XVI Semana de la Enseñanza de la Física
Memorias SEF **Vol. 2**: 1–6 (2013)

Elementos conceptuales para abordar el uso de fotones polarizados para la distribución de claves criptográficas

Andrés Vargas[1] John Suárez[2]

[1,2] *Grupo de Investigación en Física e Informática (Fisinfor), Universidad Distrital Francisco José de Caldas. Bogotá, Colombia.*

Recibido: xxxx Aceptado: xxxx Publicado: xxxx

Resumen. A partir de una revisión bibliográfica se aborda la pregunta, ¿Cómo es posible la distribución segura de claves criptográficas utilizando fotones polarizados?, para ello se realiza una breve descripción de los conceptos usados en procesos de cifrado y los principios físicos que permiten revelar la presencia de un escucha en un canal de comunicación, utilizando el problema de Allice, Bob y Eva.
Descriptores: Criptografía cuántica, fotones polarizados, distribución segura de claves.

1. Introducción

La comunicación segura entre dos partes ha representado una necesidad histórica. El cifrado permite obfuscar la información de tal manera que ésta sólo sea inteligible a las partes involucradas (Atreya, 2006). La fortaleza o debilidad de algoritmos de cifrado está determinada por el cálculo de tiempo teórico que es necesario para descubrir la clave de cifrado (por medio de ensayo-error [1]), entre más tiempo de procesamiento sea requerido para encontrar la clave de cifrado, más seguro será considerado el algoritmo. No obstante, el avistamiento de principios cuánticos que aumentan exponencial y/o cuadráticamente la capacidad de procesamiento de las máquinas actuales (Wang, 2012) hace que algoritmos que antes eran considerados seguros ahora presenten vulnerabilidades, en el sentido que se cuenta con la capacidad de cálculo necesaria para descifrar la información.

Fundamentos de la física clásica presentan la posibilidad de reproducir copias exactas de estados lo que posibilita a un escucha inmiscuirse en la comunicación entre dos partes sin notar su presencia. Por otro lado, aspectos de la mecánica cuántica impiden éste tipo de copias exactas de estados cuánticos, debido principalmente al problema de la medición: la medición de un estado cuántico produce un colapso de la función de onda alterando el sistema medido. Esta propiedad de sistemas cuánticos puede ser explotada con el fin de revelar la presencia de un escucha en una comunicación segura, sin comprometer la confidencialidad de la información.

1.1. Tipos de cifrado

Existen procesos de cifrado simétrico y asimétrico, cuya diferencia fundamental radica en que el primero utiliza una misma clave para realizar tanto el proceso de cifrado como el de descifrado; mientras que en el

amvargash@correo.udistrital.edu.co
jfsuarezp@correo.udistrital.edu.co
[1] método conocido como fuerza bruta

cifrado asimétrico se utiliza una clave para el proceso de cifrado y otra para el proceso de descifrado [2]. Atreya (2006) realiza una comparación entre las dos alternativas de cifrado, mostrando las ventajas y desventajas que presenta la una frente a la otra.

En procesos de cifrado simétrico se presenta un problema fundamental: se debe garantizar que la clave de cifrado/descifrado sólo sea distribuida a las partes involucradas en la comunicación segura. Ya que en caso de que un tercero (un escucha) obtenga esa clave, la información dejaría de ser confidencial.

2. Fotones Polarizados

Se dice que una onda electromagnética no está polarizada cuando el campo eléctrico oscila en todas las direcciones de manera aleatoria. En consecuencia, cuando se tiene una onda EM cuyo campo eléctrico oscila en un sólo sentido (por ejemplo, de arriba hacia abajo o de izquierda a derecha) o con un patrón determinado (en el caso de la polarización circular) se habla de una onda EM polarizada.

Un polarizador es un instrumento que permite establecer una polarización determinada de una fuente de radiación EM. Una onda EM polarizada, contará con paquetes de energía polarizados (fotones polarizados).

Del campo eléctrico pueden ser obtenidas las componentes en una base ortogonal. Así, se habla de una base rectilínea (representada por el símbolo +) cuando la base es formada con un eje horizontal y uno vertical, se habla de base diagonal (símbolo x) cuando se gira 45° una base rectilínea. Éstas bases pueden ser utilizadas para establecer bits de información. Por ejemplo, un fotón polarizado horizontalmente representará el 0 mientras que un fotón polarizado verticalmente representará el 1, de igual forma, un fotón polarizado a 45° representará 0 y a 135° representará 1.

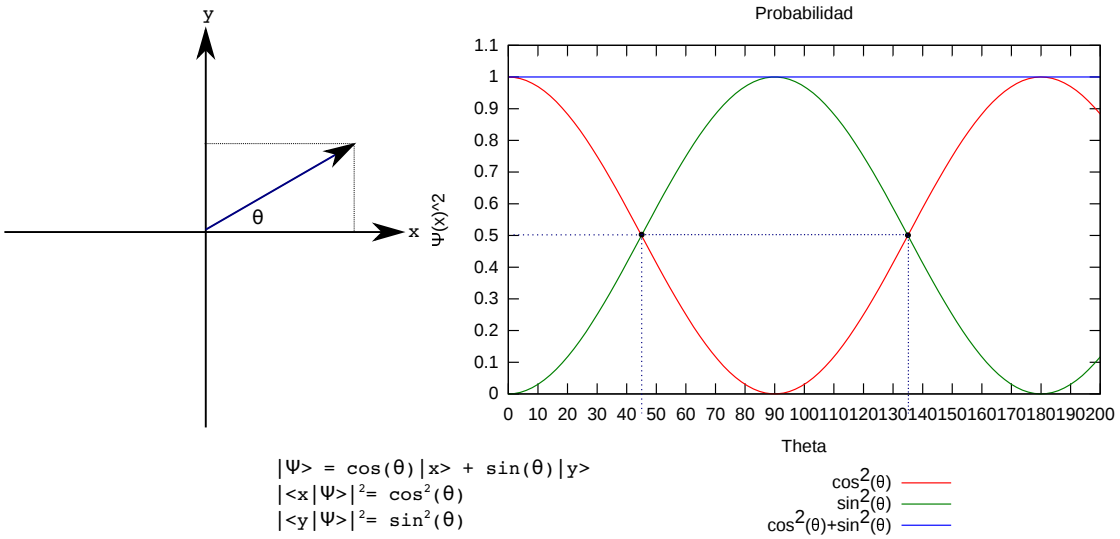

Figura 1: Análisis de las componentes de la función de onda

Si una onda polarizada se encuentra con un polarizador, éste puede ocasionar una disminución de la intensidad de la onda. Debido a que el polarizador realizará una descomposición del campo eléctrico y transmitirá la componente paralela al ángulo de polarización del instrumento, mientras que la otra componente puede ser reflejada o disipada.

la figura 1 muestra que si un fotón está polarizado con un angulo θ respecto al eje horizontal, se tendrá una probabilidad de $\cos^2\theta$ de medir el fotón como polarizado horizontalmente y una probabilidad de $\sin^2\theta$ de medir el fotón polarizado verticalmente. Si se utiliza para la medición un polarizador con una base rectilínea.

[2] En el cifrado asimétrico la clave de cifrado (clave pública) está matemáticamente vinculada a la clave de descifrado. Sin embargo, es necesario garantizar que la obtención de la clave de descifrado a partir de la clave de cifrado sea una actividad computacionalmente exigente, al pundo de ser imposible de realizar (Simmons, 1979).

Un caso especial se presenta si el fotón tiene una polarización de 45° o 135°, si se mide con una base rectilínea la medición será aleatoria (existe un 50 % de probabilidad de obtener polarización vertical y 50 % de obtener polarización horizontal). Ya que éste ángulo es relativo, sucede lo mismo si dejando intacto el vector $|\Psi\rangle$ se gira la base (los ejes coordenados). El proceso de descomposición es análogo al proceso de medición con un polarizador, la base representaría el eje coordenado.

3. Allice, Bob y Eva, desde la física clásica

Allice y Bob desean compartir información a través de un canal inseguro [3] una clave (que después será usada para cifrar simétricamente sus comunicaciones), Allice y Bob utilizan dos cables que unen sus laboratorios, a través de una fuente de voltaje Allice comunica a Bob una secuencia de unos y ceros, estableciendo de antemano qué voltaje representará 0 y qué voltaje representará 1, así como la frecuencia en la que son enviados los bits.

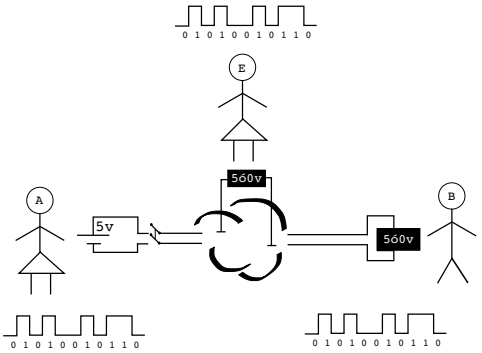

Figura 2: Ejemplo de un transporte de bits clásico entre Allice y Bob mientras Eva realiza una escucha

Bob realiza un proceso de medición del voltaje, y determina la secuencia que fue envíada por Allice.

Si Eva logra tener acceso a los dos cables, bastará con que conecte un voltímetro para obtener la misma secuencia, y lograr interceptar la clave (la secuencia de unos y ceros) que posteriormente utilizará para descifrar la información que Allice y Bob se comunican.

Eva puede realizar esta medición sin que Allice o Bob noten su presencia debido a que esta no perturbará la información transmitida.

4. Allice, Bob y Eva, utilizando fotones polarizados

Allice y Bob utilizan un canal inseguro para transmitir la clave, pero esta vez utilizan otro método basado en los principios de la mecánica cuántica: fotones polarizados.

Allice escoje una secuencia de unos y ceros que desea transmitir a Bob, luego de ello escoje de manera aleatoria una secuencia de bases con la cual desea transmitir la información. Por ejemplo, Allice enviará la secuencia 100101 a Bob y para ello utilizará la secuencia de bases x+xx+x, una base aleatoria por cada bit que desee transmitir. De éste modo, requerirá enviar un fotón polarizado a 135° (1 en la base diagonal), luego un fotón polarizado horizontalmente (0 en la base rectilínea), luego uno a 45°, y así sucesivamente.

Luego Bob en su laboratorio, escoje también de manera aleatoria una base con la cual realizar la medición. Por ejemplo, escoje la base xxx++x, al realizar la medición sobre el primer bit obtendrá 1 debido a que está codificado con la misma base de Allice, es decir, la probabilidad de medir un fotón polarizado a 135° (lo que envió Allice) con una base diagonal (con la que mide Bob) es 1:

[3] Un medio en el que se da la transimisión de un mensaje y en el que existe la posibilidad de una interceptación por parte de un escucha.

$$\begin{array}{rcl} |\psi\rangle & = & |\nearrow\rangle \\ \langle\nearrow|\psi\rangle & = & \langle\nearrow|\nearrow\rangle + \langle\nearrow|\nwarrow\rangle \\ |\langle\nearrow|\psi\rangle|^2 & = & 1 \end{array} \tag{1}$$

Para el siguiente bit la base que utilizó Allice es diferente. Allice usó una base rectilínea y Bob midió la polarización del fotón utilizando una base diagonal. En éste caso Bob puede obtener 1 (fotón polarizado a 135°) con 50 % de probabilidad:

$$\begin{array}{rcl} |\psi\rangle & = & |\updownarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle \\ \langle\nwarrow|\psi\rangle & = & \langle\nwarrow|\frac{1}{\sqrt{2}}|\nearrow\rangle + \langle\nwarrow|\frac{1}{\sqrt{2}}|\nwarrow\rangle \\ |\langle\nwarrow|\psi\rangle|^2 & = & \frac{1}{2} \end{array} \tag{2}$$

y 0 (fotón polarizado a 45°) con 50 % de probabilidad:

$$\begin{array}{rcl} |\psi\rangle & = & |\updownarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle \\ \langle\nearrow|\psi\rangle & = & \langle\nearrow|\frac{1}{\sqrt{2}}|\nearrow\rangle + \langle\nearrow|\frac{1}{\sqrt{2}}|\nwarrow\rangle \\ |\langle\nearrow|\psi\rangle|^2 & = & \frac{1}{2} \end{array} \tag{3}$$

Es decir tendrá una medida aleatoría para el segundo bit. De este mismo modo se realiza el envío (por parte de Allice) y la medición (por parte de Bob) de cada bit. (ver figura 3)

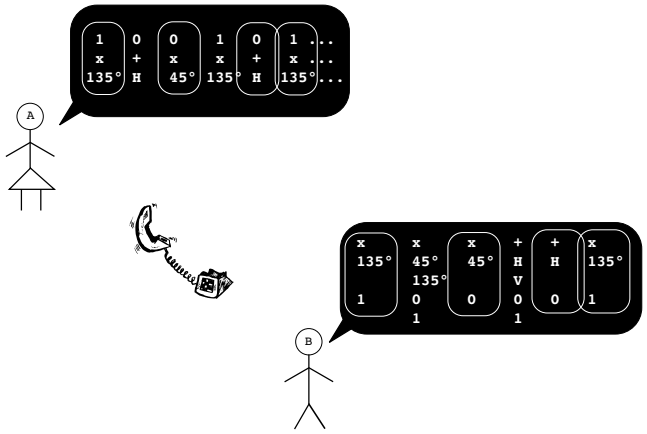

Figura 3: Ejemplo de un transporte de bits utilizando fotones polarizados entre Allice y Bob.

En general, Allice y Bob tendrán una secuencia diferente de bits. Para establecer los bits que corresponden a la clave criptográfica, Bob se comunicará con Allice a través de un canal autenticado (es decir, Bob y Allice deben tener certeza que están hablando con el otro y no con un suplantador), que puede ser interceptado sin riesgo a dañar la confidencialidad de la clave. A través de éste canal (que puede ser una llamada telefónica). Allice comunica a Bob la base que utilizó para realizar el envío, igualmente Bob comunica a Allice la base que utilizó para realizar las mediciones. Es necesario resaltar, que no se dicen los bits que recibieron sino las bases utilizadas. Así, Bob y Allice descartan los bits en los que utilizaron bases diferentes y dejan unicamente los bits en los que utilizaron la misma base. De este modo construirán la clave criptográfica común (conocida como *sifted key*).

4.1. Eva interviene

Suponga nuevamente que Allice desea enviar la secuencia de bits 100101, utilizando la secuencia de bases x+xx+x. Ahora, Eva realiza la medición escojiendo una secuencia aleatoria de bases. Supongamos que Eva utilizó la secuencia xx++xx, en ese caso la secuencia obtenida por Eva sería 1 en el primer bit, 0 o 1 (de manera aleatoria) en el segundo, tercero, cuarto y quinto bit, y en el sexto bit obtendría 1. Supongamos que Eva obtuvo la secuencia 101011, así que prepara fotones polarizados para enviar a Bob esa misma secuencia. Supongamos que Bob utiliza la secuencia de bases xxx++x, teniendo en cuenta que Bob no está recibiendo los fotones preparados por Allice sino por Eva, para Bob el primer bit será 1, el segundo bit será 0, el cuarto bit será 0, el sexto bit será 1 y el tercero, y quinto bit serán aleatorios. Supongamos que Bob, midió 101001. Vemos que todos tienen secuencias distintas, cuando Allice se comunique con Bob (con Eva escuchando) establecerán que desecharan todos los bits a excepción del primero, tercero, quinto y sexto. Para Bob la clave sería 1101 mientras que para Allice sería 1001 y para Eva sería 1111. Es posible notar que Allice y Bob tienen una clave distinta por lo que cuando Allice y Bob compartan información, Bob no podrá descifrarla (debido a que difieren las claves) revelando de éste modo la presencia de Eva. (ver figura 4)

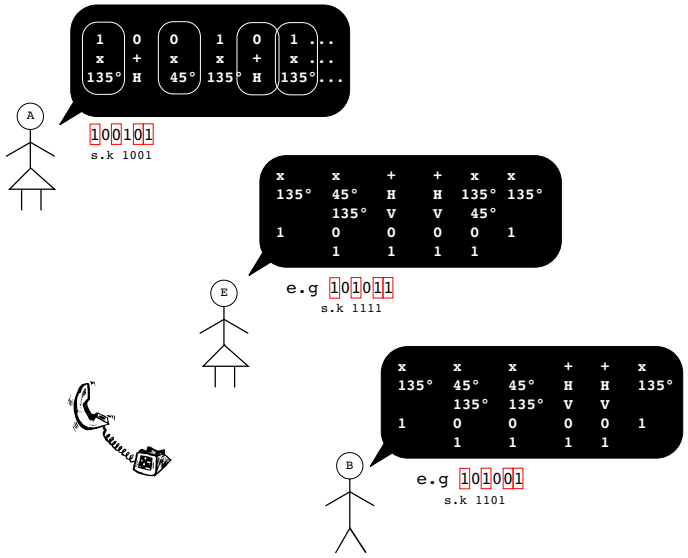

Figura 4: Ejemplo de un transporte de bits utilizando fotones polarizados entre Allice y Bob mientras Eva realiza una escucha. Fíjese que la presencia de Eva altera la medición de Bob a diferencia del transporte clásico de bits

5. Conclusiones

A través de fotones polarizados es posible realizar la distribución segura de claves criptográficas en canales inseguros. En caso de que la comunicación sea interceptada por un escucha, las mediciones de Allice y Bob diferirán, lo que permitirá establecer que la comunicación ha sido interceptada.

El ejemplo presentado de la distribución de claves criptográficas permite apreciar la aplicabilidad del problema de la medición en la mecánica cuántica, y las diferencias fundamentales que presenta la interceptación a través de medios fundamentados clásica y cuánticamente en canales inseguros.

Referencias

Atreya, M. (2006). *Introduction to cryptography.* Retrieved August.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, *68*(21), 3121.

Qi, B., Qian, L., y Lo, H.-K. (2010). A brief introduction of quantum cryptography for engineers. *arXiv preprint arXiv:1002.1237*.

Simmons, G. J. (1979). Symmetric and asymmetric encryption. *ACM Computing Surveys (CSUR)*, *11*(4), 305–330.

Wang, Y. (2012). Quantum computation and quantum information. *Statistical Science*, *27*(3), 373–394.