Criptografía cuántica

Mauricio Vargas Contreras[6]

Instituto de Matemática y Física
Universidad de Talca

¿En qué pensamos cuando alguien menciona la palabra criptografía?…. En algo oculto, secreto, algún código, ceros y unos, en el film *Una mente brillante* o *El Código Da Vinci*, etc., se nos vienen un sin fin de cosas en que pensar sobre qué es o qué es lo que se hace en criptografía, pero que pasa si alguien menciona la frase criptografía cuántica…. ¿pensamos en lo mismo….secretos, ceros y unos, en qué?

El objetivo de esta nota es dar una mirada básica a la base de la criptografía cuántica, cómo funciona, cómo se relaciona con la criptografía denominada clásica y dejando al lector el compromiso de indagar sobre los fundamentos matemáticos y físicos con los cuales se formaliza este concepto.

Criptografía

El objetivo principal de la criptografía es la transmisión de información de forma segura, es decir, que sólo pueda acceder a ella su legítimo destinatario (Bob). La pieza fundamental de los sistemas criptográficos actuales reside en un parámetro conocido como clave (K), que consistirá en cualquier cadena aleatoria de bits, suficientemente larga, donde la seguridad de un sistema de cifrado reside enteramente en mantener en secreto esta clave.

La pregunta que surge ahora es ¿cómo se ponen de acuerdo el emisor (Alice) y el receptor (Bob) sobre la clave que van a utilizar?

Para ello deben encontrar una forma segura de comunicarse para intercambiar este dato. Esto es lo que se conoce como "el problema de la distribución de claves". Como solución a este dilema aparecieron los "sistemas de cifrado de clave pública". En éstos los usuarios utilizan dos claves, una para cifrar el mensaje y otra para descifrarlo. Todo el mundo puede tener acceso a una de las claves (denominada pública) para cifrar un mensaje, pero sólo su legítimo destinatario tiene la otra clave (llamada privada) para descifrarlo. Los sistemas de cifrado de clave pública más populares, como RSA (Rivest-Shamid-Adleman), basan su seguridad en la dificultad de factorizar números enteros muy grandes. Pero esto no sería un obstáculo para un computador cuántico que ejecutase el algoritmo de factorización de Shor (1994-Peter Shor, matemático que en ese entonces trabajaba en los laboratorios de AT&T, actualmente es profesor en MIT).

[6] mvargas@utalca.cl

Criptografía Cuántica

El método de distribución de claves mediante tecnología cuántica se basa en propiedades de los fotones, las partículas que forman la luz. Cuando un fotón viaja por el espacio vibra. Cuando hay muchos fotones en juego, cada uno puede vibrar en ángulos diferentes. Este ángulo de vibración se conoce como **polarización del fotón.** Al encender una ampolleta se están creando fotones con todas las polarizaciones, vibrando en todos los ángulos posibles, pero podemos seleccionar fotones con una polarización determinada. Esto no es algo nuevo; cuando nos ponemos unas buenas gafas de sol, lo que está sucediendo es que el cristal actúa como un filtro que sólo deja pasar los fotones que están polarizados en un ángulo determinado.

Como funciona la distribución de claves cuánticas

Supongamos que Alice y Bob quieren intercambiar una clave, y Eve quiere espiar esta comunicación (figura 1).

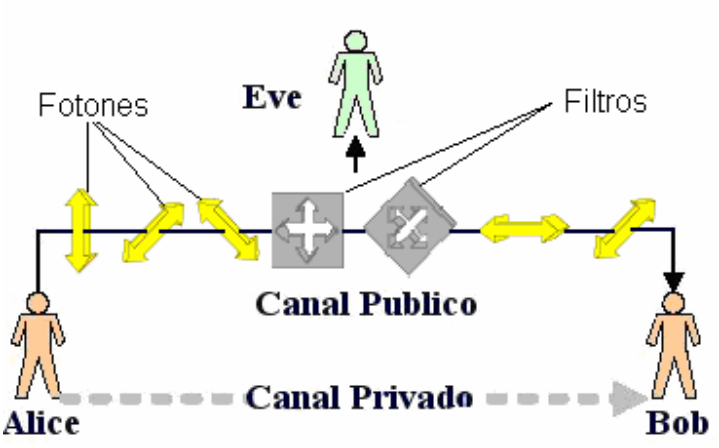


Figura 1.

Alice quiere acordar una clave con Bob para poder cifrar mensajes futuros mediante el envío de fotones polarizados, utilizando una fuente de luz y haciendo pasar los fotones por un filtro polarizador. De este modo, los fotones que envíe tendrán la polarización que ella desee. Para ello utilizará dos filtros polarizadores orientados según ángulos de 90º y 45º, y los fotones que envíe con estas polarizaciones representarán los bits 0 y 1 respectivamente. En el otro extremo Bob tiene otros dos filtros con orientaciones de 0º y 135º (ver tabla 1).

Filtros de Alice	90° (codifica: 0)	45° (codifica: 1)
Filtros de Bob	0°	135°

Tabla 1.

Para transmitir la clave, Alice manda a Bob una serie de fotones polarizados, eligiendo para cada uno un filtro al azar; es decir, unas veces enviará un fotón polarizado 90º y otras 45º. Como resultado le enviará una cadena aleatoria de 0s y 1s.

Por su parte Bob intentará medir la polarización de cada fotón que le llega, eligiendo también al azar entre sus dos filtros. En consecuencia, unas veces utilizará el filtro de 0º y otras el de 135º.

¿Cómo se comportan los fotones polarizados de Alice cuando se encuentran con los filtros de Bob?

Existen tres posibilidades:

- Cuando un fotón llegue a un filtro con la misma orientación que su polarización, lo atravesará siempre. (Ver figura 2a)

- Si un fotón se encuentra con un filtro con una orientación perpendicular a su polarización no pasará **nunca**; quedará bloqueado (ver figura 2b y tabla 2)

- Si el fotón se encuentra con un filtro orientado diagonalmente respecto a su polarización (formando un ángulo de 45º con ésta; por ejemplo, un fotón polarizado 90º que se encuentra con un filtro de 135º), tendrá un 50% de posibilidades de atravesarlo y otro 50% de quedar bloqueado. Esto significa que si lanzamos muchos fotones hacia un filtro, según las condiciones que acabamos de describir, aproximadamente la mitad de ellos lo atravesará, la otra mitad no (ver figuras 2c y 2d y tabla 2). Pero no hay forma de saber qué le sucederá a un fotón individual. Que pase o no es algo completamente aleatorio.

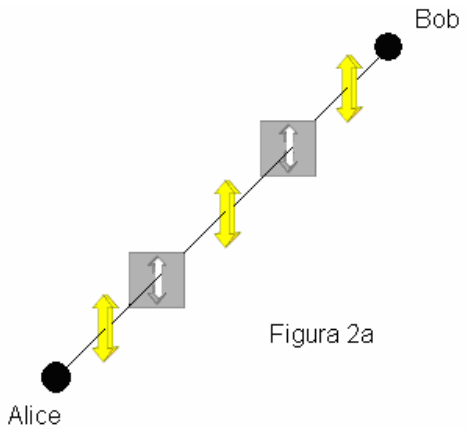


Figura 2a

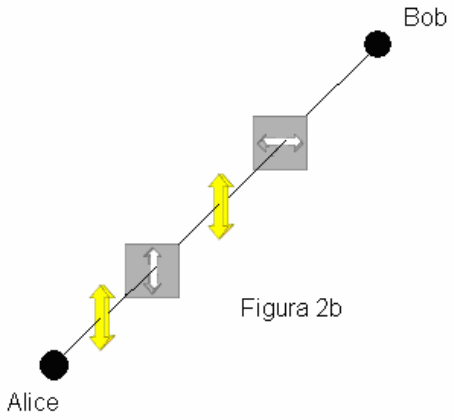


Figura 2b

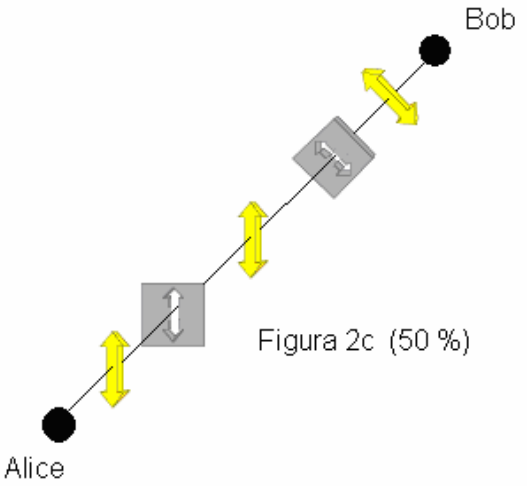


Figura 2c (50 %)

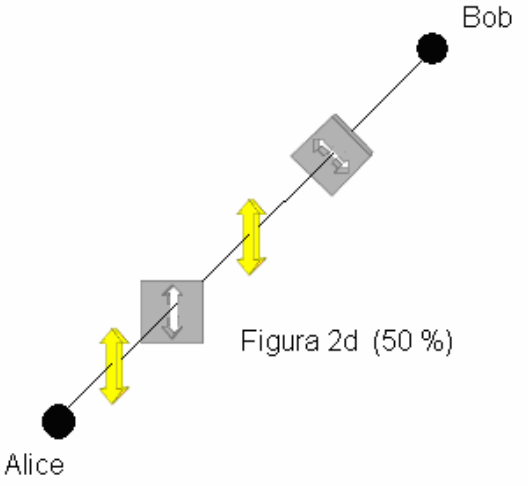


Figura 2d (50 %)

Polarización del fotón de Alice	90°	90°	45°	45°
Filtro que utiliza Bob	0°	135°	0°	135°
¿Atraviesa el filtro de Bob?	Nunca	50 % Si 50 % No	50 % Si 50 % No	Nunca

Tabla 2.

Analicemos un ejemplo concreto. Si Bob elige su filtro de 135º para medir un fotón que le llega de Alice, pueden ocurrir dos cosas:

- **El fotón no pasa el filtro:** Entonces, y teniendo en cuenta lo dicho más arriba, Bob no sabrá si Alice mandó un fotón polarizado 45º (que codifica un bit 1) y que siempre será bloqueado por su filtro, o si mandó un fotón polarizado 90º (que codifica un bit 0), en cuyo caso había una probabilidad del 50% de que su filtro de 135º lo bloquease (ver figura 2d).

- **El fotón pasa el filtro:** Entonces Bob sabrá, con certeza absoluta, que Alice mandó un fotón polarizado 90º, pues es la única polarización que tenía alguna posibilidad (50%) de atravesar su filtro de 135º. Luego si un fotón pasa su filtro, Bob puede estar seguro de que Alice le habrá mandado un fotón polarizado 90º que codifica un 0 (cero). Por el mismo razonamiento, si Bob utiliza un filtro de 0º y un fotón de Alice lo atraviesa, tendrá la certeza de que ésta lo mandó con una polarización de 45º y que por tanto codifica un bit 1 (uno). Esto se resume en el siguiente cuadro:

Si un fotón atraviesa el filtro de 135°	de Bob, entonces sabrá que Alice le envió un bit 0
Si un fotón atraviesa el filtro de 0°	de Bob, entonces sabrá que Alice le envió un bit 1

Tabla 3.

Por tanto, cuando Alice envía fotones polarizados a Bob, éste será capaz de determinar, para los que atraviesen sus filtros, el valor del bit que representan. La tabla 4 muestra un ejemplo de esta comunicación para 6 fotones.

Bit que quiere enviar Alice	0	0	1	1	0	1
Filtro polarizador de Alice	90°	90°	45°	45°	90°	90°
Filtro polarizador de Bob	135°	0°	135°	0°	135°	0°
Resultado	Pasa	No	No	Pasa	No	Pasa
Bit de la clave	0	———	———	1	———	1

Tabla 4.

Luego en este caso sencillo, la clave sería: **011** (Nótese que Alice envía los fotones 1º y 5º con la misma polarización (90º), y se encuentran con el mismo filtro de Bob, el de 135º. Sin embargo, uno pasa y el otro no. Este es un ejemplo del comportamiento cuántico que se mencionó anteriormente). Si Alice mandase 1 millón de fotones a Bob, con polarizaciones elegidas al azar entre las dos de las que dispone (90º y 45º), y a su vez Bob los va midiendo según le llegan eligiendo, también al azar, cuál de sus filtros va a utilizar (0º 135º), entonces, aproximadamente tres de cada cuatro fotones (750.000) quedarán bloqueados y no pasarán los filtros de Bob, pero al mismo tiempo sabrá con certeza qué bit codifica cada uno de los restantes fotones que pasan sus filtros; uno de cada cuatro (250.000). Estos bits formarán la clave con la cual se podrá cifrar los mensajes entre ellos. Bob puede decirle a Alice (por teléfono) **qué fotones son los que han pasado sus filtros** (por ejemplo, los que, según el orden en que Alice los envió, ocupan las posiciones, 7ª, 129ª, 7.315ª, etc.), **pero no le dice qué filtro utilizó para medirlos**, es decir, **no revela la polarización de esos fotones**. Por tanto, si alguien está espiando su conversación no conseguirá ninguna información sobre la clave. Y lo que es aún más importante, **si un espía (Eve) interceptase los fotones que viajan entre Alice y Bob, su presencia sería detectada**. Veamos por qué. Supongamos que Alice manda a Bob un fotón polarizado 90º, que

representa un bit 0 (cero), y que Eve, que dispone de los mismos filtros para medir que Bob, lo intercepta utilizando un filtro de 135º. Si el fotón queda bloqueado Eve no tiene forma de saber si es porque su polarización era de 45º (y por tanto nunca podría haber pasado su filtro) o si era de 90º y pertenece al 50% que queda bloqueado. Eve puede aventurar que era un fotón polarizado 45º, preparar otro fotón con esta polarización y reenviarlo a Bob. Si resulta que éste lo mide con un filtro de 0º, el fotón reenviado por Eve tendrá un 50% de probabilidades de pasar y en este caso Bob lo interpretará como un bit 1 (uno), justo lo contrario de lo que le envió Alice (ver tabla 5).

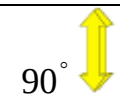
Bit que quiere enviar Alice	0
Filtro polarizador de Alice	 90°
Filtro polarizador de Eve	 45°
Filtro polarizador de Bob	0° 
Resultado	**Pasa**
Bit que registro Bob	1

Tabla 5.

Esta discrepancia es la que pone a Eve al descubierto, ya que, según este procedimiento, si nadie estuviese interceptando los fotones, Bob sólo puede obtener: O bien nada (cuando sus filtros bloquean los fotones que le llegan) o bien el resultado correcto con certeza absoluta, pero en ningún caso resultados opuestos a los de Alice. De esta manera, para saber si Eve estuvo espiando, Alice y Bob comprueban si hay discrepancias de este tipo. Para ello, una vez que han terminado la transmisión de fotones (y saben cuáles son los que han proporcionado a Bob alguna información) y cada uno tiene apuntada su cadena de 0s y 1s, escogen unos cuantos al azar y se comunican por teléfono sus valores. Si hay alguna discrepancia, sabrán inmediatamente que Eve estuvo espiando. Si no, podrán utilizar esa cadena de 0s y 1s como clave para cifrar sus comunicaciones futuras, después de tirar a la basura los bits que han utilizado para buscar errores, ya que para compararlos utilizaron un medio inseguro como el teléfono. Siempre existe la posibilidad de que Eve tenga suerte y tras interceptar y medir un fotón de Alice, lo retransmita a Bob con la polarización correcta; la que Alice preparó. Al fin y al cabo, tiene la misma probabilidad de acertar que de errar. Si Alice y Bob utilizasen el bit que codifica este fotón para el proceso de búsqueda de discrepancias, no notarían nada y no les ayudaría a descubrir a Eve. Pero si Alice y Bob hacen su comprobación de discrepancias utilizando más y más bits, las oportunidades de Eve de pasar desapercibida serán prácticamente nulas. Por emplear una analogía sencilla, sería como adivinar todos los números que van a salir en un sorteo de lotería y además en qué orden. El resultado final es que Alice y Bob tienen una clave segura para cifrar sus mensajes. Este es el método de distribución de claves más seguro jamás concebido. La razón de esto es sencilla: para que un posible espía consiguiese información sobre la clave, no bastaría que fuese capaz de vencer un complicado algoritmo o resolver un ingenioso problema matemático; tendría de saltarse las leyes de la física.

Al contrario de lo que ocurre con los computadores, ya existen productos comerciales de criptografía cuántica. Empresas como la norteamericana MagiQ anunció la puesta en el mercado del primer sistema criptográfico comercial basado en principios cuánticos, y fue seguida rápidamente por su homóloga la suiza ID Quantique. Actualmente, la tecnología disponible está limitada a conexiones punto-a-punto y a distancias máximas de 50 Km. El precio de uno de estos sistemas es hoy en día es casi astronómico (la unidad de MagiQ cuesta entre 50 y 100 mil dólares). Estas unidades son una combinación de técnicas de criptografía cuántica y criptografía tradicional.

Se dice que una de las consecuencias prácticas de la criptografía cuántica, es que por primera vez se dispone de un medio para transmitir información de forma segura. Al buscar información para estas notas encontré que un grupo de investigadores de MIT dice lo contrario, incluso cuentan con pruebas fehacientes de que este tipo de tecnología necesita muchas pruebas antes de ponerla a disposición del mercado.

Uno de los ámbitos fundamentales de la criptografía, ya sea clásica o cuántica es su aplicabilidad, es decir, que sus algoritmos sean aplicables computacionalmente. Entonces ¿no se debería pensar primero en desarrollar computadores cuánticos, antes de poder afirmar que la criptografía cuántica es la más segura?. David Mermin de la Universidad de Cornell expresa esto de la siguiente manera: “Sólo un incauto podría predecir que no habrá computadores cuánticos útiles en el año 2.050, pero sólo un incauto podría decir los habrá”.

Creo que es imposible decir hasta dónde se puede llegar. Como sucede en cualquier área de la ciencia, desarrollos que hoy parecen prometedores no llevarán a ninguna parte y al mismo tiempo, como ya ha ocurrido en el pasado, nuevas ideas conducirán a conocimientos y aplicaciones que hoy no podemos imaginar.

Bibliografía.

1. www.idquantique.com
2. www.magiqtech.com
3. “The Physics of Quantum Infomation”, Dirk Bouwmeester, Artur Ekert y Anton Zeilinger. Spinger (2000).
4. “A Course in Number Theory and Cryptography”, Neal Koblitz. Spinger (2000).
5. “Introduction to Quantum Cryptography”, Gustavo Rigolin y Andres Rieznik. http://lanl.arxiv.org/PS_cache/physics/pdf/0511/0511120.pdf.
6. “Why Quantum Cryptography”, Kenneth Paterson, Fred Piper y Rudiger Schak. http://lanl.arxiv.org/PS_cache/quant-ph/pdf/0406/0406147.pdf.
7. “Shor’s Factoring Algorithm and Modern Cryptography”, Edward Gerjuoy. http://lanl.arxiv.org/PS_cache/quant-ph/pdf/0411/0411184.pdf.
8. “The fundamental problem of quantum cryptography”, Marcin Pawlowski y Marek Czachor. http://lanl.arxiv.org/PS_cache/quant-ph/pdf/0412/0412058.pdf.
9. Criptografía Cuántica y Computación Cuántica, Ignacio Cirac, Instituto Max-Planck de Óptica Cuántica, Garching (Alemania)
10. Fast Ideal Arithmetic in Quadratic Fields, Reginald Sawilla, UNIVERSITY OF CALGARY.

11. Criptografía Cuántica, Gregoria Blanco y Ángeles Martínez, Dpto. Matemática Aplicada, Universidad Politécnica de Madrid.
12. Criptografía Cuántica, Grupo de Física Teórica, Facultad de Ciencias, Universidad Autónoma de Barcelona.
13. La criptografía Cuántica, ¿realidad o ficción?, Fausto Montoya, Departamento Tratamiento de la información y Codificación, Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas. Madrid, España.
14. Computación Y Criptografía Cuánticas: Retos para la Seguridad en la Sociedad de la Información, Alberto Villafranca Ramosa, Jefe de Servicios de Sistemas de Información, Ministerio de la presidencia, España.
15. Tecnología de la Información Cuántica, Juan José García Ripoli y J. Ignacio Cirac, Instituto Max-Planck de Óptica Cuántica, Garching (Alemania)