores con respecto a dicho nodo repetidor (R); y

● cada suscriptor posee las claves criptográficas de tráfico que él/ella ha recibido del nodo del servidor (S), las claves cuánticas de enlace respectivas, las claves de autenticación de servicio respectivas con respecto al nodo del servidor (S) y las claves de autenticación de QKD respectivas con respecto al nodo del servidor (S) y/o con respecto a uno o varios nodos repetidores.

Además, el nodo del servidor (S) monitoriza los canales cuánticos conectados directamente a dicho nodo del servidor (S) en tiempo real de manera que se establezcan, siempre en tiempo real, los parámetros óptimos necesarios para la comunicación cuántica. De la misma forma, cada nodo repetidor (R) monitoriza los canales cuánticos conectados directamente a dicho nodo repetidor (R) en tiempo real de manera que se establezcan, de nuevo en tiempo real, los parámetros óptimos necesarios para la comunicación cuántica.

El sistema de distribución de clave criptográfica de acuerdo con el segundo aspecto de la presente invención puede comprender de manera conveniente un nodo del servidor de copia de seguridad configurado para sustituir el nodo del servidor principal (S) si el último no es capaz de funcionar, por ejemplo, en el caso de un simple error del nodo del servidor principal (S) o en el caso de recuperación de desastres.

En particular, el nodo del servidor de copia de seguridad puede estar configurado de manera conveniente para:

● almacenar todas las claves de autenticación de servicio iniciales de los suscriptores con respecto al nodo del servidor principal (S) y, una vez activadas, utilizar estas claves de autenticación de servicio iniciales de los suscriptores con respecto al nodo del servidor principal (S) para distribuir las claves criptográficas de tráfico; o

● almacenar las claves de autenticación de servicio iniciales respectivas de los suscriptores con respecto a dicho nodo del servidor de copia de seguridad y, una vez activadas, utilizar estas claves de autenticación de servicio iniciales respectivas de los suscriptores con respecto a dicho nodo del servidor de copia de seguridad para distribuir

las claves criptográficas de tráfico; o

● sincronizarse de forma periódica con el nodo del servidor principal (S) de manera que se almacenen/actualicen todas las claves criptográficas de tráfico, las claves cuánticas de enlace y las claves de autenticación de servicio almacenadas por dicho nodo del servidor principal (S) en una base de datos respectiva, de manera que estén siempre alineadas con el nodo del servidor principal (S) con respecto a las claves criptográficas de tráfico, las claves cuánticas de enlace y las claves de autenticación de servicio generadas y distribuidas/utilizadas.

Además, se pueden adoptar también las tres estrategias de distribución siguientes para la clave cuántica de enlace y las claves criptográficas de tráfico con el sistema de distribución de clave criptográfica de acuerdo con el segundo aspecto de la presente invención:

1) cada vez que los suscriptores P (donde P>1) al sistema de distribución de clave criptográfica necesiten comunicarse entre sí de una manera segura, dichos suscriptores P utilizarán uno o varios nodos de cliente (y/o nodo(s) repetidor(es)) para obtener, cada uno, una clave cuántica de enlace respectiva que utilizarán entonces para obtener una y la misma clave criptográfica de tráfico desde el nodo del servidor;

2) un suscriptor al sistema de distribución de clave criptográfica utilice un nodo de cliente (o repetidor) para obtener una serie de claves cuánticas de enlace que él/ella almacene en un dispositivo electrónico respectivo (por ejemplo en un dispositivo de almacenamiento de datos portátil, tal como una unidad flash USB o una unidad de disco duro USB externa o en un ordenador de escritorio o en un ordenador portátil tal como un portátil o una tableta o en un teléfono inteligente, etc.) y entonces los utilizará de uno en uno cuando él/ella necesite obtener las claves criptográficas de tráfico desde el nodo del servidor (S); mediante el uso de las claves cuánticas de enlace almacenadas, dicho suscriptor podrá obtener las claves criptográficas de tráfico por medio de un nodo de cliente, o un nodo repetidor, o por medio de cualquier dispositivo de comunicación electrónico capaz de comunicarse con el nodo del servidor (S) por un canal público; una vez que dicho suscriptor se quede sin las claves cuánticas de enlace almacenadas, él/ella deberá utilizar de nuevo un nodo de cliente o un nodo repetidor para obtener claves cuánticas de enlace adicionales;

3) los suscriptores P (donde P>1) al sistema de distribución de clave criptográfica utilicen uno o varios nodos de cliente (y/o nodo(s) repetidor(es)) para obtener una serie de claves criptográficas de tráfico que almacenen en dispositivos electrónicos respectivos (por ejemplo en dispositivos de almacenamiento de datos portátiles, tales como unidades flash USB o unidades de disco duro USB externas o en ordenadores de escritorio o en ordenadores portátiles tales como portátiles o tabletas o en teléfonos inteligentes, etc.) y los utilicen entonces cuando necesiten comunicarse entre sí de una manera segura.

Finalmente, es importante subrayar una vez más el hecho de que, con el fin de recibir las claves criptográficas de tráfico, cada suscriptor al sistema de distribución de clave criptográfica de acuerdo con la presente invención puede utilizar:

● un dispositivo de comunicaciones electrónico respectivo (por ejemplo un ordenador de escritorio, un ordenador portátil, una tableta, un teléfono inteligente, etc.) que está configurado para conectarse al nodo del servidor (S) por medio de uno o varios canal(es) de comunicación público(s), por ejemplo a través de Internet y que comprende un módulo de software configurado para comunicarse con dicho nodo del servidor (S) y realizar las operaciones de desencriptación de OTP y de no-OTP descritas previamente; y/o

● un nodo de cliente o un nodo repetidor del sistema de distribución de clave criptográfica (el cual, por ejemplo, puede recibir las claves criptográficas de tráfico por el enlace público del canal cuántico que lo conecta al nodo del servidor (S), y que comprende de manera conveniente un módulo de software configurado para realizar las operaciones de desencriptación de OTP y de no-OTP descritas previamente).

A partir de la descripción anterior, se pueden apreciar de forma inmediata las ventajas de la presente invención.

En particular, es importante subrayar una vez más el hecho de que de acuerdo con el segundo aspecto de la presente invención, el nodo repetidor (R), aunque conoce las claves cuánticas de enlace de algunos suscriptores, no es capaz de rastrear las claves criptográficas de tráfico gracias al uso de la encriptación de no-OTP basada en las claves de autenticación de servicio actuales de los suscriptores con respecto al nodo del servidor (S) en la distribución de dichas claves criptográficas de tráfico. En otras palabras, incluso si fuese de mala fe, el nodo repetidor (R) no sería capaz de distribuir las claves criptográficas de tráfico asociadas con dos o más suscriptores

autorizados a otros usuarios no autorizados, haciendo de este modo que la comunicación entre dichos suscriptores autorizados sea verdaderamente segura. Por lo tanto, el segundo aspecto de la presente invención resuelve los problemas de seguridad del sistema descritos en WO 2007/123869 A2.

Además, es importante subrayar también el hecho de que el sistema de distribución de clave criptográfica de acuerdo con la presente invención, gracias al uso de la QKD, la encriptación de OTP y las claves de autenticación de servicio, si se utilizan, permite distribuir claves criptográficas a los suscriptores sin el riesgo de que un tercero no autorizado sea capaz de interceptar o más bien “robar”, estas claves criptográficas.

Además, el sistema de distribución de clave criptográfica de acuerdo con la presente invención supera los inconvenientes de los sistemas de QKD conocidos. De hecho, gracias a la arquitectura expandible de la red cuántica del sistema de distribución de clave criptográfica de acuerdo con la presente invención, se superan los siguientes inconvenientes:

- el inconveniente relacionado con el hecho de que dos dispositivos de comunicación deben estar relativamente cerca entre sí o más bien a una distancia de pocos kilómetros para ser capaces de explotar la QKD con el fin de generar una clave criptográfica segura común para ambos; y

- el inconveniente relacionado con el hecho de tener que configurar, para cada par de dispositivos de comunicación, un canal cuántico correspondiente que conecte dichos dispositivos de manera que se explote la QKD con el fin de generar una clave criptográfica segura común para ambos.

Finalmente, es claro que se pueden aplicar diversas modificaciones a la presente invención sin salirse del ámbito de protección de la invención definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema de distribución de clave criptográfica que comprende:

● un nodo del servidor (S);

● al menos un primer nodo de cliente (C1) conectado al nodo del servidor (S) por medio de un primer canal cuántico;

● una red de repetidor conectada al nodo del servidor (S) por medio de un segundo canal cuántico; y

● al menos un segundo nodo de cliente (C2) conectado a la red de repetidor por medio de un tercer canal cuántico;

donde:

● el nodo del servidor (S) y el primer nodo de cliente (C1) están configurados para generar en cooperación una primera clave cuántica de enlace asociada con un primer suscriptor de sistema mediante la implementación de una distribución de clave cuántica en el primer canal cuántico;

● el primer nodo de cliente (C1) está configurado para proporcionar al primer suscriptor la primera clave cuántica de enlace;

● la red de repetidor y el segundo nodo de cliente (C2) están configurados para generar en cooperación una clave cuántica de transferencia asociada con un segundo suscriptor de sistema mediante la implementación de una distribución de clave cuántica en el tercer canal cuántico;

● el segundo nodo de cliente (C2) está configurado para proporcionar al segundo suscriptor la clave cuántica de transferencia;

● el nodo del servidor (S) y la red de repetidor están configurados para generar en cooperación una segunda clave cuántica de enlace asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el segundo canal cuántico;

● la red de repetidor está configurada además para

- encriptar la segunda clave cuántica de enlace sobre la base de la clave cuántica de transferencia, y

- enviar la segunda clave cuántica de enlace encriptada al segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s); y

● el nodo del servidor (S) está configurado además para

- encriptar una clave criptográfica de tráfico asociada con el primer y el segundo suscriptor de sistema sobre la base de la primera clave cuántica de enlace y de una primera clave de autenticación de servicio asociada con el primer suscriptor,

- enviar la clave criptográfica de tráfico encriptada sobre la base de la primera clave cuántica de enlace y de la primera clave de autenticación de servicio al primer suscriptor por medio de uno o varios canal(es) de comunicación público(s),

- encriptar la clave criptográfica de tráfico asociada con el primer y el segundo suscriptor de sistema sobre la base de la segunda clave cuántica de enlace y de una segunda clave de autenticación de servicio asociada con el segundo suscriptor, y

- enviar la clave criptográfica de tráfico encriptada sobre la base de la segunda clave cuántica de enlace y de la segunda clave de autenticación de servicio al segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s).

2. El sistema de la reivindicación 1, donde el nodo del servidor (S) está configurado además para:

● almacenar una primera clave de autenticación de servicio actual asociada con el primer suscriptor y una segunda clave de autenticación de servicio actual asociada con el segundo suscriptor;

● encriptar la clave criptográfica de tráfico asociada con el primer y el segundo suscriptor y una primera clave de autenticación de servicio nueva asociada con el primer suscriptor sobre la base de la primera clave cuántica de enlace y de la primera clave de autenticación de servicio actual;

● enviar la clave criptográfica de tráfico y la primera clave de autenticación de servicio nueva encriptadas sobre la base de la primera clave cuántica de enlace y de la primera clave de autenticación de servicio actual al primer suscriptor por medio de uno o varios canal(es) de comunicación público(s);

● encriptar la clave criptográfica de tráfico asociada con el primer y el segundo suscriptor y una segunda clave de autenticación de servicio nueva asociada con el segundo suscriptor sobre la base de la segunda clave cuántica de enlace y de la segunda clave de autenticación de servicio actual;

● enviar la clave criptográfica de tráfico y la segunda clave de autenticación de servicio nueva encriptadas sobre la base de la segunda clave cuántica de enlace y de la segunda clave de autenticación de servicio actual al segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s); y

● actualizar la primera clave de autenticación de servicio actual almacenada en memoria con la primera clave de autenticación de servicio nueva y la segunda clave de autenticación de servicio actual almacenada en memoria con la segunda clave de autenticación de servicio nueva.

3. El sistema de la reivindicación 2, donde el nodo del servidor (S) está configurado para:

● encriptar la clave criptográfica de tráfico y la primera clave de autenticación de servicio nueva mediante la realización de una encriptación de libreta de un solo uso (One Time Pad, OTP) de dicha clave criptográfica de tráfico y dicha primera clave de autenticación de servicio nueva sobre la base de la primera clave cuántica de enlace, obteniendo de ese modo un primer mensaje encriptado;

● encriptar el primer mensaje encriptado sobre la base de la primera clave de autenticación de servicio actual, obteniendo de ese modo un segundo mensaje encriptado;

● enviar el segundo mensaje encriptado al primer suscriptor por medio de uno o varios canal(es) de comunicación público(s);

● encriptar la clave criptográfica de tráfico y la segunda clave de autenticación de servicio nueva mediante la realización de una encriptación de libreta de un solo uso (One Time Pad, OTP) de dicha clave criptográfica de tráfico y de dicha segunda clave de autenticación de servicio nueva sobre la base de la segunda clave cuántica de enlace, obteniendo de ese modo un tercer mensaje encriptado;

● encriptar el tercer mensaje encriptado sobre la base de la segunda clave de autenticación de servicio actual, obteniendo de ese modo un cuarto mensaje encriptado; y

● enviar el cuarto mensaje encriptado al segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s).

4. El sistema de acuerdo con una cualquiera de las reivindicaciones precedentes, donde la red de repetidor comprende un nodo repetidor (R) conectado al nodo del servidor (S) por medio del segundo canal cuántico y al segundo nodo de cliente (C2) por medio del tercer canal cuántico;

donde el nodo repetidor (R) y el segundo nodo de cliente (C2) están configurados para generar en cooperación la clave cuántica de transferencia asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el tercer canal cuántico;

donde el nodo repetidor (R) y el nodo del servidor (S) están configurados para generar en cooperación la segunda clave cuántica de enlace asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el segundo canal cuántico;

y donde el nodo repetidor (R) está configurado además para:

● encriptar la segunda clave cuántica de enlace sobre la base de la clave cuántica de transferencia; y

● enviar la segunda clave cuántica de enlace encriptada al segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s).

5. El sistema de acuerdo con una cualquiera de las reivindicaciones tales 1 a 3, donde la red de repetidor comprende:

● un primer nodo repetidor conectado al nodo del servidor (S) por medio del segundo canal cuántico; y

● un segundo nodo repetidor conectado al segundo nodo de cliente (C2) por medio del tercer canal cuántico y al primer nodo repetidor por medio de un cuarto canal cuántico;

donde el primer nodo repetidor y el nodo del servidor (S) están configurados para generar en cooperación la segunda clave cuántica de enlace asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el segundo canal cuántico;

donde el segundo nodo repetidor y el segundo nodo de cliente (C2) están configurados para generar en cooperación la clave cuántica de transferencia asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el tercer canal cuántico;

donde el primer nodo repetidor y el segundo nodo repetidor están configurados para generar en cooperación una clave cuántica de transferencia adicional mediante la implementación de una distribución de clave cuántica en el cuarto canal cuántico;

donde el primer nodo repetidor está configurado además para:

● encriptar la segunda clave cuántica de enlace sobre la base de la clave cuántica de transferencia adicional generada en cooperación con el segundo nodo repetidor, y

● enviar la segunda clave cuántica de enlace encriptada sobre la base de la clave cuántica de transferencia adicional generada en cooperación con el segundo nodo repetidor a dicho segundo nodo repetidor por medio de uno o varios canal(es) de comunicación público(s);

y donde el segundo nodo repetidor está configurado además para:

● desencriptar la segunda clave cuántica de enlace encriptada recibida del primer nodo repetidor sobre la base de la clave cuántica de transferencia adicional generada en cooperación con dicho primer nodo repetidor;

● encriptar la segunda clave cuántica de enlace sobre la base de la clave cuántica de transferencia asociada con el segundo suscriptor; y

● enviar la segunda clave cuántica de enlace encriptada sobre la base de la clave cuántica de transferencia asociada con el segundo suscriptor a dicho segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s).

6. El sistema de acuerdo con una cualquiera de las reivindicaciones tales 1 a 3, donde la red de repetidor comprende:

● un primer nodo repetidor conectado al nodo del servidor (S) por medio del segundo canal cuántico;

● un segundo nodo repetidor conectado al segundo nodo de cliente (C2) por medio del tercer canal cuántico; y

● un nodo repetidor intermedio conectado al primer nodo repetidor por medio de un cuarto canal cuántico y al segundo nodo repetidor por medio de un quinto canal cuántico;

donde el primer nodo repetidor y el nodo del servidor (S) están configurados para generar en cooperación la

segunda clave cuántica de enlace asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el segundo canal cuántico;

donde el segundo nodo repetidor y el segundo nodo de cliente (C2) están configurados para generar en cooperación la clave cuántica de transferencia asociada con el segundo suscriptor mediante la implementación de una distribución de clave cuántica en el tercer canal cuántico;

donde el primer nodo repetidor y el nodo repetidor intermedio están configurados para generar en cooperación una primera clave cuántica de transferencia adicional mediante la implementación de una distribución de clave cuántica en el cuarto canal cuántico;

donde el nodo repetidor intermedio y el segundo nodo repetidor están configurados para generar en cooperación una segunda clave cuántica de transferencia adicional mediante la implementación de una distribución de clave cuántica en el quinto canal cuántico;

donde el primer nodo repetidor está configurado además para:

● encriptar la segunda clave cuántica de enlace sobre la base de la primera clave cuántica de transferencia adicional generada en cooperación con el nodo repetidor intermedio, y

● enviar la segunda clave cuántica de enlace encriptada sobre la base de la primera clave cuántica de transferencia adicional generada en cooperación con el nodo repetidor intermedio a dicho nodo repetidor intermedio por medio de uno o varios canal(es) de comunicación público(s);

donde el nodo repetidor intermedio está configurado además para:

● desencriptar la segunda clave cuántica de enlace encriptada recibida del primer nodo repetidor sobre la base de la primera clave cuántica de transferencia adicional generada en cooperación con el primer nodo repetidor;

● encriptar la segunda clave cuántica de enlace sobre la base de la segunda clave cuántica de transferencia adicional generada en cooperación con el segundo nodo repetidor; y

● enviar la segunda clave cuántica de enlace encriptada sobre la base de la segunda clave cuántica de transferencia adicional generada en cooperación con el segundo nodo repetidor a dicho segundo nodo repetidor por medio de uno o varios canal(es) de comunicación público(s);

y donde el segundo nodo repetidor está configurado además para:

● desencriptar la segunda clave cuántica de enlace encriptada recibida del nodo repetidor intermedio sobre la base de la segunda clave cuántica de transferencia adicional generada en cooperación con dicho nodo repetidor intermedio;

● encriptar la segunda clave cuántica de enlace sobre la base de la clave cuántica de transferencia asociada con el segundo suscriptor; y

● enviar la segunda clave cuántica de enlace encriptada sobre la base de la clave cuántica de transferencia asociada con el segundo suscriptor al segundo suscriptor por medio de uno o varios canal(es) de comunicación público(s).

7. El sistema de acuerdo con una cualquiera de las reivindicaciones precedentes, donde el nodo del servidor (S) está configurado para generar las claves criptográficas de tráfico funcionando como un Generador de números aleatorios cuántico (QRNG, por sus siglas en inglés, Quantum Random Number Generator).

8. El sistema de acuerdo con una cualquiera de las reivindicaciones tales 1 a 6, donde el nodo del servidor (S) está configurado para recibir las claves criptográficas de tráfico desde un generador de claves independiente de dicho nodo del servidor (S).

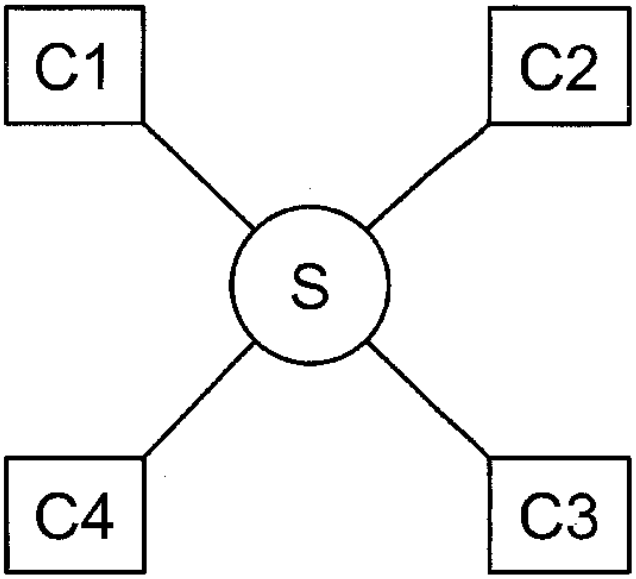

Fig. 1

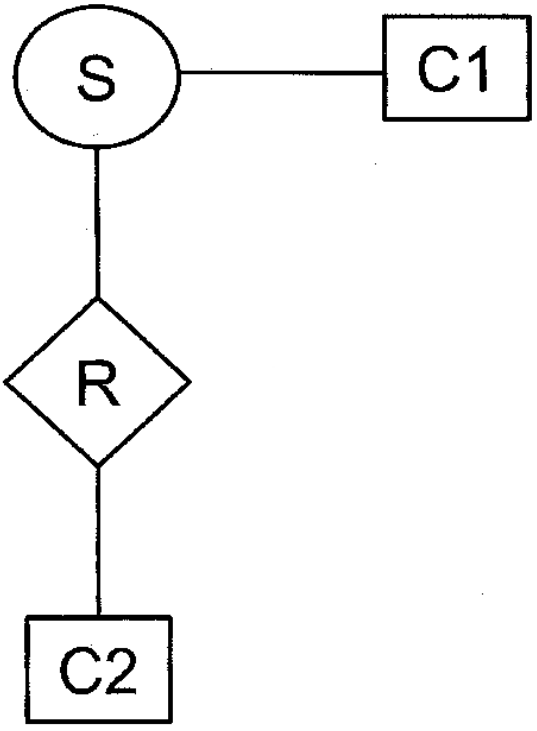

Fig. 2