Miramontes Sarabia Luis Enrique

Noviembre 18, 2019

Criptografía cuántica experimental

El artículo propone un método para implementar un sistema de distribución de llaves cuántico, en el que dos usuarios que no comparten ningún tipo de información secreta al principio pueden llegar a tener una transmisión aleatoria cuántica. El sistema adquiere su fortaleza no basándose en la complejidad matemática de problemas, sino en las propiedades cuánticas de las partículas, por lo que termina siendo un algoritmo seguro contra un adversario cuyo poder de cómputo sea ilimitado.

La criptografía cuántica nació en los sesentas, pero las publicaciones relacionadas a esta nueva área no fueron tomadas en cuenta y no fue hasta 1979 que en un simposio de la IEEE en Puerto Rico se volvió a considerar esta área, cuando se comenzó a trabajar en un protocolo de intercambio de llaves basado en la física cuántica. Al principio la criptografía cuántica era considerada en el ámbito científico como un trabajo de ciencia ficción, porque la tecnología necesaria para su implementación estaba fuera del alcance que se consideraba realista. Eventualmente algunos científicos comenzaron a investigar en el área y lograron avances en el campo teórico del área.

El propósito de un sistema de distribución de llaves es que dos entidades puedan estar de acuerdo en una clave aleatoria sin compartir ningún tipo de información confidencial, en un sistema cuántico se trabaja sobre el mismo principio pero es posible verificar cuando la información ha sido leída por un agente externo gracias a las propiedades cuánticas del sistema, esto hace que un agente externo que quiera leer la información no pueda hacerlo sin alterarla de una manera aleatoria e incontrolable, esto es una propiedad derivada del principio de incertidumbre de Heisenberg, donde se establece que existen propiedades que son incompatibles al momento de ser medidas. Como medir la polarización lineal de una partícula afecta su polarización circular y viceversa.

En el artículo se revisa un algoritmo donde Alice envía una secuencia aleatoria de fotones polarizados de forma horizontal, vertical, circular-derecha y circular-izquierda. Bob medirá los fotones polarizados en una secuencia aleatoria de bases, rectilínea y circular. Bob le dirá a Alice qué base uso para cada medir cada fotón que recibió. Alice le dirá qué bases fueron las correctas, Alice y Bob se quedarán sólo las mediciones correctas de los fotones y usando una codificación predeterminada determinarán la secuencia binaria correspondiente a los fotones enviados.

Si existe un tercero intentando ver esta transmisión de datos existe una muy alta probabilidad de introducir discrepancias a las partículas, y esto puede ser detectado por Bob y Alice.

Esta implementación no se puede implementar debido a que no tenemos detectores que carezcan de ruido, el sistema se debe poder recuperar. Además, es difícil producir pulsos de luz conteniendo exactamente un fotón.

El artículo parece ser bastante avanzado, realmente necesitas saber de física cuántica o al menos tener un curso introductorio para poder comprender las propiedades cuánticas de los fotones, ya que en eso se basa la seguridad del sistema. Principalmente en como una medición puede perturbar la partícula de distintas maneras. Realmente cuando se logre alcanzar el poder computacional que prometen tener las computadoras cuánticas la complejidad matemática no será suficiente para detener ataques, necesitaremos saltar de lo muy difícil a lo imposible, algo que la física nos puede ayudar a hacer.