Criptografía cuántica

Diego Córdoba

v2.0 - 08 de Noviembre de 2021

Nota del autor

El presente ensayo fue presentado como trabajo final del curso de Introducción a la Computación Cuántica dictado por el Dr. Federico Hernán Holik para el SADIO (Sociedad Argentina de Informática) [1] durante el mes de Septiembre de 2021.

1. Introducción

La seguridad en las comunicaciones, desde el punto de vista de la criptografía, debería cumplir al menos los siguientes tres aspectos fundamentales:

- Privacidad
- Autenticidad
- Integridad

Supóngase el criptosistema de la Fig. 1. Aquí, Alice representa el emisor de un mensaje, Bob el receptor, y Eva un atacante, un espía en el canal de comunicación. La **privacidad** implica que los mensajes enviados por Alice a Bob únicamente pueden ser leídos por él, mientras que Eva no podrá ver el contenido del mensaje. **Autenticidad** permite a Bob verificar que el mensaje recibido fue enviado efectivamente por Alice, y no existe nadie haciéndose pasar por ella. Finalmente, **integridad** implica que Bob pueda verificar si el mensaje recibido se ha modificado en el medio de comunicación respecto del mensaje enviado por Alice.

Los mecanismos criptográficos para lograr estos objetivos pueden ser simétricos (la misma clave para cifrar y descifrar datos) o asimétricos (claves distintas para cifrar y descifrar, clave pública y clave privada). El criptosistema simétrico requiere que, previo al intercambio de la información cifrada, se realice un intercambio de clave. El asimétrico soluciona este problema al no requerir el intercambio previo de una clave confidencial.

Ahora bien, el criptosistema asimétrico resulta más costoso en tiempo de procesamiento, y además está basado en supuestos matemáticos no probados, en principios de complejidad computacional. Esto significa que un criptosistema asimétrico

[1] `https://sadio.org.ar`

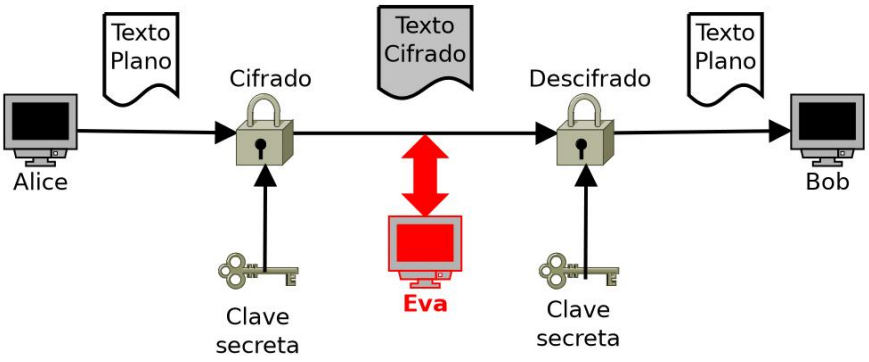

Figura 1: **Criptosistema**

se cree seguro para ataques realizados desde computadoras clásicas, pero se supone vulnerable al criptoanálisis cuántico.

Es por esto que sigue existiendo la necesidad de algoritmos y protocolos de intercambio de claves criptográficas que sean considerados seguros ante ataques realizados utilizando procesadores cuánticos.

2. Criptografía cuántica

La criptografía cuántica permite distribuir claves secretas sobre un canal de comunicación abierto, y aunque se habla de 'distribuir', más precisamente 'genera' dicha clave en forma aleatoria en ambos extremos. Las leyes de la física garantizan que un intento de espionaje o escaneo en un canal de comunicación abierto inyectará errores en la clave, y así el atacante o espía será detectado. Ese principio es la base de la criptografía cuántica, o intercambio/distribución de claves cuánticas QKE/QKD (Quantum Key Exchange/Distribution).

Un punto a tener en cuenta es que la criptografía cuántica no permite darle seguridad a la transmisión de información en la red, sino que solamente posibilita un intercambio de claves de forma segura. Una vez garantizada la seguridad de este intercambio, ambos extremos podrán compartir información cifrada utilizando esta clave en cifradores simétricos conocidos, y realizar la transmisión sobre un medio tradicional como el cobre. Un canal cuántico abierto entre dos nodos permitirá seguir generando claves para continuar transmitiendo datos.

La criptografía cuántica utiliza estados cuánticos, tales como la polarización de fotones individuales, para transmitir bits de información. No es posible hacer una copia de un estado cuántico desconocido sin modificarlo (Wootters y Zurek, 1982), por lo que un supuesto atacante no podría medir el estado de los fotones en el canal.

Esto está intrínsecamente relacionado con el principio de incertidumbre de Heisenberg: si alguien mide la posición precisa de una partícula, toda la información acerca de su momento se perderá. Es decir, el hecho de medir el estado de la partícula cuántica como un fotón, influye sobre ella alterándola. Un ejemplo simple sería la medición de la ubicación de un electrón dentro de una habitación aislada. Heisen-

berg notó que para poder localizar un electrón en el espacio debían hacerse rebotar fotones en él, pero cuando un fotón rebota en el electrón, si bien permite determinar su ubicación, también altera su momento y se pierde su estado original.

Supóngase el intercambio de claves entre dos extremos, Alice y Bob, la criptografía cuántica se basa en el intercambio de estados cuánticos en un medio físico entre estos dos extremos. Esto puede llevarse a cabo utilizando dos técnicas. Por un lado se puede usar un conjunto predefinido de estados cuánticos no ortogonales de una partícula única. Por otro lado se pueden realizar mediciones predefinidas en partículas entrelazadas, en cuyo caso la clave no existe durante la transmisión. La idea de usar estados cuánticos no ortogonales fue propuesta por Weisner en (Wiesner, 1983). En general los criptosistemas utilizan dos canales de comunicación entre Alice y Bob: uno cuántico, por ejemplo, una fibra óptica o el vacío, y otro tradicional, como una red cableada o inalámbrica. Por el medio cuántico se llevará a cabo el intercambio de claves, y por el medio tradicional el intercambio de los datos cifrados.

Considérense dos estados normalizados: $|0\rangle$ y $|1\rangle$, de modo que $\langle 0|1\rangle \neq 0$.

Ahora supóngase que existe una máquina de clonación de estados cuánticos que opera como sigue:

$$|0\rangle|B\rangle|m\rangle \rightarrow |0\rangle|0\rangle|m_0\rangle$$
$$|1\rangle|B\rangle|m\rangle \rightarrow |1\rangle|1\rangle|m_1\rangle$$

Donde 'B' es el estado inicial de una partícula que será un clon luego de la operación, y todos los estados se definen normalizados. Esta operación debe ser unitaria y debería preservar el producto interno, por lo que se requiere que se cumpla:

$$\langle 0|1\rangle = \langle 0|1\rangle\langle 0|1\rangle\langle m_0|m_1\rangle$$

Esto únicamente es posible cuando

- $\langle 0|1\rangle = 0$: cuando los dos estados son ortogonales.
- $\langle 0|1\rangle = 1$: cuando los dos estados son indistinguibles.
  Este caso no puede utilizarse para codificar dos bits diferentes, por lo que carece de utilidad.

Bennet y Brassard propusieron el uso de estados no ortogonales de fotones polarizados para distribuir claves criptográficas (Bennett y Brassard, 1984). Esto genera problemas a Eva al momento de realizar cualquier intento de medición que le permita distinguir entre estados no ortogonales $|0\rangle$ y $|1\rangle$ en el canal cuántico. Supóngase que Eva prepara su dispositivo de medición inicialmente en un estado normalizado $|m\rangle$ y quiere diferenciar un valor $|0\rangle$ de un $|1\rangle$ leído en el canal cuántico, y sin alterar dichos estados. Por ejemplo, podría implementar la siguiente operación unitaria:

$$|0\rangle|m\rangle \rightarrow |0\rangle|m_0\rangle$$
$$|1\rangle|m\rangle \rightarrow |1\rangle|m_1\rangle$$

La condición de unitaridad implica que $\langle 0|1\rangle = \langle 0|1\rangle\langle m_0|m_1\rangle$. Por ejemplo, el producto escalar $\langle m_0|m_1\rangle = 1$, el estado final de la medición, es el mismo en ambos

casos. Los dos estados no se modifican, pero Eva no gana información acerca del valor del bit codificado. Una medición más general que modifica los estados originales, de modo que $|0\rangle \to |0'\rangle$ y $|1\rangle \to |1'\rangle$ tiene la siguiente forma:

$$|0\rangle|m\rangle \to |0'\rangle|m_0\rangle$$
$$|1\rangle|m\rangle \to |1'\rangle|m_1\rangle$$

La condición de unitaridad da $\langle 0|1\rangle = \langle 0'|1'\rangle\langle m_0|m_1\rangle$. El valor mínimo del producto escalar $\langle m_0|m_1\rangle$ que corresponde con la situación en la que Eva tiene la mejor oportunidad de distinguir entre los dos estados, es obteniendo $\langle 0'|1'\rangle = 1$, y los dos estados en $|0\rangle$ y $|1\rangle$ se volverán el mismo luego de la interacción.

3. Protocolos

3.1. BB84

Stephen Wiesner en los años '70 propuso utilizar la polarización para codificar información (Wiesner, 1983). En 1984 Charles Bennett y Gilles Brassard se basaron en estos conceptos para plantear que los estados cuánticos que se propagan a través de un medio óptico pueden ser codificados de manera segura, y crearon el protocolo Bennett-Brassard 1984, más conocido como BB84, el primer protocolo de criptografía cuántica, y que sigue vigente en la actualidad (Bennett y Brassard, 1984) (Bennett et al., 1997). El experimento constó de pulsos de luz en el espacio, en una distancia de 40cm. Si bien no es práctico para realizar el intercambio de claves, representa los primeros pasos en criptografía cuántica.

Para analizar este protocolo de intercambio de claves es necesario disponer de un canal de comunicación cuántico, por ejemplo, una fibra óptica. Considérese pulsos de luz polarizada. Cada pulso contendrá un solo fotón. Se comenzará con polarización vertical u horizontal, respectivamente, $|\leftrightarrow\rangle$ y $|\updownarrow\rangle$ en notación de Dirac de mecánica cuántica.

Para transmitir la información se necesita un sistema de codificación. Supóngase que $|\updownarrow\rangle$ representa un 0 y $|\leftrightarrow\rangle$ un 1. Con este sistema, si Alice envía una serie de pulsos que representan el binario 10110, es decir:

$$|\leftrightarrow\rangle, |\updownarrow\rangle, |\leftrightarrow\rangle, |\leftrightarrow\rangle, |\updownarrow\rangle$$

Cuando Alice envía solamente los fotones $|\leftrightarrow\rangle$ o $|\updownarrow\rangle$, estará enviando los fotones polarizados en la base $\oplus$. Como la clave debe ser aleatoria, Alice enviará 0 o 1 con igual probabiliadd. Para detectar el mensaje, Bob usa un divisor de haz de polarización, o Polarization Beamsplitter (PBS), que transmite la polarización vertical y desvía la horizontal. Luego, utilza detectores de fotones en cada caso. Como se ve en la Fig. 2, la detección en el detector D0 (o D1) significará que Alice envió un 0 (o un 1). En este caso, se dice que Bob está midiendo en la base $\oplus$.

Los detectores no son perfectos, y se espera que algunos bits sean descartados en el proceso de transmisión, por lo que sólo se utilizará una fracción de los bits originales enviados por Alice. Por esto el sistema no sirve para transmitir mensajes, pero sí para intercambiar claves de cifrado.

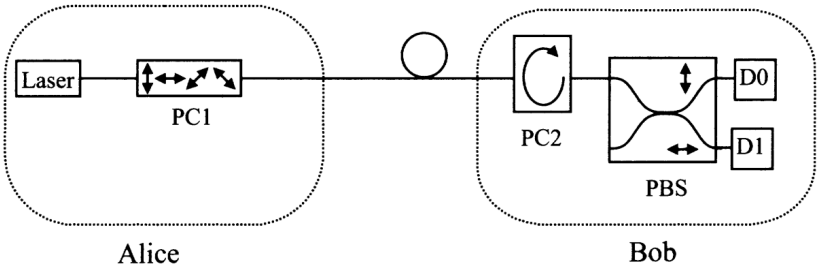

Figura 2: **Esquema de polarización y detección**

Hasta este punto el protocolo es inseguro. Eva, el atacante, podría medir los pulsos con un mecanismo similar al de Bob, y reenviar los mismos pulsos a Bob, pasando desapercibida, y conociendo la totalidad de la clave. Para evitar este problema, Alice añade otra elección aleatoria, además de los bits: una nueva base de polarización: diagonal, o $\otimes$. Ahora, se añade nueva codificación: $|\nearrow\rangle$ representa un 0 y $|\nwarrow\rangle$ un 1. Alice seleccionará una de las dos bases, $\oplus$ y $\otimes$, aleatoriamente con igual probabilidad. Bob también puede medir estos fotones rotando su configuración de PBS en 45^{o}.

Con este esquema, la seguridad se fundamenta en una propiedad de la mecánica cuántica: la indeterminación. Un fotón preparado en la base $\otimes$ y medido en la base $\oplus$ tendrá una probabilidad de $1/2$ de ser detectado por D0 o D1, y esto es totalmente aleatorio, ya que el fotón no incluye información que permita determinar con qué base medirlo.

Si Alice prepara un fotón en el estado $|\nearrow\rangle$ y Bob intenta medirlo en la base $\oplus$, será detectado en D0 o D1 con igual probabilidad. Esto no significa que la mitad de los fotones en un haz $|\nearrow\rangle$ están polarizados en la base vertical y la otra mitad en la horizontal, sino que el sistema se comporta como si eligiera aleatoriamente el camino a seguir, D0 o D1, cuando se mide.

Esto aplica también para Eva. Como Alice usa cada base de manera aleatoria, Eva no sabe qué base usar para medir. Cada vez que Eva mide con una base equivocada, obtendrá un resultado erróneo el 50 % de las veces. Otro punto importante es que Eva no puede saber cuándo un resultado de su medición es erróneo. Cuando recibe un fotón en el detector D0, no sabe si el fotón original estaba preparado en el estado $|\updownarrow\rangle$, o estaba preparado en el estado $|\nearrow\rangle$ o $|\nwarrow\rangle$ y simplemente *eligió* ir por el detector D0. Cabe resaltar aquí que es necesario que los fotones polarizados por Alice se envíen de a uno, ya que un haz de más de un fotón enviado en la base equivocada podría pasar por los detectores D0 y D1 a la vez, *diciéndole* a Eva que su base es equivocada, y permitiéndole descartar el fotón evitando considerar un fotón erróneo. Cuando Eva mide el estado del fotón, y éste es único, no tiene otra opción que considerarlo, y reenviarlo a Bob tal como lo dejó, en el estado medido. Esto generará errores en las mediciones de Bob.

Con estos conceptos base, se puede resumir un protocolo de intercambio de claves como sigue:

1. Alice genera una secuencia aleatoria de bits, y para cada bit selecciona aleatoriamente una base de polarización, $\otimes$ o $\oplus$, y la utiliza para polarizar cada bit.

Envía entonces los fotones codificados a Bob.

2. Por cada fotón recibido Bob selecciona también aleatoriamente una base de polarización y lo mide. Si para el fotón recibido se dio la coincidencia que el receptor eligió la misma base de polarización que el emisor, entonces el receptor obtendrá el mismo valor de bit que envió el emisor. Si la base elegida no es la misma que la utilizada por el emisor, el valor que obtendrá al decodificar el fotón será aleatorio. Con los bits recibidos genera la clave en bruto.

3. Bob ahora utiliza el canal público para informarle a Alice qué fotones logró detectar, y qué base utilizó para medirlos, pero no le dice el resultado de dichas mediciones. Alice le responde con las bases que ella utilizó para generar los fotones que Bob pudo medir. Si Alice y Bob usaron la misma base, los bits obtenidos serán iguales. Si usaron bases distintas, o Eva estuvo midiendo el canal, o incluso se perdieron o alteraron bits en el medio de transmisión, esos bits serán considerados erróneos. La clave que ambos arman con los bits correctos se denomina **clave tamizada**.

4. Alice y Bob finalmente realizarán algunas tareas de procesamiento para transformar su clave tamizada en una clave secreta. Estos pasos son similares en cualquier protocolo, y constan de:

   - Estimar la tasa de error del canal de comunicación.
   - Estimar la cantidad máxima de información que podría haberse filtrado a Eva.
   - Corregir los errores, reduciendo la información entregada a Eva.

   Los bits resultantes serán la clave secreta que ahora podrán utilizar Alice y Bob para cifrar información.

El Cuadro 1 plantea un ejemplo en el que se pueden apreciar los bits seleccionados por Alice, a saber, 01101001, las bases seleccionadas, y la polarización obtenida al codificar cada bit en cada base. Esos fotones polarizados son los que recibe Bob, que a su vez selecciona una base particular aleatoria para cada uno, lo mide, y obtiene sus propias decodificaciones en bits. Finalmente tanto Alice como Bob descartan aquellos bits para los que no coincidan las bases de polarización.

Cuadro 1: **Ejemplo de Intercambio BB84**

Bit de Alice	0	1	1	0	1	0	0	1
Base de Alice	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$
Alice envía	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\nwarrow\!\!\searrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\nwarrow\!\!\searrow\rangle$	$\lvert\swarrow\!\!\nearrow\rangle$	$\lvert\swarrow\!\!\nearrow\rangle$	$\lvert\leftrightarrow\rangle$
Base de Bob	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$
Medición de Bob	$\lvert\updownarrow\rangle$	$\lvert\swarrow\!\!\nearrow\rangle$	$\lvert\nwarrow\!\!\searrow\rangle$	$\lvert\swarrow\!\!\nearrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\swarrow\!\!\nearrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\leftrightarrow\rangle$
Clave Secreta	0		1			0		1

En ausencia de ruido o de cualquier error en la medición, una diferencia en tan solo un bit en esta comprobación indicaría que Eva se encuentra midiendo fotones

en el canal cuántico. En efecto, teniendo en cuenta el principio de incertidumbre de Heisenberg, la medición de un fotón por parte de Eva podría alterar sensiblemente su estado, revelando a Alice y Bob que alguien estuvo intentando interceptar la información intercambiada. En este caso Alice y Bob descartarán su clave secreta y comenzarán una nueva negociación. Además, dado que Eva no sabrá qué base se utilizó para codificar cada bit hasta después de que los nodos de la comunicación intercambien la clave tamizada, deberá adivinarla. Si Eva mide con la base incorrecta, por el mismo principio de incertidumbre la información codificada en la otra base se va a perder. Así, cuando el fotón llegue al destino Bob medirá un valor incorrecto el 50 % de las veces, y el 25 % de los bits medidos por Bob diferirán de los que codificó Alice (Rieffel y Polak, 2000).

Debe agregarse que los esquemas de polarización son relativamente fáciles de implementar en el espacio, donde la polarización se conserva, pero en una fibra óptica, en la que incurren otros factores propios del medio físico, resulta más complejo. Como alternativa pueden definirse sistemas de criptografía cuántica basados en codificación de fase (Ekert y Bouwmeester, 2000)

3.2. B92

En 1992 el mismo Bennett propuso en una investigación denominada *Criptografía cuántica usando cualquier par de estados no ortogonales* lo que es, en esencia, una versión simplificada de su paper sobre el protocolo BB84 (Bennett, 1992). Esta nueva versión se diferencia de la anterior en que son necesarios únicamente dos estados ortogonales que posibilitan cuatro polarizaciones en BB84.

Como se puede ver en la Fig. 3, Alice selecciona las bases entre la horizontal y la diagonal a 45°. Los bits polarizados horizontalmente serán 0's, los polarizados diagonalmente serán 1's. Alice envía los fotones polarizados a Bob, que los mide con base aleatoria. Las bases elegidas por Bob serán ortogonales a las de Alice, es decir, Bob medirá con base vertical a $90^{\underline{o}}$ y diagonal a $-45°$. Alice debe avisar a Bob cuándo envía cada fotón. Si Bob detecta el fotón, significa que usó una base no ortogonal a la de Alice para medirlo, y obtiene el mismo valor que Alice, 0 o 1. Por ejemplo, si Bob detecta un fotón midiendo en la base vertical a 90°, significa que Alice envió un fotón polarizado diagonalmente en 45°, ya que si Alice lo hubiera polarizado en la base horizontal, la medición vertical anularía al fotón por la condición de la mecánica cuántica denominada "borrado"(*erasure* en inglés) (Bruss et al., 2007). Bob asigna entonces 1 a los fotones que puede medir en la base vertical, y 0 a los que puede medir en la base diagonal a $-45°$.

Figura 3: **Polarización en B92 - Codificación de 2 estados**

3.3. E91

Existen algunas variantes del protocolo BB84, pero por razones de extensión únicamente se considerará una de las más estudiadas, una versión simplificada de E91, diseñado por Artur Eckert en 1991 (Eckert, 1991). Este es un sistema en el que hay una sola fuente que emite partículas entrelazadas (por ejemplo, fotones). Esta fuente puede ser externa, o puede ser uno de los dos extremos de la comunicación. La ventaja de E91 es que genera la clave aleatoriamente de manera natural, ya que es imposible determinar la polarización inicial de los fotones.

Supóngase una fuente que emite pares de fotones entrelazados de este tipo:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle)$$

Los fotones se separan y son enviados a los dos destinatarios de la comunicación, Alice y Bob, que los miden y registran su resultado en una de tres bases obtenidas de rotar la base $\oplus$ en el eje z en ángulos predefinidos:

- Ángulos de rotación de Alice: $\phi_1^a = 0$, $\phi_2^a = \frac{1}{4}\pi$ y $\phi_3^a = \frac{1}{8}\pi$
- Ángulos de rotación de Bob : $\phi_1^b = 0$, $\phi_2^a = -\frac{1}{8}\pi$ y $\phi_3^a = \frac{1}{8}\pi$

Los usuarios eligen una de sus bases de manera aleatoria, de modo que por cada medición pueden obtener dos resultados posibles: $+1$ (el fotón fue medido en el primer estado de la base elegida), y -1 (el fotón fue medido en el otro estado posible de la base elegida).

Puede calcularse el **coeficiente de correlación** de las mediciones realizadas por Alice en la base rotada por ϕ_i^a y por bob en la base rotada por ϕ_j^b como sigue:

$$E(\phi_i^a, \phi_j^b) = P_{++}(\phi_i^a, \phi_j^b) + P_{--}(\phi_i^a, \phi_j^b) + P_{+-}(\phi_i^a, \phi_j^b) + P_{-+}(\phi_i^a, \phi_j^b)$$

Donde $P_{\pm\pm}(\phi_i^a, \phi_j^b)$ representa la probabilidad de haber obtenido el resultado ± 1 con la base definida por ϕ_i^a, y ± 1 con la base definida por ϕ_j^b.

Considérese ahora la siguiente regla cuántica:

$$E(\phi_i^a, \phi_j^b) = -\cos[2(\phi_i^a - \phi_j^b)]$$

Para los dos pares de bases con la **misma orientación** (ϕ_1^a, ϕ_1^b y ϕ_3^a, ϕ_3^b) la mecánica cuántica predice que la anticorrelación total del resultado obtenido por Alice y Bob será:

$$E(\phi_1^a, \phi_1^b) = E(\phi_3^a, \phi_3^b) = -1$$

Se puede definir la cantidad S compuesta por los coeficientes de correlación para los que Alice y Bob usaron **diferentes orientaciones**:

$$S = E(\phi_1^a, \phi_3^b) + E(\phi_1^a, \phi_2^b) + E(\phi_2^a, \phi_3^b) - E(\phi_2^a, \phi_2^b)$$

Este S es el mismo que el propuesto por el teorema generalizado de Bell, y conocido como la desigualdad de CHSH:

$$S = -2\sqrt{2} \tag{A}$$

Al finalizar la transmisión, Alice y Bob pueden anunciar públicamente la orientación de sus polarizaciones elegidos para cada partícula, y dividir las medidas en dos grupos:

1. Un grupo con las medidas para las que las bases de medición fueron distintas.

2. Otro grupo con las medidas para las que las bases fueron las mismas.

Luego, Alice y Bob revelan públicamente los resultados de las mediciones del primer grupo. Esto les permite calcular el valor de S, de modo que si las partículas no fueron perturbadas por una medición de Eva, deberían reproducir el resultado de la ecuación A. Esto asegura que los valores medidos en el segundo grupo estén correlacionados, y que pueden ser convertidos en una clave secreta.

Un espía como Eva no podría obtener nada de información desde las partículas mientras están en tránsito en el canal cuántico porque no hay nada de información codificada aquí. La información será intercambiada luego de Alice y Bob hayan verificado la legitimidad de su clave tal y como se mencionó. Eva, al no conocer las bases utilizadas por Alice y Bob para medir las partículas de su clave, no podrá interactuar sin perturbar los resultados de las polarizaciones, lo que producirá una reducción del valor de S, y será detectada por los extremos legítimos de la comunicación. El teorema de Bell puede de esta forma exponer al atacante.

Referencias

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121. Publisher: APS.

Bennett, C. H., Bernstein, E., Brassard, G., y Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523.

Bennett, C. H. y Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11.

Bruss, D., Erdélyi, G., Meyer, T., Riege, T., y Rothe, J. (2007). Quantum cryptography: A survey. *ACM Computing Surveys (CSUR)*, 39(2):6–es. Publisher: ACM New York, NY, USA.

Eckert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661. Publisher: APS.

Ekert, A. y Bouwmeester, D. (2000). *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer.

Rieffel, E. y Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys (CSUR)*, 32(3):300–335. Publisher: ACM New York, NY, USA.

Wiesner, S. (1983). Conjugate coding. *ACM Sigact News*, 15(1):78–88. Publisher: ACM New York, NY, USA.

Wootters, W. K. y Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886):802–803. Publisher: Springer.