(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 805 968**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.03.2018 E 18162719 (1)**

(97) Fecha y número de publicación de la concesión europea: **13.05.2020 EP 3544223**

(54) Título: **Método y sistema de intercambio de material clave a prueba de escuchas**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.02.2021

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

GUNKEL, MATTHIAS, DR.;
WISSEL, FELIX, DR. y
KUSSEL, TOBIAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y sistema de intercambio de material clave a prueba de escuchas

La presente invención se refiere a un método y a un sistema de intercambio de material clave a prueba de escuchas entre un emisor y un receptor para una clave de encriptación de un mensaje a enviar.

En las redes de comunicación modernas, los conceptos criptológicos tal como la seguridad, la confidencialidad y la fiabilidad de los datos desempeñan un papel importante. Estos conceptos significan que dos partes, es decir, el emisor y el receptor, pueden intercambiar datos sin ser interceptados por terceros y sin que los datos se modifiquen durante el intercambio. También es importante que ambas partes sepan con certeza con quién se están comunicando. En los países de habla inglesa, esto se denomina "confidentiality" (confidencialidad), "authenticity" (autenticidad) e "integrity" (integridad). Además, el lenguaje ha evolucionado de manera que las partes que intercambian datos se denominan "Alice" y "Bob" y los terceros malintencionados, es decir, los atacantes, se denominan "Eve" (del inglés "to eavesdrop" -escuchar).

Se puede demostrar que la encriptación con el sistema denominado "one-time pad" (bloc de un solo uso), es decir, se genera una nueva clave para cada transmisión de datos, es una información teóricamente segura. Esto significa que Eve no tiene forma de deducir el contenido de información de un flujo de datos interceptado. El one-time-pad es la clave, que debe ser tan larga como el mensaje a cifrar y no debe tener una estructura interna. Esto significa que la clave o el bloc de notas de una sola vez deben ser absolutamente aleatorios y no deben tener ninguna correlación entre los componentes individuales contenidos. Normalmente un mensaje original, es decir, un mensaje original enviado de Alice a Bob, puede representarse como una secuencia de ceros y unos. Este mensaje se denomina M (mensaje). El bloc de un solo uso se denomina K (clave) y el mensaje encriptado que se transmite finalmente se denomina C (cifrado). El mensaje encriptado se genera al ejecutar la operación XOR en el mensaje M con la clave bit a bit, es decir, aplicando el operador exclusivo-o como operador bit a la clave del mensaje M. Cabe señalar que la clave K debe utilizarse una sola vez, de modo que no se puede eliminar la clave K de dos o más textos cifrados C1 y C2 que se escuchan. La seguridad de esta forma de proceder radica en el hecho de que un espacio o conjunto de posibles mensajes significativos es demasiado grande. Incluso si Eve ha reconstruido un mensaje M' a partir del cifrado del C, no puede estar segura de que M' coincida con M.

Por lo tanto, el problema de encriptación propiamente dicho parece haberse resuelto con el uso de blocs de un solo uso. Sin embargo, cabe señalar que esto plantea un problema adicional, ya que ahora es necesario intercambiar la clave K entre Alice y Bob sin que Eve pueda escuchar la clave K, manipularla o hacer que una de las partes, es decir, Alice o Bob, finja ser Alice o Bob respectivamente. Ahora es necesario un método adecuado de intercambio de claves para esto. A diferencia del cifrado real, que funciona con la misma clave K de Alice y Bob y que, por lo tanto, se denomina "simétrico", el intercambio de claves o método de intercambio de claves es un método asimétrico basado en el hecho de que Alice y Bob tienen cada una parte pública y otra privada de la clave.

Los métodos establecidos hasta ahora conocidos, que utilizan estos pares de "clave pública" y "clave privada", se basan esencialmente todos en las denominadas funciones unidireccionales. Estos representan problemas matemáticos fáciles de resolver, pero cuya función inversa sólo puede ser calculada con gran esfuerzo. Un problema típico de este tipo es el factoreo de grandes números. Si se seleccionan dos grandes números primos p y q, el producto N = p*q puede calcularse muy rápidamente, es decir, por lo general en unos pocos milisegundos. Sin embargo, si solo está dado el producto N, no hay ningún algoritmo matemático para determinar eficientemente los dos números primos o los hechos primos p y q. Con la excepción de algunas condiciones de exclusión heurística, por ejemplo, que los factores primos deben ser impares, al atacante, es decir, a Eve, solo le resta aplicar un método denominado de fuerza bruta. Es posible protegerse del hardware de ordenador cada vez mejor y las consiguientes computabilidades asociadas más rápidas cambiando a claves cada vez más grandes. En contraste con la seguridad teórica de la información de los blocs de un solo uso, esto se denomina "seguridad computacional", es decir, que en principio no se está protegido contra los ataques, sino que simplemente se dificulta al máximo la ruptura del código o la clave. Los dos métodos más conocidos actualmente en uso - DH/DHM (Diffie-Hellmann o Diffie-Hellmann-Merkle) y RSA (Rivest, Shamir y Adleman) - utilizan longitudes de clave de hasta 2.048 dígitos binarios.

Sin embargo, en un futuro previsible, habrá ordenadores cuánticos comercialmente disponibles con suficiente rendimiento. Los ordenadores cuánticos utilizan un efecto de mecánica cuántica, es decir, que en las escalas de longitudes microscópicas es posible una superposición de estados cuánticos. Sin entrar en detalles en la presente memoria, un ordenador cuántico es concebible de manera tal que no calcule con ceros o unos, es decir, con los tradicionales bits, sino con los denominados qubits, que pueden asumir simultáneamente un valor de 0 y 1. Por lo tanto, para el problema de factorización mencionado anteriormente, ya no es necesario probar todas las combinaciones una tras otra, sino que todas estas combinaciones pueden probarse simultáneamente. En condiciones de laboratorio, ya es posible en la actualidad descomponer productos más pequeños como el 15 o 21 en sus factores utilizando un ordenador cuántico.

Así que parece ser sólo cuestión de tiempo hasta que los productos de mayor número primo puedan descomponerse. En este contexto, cabe mencionar "Quantum factorization of 56153 with only 4 qubits", Nikesh S. Dattani, Nathaniel

Bryans, 2014, https://arx- iv.org/abs/1411.6758, en el que N=56143 se factoriza con cierto conocimiento previo, por lo que el método revelado en dicho documento no hace todavía ninguna declaración sobre el orden de magnitud de ningún N. Según "Cybersecurity in an era with quantum computers: will we be ready?", Michele Mosca, 2015, https://eprint.ia- cr.org/2015/1075.pdf, los expertos estiman que la probabilidad de que el RSA-2048 a se rompa para 2026 es de un séptimo y en el año 2031 de 50 %.

En general, cabe señalar que, con la inminente disponibilidad de los ordenadores cuánticos, en principio todos los métodos convencionales de cifrado asimétrico utilizados hoy en día serán obsoletos.

Ante este trasfondo, se propusieron nuevos métodos de intercambio seguro de claves garantizadas. También se basan en los efectos de la mecánica cuántica y, por lo tanto, ofrecen la posibilidad de sacar conclusiones sobre si la clave fue interceptada o no mediante un análisis estadístico de las propiedades de la clave intercambiada. Si este análisis muestra que la clave está comprometida de alguna manera, se descarta y se inicia un nuevo intercambio de claves. Esto no es crítico, porque mientras no se haya establecido una clave segura, no se ha comunicado ningún dato potencialmente sensible entre Alice y Bob, y estos datos son el objetivo real de un posible atacante, Eve.

El llamado QKD (Distribución de la Clave Cuántica - método de selección de la clave cuántica) hace uso de dos principios de la mecánica cuántica. Uno de estos es el "teorema de no clonación", que impide la creación de una copia al cien por cien de cualquier sistema mecánico cuántico desconocido. Por otro lado, es el principio que dice que cuando se mide un sistema de mecánica cuántica, el sistema es forzado a un denominado estado propio del operador, que representa matemáticamente lo observable que fue medido.

Esto se explica con el siguiente ejemplo: los fotones polarizados lineales pueden tomar la dirección "vertical" u "horizontal". Lo mismo se aplica a los filtros de polarización. Un fotón "vertical" siempre pasará a través de un filtro de polarización que se establece en la "dirección vertical" y nunca a través de un filtro de polarización "horizontal". Se dice que estas dos direcciones son ortogonales entre sí. Este hallazgo es absoluto. Sin embargo, las direcciones elegidas "vertical" y "horizontal" son arbitrarias. Los ejes deberían denominarse "V" y "H". Los dos juntos forman un sistema básico, que se denomina "+".

Otra posible elección son dos ejes ortogonales, que están giradas 45° con respecto al eje V y H. Es posible imaginarlas como las "diagonales", y esta base se denomina "x". Por consiguiente, hay dos sistemas básicos: el sistema + con los ejes H y V y el sistema x con los ejes D1 (+45°) y D2 (-45°). Para la descripción de un fotón polarizado ambos sistemas son equivalentes. Sólo los componentes respectivos del vector de polarización cambian si las bases se interpretan como un sistema de coordenadas. Un fotón que está polarizado verticalmente en la base + - tiene las coordenadas 1 y 0. El mismo fotón está representado en la base x - con las coordenadas 1/2 y -1/2. Un "fotón X" siempre dará un acierto exacto en la base X. Esto significa que un estado de polarización puede ser medido con exactitud. Sin embargo, si el "fotón x" se mide en la base + -, hay una probabilidad de 50/50 (es decir, una probabilidad de 50-50) para la detección de un estado "en la base + - vertical" o "en la base + - horizontal".

El método real de intercambio de claves mencionado anteriormente se basa en el hecho de que Alice envía a Bob fotones en un estado de polarización aleatoria con respecto a las dos posibles bases, y Bob también mide al azar los fotones en una de las bases. Después de la medición, Bob y Alice intercambian información a través de un canal de datos clásico sobre la base en la que se enviaron los fotones sin revelar el resultado de las mediciones. Estadísticamente, las bases están de acuerdo en el 50 % de los casos. Los fotones de esta medición se utilizan para generar una secuencia de ceros y unos, por ejemplo, según la convención de que el eje H corresponde a un 1 en la base + - y el eje V corresponde a un 0 y en la base x -. Dado que Eve no puede saber lo que envía Alice o lo que mide Bob, se ve obligada a cometer errores. También tiene 50 % de posibilidades de medir en la base correcta si se realiza una escucha de los fotones. Pero también tiene 50 % de posibilidades contra Bob, porque tiene que generar nuevos fotones para que no sea detectada inmediatamente como una espía. Por lo tanto, en promedio, sólo tiene razón en una cuarta parte de los casos, y Alice y Bob pueden detectar estos errores forzados mediante un análisis estadístico posterior de la secuencia de bits. Para ello, se debe sacrificar parte de la materia prima clave. Esta parte del post-procesamiento se denomina ampliación de la privacidad “privacy ampliation”.

Aparte del método esbozado anteriormente, que se basa en el llamado protocolo BB84, como se describe, por ejemplo, en “Quantum cryptography”, Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel and Hugo Zbinden, Reviews Of Modern Physics, Volume 74, January 2002, hay varias otras variantes que hacen uso de las propiedades de la mecánica cuántica de los fotones de una manera u otra. Todos los métodos conocidos, incluido el método descrito anteriormente, tienen en común que los fotones individuales, es decir, generalmente los cuantos, son portadores de información cuántica. Por lo tanto, una tasa clave alcanzable es mucho menor que las tasas de datos que de otro modo serían posibles en la tecnología de transmisión óptica. Un orden de magnitud típico para la corriente de la clave cuántica se encuentra entre pocos fotones por segundo hasta el intervalo de kbits/s o Mbit/s. Cabe señalar que las tasas clave elevadas sólo son posibles para distancias muy cortas. Por otra parte, las interfaces de transporte clásicas con varios cientos de GBit/s son de última generación y con el uso de formatos de modulación más altos y receptores coherentes, pronto se podrán alcanzar velocidades de datos de Terabit/s. Obviamente las tasas de claves QKD no son suficientes comparadas con esto.

En el documento de Kaoru Shimizu and Nobuyuki Imoto "Communication channels secured from eavesdropping via transmission of photonic Bell states" se describe un procedimientio de comunicación a prueba de escuchas por medio de fotones entrecruzados, en el que los fotones entrecruzados se utilizan para transmitir bits de un mensaje encriptado en una base cuántica y de bits de prueba en otra base cuántica. Los fotones entrecruzados se transmiten por diferentes caminos ópticos.

En el documento US 2010/265077 A1, se describe el uso de fotones cuánticos entrecruzados mecánicamente para monitorizar la integridad de un límite físico o un enlace de comunicación.

En este contexto, una de las tareas de la presente invención es prever una forma de proporcionar un intercambio de material clave a prueba de escuchas con una mayor tasa de intercambio de claves en una red de fibra óptica.

Para solucionar esta tarea, la presente invención presenta un método y un sistema con las características de las reivindicaciones independientes.

Otras ventajas y conformaciones de la invención resultan de la descripción y el dibujo adjunto.

Se propone un método de intercambio de material clave a prueba de escuchas entre un emisor y un receptor para una clave de encriptación de un mensaje en una red de fibra óptica. Al menos dos cuantos, en particular dos fotones, se entrecruzan y un fotón se envía desde el emisor al receptor a través de un canal cuántico de un cable de fibra óptica con una longitud de onda λ_{EQSE}. Los al menos dos canales cuánticos, en particular los dos canales cuánticos que corresponden exactamente a dos fotones son disyuntivos entre sí, es decir, en particular, separados y libres de elementos entre sí.

De acuerdo con la invención, en un tiempo seleccionado aleatoriamente y durante un tiempo cualquiera seleccionado se transmite ahora la clave material desde el emisor al receptor y en una duración seleccionada aleatoriamente a través de un canal de datos que se superpone a uno de los canales cuánticos disyuntivos por selección aleatoria, en una fase de transmisión de la clave desde el emisor al receptor, estando el canal de datos diseñado para una potencia que es varios órdenes de magnitud más alta que la de los respectivos, al menos, dos canales cuánticos.

De acuerdo con la invención, la transmisión de información para la clave que se va a intercambiar se separa así de la rastreabilidad si se produjo una violación de la confidencialidad durante la transmisión, es decir, que un tercero, es decir, Eve, estaba escuchando. Esta prueba de si un tercero no autorizado estaba escuchando se basa todavía en uno o más canales cuánticos, en particular dos canales cuánticos. De acuerdo con la invención, los fotones entrecruzados no modulados "Entangled Quantum State Emission", abreviado EQSE, se utilizan como portadores de una propiedad cuántica. El entrecruzamiento significa generalmente que al menos dos fotones, es decir, en general en al menos dos sistemas de mecánica cuántica, se ha impreso una propiedad común que, debido a las leyes de la mecánica cuántica, no puede mantenerse ni siquiera a grandes distancias sin destruir el entrecruzamiento de los fotones, es decir, generalmente de los sistemas/partículas de mecánica cuántica. Esto significa que los al menos dos fotones están conectados entre sí de cierta manera, es decir, las partículas entrecruzadas se encuentran en un estado cuántico común, lo que esencialmente significa que las propiedades de las partículas entrecruzadas dependen una de la otra. Si una de las partículas altera una de sus propiedades, la partícula entrecruzada debe hacerlo de inmediato, independientemente de la distancia a la que se encuentren las partículas. El entrecruzamiento se produce cuando un estado de un sistema de dos o más partículas (cuantos, por ejemplo, fotones) no puede describirse como una combinación de estados independientes de una sola partícula, sino sólo por un estado común.

Esto significa que los resultados de las mediciones de ciertos observables de partículas entrecruzadas están correlacionados, es decir, no son estadísticamente independientes, aunque las partículas estén muy alejadas entre sí. Esto se basa en la descripción de una función de onda total con coeficientes no separables de una respectiva base de una sola partícula y. En consecuencia, una medición independiente de al menos dos fotones o, en general, de cuantos que están separados espacialmente de forma arbitraria siempre da resultados complementarios que forman el estado cuántico común. A este respecto, cabe señalar la famosa formulación de Einstein del "efecto espeluznante a larga distancia". En el caso de los fotones, por ejemplo, esto significa que su polarización global, es decir, la suma de las polarizaciones individuales debe anularse siempre hasta 0 si los fotones se originan en un estado original sin polarización. Esta propiedad se aplica en cualquier base completa. En general, el entrelazamiento de los fotones previsto en la invención no tiene que limitarse a una correlación de la polarización respectiva de los fotones (cuantos). Tal entrelazamiento puede realizarse en muchas variantes conocidas por los expertos.

De acuerdo con la invención, el emisor, es decir, Alice, transmite estos fotones entrecruzados a una longitud de onda λ_{EQSE} a través de dos o más fibras ópticas guiadas independientemente, es decir, de forma disociada o canales cuánticos al receptor, es decir, a Bob.

De acuerdo con una posible configuración del método de acuerdo con la invención, el receptor, es decir Bob, comprueba en intervalos de tiempo arbitrariamente seleccionados en una denominada medición de Bell si los fotones recibidos por el receptor están todavía entrecruzados en el momento de la medición de Bell. De esta manera, se puede comprobar si en este momento, es decir, en el momento de la medición de Bell, hay un interceptor potencial en uno o

más tramos arbitrarios o en todos los tramos de la ruta entre el emisor y el receptor y en la longitud de onda λ_{EQSE} en cuestión.

Según un diseño posterior del método de acuerdo con la invención, si la medición de Bell muestra que los fotones no están entrecruzados, el receptor determina que en el momento de la medición de Bell existe un interceptor potencial en al menos uno de al menos dos canales o secciones cuánticas y en la longitud de onda λ_{EQSE}, por lo que al menos el material transmitido a través del canal de datos en la última fase de transmisión de claves precedente es descartado. Porque un tercero no autorizado, en este caso Eve, mediante una escucha de al menos una fibra óptica o uno de los varios canales cuánticos, ha realizado por sí mismo una medición en por lo menos uno de los fotones, resolviendo así o interrumpiendo el entrecruzamiento entre los fotones.

Según el método de acuerdo con la invención, el canal de datos está diseñado para un rendimiento varios órdenes de magnitud superior al de los respectivos canales cuánticos.

En momentos aleatorios y por una duración aleatoria y, es decir, impredecible para un oyente, es decir, Eve, el emisor, es decir, Alice, transmite material clave secreto en el canal de datos de alta potencia, que se superpone a uno de los al menos dos canales cuánticos disociados, también en la longitud de onda λ_{EQSE}.

De acuerdo con una conformación posible, es concebible que se desactive o se apague el canal cuántico en el que se superpone el canal de datos mientras dure la transmisión del material clave a través del canal de datos. Sin embargo, esto no tiene que producirse necesariamente, porque los fotones transmitidos por los canales cuánticos están prácticamente enmascarados por la masiva corriente de fotones con la que se transmite el material clave por el canal de datos, por lo que el canal de datos, como se ha mencionado anteriormente, tiene una potencia varios órdenes de magnitud superior a la del canal de datos y, por lo tanto, tiene un ruido inherente cuya variación es también muchas veces superior a la de uno de los por lo menos dos canales cuánticos.

En una posible conformación del método de acuerdo con la invención, los fotones, que originalmente surgieron de un estado original sin polarización, están o están entrecruzados en el lado del emisor de tal manera que la suma de las respectivas polarizaciones de los fotones resulta en una polarización total de 0. Como ya se ha mencionado, el entrelazamiento de los fotones, tal como se ha previsto en la invención, no tiene por qué limitarse a una correlación de la polarización respectiva de los fotones (cuantos). Tal entrecruzamiento puede realizarse en muchas variantes conocidas por los expertos.

En otra conformación del método de acuerdo con la invención, el receptor, es decir Bob, determina en un caso en que la medición de Bell muestra que los fotones siguen entrecruzados, que en el momento de la medición de Bell existe un interceptor potencial en ninguno de los al menos dos canales cuánticos y en la longitud de onda λ_{EQSE} y confirma los componentes clave del material clave transmitido al emisor, es decir, Alice, a través del canal de datos en una fase de transmisión clave que comprende el tiempo de la medición de Bell e inmediatamente anterior al tiempo de la medición de Bell. Una fase final clave inmediatamente anterior significa la fase final clave que estuvo presente por última vez o tuvo lugar antes de que se realizara la medición de Bell. El receptor, es decir, Bob, determina en una fase de posprocesamiento a la medición de Bell por medio de un análisis estadístico si hubo algún indicio de escuchas, y si no, confirma al emisor el material transmitido en la fase previa de envío de claves por el canal de datos.

Este reconocimiento puede confirmarse mediante una sincronización temporal entre el emisor y el receptor y/o mediante un número de transmisión asignado a la fase de transmisión de la clave que comprende la hora de la medición de Bell o inmediatamente anterior a la hora de la medición de Bell, en la que todas las fases de transmisión de la clave se numeran consecutivamente con un número de transmisión respectivo, y/o se confirman mediante un protocolo de control.

El canal de datos, que es de alta potencia comparado con los respectivos canales cuánticos, puede, de acuerdo con la invención, simplemente ser encendido y apagado. Esta adición temporalmente aleatoria del canal de datos que interesa al oyente, es decir, Eve, obliga al oyente Eve a tener que realizar mediciones constantemente o a intervalos regulares cortos. En la medida en que Eve en este caso se encuentra a tiempo con la fase de la transmisión de los fotones entrecruzados a través de los canales cuánticos, ella interfiere cada vez con el entrecruzamiento, lo que a su vez se puede demostrar que es una escucha en el receptor, es decir, en Bob. Como Eve no puede saber cuál de los dos canales cuánticos desarticulados será superpuesto por el canal de datos en la siguiente etapa o en la siguiente fase de transmisión clave, no puede confiar en la supervisión de la intensidad por sí sola, donde ella misma disolvería el entrecruzamiento de los fotones. Es importante que tanto el momento de la conexión del canal de datos como la duración de las respectivas fases de envío de las claves sean aleatorios, de modo que Eve no pueda desarrollar una estrategia óptima para obtener una pequeña ventaja de información.

Para asegurar en forma adicional el intercambio real de información, es decir, del material clave entre el emisor y el receptor, se implementa un método similar al método de acuerdo con la invención entre el emisor y el receptor, es decir, entre Alice y Bob. En otras palabras, el método se realiza de la misma manera para todos los receptores y emisores, con roles intercambiados.

De acuerdo con la invención, se prevé que además del material transmitido del emisor al receptor, se transmita material inverso del receptor al emisor, por lo que el receptor actúa entonces como emisor y el emisor como receptor, y se lleva a cabo un método descrito anteriormente.

Además, se ha previsto que el emisor y los receptores clave acuerden en intervalos de tiempo fijos el material acumulado en un intervalo respectivo en el lado del emisor y el receptor, que luego es sometido a la operación XOR tanto en el lado del emisor como en el del receptor, por lo que tanto en el lado del emisor como en el del receptor se genera una parte de una clave simétrica como la clave de encriptación del mensaje.

El material clave de ambos lados consiste en la respectiva clave bruta auto-transmitida y la respectiva clave bruta recibida y a prueba de escuchas. Cada una de las partes, es decir, emisor y receptor, someten a la operación XOR estos dos tipos de clave y por lo tanto generan su parte de la clave simétrica en su propio lado.

Dado que las longitudes de onda de los pares de fotosíntesis entrelazados y las del canal de datos son idénticas, denominado λ_{EQSE} en este caso, no es posible un ataque con un filtro óptico. También se puede descartar un ataque dirigido o un ataque a las fases temporales del canal de datos, es decir, a las fases finales clave. Si un tercero no autorizado, como Eve en particular, escuchara accidentalmente la fase del canal de datos de alto rendimiento que contiene la clave secreta, es decir, la fase de transmisión de la clave podría escuchar partes del secreto. Por lo tanto, el desplazamiento temporal de las transmisiones cuánticas individuales, es decir, la transmisión de los fotones entrecruzados a través de los canales cuánticos de los potentes canales de datos, es decir, la transmisión del material clave en las fases de envío clave a través del canal de datos, se realiza como un proceso aleatorio. De acuerdo con la invención, se ha previsto que esta se seleccione de manera que la ventana de tiempo para el componente mecánico cuántico EQSE, es decir, la única transmisión de los fotones entrecruzados por los al menos dos canales cuánticos mutuamente disyuntivos, sea lo suficientemente larga para que las estadísticas fiables de la medición de Bell se realicen por el lado del receptor, pero también lo más corta posible para lograr un tipo de cambio de claves aceptablemente alto por el potente canal de datos, es decir, un tipo aceptablemente alto de fases sucesivas de transmisión de claves.

La presente invención además se refiere a un sistema de intercambio de material clave a prueba de escuchas entre un emisor y un receptor para una clave de encriptación de un mensaje en una red de fibra óptica. El sistema de acuerdo con la invención comprende al menos el emisor y el receptor y al menos dos canales cuánticos de una fibra óptica respectiva que conecta el emisor y el receptor y al menos un canal de datos temporalmente superpuesto a uno de los canales cuánticos disociados por selección aleatoria. Al menos el emisor está previsto para entrecruzar al menos dos fotones entre sí y para transmitir en cada caso un fotón a través de en cada caso un canal cuántico de los al menos dos canales cuánticos con una longitud de onda Z_{EQSE} desde el emisor al receptor, siendo los al menos dos canales cuánticos disyuntivos entre sí.

Además, al menos el emisor está diseñado para transmitir la clave material desde el emisor al receptor en un tiempo y una duración elegidos al azar a través del canal de datos que se superpone por selección aleatoria en uno de los canales cuánticos disociados durante la duración elegida al azar, en una fase de transmisión de clave, estando el canal de datos diseñado para una potencia varios órdenes de magnitud superior a la de los al menos dos canales cuánticos respectivos.

En una configuración ulterior del sistema de acuerdo con la invención, el receptor está diseñado para comprobar en una medición de Bell en cualquier intervalo de tiempo elegido si los fotones recibidos por el receptor a través de los canales cuánticos mutuamente disyuntivos están todavía entrecruzados en el momento de la medición de Bell y, si de la medición de Bell resulta que los fotones no están entrecruzados, comprobar que en el momento de la medición de Bell respectiva, existe una potencial escucha en por lo menos uno de los dos canales cuánticos y en la longitud de onda λ_{EQSE}, en cuyo caso se descarta por lo menos el material transmitido en la fase de transmisión clave que precede por última vez a la medición de Bell

En una conformación posterior del sistema de acuerdo con la invención, el receptor se configura como receptor y como emisor y el emisor como emisor y los receptores pueden actuar de acuerdo con los roles intercambiados.

El sistema de acuerdo con la invención está configurado en particular para realizar un método descrito anteriormente.

Además, la presente invención se refiere a un producto de programa informático que comprende un medio legible por ordenador, un programa informático almacenado en el medio legible por ordenador, y el código de programa que está configurado para realizar un proceso inventivo descrito anteriormente en una unidad informática cuando el programa informático se ejecuta, en particular como un componente de un sistema de la invención descrito anteriormente.

Con el sistema de acuerdo con la invención, se puede implementar que los requisitos de seguridad y el rendimiento, es decir, el tipo de cambio clave, se pueden ajustar continuamente. Los parámetros de desvanecimiento es el ciclo de trabajo medio, la relación de la duración media respectiva entre la transmisión cuántica, es decir, la transmisión de los fotones entrecruzados, y un poderoso canal de datos con el material clave, es decir, las fases de emisión de datos. Como la duración respectiva es un proceso aleatorio, Eve no puede hacer una predicción en este caso y destruye los

estados cuánticos entrecruzados, es decir, el entrelazamiento de los fotones, y pierde grandes partes de la clave en un ataque con una regularidad predecible.

Las principales ventajas de la invención son que mediante un desacoplamiento de una transmisión de material clave y una función de vigilancia mecánica cuántica puede aumentarse en varios órdenes de magnitud en comparación con los métodos conocidos. Además, ya no son necesarios los métodos de cifrado por bloques como el AES, en el que se utilizan métodos matemáticos complejos para formular una especie de "extensión de clave". Por supuesto, la invención también puede utilizarse en combinación con el AES u otros métodos conocidos. Se pueden usar los blocs de un solo uso que no están expuestos a los ataques de canal lateral o de libro de códigos.

De acuerdo con la invención, los canales cuánticos a ser provistos son operados por cuantos o fotones no modulados, lo que significa que no se requieren costosos moduladores ópticos en este punto. La vigilancia del lado del receptor o bien de parte de Bob, se simplifica porque las complejas mediciones de los estados cuánticos en las diferentes variantes de los métodos QKD conocidos hasta ahora, como los estados de polarización que cambian rápidamente, se sustituyen por mediciones de Bell relativamente sencillas, ya que el entrelazamiento de los fotones debe ser el mismo en todas las bases.

Se sobreentiende que las características antes mencionadas y las que se explicarán a continuación pueden utilizarse no sólo en la combinación indicada en cada caso, sino también en otras combinaciones o en una posición única, sin dejar el alcance de la presente invención.

La invención se muestra esquemáticamente en el dibujo sobre la base de un ejemplo y se describe en detalle a continuación con referencia al dibujo.

La figura 1 muestra en una representación esquemática una realización del método de la invención usando una realización del sistema de acuerdo con la invención.

La figura 1a muestra una representación esquemática de una encarnación del sistema de acuerdo con la invención 10 para el intercambio de material clave a prueba de escuchas entre un emisor 11 y un receptor 12 para una clave de encriptación de un mensaje en una red de fibra óptica. El sistema 10, mostrado esquemáticamente, es también una representación esquemática de una realización del método de acuerdo con la invención. Por lo menos dos fotones de un emisor 11, que también se denomina Alice como se ha explicado anteriormente, están entrecruzados , lo que significa que los fotones están acoplados entre sí por tener una propiedad común que, debido a las leyes de la mecánica cuántica, no puede resolverse sin interferencias ni siquiera a grandes distancias, es decir, a la distancia del receptor 12 y a la distancia entre los canales cuánticos mutuamente disociados a través de los cuales se transmiten los fotones entrecruzados. Por ejemplo, los fotones, que han surgido de un estado original sin polarización, están polarizados de tal manera que las polarizaciones respectivas de todos los fotones preparados por el emisor 11 y transmitidos simultáneamente al receptor 12 suman una polarización total de 0. Los fotones entrecruzados de esta manera, por lo que en el ejemplo que se muestra aquí dos fotones se entrecruzan, se transmiten cada uno desde el emisor 11 al receptor 12 a través de un canal cuántico 13a o 13b de una respectiva fibra óptica 15 de la red de fibra óptica con una longitud de onda λ_{EQSE}.

Los dos canales cuánticos 13a y 13b son disyuntivos entre sí, es decir, completamente independientes el uno del otro y no están conectados de ninguna manera entre sí. El emisor 11 transmite fotones entrecruzados al receptor, utilizando un canal cuántico 13a y 13b y por fotón, es decir, una fibra óptica por fotón. Estos fotones entrecruzados son recibidos por el receptor 12 a intervalos arbitrariamente elegidos y su entrelazamiento es comprobado por una medición de Bell. Si el receptor 12 determina que los fotones recibidos por él no están entrecruzados en el momento de la medición de Bell realizada por él, puede determinar que en el momento de la medición de Bell hay una escucha potencial en al menos uno de los dos canales cuánticos 13a o 13b y en la longitud de onda λ_{EQSE} que ha perturbado los fotones entrecruzados de manera que se ha resuelto el entrelazamiento de los fotones entre sí. Como consecuencia de la determinación de la resolución del entrelazamiento y de la conclusión de que existe una escucha potencial, el material transmitido en último lugar por el canal de datos se descarta en clave, de modo que la potencial escucha no tiene posibilidad de ver el material clave que finalmente se utiliza realmente para encriptar el mensaje.

Mientras que la transmisión de fotones por los respectivos canales cuánticos 13a y 13b desde el emisor 11 al receptor 12 es esencialmente continua, en un tiempo seleccionado aleatoriamente y durante una duración seleccionada al azar por medio de un canal de datos 14, que se superpone a uno de los canales cuánticos disociados, en este caso el canal cuántico 13a, por selección aleatoria, la clave material se transmite del emisor 11 al receptor 12 en una fase de transmisión de clave. Durante la duración de la fase de envío de clave el canal cuántico superpuesto por el canal de datos, aquí el canal cuántico 13a, puede ser apagado. Sin embargo, esto último no tiene que producirse necesariamente, porque los fotones individuales enviados a través de los respectivos canales cuánticos 13a, 13b están casi completamente enmascarados por el flujo masivo de fotones del canal de datos 14, que abarca la clave material, ya que este canal tiene una potencia muchos órdenes de magnitud superior a la de la clave material y tiene un ruido inherente cuya variación es también muchas veces superior a la del respectivo canal cuántico 13a o 13b. Esto se muestra en la Figura 1b.

La Figura 1b muestra un diagrama 20, que se extiende sobre una abscisa 21 y una ordenada 22. En la abscisa 21 el tiempo t y se traza en la ordenada 22 la potencia P. Los datos transmitidos por el canal de datos 14 en fases finales clave seleccionadas al azar están representados aquí por los bloques de datos 23 que parecen irregulares en el tiempo. La corriente de fotones entrecruzados transmitida a través de los respectivos canales cuánticos 13a y 13b está indicada por el signo de referencia 24. Como puede verse en el diagrama, los fotones individuales 24 están enmascarados durante una fase de envío de clave 23 por los fotones transmitidos durante la fase de envío de clave 23, es decir, la potencia correspondiente a la transmisión de los fotones individuales está muy por debajo de la potencia correspondiente a los datos transmitidos en las fases de envío de clave, de modo que durante una fase de envío de clave 23 no es necesario desactivar el canal cuántico 13a superpuesto por el canal de datos clásico 14.

El canal de datos 14, que es más poderoso que los canales cuánticos 13a y 13b, de acuerdo con la invención se enciende y apaga al azar. Esta adición temporalmente aleatoria del canal de datos 14, que en realidad es de interés para un potencial escucha, obliga a éste a tomar medidas constantemente o a intervalos regulares cortos. Si la escucha llega a una fase de transmisión de la transmisión de fotones entrecruzados, perturba cada vez el entrelazamiento de los fotones, lo que a su vez puede probarse como una escucha en el receptor 12. Si el receptor 12 determina en el momento de la medición de Bell que el entrelazamiento esperado no está presente en los fotones recibidos, es rechazado el material clave transmitido por última vez en el canal de datos superpuesto al canal cuántico.

Dado que una escucha potencial no puede saber en cuál de los dos canales cuánticos disociados 13a o 13b se transmite el material clave en la siguiente etapa o en la siguiente fase de envío de clave a través de un canal de datos 14 superpuesto en el canal cuántico respectivo, el interceptor no puede confiar en la vigilancia de la intensidad por sí sola, por lo que incluso si la intensidad fuera meramente vigilada, se disolvería el entrelazamiento de los fotones. De acuerdo con la invención, tanto el tiempo de encendido del canal de datos 14 como la duración de las fases de envío de claves 23, como indica la diferente anchura de tiempo de los bloques de datos 23, se seleccionan al azar, de modo que una escucha no puede desarrollar una estrategia óptima para obtener una pequeña ventaja de información.

Dado que el emisor 11 sabe qué material se ha enviado al receptor 12, este solo tiene que procesar esas partes clave en una fase de posprocesamiento a través del canal de datos 14, en el que el análisis estadístico no ha revelado ninguna desviación y, por lo tanto, ninguna indicación de escucha por parte de un posible fisgón. Esa confirmación puede hacerse, por ejemplo, para una sincronización temporal entre el emisor 11 y el receptor 12, numerando las fases finales clave 23, en las que el material se transmite por medio de claves, consecutivamente en el tiempo. Sin embargo, también se pueden concebir otros protocolos de control adecuados.

Para asegurar en forma adicional el intercambio de información real, es decir, la transmisión del material clave al emisor 11 y al receptor 12, es concebible utilizar un método de transmisión similar al método para el emisor 11 y el receptor 12 con funciones intercambiadas. Esto significa que en este caso el receptor 12 actúa como emisor y el emisor 11 como receptor.

En intervalos de tiempo apropiados, el emisor 11 y el receptor 12 se ponen de acuerdo sobre un material clave acumulado en los lados. Este material clave consiste en ambos lados del material clave en bruto enviado por el propio emisor y del material clave protegido contra las escuchas y recibida por el otro lado. Cada una de las partes, es decir, el emisor 11 y el receptor 12, someten a la operación XOR independientemente estos dos tipos de material clave y generan así una parte de la clave simétrica.

Para que el método de acuerdo con la invención sea lo más seguro posible, se realiza un desplazamiento temporal de la transmisión cuántica única, es decir, la transmisión de los fotones entrelazados a través de los respectivos canales cuánticos 13a y 13b y el potente canal de datos 14, es decir, la fase de envío de clave, mediante un proceso aleatorio. Se selecciona de manera tal que una ventana de tiempo para la transmisión de los fotones entrecruzados sea lo suficientemente grande para que el receptor 12 pueda realizar estadísticas fiables de la medición de Bell, pero también lo más corta posible para lograr un tipo de cambio aceptablemente alto para el material clave que se transmitirá del emisor 11 al receptor 12.

REIVINDICACIONES

1. Método de intercambio de material clave a prueba de escuchas entre un emisor (11) y un receptor (12) para una clave de encriptación de un mensaje en una red de fibra óptica, en el que se entrelazaron al menos dos fotones entre sí y en cada caso un fotón a través de un canal cuántico (13a, 13b) de una fibra óptica (15) con una longitud de onda λ_{EQSE} se transmite del emisor (11) al receptor (12), mientras los al menos dos canales cuánticos (13a, 13b) son disyuntivos entre sí, y en el que en un momento seleccionado al azar y durante una duración seleccionada al azar a través de un canal de datos (14) superpuesto a uno de los canales cuánticos disociados (13a, 13b) por selección aleatoria, en una fase de transmisión de claves se transmite el material clave del emisor (11) al receptor (12), estando el canal de datos (14) diseñado para un rendimiento superior en varios órdenes de magnitud en comparación con los como mínimo dos canales cuánticos respectivos (13a, 13b).

2. Método de acuerdo con la reivindicación 1, en el que el receptor (12) comprueba en una medición de Bell a intervalos de tiempo arbitrariamente seleccionados si los fotones recibidos por el receptor (12) están todavía entrecruzados en el momento de la medición de Bell.

3. Método de acuerdo con la reivindicación 2, en el que, si la medición de Bell muestra que los fotones no están entrecruzados, el receptor (12) comprueba que en el momento de la medición de Bell existe una escucha potencial en al menos uno de al menos dos canales cuánticos (13a, 13b) y en la longitud de onda λ_{EQSE}, desechándose entonces el material clave transmitido por última vez a través del canal de datos (14).

4. Método de acuerdo con una de las reivindicaciones anteriores, en el que los fotones, que originalmente surgieron de un estado original sin polarización, se entrelazan en el lado del emisor (11) de tal manera que la suma de las polarizaciones respectivas de los fotones da como resultado una polarización total de cero.

5. Método de acuerdo con una de las reivindicaciones anteriores, en el que aquel canal cuántico (13a) en el que se superpone el canal de datos (14) se desactiva o apaga mientras dura la transmisión del material clave a través del canal de datos (14).

6. Método de acuerdo con una de las reivindicaciones 2 a 5, en el que el receptor (12), si la medición de Bell revela que los fotones están todavía entrecruzados, comprueba que en el momento de la medición de Bell no existe una escucha potencial en ninguno de los al menos dos canales cuánticos (13a, 13b) en la longitud de onda λ_{EQSE}, y el receptor (12) confirma las porciones clave del material clave transmitidas al emisor (11) a través del canal de datos (14) durante una fase de transmisión clave que comprende el tiempo de la medición de Bell o que precede al tiempo de la medición de Bell.

7. Método de acuerdo con la reivindicación 6, en el que el receptor (12) transmite las porciones clave del material clave, transmitidas en la fase de transmisión clave que comprende el tiempo de la medición de Bell o que precede al tiempo de la última medición de Bell, con relación al transmisor (11) mediante una sincronización temporal entre el transmisor (11) y el receptor (12) y/o sobre la base de un número de transmisión asignado a la fase de transmisión clave que comprende el tiempo de la medición de Bell o que precede al tiempo de la última medición de Bell, mientras todas las fases finales clave están numeradas y se les asigna un número de transmisión respectivo y/o son confirmadas por un protocolo de control.

8. Método de acuerdo con una de las reivindicaciones anteriores, en el que, además del material clave transmitido desde el emisor (11) al receptor (12), el material clave se transmite a la inversa desde el receptor (12) al emisor (11), actuando entonces el receptor (12) como emisor y el emisor (11) como receptor, y se lleva a cabo un método de acuerdo con una de las reivindicaciones anteriores.

9. Método de acuerdo con una de las reivindicaciones anteriores, en el que el emisor (11) y el receptor (12) están de acuerdo en intervalos de tiempo predeterminados sobre el material clave acumulado en un intervalo respectivo tanto en el lado del emisor como en el del receptor, que luego someten a la operación XOR del lado del emisor y del receptor, generando así tanto del lado del emisor como en el del receptor una parte de una clave simétrica como clave de encriptación del mensaje.

10. Sistema de intercambio de material clave a prueba de escuchas entre un emisor (11) y un receptor (12) para una clave de encriptación de un mensaje en una red de fibra óptica que comprende al menos el emisor (11) y el receptor (12) y al menos dos canales cuánticos (13a, 13b) que conectan el emisor (11) y el receptor (12) y al menos un canal de datos (14), que está superpuesto temporalmente a uno de los canales cuánticos (13a, 13b) disyuntivos de, en cada caso, una fibra óptica (15) mediante una selección al azar, siendo que al menos el emisor (11) se concibe para entrelazar al menos dos fotones entre sí y emitir en cada caso un fotón a través de en cada caso un canal cuántico (13a, 13b) de los al menos dos canales cuánticos (13a, 13b) con una longitud de onda λ_{EQSE} desde el emisor (11) al receptor (12), en el que los al menos dos canales cuánticos (13a, 13b) son disyuntivos entre sí y en el que en un momento seleccionado al azar y durante una duración seleccionada al azar a través de un canal de datos (14) superpuesto a uno de los canales cuánticos disociados (13a, 13b) por selección aleatoria, en una fase de transmisión de claves, se transmite el material clave del emisor (11) al receptor (12), estando el canal de datos (14) diseñado para

un rendimiento superior en varios órdenes de magnitud en comparación con los como mínimo dos canales cuánticos respectivos (13a, 13b).

11. Sistema de acuerdo con la reivindicación 10, en el que el receptor (11) está configurado para comprobar en intervalos de tiempo arbitrariamente seleccionados en una medición de Bell respectiva si los fotones recibidos por el receptor (12) están todavía entrelazados en el momento de la medición de Bell respectiva y, si de la medición de Bell respectiva resulta que los fotones no están entrelazados, comprobar que en el momento de la medición de Bell exista una potencial escucha en al menos uno de los dos canales cuánticos (13a, 13b) y en la longitud de onda λ_{EQSE} en cuyo caso se descarta el material clave transmitido en la fase final clave anterior al momento de la medición de Bell.

12. Sistema de acuerdo con la reivindicación 10 o 11, en el que el receptor (12) está configurado como receptor y como emisor y el emisor (11) está configurado como emisor y receptor y correspondientemente pueden actuar con roles intercambiados.

13. Sistema de acuerdo con una de las reivindicaciones 10 a 12, que está configurado para llevar a cabo un método de acuerdo con una de las reivindicaciones 1 a 9.

14. Un producto de programa de ordenador que comprende un medio legible por ordenador y un programa de ordenador almacenado en el medio legible por ordenador y que presenta medios de codificación de programa que está configurado para llevar a cabo un método de acuerdo con cualquiera de las reivindicaciones 1 a 9 cuando el programa de ordenador se ejecuta en una unidad de computación como un componente de un sistema de acuerdo con cualquiera de las reivindicaciones 10 a 13.

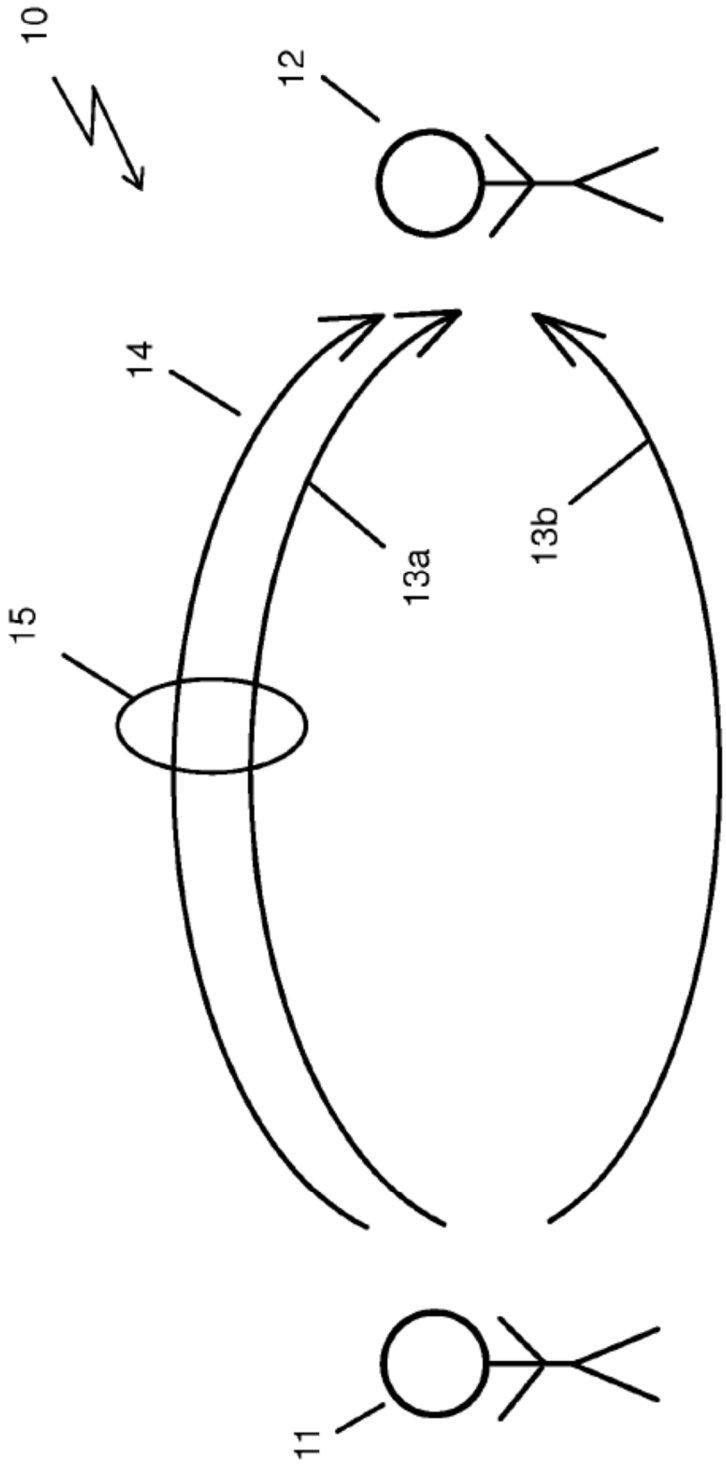

Fig. 1a

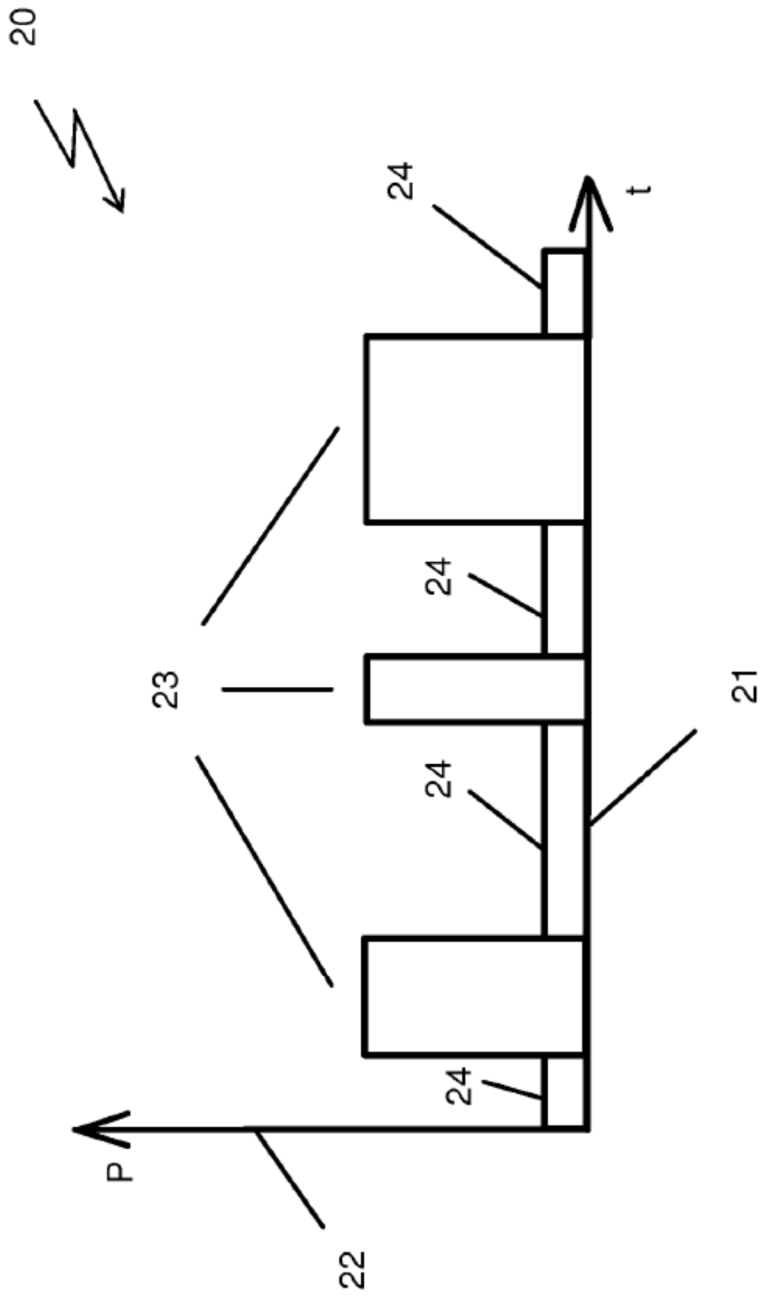

Fig. 1b