Algoritmos de Criptografía

Jose David Mamani Vilca
Kevin Jhomar Sanchez Sanchez
Percy Maldonado Quispe
Luis Fernando Ttito Surco
Angel Cutipa Samayani

I. ¿Qué es la criptografía?

I-A. Criptografia Cuantica

I-A1. **Mecanica Cuantica en Criptografia:**

- Principio de Incertidumbre.
- Polarizacion de un Foton.
- Qubits.
- Verschrankung
- Teorema de no-clonacion.

I-A2. **Distribucion de Claves Cuanticas:** Se deben cumplir las siguientes condiciones:

- Ningun intruso puede obtener la clave transmitida
- Cualquier intento de intromisión para obtener la clave transmitida puede ser detectado con alta probabilidad
- Los usuarios pueden estar seguros de que están compartiendo la misma clave

I-A3. **Protocolo BB84:** El esquema propuesto en 1984 por Brassard y Bennett implica el envío de fotones preparados en diferentes estados de polarización. Usando

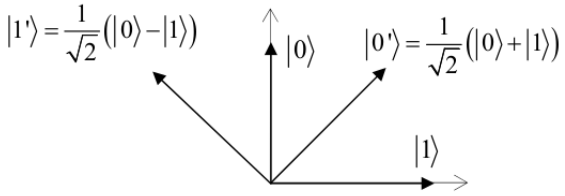

Figura 1. Representacion de la polarizacion de fotones en el protocolo BB84

un filtro de polarización, se selecciona el ángulo de polarización con respecto a la horizontal. Los fotones polarizados $\leftrightarrow\nearrow$ representan el binario 0, los fotones polarizados $\updownarrow\searrow$ representan el binario 1; entonces una secuencia de bits puede ser convertida en una secuencia de fotones polarizados.

1. Sin la Presencia de Eve.-

- Alicia codifica bits como fotones polarizados. La primera fila indica la secuencia de bits. La segunda indica la orientación usada por el filtro. La tercera indica el resultado de la polarización.

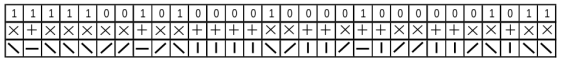

Figura 2. Alice codifica bits como fotones polarizados

Alicia genera una secuencia de fotones. Cuando Bob recibe los fotones, decide aleatoriamente si medir las polarizaciones a lo largo de las direcciones rectilíneas o a lo largo de las diagonales. De esta forma Bob podría extraer un bit de información por cada fotón.

- Bob decodifica fotones polarizados como bits. La primera fila indica la secuencia de fotones recibida. La segunda fila indica la configuración del cristal de calcita de Bob. La tercera fila indica el resultado de la medición.

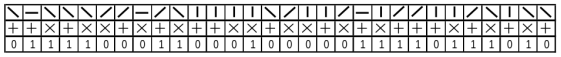

Figura 3. Bob decodifica fotones polarizados como bits

Este comportamiento se explica por el principio de incertidumbre de Heisenberg.
Alicia le dice a Bob (canal clasico) el valor de los bits que debió haber medido, y la verificación debe asegurar que los bits de Bob concuerdan al 100 % con los de Alicia.
La probabilidad de detectar un espía que esté presente es $1 - \left(\frac{3}{4}\right)^N$.

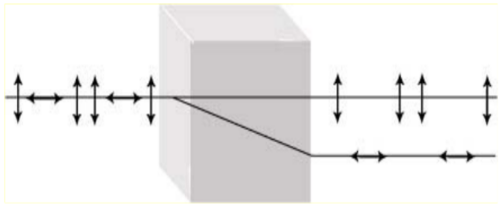

Figura 4. Cristal de Calcita que separa fotones de diferente polarización

- Alicia y Bob comparan un subgrupo de bits para probar, y verificar la presencia de un espía. En todos los bits se usó la misma orientación para polarizar y medir, y el valor del bit es igual, mostrando que no hay un espía presente.

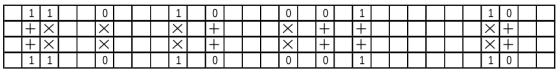

Figura 5. Alicia y Bob comparan un subgrupo de bits

- Clave generada. Los casos en que la orientación del polarizador es igual a la orientación del cristal, se representan por :), y esto significa que el bit se tomó como parte de la clave.

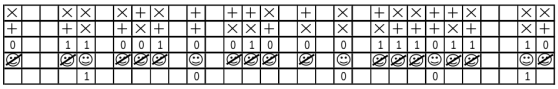

Figura 6. Clave Generada

2. Eve Presente.- En este caso, para que Eva pueda medir los fotones interceptados, debe haber escogido una orientación de polarización. Si Eva quisiera tener certeza de no ser detectada, necesitaría correr la suerte de escoger para cada bit transmitido la misma orientación de polarización que Alicia, lo cual, si el tamaño de la clave es lo suficientemente largo, sería prácticamente imposible. Si Eva elige la orientación incorrecta, modificará la polarización del fotón y su presencia podrá ser detectada en la fase de prueba.

- Codificación de los bits de Alicia a estados de polarización:
- Intercepción y medición de Eva (Si las polarizaciones no son iguales, Eva modifica irreparablemente

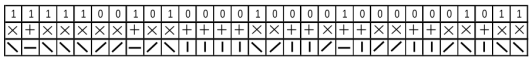

Figura 7. Codificación de los bits de Alicia

el estado original):

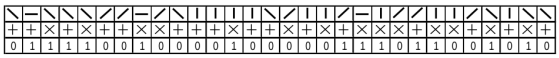

Figura 8. Intercepción y medición de Eva

- Bob, aún sin estar consciente de la presencia de Eva, realiza sus mediciones:

Figura 9. Bob realiza mediciones

- Pero en la fase de prueba, Alicia y Bob detectan la presencia de Eva y deciden desechar toda la secuencia de fotones para empezar de nuevo el procedimiento.

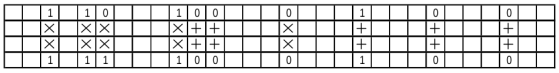

Figura 10. Detectan la presencia de Eva

I-A4. **Conclusiones:** La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional la cual descansa en supuestos de complejidad computacional no demostrada de ciertas funciones matemáticas