(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 168 204**

(21) Número de solicitud: 200000713

(51) Int. Cl.[7]: H04B 10/00

H04L 9/08

(12) PATENTE DE INVENCION B1

(22) Fecha de presentación: **21.03.2000**

(43) Fecha de publicación de la solicitud: **01.06.2002**

Fecha de concesión: **01.10.2003**

(45) Fecha de anuncio de la concesión: **01.11.2003**

(45) Fecha de publicación del folleto de patente: **01.11.2003**

(73) Titular/es: **Universidad de Sevilla**
Valparaiso, 5, 2
41013 Sevilla, ES

(72) Inventor/es: **Cabello Quintero, Adán**

(74) Agente: **No consta**

(54) Título: **Procedimiento cuántico para distribuir claves criptográficas sin descartar datos.**

(57) Resumen:
Procedimiento cuántico para distribuir claves criptográficas sin descartar datos.
El invento es un procedimiento para distribuir claves criptográficas entre dos usuarios distantes que usan una propiedad de la mecánica cuántica. La novedad de la invención reside en que el número de datos útiles para generar la clave, por cada dato transmitido, es mayor que en cualquier otro procedimiento cuántico de distribución de claves criptográficas previo. El invento se basa en la creación de "enredo" a distancia. El invento simplifica el proceso de comprobación de que la clave no ha sido espiada. En todos los procedimientos cuánticos previos, cualquier intento de espionaje se traduce inevitablemente en que las claves que reciben ambos usuarios dejan de ser iguales. Con la presente invención la acción del espía altera el 75 % de la clave, lo que facilita su detección.

ES 2 168 204 B1

DESCRIPCION

Procedimiento cuántico para distribuir claves criptográficas sin descartar datos.

El invento es un procedimiento para distribuir claves criptográficas entre dos usuarios distantes que usa una propiedad de la mecánica cuántica. La novedad de la invención reside en que el número de datos útiles para generar la clave, por cada dato transmitido, es mayor que en cualquier otro procedimiento cuántico de distribución de claves criptográficas previo. En los procedimientos cuánticos tradicionales, para garantizar la privacidad de la clave es necesario que ambos usuarios elijan aleatoriamente e independientemente entre hacer dos posibles experimentos sobre cada dato transmitido. Sólo cuando estas elecciones aleatorias coinciden se genera un dato útil para la clave criptográfica. Si no coinciden, el dato transmitido se desecha. Esta forma de proceder garantiza la privacidad de la clave gracias a una propiedad de la mecánica cuántica según la cual es imposible copiar de manera fidedigna un estado cuántico desconocido.

El invento se basa en otra propiedad de la mecánica cuántica: la creación de "enredo" a distancia. En él ambos usuarios siempre hacen el mismo experimento, y el número de datos útiles para la clave (por cada dato transmitido) duplica el del conocido procedimiento propuesto por Bennett y Brassard en 1984 ("BB84"), e incluso mejora los resultados del procedimiento propuesto por Lo y Chau en 1998 ("Quantum cryptographic system with reduced data loss", patente US5732139). Otra ventaja del invento es que simplifica el proceso de comprobación de que la clave no ha sido espiada. En todos los procedimientos cuánticos previos, cualquier intento de espionaje se traduce inevitablemente en que las claves que reciben ambos usuarios dejan de ser iguales. Para averiguar si se ha producido espionaje los usuarios deben comparar públicamente un mismo fragmento de sus respectivas claves. En el procedimiento "BB84" la acción de un espía altera el 25 % de la clave. En el invento la acción del espía altera el 75 % de la clave, lo que facilita su detección. Se detalla un modo de realizar la invención con tecnología disponible hoy en día con pares de fotones "enredados" en polarización.

Estado previo de la técnica

Los dos objetivos principales de la criptografía son: (1°) Lograr que dos usuarios distantes, a los que tradicionalmente se llama "Alicia" y "Bob", se comuniquen de una manera ininteligible para un usuario no autorizado, al que tradicionalmente se llama "Eva". (2°) Garantizar que el mensaje no ha sufrido alteración durante el proceso de transmisión. En 1949, Shannon [C. E. **Shannon**, *Bell Syst. Tech. J.* 28, 657 (1949)] demostró que ambos objetivos pueden alcanzarse usando el procedimiento cifrador (o encriptador) de Vernam [G. S. **Vernam**, *J. AIEE* 45, 109 (1926)], también conocido como "one-time pad". Tal procedimiento requiere que Alicia y Bob posean una misma secuencia aleatoria de bits (i.e., de ceros o unos) que sólo ellos conocen, que es lo que se llama una "clave criptográfica". El procedimiento funciona de la siguiente manera: Alicia escribe el mensaje secreto que quiere transmitir a Bob como secuencia de bits, y le suma, bit a bit, la clave, módulo 2 (es decir, teniendo en cuenta que 0+0=0, 0+1=1, 1+1=0). El resultado es un mensaje cifrado. Este se transmite por una canal público (es decir, un canal en el que puede haber espías). Para descifrar (es decir, recuperar) el mensaje original a partir del mensaje cifrado, Bob sólo tiene que sumarle (módulo 2) la clave. Este procedimiento impone dos exigencias a la clave: (1ª) La clave tiene que ser al menos tan larga como el mensaje enviado. (2ª) La misma clave no puede emplearse dos veces. Si se usa la misma clave para encriptar un segundo mensaje, sumando módulo 2 los dos mensajes cifrados se obtiene la suma módulo 2 de los dos mensajes originales. Se puede demostrar que esta información es suficiente para que un espía descifre ambos mensajes (si en ellos se ha empleado un vocabulario finito). Más adelante se señalará una 3ª razón por la cuál es importante disponer de procedimientos para distribuir con la mayor rapidez claves criptográficas de longitud arbitraria.

Por tanto, el problema fundamental de la criptografía moderna es el "problema de la distribución segura de claves", es decir, cómo conseguir que Alicia y Bob, que no comparten inicialmente información secreta, lleguen a tener la misma clave, garantizando además que esta clave es sólo conocida por ellos. Como las claves (como cualquier otro tipo de información) se codifican en propiedades medibles de algún sistema físico portador, las leyes de la Física clásica siempre dejan abierta la posibilidad de un espionaje "pasivo": Un espía puede intervenir el canal de comunicación y hacer simples copias (clones) de la información, averiguando cuál es la clave a partir de esas copias, sin con ello alterar de una manera detectable el estado físico del portador, de forma que cuando el espía restituye el portador al canal, su intervención pasa inadvertida a los usuarios legítimos. En ese sentido, el problema de la distribución segura de claves criptográficas no tiene solución con las leyes de la Física clásica. Sin embargo, sí es resoluble usando dos propiedades de la Mecánica Cuántica: (a) El teorema de imposibilidad de clonaje [W. K. **Wootters** y W. H. **Zurek**, *Nature* 299, 802 (1982)], que establece que un estado cuántico desconocido de un sistema

individual no pueden ser clonado de forma fidedigna. (b) El principio de incertidumbre de Heisenberg, según el cual ciertas magnitudes físicas son complementarias entre sí en el sentido de que al medir una de ellas, otra u otras se ven inevitablemente alteradas. Ambas propiedades no sólo se refieren a limitaciones atribuibles a una tecnología particular, sino que indican limitaciones inherentes a la naturaleza. Por tanto, si el portador de la clave criptográfica es un sistema cuántico (usualmente un fotón, pero también un electrón, un átomo, una molécula, etc.) y la información sobre la clave se ha codificado preparando ese sistema en un estado cuántico desconocido (tanto para el receptor como para los potenciales espías, pero no para el emisor), cualquier intento de averiguar cuál es el estado cuántico del sistema haciendo copias de él es, en general, inútil (por el teorema de imposibilidad de clonaje), y además perturba inevitablemente y de una manera detectable para los usuarios autorizados el estado del portador (por el principio de incertidumbre).

El primer procedimiento cuántico de distribución de claves fue propuesto por Bennett y Brassard en 1984 ("BB84") [C. H. **Bennett** y G. **Brassard**, "Quantum key distribution and coin tossing", en *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175; C. H. **Bennett**, *IBM Technical Disclosure Bulletin*, enero 1984, p. 4363, y diciembre 1985. p. 3153], y ha sido posteriormente modificado e implementado de diversas formas [C. H. **Bennett**, F. **Bessette**, G. **Brassard**, L. **Salvail** y J. **Smolin**, "Experimental quantum cryptography", *J. Cryptology* 5, 3 (1992); C. H. Bennett, "Interferometric quantum cryptographic key distribution system", patente US5307410 (1994)]. Este procedimiento funciona de la siguiente manera:

(i) El emisor, Alicia, prepara una secuencia de sistemas cuánticos de dos niveles (por ejemplo, fotones polarizados), cada uno de ellos en un estado elegido aleatoriamente entre cuatro posibles "A0", "A1", "B0" y "B1" (por ejemplo, linealmente polarizado a 0, 90, 45 o 135 grados, respectivamente) y se los envía por un canal público a Bob, sin decirle a nadie en qué estado concreto está cada uno de los fotones. Por ejemplo, Alicia prepara la siguiente secuencia: "B1", "B0", "A0", "A0", "A1", etc. Según la mecánica cuántica ninguna medida permite averiguar simultáneamente en cuál de los cuatro estados ha sido preparado cada fotón. Como mucho, se puede elegir entre hacer un experimento "A" que sólo le permite distinguir entre "A0" y "A1" o un experimento "B" que sólo le permite distinguir entre "B0" y "B1". Si hace el experimento "A" sobre un estado preparado en "A0", obtendrá "A0"; pero si hace el experimento "A" sobre un estado preparado en "B0", la mitad de las veces obtendrá "A0" y la mitad "A1", y perderá toda información sobre qué hubiera pasado si en lugar de hacer el experimento "A" hubiese hecho el experimento "B".

(ii) Para cada fotón que recibe, Bob mide bien "A" o bien "B", aleatoriamente, y registra los resultados obtenidos. Por ejemplo: "A1", "B0", "B1", "A0", "A1", etc.

(iii) Bob anuncia públicamente qué tipo de experimento ("A" o "B") ha realizado sobre cada fotón. Por ejemplo, Bob anuncia que su secuencia de experimentos ha sido: "A", "B", "B", "A", "A", etc. Pero no dice qué resultado concreto ha obtenido en cada experimento.

(iv) Alicia le comunica a Bob usando un canal público para qué fotones ha hecho el experimento "correcto" que le permite averiguar con certeza en qué estado había preparado ella el fotón. En nuestro ejemplo, Alicia le diría a Bob que sus experimentos correctos han sido los realizados sobre el segundo, el cuarto y el quinto fotón.

(v) Alicia y Bob desechan la información que iba en los otros fotones (el primero, el tercero, etc.). Con la información restante generan la clave criptográfica. Por ejemplo, con los resultados "correctos": "...", "B0", "...", "A0", "A1", etc., generarían la clave "001...". Nótese que usando este procedimiento. la información desechada es la mitad de la transmitida. Este proceder es necesario para que Eva no pueda averiguar la clave.

(vi) Si Eva intercepta un fotón preparado en el estado, por ejemplo, "A0" y hace el experimento "A", obtendrá "A0" y restituirá el fotón en ese estado y su acción pasará desapercibida, pero si el fotón estaba preparado en el estado "B1", al medir "A", Eva obtendrá o "A0" o "A1", y al restituir el fotón cuando Bob mida "B" obtendrá "B0" la mitad de las veces (aun cuando Alicia lo había preparado en "B1" y él ha efectuado la medida "correcta"). Para averiguar si se ha producido espionaje Alicia y Bob comparan públicamente un fragmento de la clave (que luego desechan). Si coincide, o presenta discrepancias suficientemente pequeñas, inferirán que no se ha producido espionaje y que esas discrepancias son atribuibles a errores en la transmisión (y en ningún caso pueden enmascarar la presencia de un espía que esté extrayendo suficiente información para averiguar parte de la clave), y por tanto deducirán que sus respectivas claves (prácticamente) coinciden y son seguras. Si no, concluirán que el canal de transmisión está siendo espiado y pospondrán el proceso de generación de la clave. En concreto, en el procedimiento "BB84", por cada bit que comparan Alicia y Bob, la

probabilidad de que ese bit revele la presencia de Eva (en el supuesto de que Eva haya intentado espiar) es 1/4. Por tanto, si comparan N bits, la probabilidad de detectar la presencia de Eva es $1-\left(\frac{3}{4}\right)^{N}$.

(vii) Si no se ha detectado espionaje, Alicia y Bob podrán usar la clave para cifrar y descifrar mensajes sin peligro. Pero incluso si detectan discrepancias suficientemente pequeñas entre sus claves (atribuibles bien a la presencia de un espía ocasional o más probablemente a los inevitables errores en el proceso de transmisión), Alicia y Bob pueden usar técnicas clásicas de amplificación de la privacidad [C. H. **Bennett**, G. **Brassard** y J.-M. **Robert**, *Soc. Ind Appl. Math. J. Comp.* 17, 210 (1988); **Bennett**, C. H., **Brassard**, C. **Crépeau** y U. M. **Maurer**, *IEEE Trans. Inform. Theory* 41, 1915 (1995)] y reducir tanto como deseen la cantidad de información útil sobre la clave que obtiene el supuesto espía. El precio que hay que pagar por usar estas técnicas es el de reducir la longitud útil de la clave (esta otra razón que indica lo importante que es disponer de procedimientos para distribuir rápidamente claves de longitud arbitraria).

Posteriormente se han propuesto otros procedimientos de distribución de claves criptográficas que también usan la mecánica cuántica de forma similar al procedimiento "BB84" ["E91": A. K. **Ekert**, *Phys. Rev. Lett.* 67, 661 (1991); "B92": C. H. **Bennett**, *Phys. Rev. Lett.* 68, 3121 (1992); "GV95": L. **Goldenberg** y L. **Vaidman**, *Phys. Rev. Lett.* 75, 1239 (1995); "LC98": M. **Ardehali**, G. **Brassard**, H. F. **Chau** y **H.-K.** Lo, *Los Alamos preprint archive*, quant-ph/9803007; **H.-K.** Lo y H. F. **Chau**, patente US5732139 (1998)], así como múltiples formas de implementar estos procedimientos de distribución de claves [las referencias que figuran a continuación han sido agrupadas por entidades solicitantes de las patentes: (a) IBM: C. H. **Bennett**, F. **Bessette**, G. **Brassard**, L. **Salvail** y J. **Smolin**, *J. Cryptology* 5, 3 (1992); C. H. **Bennett**, patente US5307410 (1994); **Bennett** y S. J. **Wiesner**, patente US5515438 (1996). (b) UNIVERSIDAD JOHN HOPKINS, BALTIMORE: J. D. **Franson**, patente US5243649 (1993); J. D. **Franson** y H. **Ilves**, *J. Mod. Opt.* 41, 2391 (1994); J. D. **Franson** y B. C. **Jacobs**, *Electron. Lett.* 31, 232 (1995); B. C. **Jacobs** y J. D. **Franson**. *Opt. Lett.* 21, 1854 (1996). (c) BRITISH TELECOMMUNICATIONS: A. K. **Ekert**, J. G. **Rarity**, P. R. **Tapster** y G. M. **Palma**, *Phys. Rev. Lett.* 69, 1293 (1992); P. D. **Townsend**, J. G. **Rarity** y P. R. **Tapster**, *Electron. Lett.* 29, 634 (1993); *Electron. Lett.* 29, 1291 (1993); P. D. **Townsend**, *Electron. Lett.* 30, 809 (1994); P. D. **Townsend**, ?. **Thompson**, *J. Mod. Opt.* 41, 2425 (1994); K. J. **Blow**, patente EP717897B1 (1994); J. G. **Rarity**, P. C. M. **Owens** y P. R. **Tapster**, *J. Mod Opt.* 41, 2435 (1994); J. G. **Rarity** y P. R. **Tapster**, patente US5418905H (1995); C. **Marand** y P. D. **Townsend**, *Opt. Lett.* 20, 1695 (1995); P. D. **Townsend**, *Nature* 385, 47 (1997); patente EP776558A1G (1997); patente WO9744936A1 (1997); patente US5675648 (1997); K. J. **Blow**, patente US5757912 (1998); P. D. **Townsend** y D. W. **Smith**, patente US5768378 (1998); patente EP717895B1 (1998); P. D. **Townsend** y K. J. **Blow**, patente US5850441 (1998); patente EP717896B1 (1999); P. D. **Townsend**, patente US5953421 (1999); patente EP972373A1 (2000); S. J. D. **Phoenix** y S. M. **Barnett**, patente US5764765 (1998). (d) SWISSCOM AG y TELECOM PTT: A. **Muller**, J. **Breguet** y N. **Gisin**, *Europhys. Lett.* 23, 383 (1993); A. **Muller**, H. **Zbinden** y N. **Gisin**, *Nature* 378, 449 (1995); *Europhys. Lett.* 33, 335 (1996); G. **Ribordy**, J-D. **Gautier**, N. **Gisin**, O. **Guinnard** y H. **Zbinden**, *Electron. Lett.* 34, 2116 (1998); Los Alamos preprint archive, quant-ph/9905056; N. **Gisin** *et al.*, patente W9810560A1 (1998); patente EP923828A1 (1999). (e) UNIVERSIDAD DE CALIFORNIA y LABORATORIO DE LOS ALAMOS: T. **Buttler** *et al.*, *Phys. Rev. Lett.* 81, 3283 (1998); *Phys. Rev. A* 57, 2379 (1998); patente US5966224 (1999); Los Alamos preprint archive, quant-ph/0001088 (2000). (f) CALIFORNIA INSTITUTE OF TECHNOLOGY: H. J. **Kimble**, Z. Y. **Ou** y S. E. **Pereira**, patente US5339182C (1994). (g) NIPPON TELEGRAPH & TELEPHONE: K. **Masato** y I. **Nobuyuki**, patente JP10322329A (1998). (h) FRANCE TELECOM: Y. **Mazourenko**, J.-M. **Merolla** y J.-P. **Goedgebuer**, patente EP877508A1 (1998)]. Un resumen de los primeros desarrollos en criptografía cuántica puede encontrarse en C. H. **Bennett**, G. **Brassard** y A. K. **Ekert**, "Criptografía cuántica", *Investigación y Ciencia* n° 195, p. 14 (1992), reimpreso en A. **Cabello**, "Misterios de la física cuántica", *Temas de Investigación y Ciencia* n° 10, Prensa Científica, Barcelona, 1997, p. 75.

En todos los procedimientos cuánticos de distribución de claves previos, los usuarios legítimos deben elegir entre experimentos alternativos y posteriormente descartar una parte de los datos transmitidos. Especial atención merece el sistema patentado por Lo y Chau ("Quantum cryptographic system with reduced data loss", patente US5732139) que es una variante de "BB84" en la cual la cantidad de datos descartados se reduce notoriamente. Este procedimiento "LC98" asigna diferentes probabilidades a los observables "A" y "B" (en el procedimiento "BB84" ambas probabilidades eran 1/2) tanto durante la transmisión como durante la recepción, y usa un análisis refinado sobre los datos aceptados para reducir la fracción de datos descartados.

Descripción de la invención

El invento es un sistema cuántico de distribución de claves criptográficas que utiliza un efecto cuántico conocido como creación de "enredo" a distancia, descrito por primera vez en 1993 [C. H. **Bennett**, G. **Brassard**, C. **Crépeau**, R. **Jozsa**, A. **Peres** y W. K. **Wootters**, *Phys. Rev. Lett.* 70, 1895 (1993); M. **Zukowski**, A. **Zeilinger**, M. A. **Horne** y A. K. **Ekert**, *Phys. Rev. Lett.* 71, 4287 (1993); S. **Bose**, V. **Vedral** y P. L. **Knight**, *Phys. Rev. A* 57, 822 (1998)]. Es un efecto que se produce entre cuatro fotones, y que se provoca haciendo un determinado experimento sobre dos de ellos. Ese experimento consiste en medir el "observable de Bell" [S. L. **Braunstein**, A. **Mann** y M. **Revzen**, *Phys. Rev. Lett.* 68, 3259 (1992)]. La medida del observable de Bell sobre dos fotones hace que tras la misma estos dos fotones se encuentren necesariamente en uno de los cuatro "estados de Bell". Estos estados son lo que se llama en mecánica cuántica estados "enredados" (un estado de dos fotones es enredado si no se puede describir a partir de los estados de cada uno de los fotones). Para nuestro propósito será suficiente con denotarlos por 00, 01, 10 y 11, y describir cómo se comportan en el efecto de creación de enredo a distancia. La creación de enredo a distancia funciona de la manera siguiente: Consideremos cuatro fotones, i, j, k y l. Los dos primeros (i y j) han sido preparados en uno de los estados de Bell, por ejemplo en el estado 11; los otros dos (k y l) han sido preparados en otro estado de Bell, por ejemplo, en el 01. Al medir el observable de Bell sobre i y k, los cuatro resultados posibles "00", "01", "10" y "1" van a ocurrir con idéntica probabilidad (1/4), puesto que la mecánica cuántica asegura que el resultado de esa medida es completamente aleatorio. Supongamos, por ejemplo, que se obtiene el resultado "00". Tal resultado indica además que el estado de los fotones i y k tras el experimento es el 00. Ese experimento sobre los fotones i y k hace que los otros dos fotones, j y l, pasen a estar en un estado de Bell determinado, el 10 (en nuestro ejemplo). Y todo esto sin que haya habido una interacción directa sobre estos últimos fotones. Este efecto ha sido comprobado experimentalmente [D. **Bouwmeester**, J. **Pan**, K. **Mattle**, M. **Eibl**, H. **Weinfurter** y A. **Zeilinger**, *Nature* 390, 575 (1997); D. **Boschi**, S. **Branca**, F. **De Martini**, L. **Hardy** y S. **Popescu**, *Phys. Rev. Lett.* 80, 1121 (1998); J-W. **Pan**, D. **Bouwmeester**, H. **Weinfurter** y A. **Zeilinger**, *Phys. Rev. Lett.* 80, 3891 (1998)].

Si los estados iniciales de i y j, y k y l fueran otros estados de Bell diferentes a los que hemos considerado en el ejemplo anterior, o/y si el resultado del experimento (sobre i y k) para medir el observable de Bell fuese diferente, entonces también cambiaría el estado final de j y l. La mecánica cuántica permite calcular cuál sería el estado final en cada caso. La siguiente tabla recoge todas las posibilidades.

Estados iniciales de i y j, y de k y l				Posibles estados finales de i y k, y de j y l			
0000,	0101,	1010,	1111	0000,	0101,	1010,	1111
0001,	0100,	1011,	1110	0001,	0100,	1011,	1110
0010,	0111,	1000,	1101	0010,	0111,	1000,	1101
0011,	0110,	1001,	1100	0011,	0110,	1001,	1100

La tabla debe usarse de la manera siguiente. Si, por ejemplo, el estado inicial de i y j fuese 11, y el de k y l fuese 01, deberíamos buscar el "1101" en la parte izquierda de la tabla. En nuestro caso aparece en la cuarta columna, en la tercera fila. Esa misma fila pero en la parte de la derecha nos indica en qué cuatro estados pueden quedar i y k, y j y l, después de medir el observable de Bell sobre i y k. Así, si conocemos el estado en que quedan i y k, la tabla nos permite averiguar el estado en que han quedado j y l. Por ejemplo, si i y k han quedado en el estado 00, habrá que buscar en la parte derecha de la tercera fila la secuencia que empiece por "00". Esa es "0010", la que está en la quinta columna. Ello indicará que el estado de j y l es 10. En resumen: conocidos los estados iniciales, si uno conoce uno de los estados finales, con ayuda de la tabla puede determinar el otro.

El procedimiento inventado para la distribución de claves criptográficas se ilustra esquemáticamente en la Figura 1 y se describe a continuación.

(i) Son necesarios seis fotones (u otros sistemas cuánticos de dos niveles), que numeraremos del 1 al 6. Alicia prepara los fotones 1 y 2 en el estado de Bell 11, y los fotones 3 y 5 en el estado de Bell 10. En otro lugar distante, Bob prepara los fotones 4 y 6 en el estado de Bell 10. La información de cómo están inicialmente preparados los fotones no es secreta. Los únicos fotones transmitidos

durante el proceso serán los fotones 2 y 6. Alicia siempre conservará los fotones 1, 3 y 5; y Bob siempre conservará el fotón 4.

(ii) Alicia envía el fotón 2 a Bob usando un canal público. Este canal debe de ser un medio de transmisión que preserve el estado cuántico de los fotones de interacciones con el entorno (por ejemplo, una fibra óptica).

(iii) Alicia mide en secreto (es decir, sin comunicar a nadie el resultado) el observable de Bell sobre los fotones 1 y 3, y Bob mide en secreto el observable de Bell sobre los fotones 2 y 4. Los resultados de ambos experimentos están correlacionados; pero ni Alicia ni Bob (ni nadie que no conozca ambos resultados) saben todavía de qué manera concreta lo están. El propósito del siguiente paso es precisamente conseguir que Alicia y Bob descubran cuál es la correlación entre sus resultados, sin tener que hacer públicos ninguno de ellos.

(iv) Para ello, Bob transmite el fotón 6 a Alicia usando el canal público. Cuando lo recibe, Alicia mide el observable de Bell sobre los fotones 5 y 6, y anuncia públicamente el resultado. Supongamos que Alicia hubiese obtenido el resultado "11" en la medida que realizó anteriormente en secreto sobre los fotones 1 y 3. Entonces, como el estado inicial de los fotones 1, 2, 3 y 5 era "1110", usando la tabla anterior Alicia averigua que el estado de 2 y 5 es "00". Además, si en la medida pública sobre 5 y 6, Alicia ha obtenido el resultado "00", entonces, como sabe que el estado de 2, 4, 5 y 6 antes de esa medida pública era el 1010, usando de nuevo la tabla, Alicia sabe que Bob ha tenido que obtener el resultado "00" en su medida secreta sobre 2 y 4. Con ayuda del resultado que ha anunciado públicamente Alicia y mediante un razonamiento similar, Bob puede averiguar que Alicia ha obtenido el resultado "11" en su medida secreta sobre los fotones 1 y 3. Previamente, Alicia y Bob han acordado que la secuencia formada por los resultados de las medidas secretas de Alicia forme la clave. Por tanto, los dos bits iniciales de la clave serían "11".

(v) La información pública que comparten Alicia y Bob es insuficiente para que Eva conozca la clave. Con esta información, lo único que Eva sabe es que ha ocurrido una de las siguientes cuatro parejas de resultados: el resultado "00" en la medida secreta de Alicia y el resultado "1" en la medida secreta de Bob, "01" en la de Alicia y "10" en la de Bob, "10" en la de Alicia y "01" en la de Bob, o "11" en la de Alicia y "00" en la de Bob. Sin embargo, sí existe un método con el que Eva puede intentar averiguar la clave. Tal método se detalla más adelante, lo importante aquí es que ese intento de espionaje tiene por resultado que las claves de Alicia y Bob no coincidan y, por tanto, para comprobar la presencia de espías se puede usar un procedimiento igual al descrito para "BB84" [en el punto (vi)].

(vi) Cualquier estado de Bell puede obtenerse a partir de cualquier otro sin más que rotar adecuadamente la polarización de uno de los fotones. Usando esta propiedad, Alicia y Bob pueden cambiar el estado de Bell de los fotones 1 y 3 (Alicia), y 2 y 4 (Bob), y convertirlos en unos estados previamente acordados. Esta maniobra tiene como único objetivo que si se ha producido un error (o un acto de espionaje) entre los pasos (i) y (iv), éste no afecte a los pasos siguientes. Tras esta maniobra la situación es igual a la que había en inicialmente, y el proceso sigue cíclicamente. En cada ciclo Alicia y Bob obtienen una nueva pareja de bits secretos. El proceso se detiene cuando han logrado una cadena de bits de la longitud deseada.

El invento tiene dos características novedosas frente a todos los procedimientos previos de distribución de claves que usan la mecánica cuántica (los únicos 100 % seguros):

(a) Mejora el número de bits secretos generados por cada fotón transmitido. En "BB84", en "E91" y en "B92", Alicia y Bob deben de elegir aleatoriamente entre dos medidas alternativas para garantizar la privacidad de la clave. Esto implica que el número de bits útiles de clave es 0,5 bits por cada fotón transmitido en "BB84" y en "B92", y 0,25 bits por fotón en "E91". El máximo valor para este número en todos los procedimientos de distribución de claves es el que se obtiene en "LC98": 1-ε, donde ε es una cantidad pequeña, pero nunca cero. En el invento ese número es exactamente 1. Siempre se genera un bit de clave secreta por cada fotón transmitido.

(b) Requiere que Alicia y Bob desechen menos bits en el proceso de detección de espías. Para comprobar si un espía a alterado la secuencia de bits, todos los procedimientos de distribución de claves basados en la mecánica cuántica usan la misma estrategia: Alicia y Bob hacen pública una pequeña parte de sus respectivas secuencias de bits secretos, por ejemplo los bits números 20, 43, 57, etc. Si no ha habido ningún error durante la transmisión, ambas secuencias deben ser idénticas. Si eso ocurre, Alicia y Bob pueden estar razonablemente seguros de que sus restantes bits también son idénticos y pueden usarse como clave. El punto esencial en todos los procedimientos cuánticos de distribución

de claves es que cualquier intento de averiguar la clave por parte de Eva se traduce en que las secuencias de Alicia y Bob dejan de ser iguales. Por tanto, si ha habido espionaje, éste se pondrá de manifiesto cuando Alicia y Bob comparen públicamente un trozo de sus secuencias. El invento tiene la ventaja adicional de que cada vez que actúa Eva perturba no uno sino dos bits consecutivos y, por lo tanto, detectar tal actuación requiere comparar menos bits que con procedimientos anteriores. En concreto, en "BB84". para cada bit que comparan Alicia y Bob, la probabilidad de que ese bit revele la presencia de Eva (en el supuesto de que Eva haya intentado espiar) es 1/4, por tanto si comparan N bits, la probabilidad de detectar a Eva es $1-\left(\frac{3}{4}\right)^{N}$. En el invento, si Alicia y Bob comparan un par de bits generados en la misma secuencia, la probabilidad de detectar la presencia de Eva es 3/4, por tanto si comparan n pares (N = 2n bits), la probabilidad de detectar la presencia de Eva es $1-\left(\frac{1}{2}\right)^{N}$.

En el invento descrito, la creación de "enredo" a distancia clave no está codificada directamente en los fotones que se transmiten, éstos sólo contienen información sobre qué correlación existe entre los experimentos que permiten a Alicia y a Bob generar la clave. Por ello, interceptar y copiar los fotones transmitidos no sirven para que Eva adquiera información sobre la clave. De hecho, el estado cuántico de los fotones transmitidos es de conocimiento público. Sin embargo, ello no quiere decir que es imposible que Eva obtenga información sobre la clave. Existe una posible estrategia de espionaje basada en el efecto de creación de enredo a distancia. Esta estrategia se ilustra en la Figura 2 y se describe a continuación. Ello no compromete la seguridad de la clave ya que, como veremos, esta forma de espionaje es inmediatamente detectable.

(1a) Consideremos la misma situación que teníamos en (i) pero supongamos que hubiese un espía, Eva (al que Alicia y Bob no pueden ver), que tiene dos fotones adicionales que llamaremos 7 y 8, preparados inicialmente en el estado de Bell 00.

(1b) Eva intercepta el fotón 2 que Alicia manda a Bob y hace una medida del observable de Bell sobre los fotones 2 y 8. Entonces los fotones pasan a estar en un estado de Bell conocido por Eva. Por ejemplo, si tras la medición de Eva el estado de 2 y 8 es 00, entonces el estado de 1 y 7 pasa a ser 11.

(2) Por lo tanto, tras esta intervención de Eva, la situación ya no sería la descrita en Ahora el fotón 1 está en un estado de Bell con el fotón 7 de Eva, y el fotón 2 está en un estado de Bell con el fotón 8.

(3a) En este nuevo escenario, tras el experimento que hace Alicia (Bob) sobre los fotones 1 y 3 (2 y 4), el estado de los fotones 5 y 7 (6 y 8) pasa a ser un estado de Bell. Por ejemplo, si Alicia (Bob) obtiene el resultado "11" ("00"), el estado de los fotones 5 y 7 (6 y 8), 10 (10). Sin embargo, estos estados todavía son desconocidos para Eva, ya que todavía no sabe cuáles son los resultados de las mediciones que han hecho Alicia y Bob.

(3b) Para averiguar el resultado de Bob, Eva intercepta el fotón 6 que Bob manda a Alicia y efectúa una medida del observable de Bell sobre los fotones 6 y 8. Esta revela en qué estado de Bell están. Entonces Eva (con ayuda de la tabla) puede conocer el resultado de Bob. En nuestro ejemplo Eva obtendría el resultado "10" y sabría que el resultado que obtuvo Bob fue "00".

(3c) Para averiguar el resultado de Alicia (que es el realmente interesante puesto que es la clave) Eva efectúa una medida del observable de Bell sobre los fotones 7 y 8. Entonces los fotones 5 y 6 pasan a estar en un estado de Bell que todavía es desconocido para Eva, ya que todavía no conoce el resultado de Alicia. Por ejemplo, si Eva obtiene "01", entonces los fotones 5 y 6 estarían en el estado 01.

(4) A continuación Eva hace llegar a Alicia el fotón 6. Alicia (que no sabe de la presencia de Eva) hace el experimento que corresponde sobre los fotones 5 y 6 y anuncia públicamente el resultado. Con esa información Eva puede conocer cuál era el estado previo de 5 y 7 (10, en nuestro ejemplo), y el resultado de la medida secreta que hace Alicia sobre 1 y 3, que es parte de la clave ("11", en nuestro ejemplo).

Sin embargo, y esto es lo importante desde el punto de vista de la seguridad del procedimiento, esta intervención de Eva ha cambiado inevitablemente la correlación que Alicia y Bob esperaban encontrar entre sus resultados secretos, o equivalentemente hace que las claves de Alicia y Bob dejen de ser iguales. En nuestro ejemplo, Bob usando su resultado secreto y el resultado hecho público por Alicia, llega a la

conclusión de que el resultado de Alicia (y por tanto, los dos primeros bits de la clave) es "10". Como en los métodos cuánticos tradicionales cualquier espionaje queda en evidencia cuando Alicia y Bob hacen públicos algunos fragmentos de la clave. La ventaja de nuestro invento en esta faceta es que en el invento la intervención de Eva cambia 3 de cada 4 pares de bits de la clave, mientras que en los procedimientos anteriores sólo cambia uno de cada dos bits.

Descripción de las figuras

Fig. 1: Esquema del procedimiento de distribución de claves criptográficas:

- Figura (i): Alicia prepara los sistemas cuánticos 1 y 2 en el estado de Bell 11, y los sistemas 3 y 5 en el estado 11. Bob prepara los sistemas 4 y 6 en el estado 10. Cada círculo representa un sistema cuántico de dos niveles. Dos sistemas están unidos por una línea continua si están en un estado de Bell.

- Figura (ii): Alicia envía a Bob el sistema 2.

- Figura (iii): Alicia mide el observable de Bell sobre 1 y 3, y obtiene (por ejemplo) el resultado 11, que mantiene en secreto. Bob mide el observable de Bell sobre 2 y 4, y obtiene (por ejemplo) el resultado 00, que mantiene en secreto. 5 y 6 pasan a estar (debido al efecto de creación de enredo a distancia) en el estado 00.

- Figura (iv): Bob envía a Alicia el sistema 6. Alicia mide el observable de Bell sobre 5 y 6, y obtiene 00. Alicia anuncia públicamente este resultado. Con esta información y el resultado de su medida secreta, Bob llega a la conclusión de que el resultado de la medida secreta de Alicia ha sido 11. La clave secreta que comparten Alicia y Bob es "11". El proceso se repite cíclicamente.

Fig. 2: Esquema del método de espionaje:

- Figura (1a): Alicia prepara los sistemas 1 y 2 en el estado 11, y los sistemas 3 y 5 en el estado 11. Bob prepara los sistemas 4 y 6 en el estado 10. Eva (el espía) prepara secretamente los sistemas 7 y 8 en el estado 00.

- Figura (1b): Alicia envía a Bob el sistema 2. Eva secretamente lo intercepta y hace una medida del observable de Bell sobre 2 y 8, y obtiene (por ejemplo) el resultado 00. 1 y 7 pasan a estar (debido al efecto de creación de enredo a distancia) en el estado 11.

- Figura (2, 3a): Alicia mide el observable de Bell sobre 1 y 3, y obtiene (por ejemplo) el resultado 11, que mantiene en secreto. 5 y 7 pasan a estar en el estado 10. Bob mide el observable de Bell sobre 2 y 4, y obtiene (por ejemplo) el resultado 00, que mantiene en secreto. 6 y 8 pasan a estar en el estado 10.

- Figura (3b): Bob envía a Alicia el sistema 6.

- Figura (3c): Eva secretamente intercepta el sistema 6 y hace una medida del observable de Bell sobre 6 y 8, y obtiene (por ejemplo) el resultado 10. 5 y 6 pasan a estar en el estado 01.

- Figura (4): Alicia mide el observable de Bell sobre 5 y 6, y obtiene 01. Anuncia públicamente este resultado. Con esta información y el resultado de sus medidas. Eva llega a la conclusión de que el resultado de la medida secreta de Alicia ha sido 11. Sin embargo, 3 de cada 4 veces Bob llega a una conclusión incorrecta sobre el resultado de la medida secreta de Alicia, lo que permite detectar la intervención de Eva.

Modo de realizar la invención

El invento es un "procedimiento" de generación de claves, no un mecanismo concreto. Con la tecnología y conocimientos actuales se puede implementar de cuatro formas, que en orden de dificultad experimental creciente son: (a) Con modos de un campo electromagnético. (b) Con pares de fotones "enredados" sólo en polarización. (c) Con pares de fotones enredados en polarización y en energía. (d) Con pares de fotones enredados en polarización y en momento. Cabe de esperar que en un futuro inmediato este procedimiento también pueda implementarse con pares de iones atrapados en cavidades electromagnéticas.

La preparación de modos de un campo electromagnético o de pares de fotones en un estado de Bell (en polarización, etc.) concreto no presenta problema tecnológico alguno. La descripción de "fuentes" apropiadas abunda en la literatura. Es oportuno señalar que, en el caso de los fotones enredados en polarización, hasta con disponer de una fuente que prepare los pares en uno de los cuatro estados de Bell, ya que los otros tres estados de Bell pueden obtenerse a partir de aquél sin más que efectuar una simple rotación de la polarización en uno de los dos fotones.

La transmisión de los fotones entre los usuarios distantes puede hacerse mediante fibras ópticas. Actualmente esta tecnología limita la distancia de los usuarios a unos 26 km [A. **Muller**, J. **Breguet** y N. **Gisin**, *Europhys. Lett.* 23, 383 (1993); A. **Muller**, H. **Zbinden** y N. **Gisin**, *Nature* 378, 449 (1995); *Europhys. Lett.* 33, 335 (1996); G. **Ribordy**, J-D. **Gautier**, N. **Gisin**, O. **Guinnard** y H. **Zbinden**, *Electron. Lett.* 34, 2116 (1998)].

Alternativamente, si en lugar de pares de fotones se emplean pares de pulsos electromagnéticos, la transmisión puede hacerse por el aire. Con este tipo de tecnología se pueden transmitir las señales a satélites en órbitas bajas [T. **Buttler** *et al.*, *Phys. Rey. Lett.* 81, 3283 (1998); *Phys. Rev. A* 57, 2379 (1998); patente US5966224 (1999); *Los Alamos preprint archive*, quant-ph/0001088 (2000)].

La medida del observable de Bell requiere una tecnología específica, inhabitual en la literatura sobre criptografía. Es por ello que le prestaremos especial atención. Para medir el observable de Bell en los contextos descritos antes existen varios métodos. En primer lugar los desarrollados para hacer "codificación cuántica de doble densidad" [C. H. **Bennett** y J. **Wiesner**, *Phys. Rev. Lett.* 69, 2881 (1992)] y "teletransporte" de estados cuánticos [C. H. **Bennett**, G. **Brassard**, C. **Crépeau**, R. **Jozsa**, A. **Peres** y W. K. **Wootters**, *Phys. Rev. Lett.* 70, 1895 (1993)]. Para lograr ambos efectos se requieren experimentos para medir el operador de Bell. Ambos efectos se han demostrado experimentalmente en diferentes laboratorios [Experimentos de codificación densa con fotones: K. **Mattle**, H. **Weinfurter**, P. G. **Kwiat** y A. **Zeilinger**, *Phys. Rev. Lett.* 76, 4656 (1996). Experimentos de teletransporte con fotones: D. **Bouwmeester**, J. **Pan**, K. **Mattle**, M. **Eibl**, H. **Weinfurter** y A. **Zeilinger**, *Nature* 390. 575 (1997); D. **Boschi**, S. **Branca**, F. **De Martini**, L. **Hardy** y S. **Popescu**, *Phys. Rev, Lett.* 80, 1121 (1998); J-W. **Pan**, D. **Bouwmeester**, H. **Weinfurter** y A. **Zeilinger**, *Phys. Rev. Lett.* 80, 3891 (1998). Experimentos de teletransporte con modos de campos electromagnéticos: A. **Furusawa**, J. **Sorenson**, S. L. **Braunstein**, C. A. **Fuchs**, H. J. **Kimble** y E. S. **Polzik**, *Science* 282, 706 (1998)]. La técnica descrita en el trabajo de Furusawa *et al.* serviría para implementar el invento en el contexto (a). Las técnicas descritas en los trabajos con fotones también podrían servir para nuestro propósito. Sin embargo, existen otros métodos que son más adecuados en nuestro caso (porque distinguen entre los cuatro estados de Bell, y no sólo entre dos de ellos y una combinación lineal de los otros dos, como ocurre en las referencias citadas). Son los de Kwiat y Weinfurter [P. G. **Kwiat** y H. **Weinfurter**, *Phys. Rev. A* 58, R2623 (1998)] para los contextos (c) y (d), y el de Scully, Englert y Bednar [M. O. **Scully**. B.-G. **Englert** y C. J. **Bednar**, *Phys. Rev. Lett.* 83, 4433 (1999)] para el contexto (b). Los detalles deben consultarse en las referencias citadas.

REIVINDICACIONES

1. Un procedimiento cuántico para distribuir de manera segura una clave criptográfica entre dos usuarios autorizados, A y B, **caracterizado** porque consta de los siguientes pasos:

a. Preparación de cuatro señales cuánticas en A y 2 en B.

b. Transmisión de una señal cuántica de A a B por un canal.

c. Medición en A y en B de una propiedad (la misma en A y B) de dos señales cuánticas.

d. Transmisión de una señal cuántica de B a A por el mismo canal mencionado en b.

e. Medición en A de una propiedad de dos señales cuánticas y anuncio público del resultado.

f. Los pasos b-e del proceso se repiten cíclicamente, hasta lograr una cadena de bits de la longitud deseada.

g. Verificación de la clave obtenida, por comparación pública de las claves obtenidas tras el proceso seguido de a a f.

2. Un procedimiento cuántico para distribuir de manera segura una clave criptográfica entre dos usuarios autorizados, A y B, según reivindicación 1, **caracterizado** porque todas las señales cuánticas se utilizan para generar la clave (ninguna ha de ser desechada).

3. Un procedimiento cuántico para distribuir de manera segura una clave criptográfica entre dos usuarios autorizados, A y B, según reivindicaciones 1 a 2, **caracterizado** porque, el número de bits útiles de clave, antes de la verificación, es igual al de señales cuánticas transmitidas.

4. Un procedimiento cuántico para distribuir de manera segura una clave criptográfica entre dos usuarios autorizados, A y B, según reivindicaciones 1 a 3, **caracterizado** porque cualquier intervención no autorizada en el canal de transmisión altera de manera detectable por los usuarios autorizados el 75 % de la clave distribuida a B.

5. Un procedimiento cuántico para distribuir de manera segura una clave criptográfica entre dos usuarios autorizados, A y B, según reivindicaciones 1 a 4, **caracterizado** porque requiere que A y B comparen un fragmento de clave menor que en cualquier otro procedimiento cuántico previo de distribución de claves criptográficas.

FIG. 1

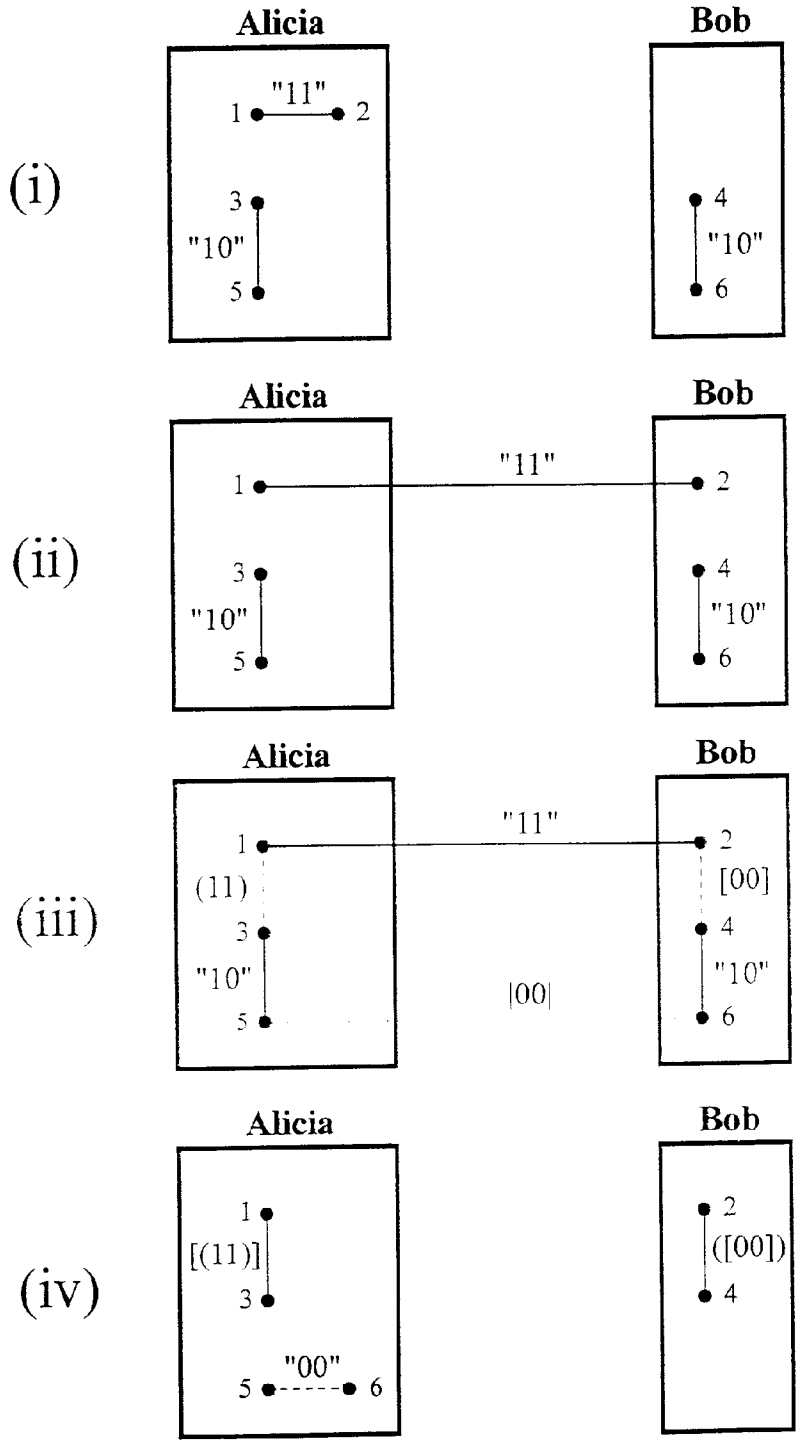
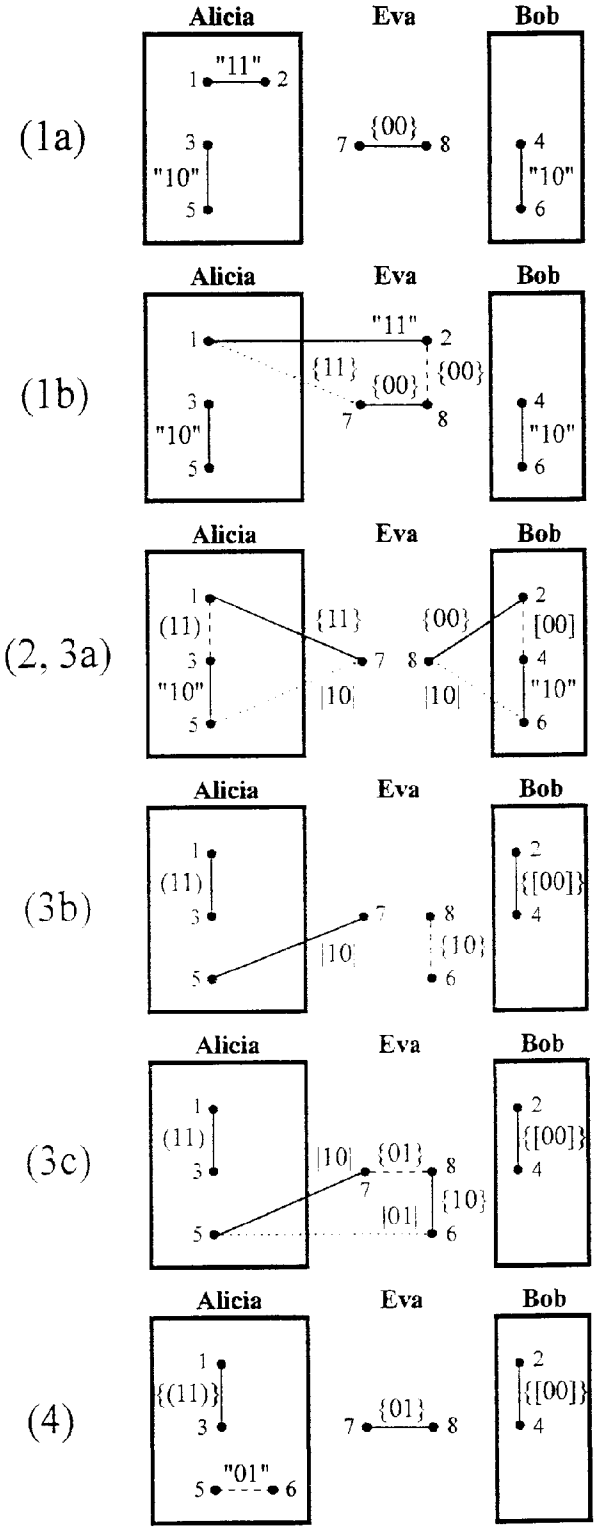

(i)
Alicia
Bob
"11"
1
2
3
"10"
5
4
"10"
6
(ii)
Alicia
Bob
"11"
1
2
3
"10"
5
4
"10"
6
(iii)
Alicia
Bob
"11"
1
2
(11)
[00]
3
4
"10"
"10"
5
6
|00|
(iv)
Alicia
Bob
1
2
[(11)]
([00])
3
4
"00"
5
6

FIG. 2


(1a)
Alicia
Eva
Bob
"11"
1
2
3
"10"
5
{00}
7
8
4
"10"
6
(1b)
Alicia
Eva
Bob
"11"
1
2
{11}
{00}
{00}
3
"10"
5
7
8
4
"10"
6
(2, 3a)
Alicia
Eva
Bob
1
(11)
3
"10"
5
{11}
7
|10|
{00}
8
|10|
2
[00]
4
"10"
6
(3b)
Alicia
Eva
Bob
1
(11)
3
5
7
|10|
8
{10}
6
2
{[00]}
4
(3c)
Alicia
Eva
Bob
1
(11)
3
5
|10|
{01}
7
8
{10}
|01|
6
2
{[00]}
4
(4)
Alicia
Eva
Bob
1
{(11)}
3
"01"
5
6
{01}
7
8
2
{[00]}
4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 168 204

(21) N.° solicitud: 200000713

(22) Fecha de presentación de la solicitud: **21.03.2000**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl.**[7]**:** H04B 10/00, H04L 9/08

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
A	US 5764765 A (PHOENIX et al.) 09.06.1998	
A	US 5768378 A (TOWNSEND et al.) 16.06.1998	
A	EP 0920149 A (MOTOYOSHI; MATSUOKA) 02.06.1999	

Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

[×] para todas las reivindicaciones

[ ] para las reivindicaciones n°:

Fecha de realización del informe	Examinador	Página
26.04.2002	J. Botella Maldonado	1/1