(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 431 465**

(21) Número de solicitud: 201230599

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

23.04.2012

(43) Fecha de publicación de la solicitud:

26.11.2013

Fecha de la concesión:

09.12.2014

(45) Fecha de publicación de la concesión:

16.12.2014

(56) Se remite a la solicitud internacional:

PCT/ES2013/070259

(73) Titular/es:

UNIVERSIDAD DE VALLADOLID (100.0%)
Real de Burgos, s/nº CTT-OTRI (CASA DEL ESTUDIANTE)
47001 Valladolid (Valladolid) ES

(72) Inventor/es:

GARCÍA ESCARTÍN, Juan Carlos y
CHAMORRO POSADA, Pedro

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

(54) Título: **PROCEDIMIENTO Y EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS**

(57) Resumen:

Procedimiento y equipo de autenticación de contraseñas cuánticas.

La invención consiste en un procedimiento y un equipo de usuario que permiten comprobar que dos usuarios comparten una contraseña c de p bits sin revelar ninguna información sobre esa contraseña. Para ello se codifica la función XOR de esa contraseña c con una secuencia aleatoria a en el estado cuántico de un único fotón. En el equipo de cada usuario se compara mediante el efecto Hong-Ou-Mandel un estado cuántico generado localmente con un estado que proporciona el otro usuario. Tras n fases de comprobación los usuarios pueden determinar que el otro usuario conoce la contraseña. El procedimiento y el equipo de usuario incluyen técnicas para detectar participantes deshonestos. La invención describe el equipo que implementa el procedimiento e incluye dos técnicas de codificación en sistemas cuánticos, una basada en una codificación temporal y la otra basada en una codificación en el momento orbital angular de un fotón.

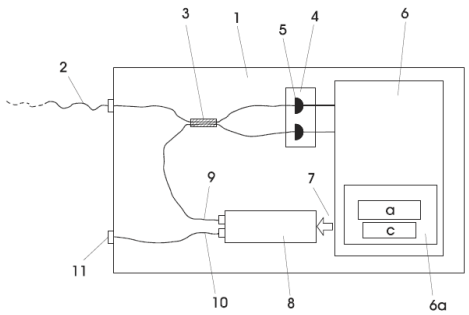

FIG. 1

ES 2 431 465 B1

DESCRIPCIÓN

Procedimiento y equipo de autenticación de contraseñas cuánticas

OBJETO DE LA INVENCIÓN

La presente invención se refiere a un procedimiento con el objeto de autenticar contraseñas codificadas en sistemas cuánticos sin poner en riesgo la privacidad de las mismas aún en el caso de haber participantes deshonestos.

El procedimiento se basa en la codificación de una contraseña en un sistema cuántico de una dimensión tal que no es posible recuperar ninguna parte de la contraseña pero que permite comparar en un equipo de usuario los estados recibidos con estados generados en el propio equipo para determinar si son iguales.

Además la invención se refiere a un equipo que implementa el procedimiento para efectuar la autenticación mediante la comparación señalada.

En general la invención es aplicable en el sector de las tecnologías de la información. En particular se trata de una aplicación de la física cuántica a los sistemas informáticos de seguridad y privacidad como son los sistemas de comercio electrónico, banca, acceso a recursos informáticos compartidos o los sistemas de identificación nacionales (como el documento nacional de identidad, DNI).

ANTECEDENTES DE LA INVENCIÓN

En sistemas complejos con un gran número de usuarios que no se conocen entre sí, es necesario disponer de mecanismos eficientes de identificación y autenticación de los usuarios y sus equipos.

Los usuarios pueden tener derecho a acceder a una parte de la información pero no al resto. Un ejemplo son las aplicaciones de banca por Internet. Cada usuario debe poder operar con su cuenta bancaria con la garantía de que ningún otro usuario pueda utilizarla.

En este contexto, es necesario probar que se conoce cierta información privada, como una contraseña, que posee únicamente el usuario legítimo. La comprobación de esta contraseña presenta problemas de seguridad: la privacidad de la contraseña se puede poner en peligro si hay usuarios deshonestos que se hagan pasar por el receptor de la información o si el canal está intervenido por espías que graben la información transmitida.

Para solucionar este tipo de problemas, se recurre a las pruebas de conocimiento cero o ZKP *(Zero-Knowledge Proofs*), mediante las que un usuario puede convencer a otro de que conoce cierta información sin necesidad de revelar ninguna parte de dicha información (S. Goldwasser, S. Micali y C. Rackoff, *The knowledge complexity of interactive proof systems,* SIAM Journal on Computing, 18:186, 1989). Un caso restringido de prueba de conocimiento cero son los protocolos de comprobación de contraseña de conocimiento cero o ZKPP (*Zero-Knowledge Password Proofs*), mediante los que dos usuarios que comparten una contraseña pueden asegurarse de que el otro usuario la conoce sin tener que hacerla pública (S. M. Bellovin y M. Merritt, *Encrypted key exchange: Password-based protocols secure against dictionary attacks,* IEEE Symposium on Security and Privacy, 72, 1992). Además, si uno de los participantes no conoce la contraseña, no puede obtener ninguna información sobre ella o, como mucho, una cantidad exponencialmente pequeña.

Los protocolos ZKPP existentes se basan en la complejidad computacional de ciertos problemas matemáticos como la factorización o el logaritmo discreto que aparecen en esquemas muy similares a los usados en sistemas de criptografía de clave pública como RSA (Rivest, Shamir, Adleman), descrito en el documento de Patente US 4.405.829. En los problemas escogidos hay un problema directo sencillo y un problema inverso difícil de resolver con los ordenadores actuales. Un ejemplo son los sistemas basados en la factorización, como el protocolo RSA, en los que el problema directo consiste en multiplicar dos números, mientras que el inverso consiste en hallar los factores primos de un número.

Un ejemplo concreto de protocolo ZKPP es el protocolo SPEKE (*Simple Password Exponential Key Exchange*) basado en la exponenciación modular (D. P. Jablon, *Strong password-only authenticated key exchange*, SIGCOMM Computer *Communication Review*, 26:5–26, 1996) o los protocolos del estándar P1363.2 del IEEE (*Institute of Electrical and Electronics Engineers*). Estos protocolos se emplean en distintos sistemas comerciales como, por ejemplo, los descritos en los documentos de Patente US 7.010.692, US 6.539.479 o US 324.508.

Aunque estos protocolos son capaces de garantizar cierto nivel de seguridad, se basan en la suposición no demostrada de que no existen métodos eficientes para resolver los problemas matemáticos elegidos. Los métodos basados en complejidad computacional, además, hacen suposiciones sobre la capacidad de cálculo de un posible atacante. No se tiene en cuenta que sistemas considerados seguros en el pasado pueden ser vulnerables ante los ordenadores del futuro. Una transmisión que se capture y almacene en el presente podría ser comprometida en el futuro si la capacidad de cálculo mejora.

Las leyes de la mecánica cuántica ofrecen una alternativa a la seguridad basada en la complejidad computacional. Un ejemplo son los sistemas de criptografía cuántica (C. H. Bennett y G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India, pág. 175, 1984), (A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Physical Review Letters, 67(6):661–663, 1991) en los que se aplican procedimientos de distribución cuántica de claves (*Quantum Key Distribution* o QKD). La distribución cuántica de claves basa su seguridad en las leyes de la física, que impiden copiar un estado cuántico desconocido (W.K. Wootters y W.H. Zurek, *A single quantum cannot be cloned*, Nature, 299(5886):802–803, 1982) o medirlo sin alterarlo. Al final de un proceso de distribución cuántica de claves, dos usuarios poseen una secuencia aleatoria de bits que ningún espía puede conocer. Cualquier intento de escuchar el canal puede detectarse y corregirse.

En este sentido pueden citarse documentos de patentes de criptografía cuántica con tecnología óptica, como por ejemplo EP 97940111.4, EP 93307120, EP 93307121, WO GB 93/0275, WO GB 93/02637, WO/2011/036322, PCT/ES2007/000323 o la Patente española con número de publicación 2168204.

Los sistemas de seguridad cuántica aportan dos ventajas fundamentales con respecto a los métodos basados en complejidad computacional. Por un lado, proporcionan una seguridad basada en las leyes de la física que no depende de ninguna hipótesis sobre la dificultad de ciertos problemas. Por otro lado, se trata de una seguridad independiente de la tecnología, ya que la seguridad proviene de limitaciones físicas independientes del dispositivo que use el atacante, lo que garantiza seguridad presente y futura contra ataques con cualquier tipo de recurso de cálculo, aunque mejore la tecnología.

Los documentos anteriores se limitan al campo del cifrado de la información, pero es deseable extender las ventajas de la seguridad cuántica a otros sistemas. La invención es una aplicación de la seguridad cuántica a los sistemas de comprobación de contraseña de conocimiento cero y consiste en un nuevo método de comprobación de contraseña y un equipo que lo implementa mediante tecnologías fotónicas.

DESCRIPCIÓN DE LA INVENCIÓN

Para conseguir los objetivos y resolver los inconvenientes anteriormente indicados, la invención incluye un nuevo procedimiento y equipo de autenticación de contraseñas cuánticas basados en la codificación de una contraseña **c** constituida por una secuencia de p bits en un estado cuántico de una dimensión demasiado pequeña como para poder recuperar el valor de la contraseña. El procedimiento comprende una fase previa en la que la contraseña **c** de p bits se almacena en los equipos de usuario que realizan la autenticación.

Además, se prevé el empleo de una secuencia aleatoria **a**, también de p bits, que comparten los usuarios y que permite evitar ciertos ataques al sistema y reforzar su seguridad.

El procedimiento de la invención se aplica en equipos de usuario compuestos por un módulo óptico y un módulo electrónico, ambos formados por elementos convencionales. El procedimiento consiste en una etapa de comparación de estados con cinco fases que se repite un número de veces n, siendo n un parámetro de seguridad que escogen los usuarios. Una característica fundamental del procedimiento es el reparto de funciones: un equipo de usuario que desea identificarse actúa como solicitante S y otro equipo de usuario actúa como verificador V. Al final de las n etapas del procedimiento, un equipo verificador que conoce la contraseña puede determinar que el solicitante la conoce y un verificador que no conoce la contraseña no puede deducirla a partir de los datos que le ha entregado el solicitante.

Cada una de la n etapas se divide en cinco fases:

- En la primera fase S y V utilizan sus equipos para generar y almacenar una secuencia aleatoria **a** compartida de p bits que ambos usuarios almacenan en las memorias de la parte electrónica de sus respectivos equipos de usuario. La secuencia compartida **a** puede hacerse pública.

- En la segunda fase los equipos S y V calculan la función lógica XOR bit a bit de la contraseña **c** y la secuencia compartida **a** para generar una nueva contraseña $\mathbf{c'}=\mathbf{c}\oplus\mathbf{a}$. Si ambos usuarios conocen la contraseña **c**, la secuencia de bits **c′** que generan los equipos S y V son idénticas.

- En la tercera fase los equipos S y V codifican la secuencia **c′** en el estado cuántico de un sistema con $D = 2^d$ estados posibles, escogiéndose en la realización preferente un valor de d menor a 0,71 veces el número de bits p de la contraseña. Para ese valor de $d<0{,}71\cdot p$ es imposible extraer del estado cuántico los bits de **c′** con una probabilidad mejor que la de adivinarlos azar (A. Ben-Aroya, O. Regev y R. de Wolf, *A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs*, Annual IEEE Symposium on *Foundations of Computer Science*, 477–486, 2008). En la realización preferente **c′** se codificará en estados simétricos que son una superposición de estados base $|i\rangle$ de la forma

$$\left|\Psi^{c'}\right\rangle = \frac{1}{\sqrt{D}}\sum_{i=0}^{D-1} e^{j\frac{2\pi i C'}{2^p}}\left|i\right\rangle,$$

donde C' es el valor decimal de la secuencia de bits **c'**. Según la codificación elegida, los estados base $\left|i\right\rangle$ pueden escogerse entre estados $\left|T_i\right\rangle$ con fotones localizados en la ventana de tiempo T_i o estados $\left|\ell\right\rangle$ con momento orbital angular $\ell\hbar$. Si tanto S como V conocen la contraseña, generan el mismo estado $\left|\Psi^{c'}\right\rangle$.

- En la cuarta fase el equipo solicitante entrega su copia del estado al equipo verificador. En el equipo verificador se compara el estado que V generó en la fase anterior con el estado que le ha entregado el equipo solicitante. Para ello utiliza el comparador óptico de su equipo de usuario.

- En la quinta fase el equipo verificador comprueba el resultado del comparador. Si el resultado es positivo, se sigue con el procedimiento hasta alcanzar las n repeticiones. Si en algún momento la comparación resulta negativa, se aborta el procedimiento de autenticación y se deduce que el solicitante no conoce la contraseña. La secuencia aleatoria **a** que se genera en la primera fase debe ser diferente en cada repetición de la comprobación. El número n de repeticiones se establece previamente y es función de la seguridad que se desee obtener en la autenticación. Cuanto mayor sea n, mayor seguridad de autenticación se obtendrá.

Mediante el procedimiento y el equipo de la invención, aunque las leyes de la física impiden leer la información, sí es posible comparar dos estados en un único intento que detecta estados diferentes con una buena probabilidad. De este modo se permite detectar usuarios ilegítimos que se hagan pasar por el receptor de la información y se gana seguridad frente a espías que escuchen el canal de comunicación.

En la realización preferente de la invención se prevé que ambos usuarios necesitan probar su identidad. En este caso, las n repeticiones de las fases primera a quinta de la etapa de comparación no se harán seguidas sino que se alternarán etapas en las que las funciones del equipo solicitante y verificador se intercambia entre los usuarios y sus equipos. De este modo se puede detectar prematuramente a un usuario ilegítimo.

En la realización preferente de la invención, la secuencia aleatoria **a** compartida se establece a través de un canal público. La invención incluye un procedimiento para que los usuarios generen de forma conjunta la secuencia aleatoria **a** mediante sus equipos de usuario del solicitante y verificador y que será explicado posteriormente.

La seguridad del procedimiento se basa en la elección de los parámetros p, n y d. La invención prevé que, tal y como se ha señalado, d sea menor que 0,71·p, de forma que la probabilidad de recuperar k de los p bits de la contraseña tiende a 2^{-k}. Esta probabilidad es la misma que la de adivinar los bits de la contraseña al azar. Por lo tanto, con la codificación elegida, un espía que capture el estado cuántico es incapaz de extraer un solo bit de información. Además, la operación XOR con la secuencia aleatoria **a** evita un ataque de repetición en el que el adversario intercepta estados de un usuario legítimo y los utiliza luego para hacerse pasar por él, ya que los estados cuánticos que se usan en cada etapa son diferentes.

Además, para que el procedimiento de la invención resulte más seguro, se prevé que el valor máximo de etapas n se escoge de forma que n·d < 0,71·p. Con esta elección, un espía que capturase todos los estados sin ser detectado tampoco podría averiguar la contraseña, ya que el espacio de n estados de dimensión $D = 2^d$ tiene dimensión $2^{n\cdot d}$. Mientras n·d sea menor que 0,71·p ningún proceso de codificación y decodificación permite recuperar k bits más que con una probabilidad de 2^{-k}.

La parte fundamental del procedimiento es la codificación de la secuencia **c'** en un estado cuántico. En el equipo de usuario de la invención, la codificación se realiza sobre el estado cuántico de un único fotón. La codificación de **c'** se puede realizar o bien mediante una codificación temporal que module la forma de onda de un único fotón generando diferentes desfases en ventanas de tiempo predefinidas (H.P. Specht, J. Bochmann, M. Mücke, B. Weber, E. Figueroa, D.L. Moehring y G. Rempe, *Phase shaping of single-photon wave packets*, Nature Photonics, 3(8):469–472, 2009), o bien mediante una codificación en el momento orbital angular de un único fotón (G. Molina-Terriza, J. P. Torres y L. Torner, *Management of the angular momentum of light: Preparation of photons in multidimensional vector states of angular momentum*, Physical Review Letters, 88(1):013601, Dec 2001). En la descripción de la implementación preferida se detallan estos dos métodos de codificación.

La invención se refiere también al equipo de usuario que implementa el procedimiento descrito. El equipo, tal y como fue señalado, incluye dos partes: un módulo electrónico y un módulo óptico. El módulo electrónico está formado por una memoria y un procesador. La memoria almacena las secuencias con la contraseña **c** y la secuencia aleatoria **a**. El procesador se encarga de dirigir el procedimiento de autenticación. Sus tareas incluyen el análisis de los datos que llegan desde los detectores conectados al comparador para decidir si se prosigue el procedimiento o no y calcular la función lógica XOR bit a bit de **c** y **a** para generar la cadena **c'** que determina una señal de control

que se aplica a un generador de estados cuánticos del módulo óptico. El módulo óptico comprende un comparador de estados cuánticos, un generador de estados cuánticos y un bloque detector situado a la salida del comparador que se conectan al módulo electrónico. El bloque detector comprende al menos dos elementos de detección.

El comparador de estados cuánticos es un dispositivo óptico con dos entradas y dos salidas. Las entradas incluyen una conexión al exterior por la que llega el fotón del equipo solicitante con el estado que codifica su secuencia **c'** y una conexión interna al generador de estados cuánticos. Cada puerto de salida del comparador está conectado a un elemento detector, que, a su vez, está conectado al procesador. Si los estados son iguales se deduce que las secuencias coinciden. El comparador funciona de manera probabilista. Dos estados diferentes pueden clasificarse como iguales, pero siempre con una probabilidad menor que uno. Dos estados iguales siempre superan la comprobación. Siguiendo el procedimiento de la invención, se puede emplear esta comparación parcial para ofrecer un sistema de comprobación tan fiable como se desee.

De acuerdo con el procedimiento descrito, se prevé que el comparador pueda estar constituido por un divisor de haz o por un acoplador de fibra óptica. En cualquiera de los dos casos, dichos comparadores se encuentran configurados para producir una interferencia óptica entre los caminos de los dos fotones aplicados en su entrada. La comparación se realiza mediante el efecto Hong-Ou-Mandel (C. K. Hong, Z. Y. Ou y L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference*, Physical Review Letters, 59(18):2044–2046, Nov 1987) de forma que, si los dos estados son iguales, la interferencia entre caminos hace que los dos fotones tomen la misma salida. Si los fotones a la entrada del comparador tienen estados distintos, es posible encontrar los fotones en distintas salidas.

Los detectores del equipo de usuario son detectores de fotones individuales que pueden ser, por ejemplo, fotodiodos de avalancha (APD) convencionales. Los detectores se colocan en los dos puertos de salida del comparador. Esta configuración de los detectores indica al procesador si los caminos de salida de los dos fotones coinciden o no. El procesador está configurado para parar la autenticación cuando los puertos de salida son distintos y para generar un nuevo estado $\left|\psi^{c'}\right\rangle$ cuando los dos fotones activan el mismo detector, repitiendo la etapa de comparación con nuevos estados $\left|\psi^{c'}\right\rangle$ hasta un número de veces n, según fue comentado anteriormente.

El generador de estados cuánticos comprende un bloque de control, un láser, un modulador, un atenuador y un conmutador. El bloque de control recibe la señal de control generada por el procesador y dirige la acción del modulador y del conmutador. El láser genera estados de baja intensidad que pasan al modulador. El modulador está gobernado por el bloque de control y se encarga de codificar la secuencia **c'** en los estados generados por el láser. La invención prevé que el modulador pueda ser un modulador óptico que actúe sobre la fase o un modulador con momento orbital angular, de acuerdo con lo descrito para el procedimiento. Tras el modulador se encuentra un atenuador con un factor de atenuación escogido para que a su salida el número medio de fotones sea menor o igual que uno. De este modo, el estado de salida tendrá un fotón o menos. Al final del generador se incluye un conmutador. El conmutador dirige el fotón hacia dos posibles salidas en función de la señal de control. La elección de la salida del conmutador permite usar el mismo equipo para el usuario que actúa como solicitante y el usuario que actúa como verificador. Una de las salidas previstas lleva el estado cuántico que codifica **c'** al comparador. En este caso el equipo funciona como verificador. El estado generado localmente se compara con el estado procedente del solicitante. La segunda salida está conectada al exterior de modo que puede entregarse el estado que codifica **c'** a un equipo de usuario verificador externo en el que se realizaría la comparación descrita en el procedimiento.

En la realización preferente de la invención el modulador óptico para la codificación temporal es un modulador de fibra óptica configurado para introducir desfases diferentes en períodos de tiempo predefinidos. El modulador con momento orbital angular comprende un bloque de generación de estados con un holograma y un prisma de Dove. El holograma puede generarse con técnicas fotográficas convencionales de modo que genere un estado inicial $\left|\Phi_0\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1}\left|\ell\right\rangle$, que es una superposición de estados $\left|\ell\right\rangle$ con un momento orbital angular $\ell\hbar$. El estado que sale del holograma se dirige a un prisma de Dove convencional rotado un ángulo $\alpha = \frac{2\pi C'}{2^p}$. La rotación está controlada por el bloque de control para generar un estado simétrico

$\left|\Psi^{c'}\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1} e^{j\frac{2\pi\ell C'}{2^p}}\left|\ell\right\rangle$, según fue descrito.

En el procedimiento de la invención, se indicó que la secuencia aleatoria **a** podía generarse en el propio equipo de usuario. En ese caso, la secuencia aleatoria se genera mediante el generador de estados, el comparador, el detector y el procesador, de forma convencional, como se describe en mayor detalle en el ejemplo de realización de la invención.

De acuerdo con la descripción realizada, cabe la posibilidad de sufrir un ataque en el que el atacante no introduzca ningún fotón. Aunque el atacante no puede descubrir la contraseña **c**, al haber sólo un fotón en una de las salidas del comparador se activa un único detector y el verificador puede llegar a interpretar que el atacante conoce la contraseña **c**.

Para evitar este inconveniente la invención incluye un bloque que realiza la cuenta de fotones presentes. De este modo se puede detectar cuándo ha ocurrido un ataque por ausencia de fotones. Para ello se utiliza una pluralidad de etapas con comparadores, cuya última etapa está conectada a una pluralidad de elementos detectores. El número de comparadores se duplica en cada etapa. Cada una de las salidas del primer comparador se conecta a un comparador, cuyas salidas a su vez se conectan a otros dos comparadores y así sucesivamente hasta la última etapa de comparadores, que tienen un detector en cada una de sus salidas. El número de elementos de detección es el doble del número de comparadores de la última etapa. Para realizar la cuenta sin errores, la entrada libre de los comparadores adicionales se encuentra bloqueada. El procesador está configurado para parar la autenticación al detectar una suma de fotones diferente de dos o cero en una sola rama, entendiéndose por rama cada una de las dos salidas del primer comparador y las diferentes ramificaciones que comporta cada una de las etapas. En caso de que el procesador detecte una suma de fotones correcta realiza la autenticación. De este modo se evita un ataque por falta de fotones. Si el equipo solicitante no envía ningún fotón, la suma de fotones en todas las ramas será uno en vez de dos.

A continuación, para facilitar una mejor comprensión de esta memoria descriptiva, y formando parte integrante de la misma, se acompaña una serie de figuras en las que con carácter ilustrativo y no limitativo se ha representado el objeto de la invención.

BREVE ENUNCIADO DE LAS FIGURAS

Figura 1.- Muestra un diagrama de bloques funcional de un posible ejemplo de realización de un equipo de usuario para realizar la comprobación de contraseña de acuerdo con la invención.

Figura 2.- Muestra un posible ejemplo de realización del generador de estados cuánticos de la figura anterior en el que se emplea un modulador óptico para fibra óptica.

Figura 3.- Muestra otro posible ejemplo de realización del modulador de la invención de la figura 1. En este caso el modulador es un modulador con momento orbital angular.

Figura 4.- Muestra una representación esquemática de una realización de la invención en la que se incorporan una pluralidad de comparadores y detectores para evitar un ataque por falta de fotones. No se ha representado ni la memoria del procesador ni el generador de fotones para simplificar la figura.

DESCRIPCIÓN DE LA FORMA DE REALIZACIÓN PREFERIDA

A continuación se realiza una descripción de la invención basada en las figuras anteriormente comentadas.

El procedimiento de la invención se describe suponiendo dos usuarios con sus correspondientes equipos 1, un usuario solicitante con su equipo solicitante S y un usuario verificador con su equipo verificador V. Se parte de una fase previa en la que los equipos de usuario 1 almacenan la contraseña **c** constituida por una secuencia de p bits que se desea comprobar en una memoria 6a de un procesador 6 de los respectivos equipos de usuario 1, según se muestra en la figura 1.

Se detalla el procedimiento de la invención para el caso en el que el equipo solicitante S se identifica ante el equipo verificador V. El equipo solicitante S es quien debe demostrar que tiene la misma secuencia de bits **c** que el equipo verificador V. Todas las fases son iguales para el caso contrario intercambiando las funciones de S y V. Si ambos usuarios deben convencer al otro de que poseen la contraseña, es preferible establecer turnos con rondas de identificación intercaladas para detectar de forma temprana a un posible usuario deshonesto. El procedimiento consiste en la repetición de cinco fases:

- En la primera fase, S y V generan conjuntamente una secuencia aleatoria **a** de p bits, tal y como será descrito con posterioridad, de forma que ambos la almacenan en sus respectivas memorias 6a. En el ejemplo de realización la secuencia **a** es una secuencia pública.

- A continuación, en la segunda fase, S y V calculan la función lógica XOR bit a bit de la contraseña **c** y de la secuencia aleatoria **a** generando una clave nueva **c′ = c** $\oplus$ **a**.

- En la tercera fase, S y V codifican **c′** en los estados $\left|\Psi_S^{c'}\right\rangle$ y $\left|\Psi_V^{c'}\right\rangle$ de un sistema cuántico con $D = 2^d$ estados. En la implementación preferente estos estados se corresponden con estados de fotones individuales. Si los dos equipos conocen la contraseña, generan estados idénticos $\left|\Psi^{c'}\right\rangle$. Se debe escoger un d mucho menor que p para proteger la contraseña. Una posible codificación es la que asigna cada secuencia de la clave **c′** a un estado

simétrico de la forma $\left|\Psi^{c'}\right\rangle = \frac{1}{\sqrt{D}}\sum_{i=0}^{D-1} e^{j\frac{2\pi i C'}{2^p}}\left|i\right\rangle$, donde C' es el número que tiene como representación binaria la secuencia de la clave **c**'.

- En la cuarta fase, el equipo de usuario solicitante S entrega su estado al equipo verificador V.

- En la quinta fase el equipo V realiza una comparación entre el estado recibido y el estado generado localmente en la tercera fase, mediante un comparador cuántico 3. De esta forma, si el resultado de la comparación es positivo, se continúa el procedimiento de autenticación y, si es negativo, se aborta y se considera que S no posee la contraseña **c**.

El procedimiento de comprobación, con todas las fases mencionadas, se repite n veces escogiendo una nueva secuencia aleatoria **a**. El valor de n se estima en función de la seguridad deseada.

Este procedimiento se implementa mediante equipos de usuario 1 con una entrada 2 por la que llegan los estados del solicitante S hasta un comparador de estados cuánticos 3 donde interfiere con el estado local procedente de un generador de estados cuánticos 8. El comparador de estados 3 está conectado a un bloque de detección 4 con dos detectores 5 que indican al procesador 6 si los caminos de salida de los fotones coinciden o no. El procesador 6 contiene la memoria 6a que almacena las secuencias **a** y **c** y, a partir de ellas, es capaz de calcular la secuencia **c**' descrita en el procedimiento. Tomando como referencia esa secuencia **c'**, el procesador 6 genera una señal de control 7 que dirige el funcionamiento del generador de estados cuánticos 8. El generador de estados cuánticos 8 tiene dos salidas, 9 y 10. La salida 9 se conecta con el comparador 3 y la salida 10 se conecta con el exterior 11, que es la salida del equipo de usuario 1 para los escenarios en los que el usuario y su equipo actúan como solicitante y entrega sus estados al equipo de usuario verificador.

El generador de estados cuánticos 8 codifica la secuencia **c'** en fotones individuales de acuerdo con distintas codificaciones con los esquemas que se muestran en las figuras 2 y 3. Así en la figura 2 se muestra una configuración del generador de estados cuánticos 8 en la que la modulación se basa en la modificación de la forma de onda de un fotón en distintos instantes (codificación temporal). En el ejemplo de la figura 3 el generador de estados cuánticos 8 se basa en una codificación en el momento orbital angular de un único fotón. Estos generadores serán descritos en mayor detalle más adelante.

La comparación entre los estados se produce en el comparador 3 que tiene como entradas el estado $\left|\Psi_V^{c'}\right\rangle$, generado localmente en el bloque de generación de estados 8, y el estado $\left|\Psi_S^{c'}\right\rangle$ que se recibe de un solicitante en el exterior y que entra en el equipo de usuario 1 a través de la entrada 2. El bloque detector 4 está constituido por dos fotodiodos de avalancha APD 5, ambos conectados al procesador 6. El procesador 6, en función de si los dos detectores 5 se activan a la vez o no, decide si debe parar el procedimiento o seguir con él. El estado local $\left|\Psi_V^{c'}\right\rangle$ se genera según los contenidos **a** y **c** de la memoria 6a.

El funcionamiento del comparador 3 se basa en el efecto Hong-Ou-Mandel, que ocurre cuando los caminos de dos fotones interfieren en un dispositivo óptico, como por ejemplo puede ser un divisor de haz o un acoplador de fibra. Sólo dos fotones que tengan el mismo estado presentan la máxima interferencia. En la figura 1 se muestra un ejemplo en el que la comparación se realiza mediante un comparador de fibra óptica en el que la interferencia entre fotones tiene lugar en un acoplador de fibra óptica. En la codificación con momento orbital angular la interferencia ocurre en un divisor de haz (*beamsplitter*) con una transmitividad del 50%.

La probabilidad de que los dos fotones de entrada salgan por el mismo puerto de salida es del 100% para estados idénticos. Para un número grande de estados cuánticos posibles, la probabilidad de que los fotones de dos estados escogidos al azar salgan por puertos diferentes es del 50%. Los diodos de avalancha 5 de detección de fotones distinguen estos dos casos al encontrarse colocados en las salidas del comparador 3. El procesador 6 interpreta los datos y está configurado para dirigir el procedimiento de autenticación. Si los dos detectores 5 encuentran un fotón, los estados son diferentes y el procesador 6 acaba con el proceso de comprobación. Por el contrario, si sólo se activa uno de los detectores 5, se continúa la comprobación usando un nuevo valor de secuencia aleatoria **a**. Tras n comprobaciones, la probabilidad de que el equipo S no tenga la contraseña es exponencialmente pequeña, del orden de 2^{-n}.

Tal y como se ha comentado, para el generador de estados cuánticos 8 se sugieren dos posibles realizaciones en las figuras 2 y 3.

En el ejemplo de realización de la figura 2, el generador de estados cuánticos 8 comprende un bloque de control 12 en el que se recibe la secuencia de control 7 procedente del procesador 6 para gobernar el funcionamiento de un modulador óptico 14. El modulador óptico 14 es un modulador de fibra óptica que introduce desfases diferentes en ventanas de tiempo predefinidas y actúa sobre la señal de un láser 13 que genera una señal

óptica de baja potencia que tras la modulación lleva la información de la secuencia **c**'. Tras el modulador óptico 14, el estado codificado pasa por un atenuador 15 ajustado para que el estado a la salida del generador de estados cuánticos 8 tenga, en promedio, un fotón o menos. Mediante un conmutador 16 se dirige el fotón con el estado final hacia la salida 9 o 10 en función de la información de control 7. Se toma la salida 9 cuando el comparador 3 se utiliza para comprobar contraseñas de un usuario externo. Se escoge la salida 10 cuando el usuario local genera fotones para que un usuario externo los compruebe.

En la figura 3 se muestra otro posible ejemplo de realización del generador de estados 8 que presenta una configuración similar a la de la figura 2, pero, en este caso, con un modulador con momento orbital 14a que codifica la información en el momento orbital angular de un fotón. El modulador 14a está constituido por dos etapas. En la primera etapa se crea una superposición uniforme $\left|\Phi_0\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1}\left|\ell\right\rangle$ de estados base $\left|\ell\right\rangle$ con un momento orbital angular $\ell\hbar$. En este sentido cabe señalar que existen diferentes técnicas para generar estos estados de forma convencional (G. Molina-Terriza, J. P. Torres y L. Torner, *Management of the angular momentum of light: Preparation of photons in multidimensional vector states of angular momentum*, Physical Review Letters, 88(1):013601, Dec 2001), (S. Slussarenko, E. Karimi, B. Piccirillo, L. Marrucci y E. Santamato, *Efficient generation and control of different-order orbital angular momentum states for communication links*, Journal of the Optical Society of America A, 28(1):61–65, Jan 2011). En la figura 3 se propone un ejemplo en el que se emplea un bloque de generación de estados con un holograma 17 que puede generarse con técnicas fotográficas convencionales. En la segunda parte de la modulación, se dirige la superposición de estados a un prisma de Dove convencional 18 rotado un ángulo $\alpha = \frac{2\pi C'}{2^p}$. El ángulo de rotación se ajusta en función de las indicaciones de la señal de control 7 generada por el procesador 6. Tras el prisma de Dove 18 y el atenuador 15, se genera el estado simétrico de un fotón $\left|\Psi^{c'}\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1} e^{j\frac{2\pi\ell C'}{2^p}}\left|\ell\right\rangle$.

Tal y como se ha comentado, la invención prevé que los equipos de usuario 1 generen de forma conjunta una secuencia aleatoria **a** nueva para cada una de las diferentes comparaciones a realizar. La secuencia **a** debe ser diferente en cada comprobación para evitar un ataque de repetición en el que un usuario deshonesto que no conoce la contraseña captura y almacena un estado válido de un usuario que sí conoce la contraseña y lo utiliza posteriormente para hacerse pasar por él. Para establecer la secuencia común **a**, los usuarios generan por turnos 1 bit de la secuencia **a** y lo comunican al otro participante. Basta con que uno de los usuarios sea honesto para que la secuencia **a** no se repita en diferentes rondas y, por lo tanto, no pueda usarse un ataque de repetición. S y V pueden usar distintos generadores de números aleatorios. El equipo de usuario 1 está configurado para generar los números aleatorios cuánticos según se conoce en el estado de la técnica. La generación de números aleatorios cuánticos se basa en el carácter intrínsecamente probabilístico de la medida cuántica y se puede implementar con equipos ópticos como por ejemplo se describe en los documentos de Patente US6249009, WO 2007124089, JP 2033-36188 A, EP 2013706B1 y US 6393448.

Así, con el equipo representado en la figura 1, cada usuario puede generar un fotón localmente con el generador de estados 8 y cerrar la entrada 2 de forma que la probabilidad de detectar el fotón en cada uno de los detectores 5 es del 50%. Por cada fotón generado se produce un bit aleatorio en función del detector 5 que se active, de forma que el procesador 6 asigna un 0 si se activa el detector superior y un 1 si se activa el inferior.

La configuración básica descrita de la invención es vulnerable a un ataque en el que el usuario de un equipo S no introduce ningún fotón. Aunque no puede descubrir la contraseña **c**, al haber sólo un fotón nunca se activarán los dos detectores 5 y V puede llegar a creer que S conoce la contraseña **c**. Si los detectores 5 pueden contar el número de fotones presentes, este ataque puede ser detectado. Para evitar el ataque, la invención prevé el uso de una pluralidad de etapas de comparadores 3 y una pluralidad de detectores 5 de forma que el número de salidas se multiplica por 2 con cada etapa de 3, según se representa en la figura 4. Cada salida del comparador 3 se conecta a un comparador adicional. Los nuevos comparadores, a su vez, tienen sus salidas conectadas a una nueva etapa de comparadores. Esta ramificación de las salidas puede repetirse varias veces. Todos los comparadores adicionales tienen una de sus entradas bloqueada, de modo que sólo reciben los fotones que provienen del primer comparador 3. La probabilidad de que dos fotones acaben en el mismo puerto de salida puede hacerse tan pequeña como se desee añadiendo varias etapas de comparadores 3. Si se coloca un detector a cada salida de los comparadores 3 de la última etapa, se puede estimar cuántos fotones han salido por las ramas superior e inferior del primer comparador 3. El procesador 6 analiza los resultados y, si la suma de fotones detectados en cada una de las dos ramas del primer comparador 3 es 2 o 0, continúa con el procedimiento de autenticación. Si los detectores 5 correspondientes a una de las dos ramas encuentran un número de fotones distinto de 2 o 0, se considera que el usuario S no conoce la contraseña y se aborta el procedimiento. Este requisito se puede relajar si hay una probabilidad alta de que durante la medida se pierda algún fotón ya sea por pérdidas en el sistema o porque se generan estados coherentes con mucho menos de un fotón en promedio. Esta configuración capaz de estimar el número de fotones permite, por lo tanto, evitar un ataque por ausencia de fotones.

REIVINDICACIONES

1.- PROCEDIMIENTO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS que comprende:

- una fase previa de almacenamiento de una contraseña **c** constituida por una secuencia de p bits en unos equipos de usuario donde se lleva a cabo el procedimiento de autenticación;

caracterizado por que además comprende etapas repetidas de comparación con las siguientes fases:

- una primera fase de generación y almacenamiento en los equipos de usuario de una secuencia aleatoria **a** de p bits compartida;

- una segunda fase en la que cada equipo de usuario calcula la función lógica XOR bit a bit correspondiente a la contraseña **c** y a la secuencia aleatoria **a** y genera una nueva secuencia **c′**=**c** $\oplus$ **a**;

- una tercera fase en la que cada equipo de usuario codifica **c′** en estados cuánticos $\left|\Psi^{c'}\right\rangle$ de un espacio de dimensión $D = 2^d$, donde d es menor que 0,71·p;

- una cuarta fase en la que un equipo de un usuario solicitante que desea identificarse entrega el estado cuántico que codifica la contraseña **c**' a un equipo de usuario verificador que debe autenticar la contraseña;

- una quinta fase en la que el equipo de usuario verificador que debe autenticar la contraseña compara el estado cuántico recibido con el generado en la tercera fase por dicho equipo de usuario verificador y, si no coinciden los estados cuánticos comparados, se aborta el proceso de autenticación y, si coinciden dichos estados cuánticos comparados, se continúa dicho proceso de autenticación;

- en caso de continuar el proceso de autenticación se repiten las fases primera a quinta anteriores un número preestablecido de veces n con una nueva secuencia aleatoria **a** considerando que la contraseña es válida si las n comparaciones son positivas.

2.- PROCEDIMIENTO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 1, caracterizado por que los equipos de usuario que actúan como solicitante y verificador cambian sus funciones en cada una de las n repeticiones de las fases primera a quinta, para que ambos usuarios puedan confirmar que el otro usuario conoce la contraseña.

3.- PROCEDIMIENTO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 1, caracterizado por que la secuencia aleatoria **a** compartida es pública.

4.- PROCEDIMIENTO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 1, caracterizado por que n·d es menor que 0,71·p.

5.- PROCEDIMIENTO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 1, caracterizado por que la codificación de **c**' en un estado cuántico está seleccionada entre una codificación temporal de la forma de onda de un único fotón mediante la generación de diferentes desfases en ventanas de tiempo predefinidas y una codificación en el momento orbital angular de un único fotón mediante la creación de una superposición uniforme de estados $\left|\Phi_0\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1}\left|\ell\right\rangle$ y la posterior generación de un estado simétrico $\left|\Psi^{c'}\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1} e^{j\frac{2\pi\ell C'}{2^p}}\left|\ell\right\rangle$, donde C' es el valor decimal de la secuencia de bits **c′** y $\left|\ell\right\rangle$ los estados base de fotones con momento orbital angular $\ell\hbar$.

6.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS de acuerdo con el procedimiento de las reivindicaciones 1 a 6, que comprende medios de almacenamiento de una contraseña **c** constituida por una secuencia de p bits y de al menos una secuencia aleatoria **a** de p bits que comparten los equipos a autenticar, caracterizado por que comprende:

- un procesador (6) configurado para calcular la función lógica XOR bit a bit de la contraseña **c** y la secuencia aleatoria **a** y generar una señal de control (7) correspondiente al cálculo **c′**=**c** $\oplus$ **a** realizado que se aplica a

- un generador de estados cuánticos (8) que codifica la secuencia **c′** en el estado cuántico de un fotón, que se dirige a

- un comparador de estados cuánticos (3) que compara un estado procedente de un equipo de usuario solicitante que desea identificarse y el estado que codifica **c′** y que proviene del generador de estados

cuánticos (8) del propio equipo de usuario verificador que debe autenticar la contraseña,

- un bloque detector (4) configurado para indicar cuándo los dos fotones de entrada al comparador (3) salen por el mismo puerto de salida de dicho comparador (3) y cuándo salen por puertos distintos, y

- estando el procesador (6), además, configurado para parar la autenticación cuando los puertos de salida del comparador (3) por los que salen los dos fotones son distintos y para generar un nuevo estado **c**' cuando los dos fotones salen por el mismo puerto, generando dichos nuevos estados **c**' hasta un número de veces n, previamente establecido, para realizar la autenticación.

7.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 7, caracterizado por que el comparador (3) está seleccionado entre un divisor de haz y un acoplador de fibra óptica configurados para producir una interferencia óptica entre los caminos de dos fotones aplicados en sus entradas y realizar la comparación de acuerdo con el efecto Hong-Ou-Mandel, donde cuando los estados son iguales los dos fotones salen por el mismo puerto de salida del comparador (3) con una probabilidad del 100% y donde cuando los estados son diferentes la probabilidad de que dos fotones salgan por el mismo puerto de salida son cercanas al 50%.

8.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 7, caracterizado por que el bloque detector (4) comprende elementos detectores (5) de fotones individuales conectados a cada uno de los puertos de salida del comparador (3) que se activan al detectar un fotón para indicar al procesador (6) cuándo se detectan fotones simultáneamente en ambos puertos de salida del comparador (3) y cuándo se detectan en uno solo de los puertos de salida del comparador (3).

9.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 7, caracterizado por que el generador de estados cuánticos (8) comprende:

- un bloque de control (12) que recibe la señal de control (7) del procesador (6),
- un láser (13) de baja potencia conectado a
- un modulador seleccionado entre un modulador óptico (14) y un modulador con momento orbital angular (14a),
- un atenuador (15) que presenta a su salida estados cuánticos con un número medio de fotones menor o igual que uno,
- un conmutador (16) configurado para dirigir el fotón hacia una salida seleccionada entre una primera salida (9) y una segunda salida (10) en función de la señal de control (7), seleccionando la primera salida (9) cuando el equipo de usuario funciona como verificador y el estado generado debe aplicarse al comparador (3) para compararlo con el estado proporcionado por un equipo de usuario solicitante y seleccionando la segunda salida (10) cuando el equipo de usuario funciona como solicitante y el estado generado debe entregarse a un equipo de usuario verificador.

10.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 10, caracterizado por que el modulador óptico (14) es un modulador de fibra óptica configurado para introducir desfases diferentes en períodos de tiempo predefinidos.

11.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 10, caracterizado por que el modulador con momento orbital angular (14a) comprende un bloque de generación de estados con un holograma (17) para generar estados iniciales $\left|\Phi_0\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1}\left|\ell\right\rangle$ y un prisma de Dove (18) rotado un ángulo $\alpha = \frac{2\pi C'}{2^p}$ gobernado por el bloque de control (12) para generar el estado simétrico $\left|\Psi^{c'}\right\rangle = \frac{1}{\sqrt{D}}\sum_{\ell=0}^{D-1} e^{j\frac{2\pi\ell C'}{2^p}}\left|\ell\right\rangle$.

12.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 7, caracterizado por que la secuencia aleatoria **a** se genera mediante el generador de estados cuánticos (8), el comparador (3), el bloque detector (4) y el procesador (6) de forma convencional.

13.- EQUIPO DE AUTENTICACIÓN DE CONTRASEÑAS CUÁNTICAS, según reivindicación 9, caracterizado por que comprende una pluralidad de etapas de comparadores (3), donde la última etapa está conectada a un bloque de detección (4) dotado de una pluralidad de elementos detectores (5), estando las etapas de comparadores (3) configuradas en etapas sucesivas en las que cada una de las salidas de la etapa anterior se conecta a un nuevo comparador (3) con su segunda entrada bloqueada, duplicando el número de salidas de cada etapa de comparadores (3); donde el número de elementos de detección (5) es el doble del número de comparadores (3) de la última etapa para que, al llegar los fotones a los detectores (5), indiquen al procesador (6) el número de fotones que ha salido por cada uno de los puertos de salida del primer comparador (3), estando el procesador (6)

configurado para parar el procedimiento de autenticación al detectar un número de fotones en alguno de los puertos de salida del primer comparador (3) distinto de cero o dos.

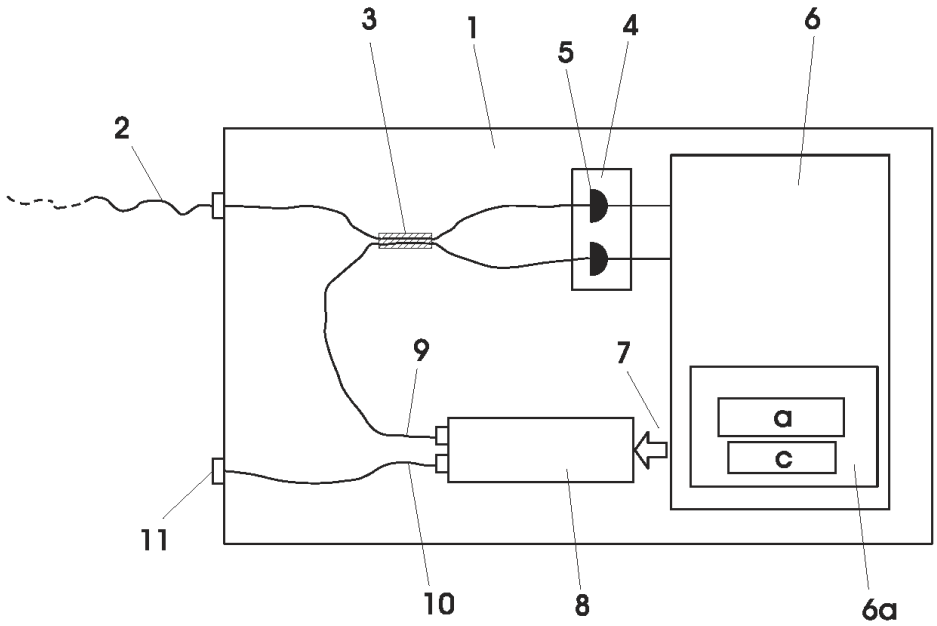

FIG. 1

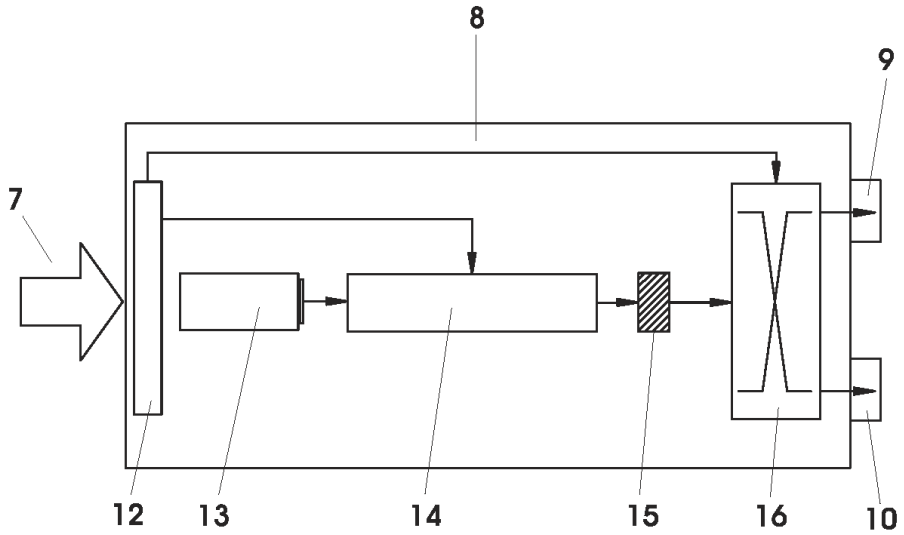

FIG. 2

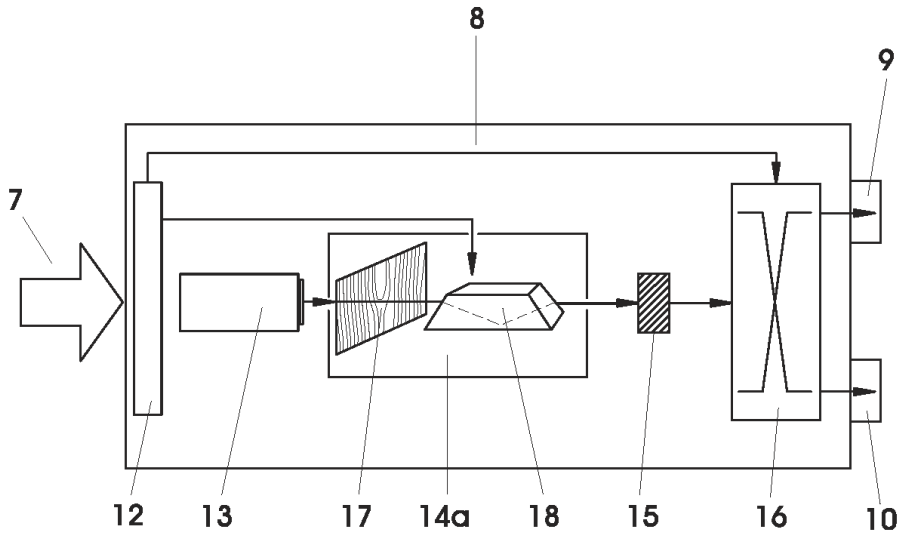

FIG. 3

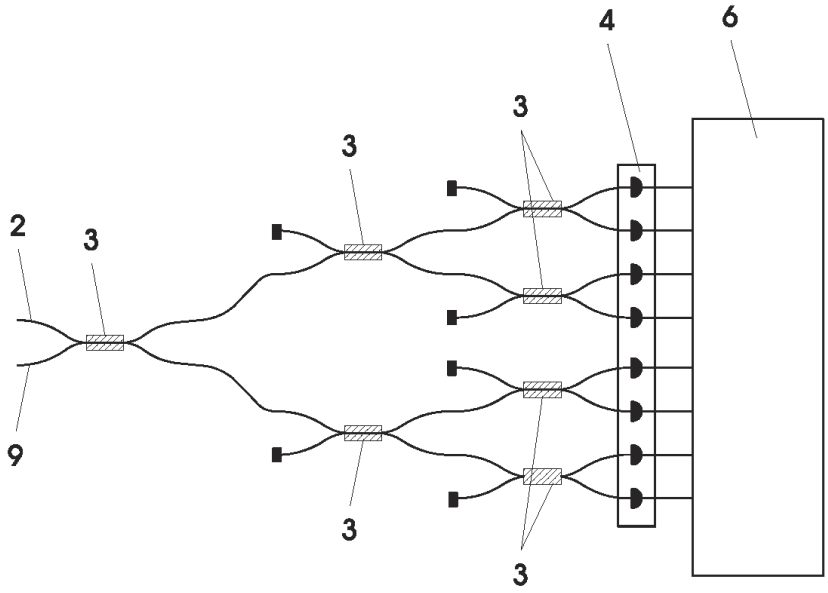

FIG. 4