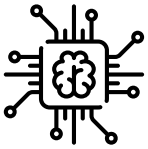

M1AC2. Actividad colaborativa 2: Criptografía cuántica. ¿Una amenaza real?

INTERCAMBIO SEGURO DE CLAVES - QKD
MÓDULO 1. CRIPTOGRAFÍA

Criptografía cuántica: intercambio seguro de claves QKD. Cómo llevar a cabo las comunicaciones cuánticas.

Santiago Raúl Vallés (Responsable)
Elena Arce Marín (Responsable)
Daniel Fernández Aller
Francisco Javier Martínez del Moral
Raimundo Jiménez Puerto
Raúl Manzano Iglesias
Javier Luciano Peña Guadalfajara
Razvan Alexandru Bobes

Resumen

1. Esquema QKD

QKD (del inglés *Quantum Key Distribution* o Intercambio Cuántico Seguro de Claves).

El objetivo de QKD es establecer una secuencia aleatoria de bits (la clave) entre Alicia y Bob a través de un canal cuántico para luego transmitir los datos cifrados con esta clave a través de un canal tradicional. (Ver Figura 1)

Esta técnica se basa en un principio de la física cuántica que consiste en un emisor (Alicia) y un receptor (Bob) que están comunicados mediante un medio que puede transmitir fotones (p. ej.: fibra óptica). Estos están polarizados y a cada polarización se le establece una relación de bits.

El emisor establece una base para relacionar fotones con bits. Como el receptor no sabe qué base ha escogido el emisor, crea una aleatoria. Cuando al receptor recibe los fotones emitidos este va comparando con su base y simplemente se va escogiendo los que coinciden con la que él ha generado. Con eso se construiría la clave. Esta luego podría ser usada por algoritmos simétricos para cifrar la información que circula por el canal clásico (p.ej.: Ethernet en la Figura 1). La gran ventaja de usar esta técnica es que si hubiera una tercera persona observando la comunicación (Eve), por la propiedades cuánticas, la transmisión de datos se vería afectada y contendría muchos errores, por lo que habría que descartar la clave.

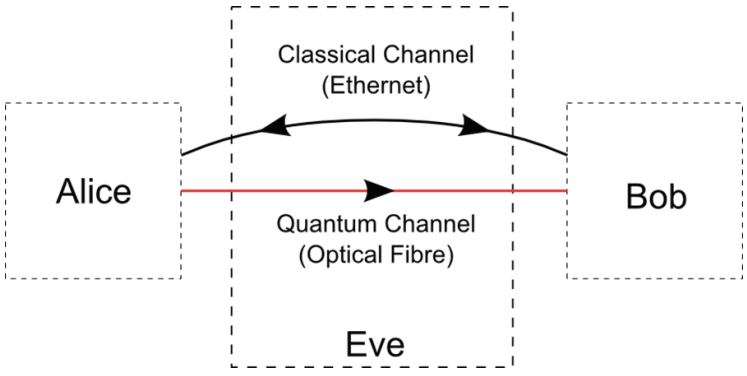

Figura 1 - *Esquema de comunicación con QKD [1]*

2. Protocolos

Según el principio físico en que se basan para realizar la distribución de claves, pueden dividirse en dos categorías:

2.1. Protocolos *prepare-and-measure*

Se basan en el principio de incertidumbre de Heisenberg, el cual supone una de las diferencias fundamentales existentes entre la física clásica y la física cuántica: no se puede determinar, simultáneamente y con cierto grado de precisión, el valor de la posición y cantidad de movimiento de una partícula, ya que el mero hecho de intentar esta medición puede introducir cierto "ruido" en estos valores, lo cual indicaría que ha habido un intento de medición.

Por ejemplo BB84 (Bennet-Brassard-84) y B92 (Bennet-92).

2.2. Protocolos basados en "entrelazamiento" (*entanglement*)

En pares de partículas cuánticas, como por ejemplo los fotones, se da el hecho de que sus propiedades físicas están fuertemente correlacionadas, de forma que la información relativa a estas partículas no puede ser explicada de manera individual, si no como parte de un grupo. Este fenómeno es independiente de la distancia de las partículas, y significa, entre otras cosas, que una medición realizadas a una de las partículas afecta también a la otra. Esta categoría parece ser un buen camino a seguir en el ámbito de la distribución de claves en distancias largas.

Por ejempo E91 (Ekert-91) y una variante de BB84.

3. Implementaciones realizadas

El rendimiento de un sistema QKD se mide en la velocidad de intercambio de claves en una determinada de distancia, por lo tanto la propagación de las claves pasa a ser un tema crítico.

En aplicaciones terrestres el límite de la distancia en redes de fibra es de unos 100 Km sin utilizar repetidores, pero en el espacio se pueden lograr distancias mucho mayores. Por ejemplo, un enlace de fibra entre Munich y Berlín de 600 Km tiene pérdidas nominales de 120 dB asumiendo unas pérdidas optimistas de 0,2dB/Km, lo que hace que no sea factible el enlace QKD. Sin embargo un enlace de 600Km con la órbita terrestre baja (LEO) se podría realizar con una pérdida de 50dB, lo que sería bastante aceptable para la mayoría de protocolos QKD.

Por lo tanto una red QKD global de Satélites y Estaciones Terrestres para enviar claves seguras podría ser posible. Y dado que las claves pueden distribuirse y almacenarse para su uso posterior en un sistema de almacenamiento de claves, tal sistema no tiene que depender mucho de las condiciones climáticas que afectan a este tipo de enlaces satelitales.

En la actualidad los repetidores se colocan aproximadamente cada 80 km [2] para amplificar y regenerar la señal óptica. Estos repetidores ópticos generarían el efecto de un tercero (espía) observando la comunicación introduciendo ruido y perturbaciones. Tendríamos que tener repetidores “confiables” que conozcan nuestras claves y esto rompe el paradigma de privacidad punto a punto.

4. Vulnerabilidades

El QKD se aprovecha de un principio de la física cuántica por el que no se puede medir o examinar un fotón sin alterar su estado. Si un espía intenta interceptarlo, termina destruyendo trazas de información, y el emisor y destinatario originales pueden saber que hay alguien "espiando" su comunicación.

La técnica es tan efectiva, teóricamente hablando, que ha recibido inversiones de los sectores bancario, comercial y de defensa.

Sin embargo, en agosto de 2011, un equipo de la Universidad de Ciencia y Tecnología de Noruega (UCTN) logró vencerla. ¿Violaron los principios cuánticos para hacerlo?

La respuesta es no, simplemente engañaron al sistema.

Se colocaron entre emisor y receptor e interceptaron la clave (MitM). Esto, que sería detectado en condiciones normales, no lo fue en esta ocasión. Por medio de un rayo láser, el equipo de la UCTN envió una copia falsa del mensaje de fotones. Simulando fotones con la emisión de flashes.

Las conclusiones arrojadas sobre esta experiencia afirman que el ataque aprovechó errores en el equipo, y no en los fundamentos cuánticos.

En defensa de la seguridad del QKD, la mejora de los equipos, concretamente los detectores de fotones (elemento “engañado” en el ataque), dificultarían o harían casi imposible que se repitiese esta experiencia.

Por otro lado, los más escépticos, piensan que mientras las máquinas que soporten esta tecnología no sean perfectas (sólo posible en un sueño), los ataques podrán tener éxito.

Referencias

[1]
https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf

[2]
https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf