# Distribución de Llaves Cuánticas

Domínguez Juárez Jorge Uriel, Lucio Martinez José Luis, Mancilla Frausto Octavio Eduardo, Martin Varela Kylian Alfonso, Ojeda Rosas Jesus Ezequiel.

Universidad de Guanajuato
División de Ciencias e Ingenierías - Campus León
Lomas del Bosque 103, Lomas del Campestre, 37150 León, Gto.

ju.dominguezjuarez,jllucio,oe.mancillafruasto
ka.martinvarela,je.ojedarosas,@ugto.mx

## 1. Objetivos

1. Exponer la aplicación de la física cuántica en la distribución de llaves cuánticas
2. Introducir los protocolo BB84 y BBM92 de QKD

## 2. Introducción

Para abordar el tema del proyecto conviene primero introducir elementos de la información clásica la problemática que surge. En la teoría de la información se considera necesario codificar los mensajes qeu se intercambian entre personas. Esta aseveración es dudosa ¿la información es organización?

La encriptación consiste en lo siguiente; imaginemos que tenemos dos personas **Alice** y **Bob** que quieren compartir información secreta entre ellos, ambos acuerdan usar un código (por ejemplo el código binario) para traducir el mensaje a una secuencia de caracteres, el mensaje es codificado usando una llave que Alice y Bob comparten, el mensaje se ve alterado y es irreconocible para cualquier persona, cuando Bob recibe el mensaje usa la llave para decodificar el mensaje, de esta manera la comunicación segura. El problema es que este método no es infalible debido a que la llave sólo puede ser usada una vez ya que si se utiliza varias veces, el espía podría encontrar la llave comprometiendo la información. Estos problemas se resuelven usado diferentes llaves y usando la distribución de llaves cuánticas.

La mecánica cuántica se implementa una descripción probabilística que realiza predicciones sobre resultados de mediciones. En donde cada valor medido tiene una asociado una probabilidad. Matemáticamente un sistema cuántico se describe con la función de onda, una herramienta matemática que tiene dominio en un espacio vectorial complejo.

$$|0\rangle = \binom{0}{1} \quad \& \quad |1\rangle = \binom{1}{0} \quad \Rightarrow |\Psi\rangle = a|0\rangle + b|1\rangle$$

Con $a, b \in \mathbb{C}$. Un sistema que se implementa con qubits puede estar dado por el espín de un electrón o la polarización de un fotón, lo relevante es que se pueda establecer la base para la codificación en el sistema binario, por eso se usan sistemas cuánticos con dos grados de libertad ($\mathbb{C}^2$).

## 3. Marco Teórico

Consideramos oportuno realizar un resumen de las propiedades básicas de la mecánica cuántica que juegan un rol protagonista en la distribución de llaves cuánticas. No todos objetos tienen comportamiento cuántico (esto es evidente por que en la vida cotidiana no notamos el efecto cuántico) la manera de distinguirlos es analizando las cantidades físicas conocidas tales como la posición, momento, momento angular, etc. El problema de la mecánica cuántica radica en hacer predicciones sobre los posibles resultados que puede tener un evento que involucra entes cuánticos. Un evento cuántico consiste en un proceso que tiene un origen y como resultado la medición de un observable. Los eventos en mecánica cuántica pueden tener diferentes *Historias*. Las historias están asociadas a las alternativas que tiene un ente para llegar al resultado del evento, se caracterizan por tener asociada una amplitud, un numero complejo, que implica una fase, que en general difiere y genera el comportamiento ondulatorio del ente cuántico. Cuando las historias de un evento son indistinguibles entre sí, entonces las amplitudes de la historia se suman y es lo que llamamos función de onda del estado cuántico de manera que el ente queda descrito por el estado del sistema.

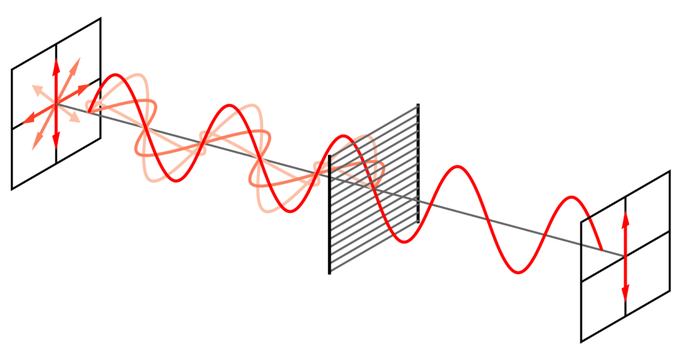

**Figura 2:** Luz atravesando un filtro polarizador. Obtenido de: https://es.wikipedia.org/wiki/Polarizaci %C3 %B3n_electromagn %C3 %A9tica, accedido el día: 21/07/21

Necesitamos introducir la polarización de fotones y su implementación. La polarización servirá como la base de la función de onda de los qubits. Hay dos bases que se usan comúnmente para describir los fotones. Una corresponde a polarización (dirección del campo eléctrico) vertical y horizontal y la otra base a polarización diagonal anti-diagonal. Esto se muestra en la figura 2. Cuando la polarización de un fotón se implementa en un qubit, en la base horizontal-vertical el 0 se asocia a la polarización horizontal y el 1 a la vertical de igual manera para la base diagonal(0)-antidiagonal(1). En este contexto la medición de un fotón en una base consiste en hacer pasar el fotón sobre un filtro polarizador. En el proceso de medición ocurre lo que se conoce como colapso de la función de onda; al tratarse de un sistema cuántico el fotón puede tener los valores 0 o 1 en las diferentes bases o en un estado que consiste en una superposición de estados, lo que otorga las propiedades de onda al fotón. Cuando se realiza la medición el estado del sistema *colapsa* i.e. se proyecta al estado definido por el polarizador. En otras palabras, cuando se realiza una medición, el ente cuántico se materializa y deja entonces de existir en la superposición de estados, esto es lo que se conoce como el colapso de la función de onda. En el caso de un fotón la medición la hacemos cuando la luz atraviesa el polarizador, cuando lo hace la luz que lo atraviesa solo es la del estado de polarización del filtro.

## 4. Sistema de Distribución de Llaves Cuánticas

Para aumentar la seguridad al encriptar la información se diseñó la distribución de llaves cuánticas, que aprovecha las poropiedades de la mecánica cuántica para evitar que los espías puedan acceder a las llaves y si lo hacen puedan ser detectados. En la práctica existen fuentes de error debido al ruido que puede haber en el canal o los espías que intentan acceder a la información.

### 4.1 BB84

La figura 4 muestra el setup de la distribución de llaves con el protocolo BB82 en donde Alice envía qubits atreves de un canal cuántico (los fotones) a Bob. Para detectar cada fotón Bob utiliza en forma aleatoria una de las dos bases usadas por Alice de modo que aunque recibe resultados aleatorios, se comunica con Alice para conocer la base que usó Alice para codificar cada bit, y descartan todos los bits que no usaron la misma base para detectar y de esta manera ambos logran compartir la llave.

Debido a las diversas fuentes de error que hay en el setup parte de la información se pierde. Además si hay espías escuchando pueden tener información parcial de la llave porque Alice y Bob. Esto obliga a establecer lo que se concoce como privacidad amplificada; consiste en establecer una tolerancia sobre el error que existe al recibir los qubits de Alice de esta manera se consideran menos qubits de los que originalmente había.

Hay algunas suposiciones que se han hecho sobre el setup: Se supuso que en el canal cuántico no hay pérdidas de ningún tipo, se asumió que los detectores son perfectos y detectan los fotones sin pérdidas, también que las bases de los qubits son perfectas. En la práctica las suposiciones anteriores representarías fuentes de error en el laboratorio. Dentro de la universidad se trabaja en cajas que permitan distribuir los qubits afrontando los retos tecnológicos que esto conlleva. Trabajar fuera de las suposiciones hechas no garantiza la seguridad, pero sí la aumenta porque permite detectar espías.

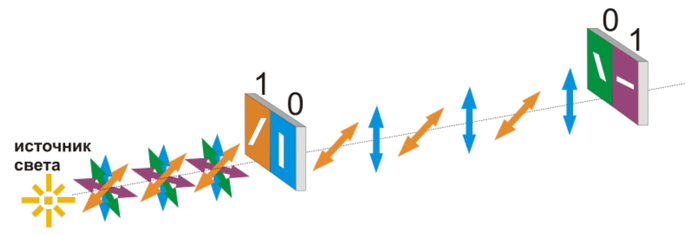


**Figura 4:** Distribución de llaves cuánticas. Obtenido de: https://commons.wikimedia.org/wiki/File:B92_protocol_quantum_key_distribution.svg, accedido el día: 21/07/21

### 4.2 Protocolo BBM92

Cuando se consideran dos o más entes cuánticos pueden estar correlacionados, y esta propiedad junto con la superposición da lugar a lo que se conoce como entrelazamiento, lo que ofrece ventajas para QKD. Un par de entes entrelazado tienen la característica de que al realizar una medición sobre uno de ellos, al estar correlacionado con el compañero, el otro presenta el colapso de la función de onda. Esto permite construir nuevos protocolos de QKD como es el caso del BBM92. El protocolo consiste en lo siguiente: El sistema es similar al del protocolo BB84, pero con la distinción radica en que se generan pares de fotones enredados a medio camino entre Alice y Bob. Los fotones enredados son enviados a Alice y Bob realiza una medición por cada fotón que recibe e informa a Bob la base que utilizó para medir cada fotón. Bob descarta las detecciones en bases distintas a la que él usó y comunica a Alice en cuáles coincidieron. De esta manera Alice y Bob comparten una secuencia de bits perfectamente correlacionados.

## 5. Conclusiones

La mecánica cuántica tiene propiedades que pueden ser un recurso para incrementar la seguridad de la comunicación. La propiedad del colapso de la función de onda es la principal ventaja que ofrece la distribución cuántica de llaves porque nos permite detectar indirectamente a un posible espía. Los retos ahora consisten en construir adecuadamente un setup y establecer el umbral mínimo. Una dificultad que surge de establecer la distribución de llaves cuánticas es la distancia entre Alice y Bob, por la absorción óptica del canal, lo que representa un reto tecnológico. El entrelazamiento es una propiedad más de la mecánica cuántica que abre las posibilidades a nuevos protocolos como lo es el BBM92.

## Referencias

[1] J. L. Lucio (2021) “Cuántica: el futuro de la información”. Seminario del grupo.

[2] Barak Shoshany (2019). “Thinking Quantum”: Lectures on Quantum Theory; arXiv:1803.07098 physics.pop-ph

[3] Ish Dand (2018). Understanding quantum physics through simple experiments: from wave-particle duality to Bell’s theorem. arXiv:1806.09958v3 physics.ed-ph

[4] Popescu, S. Nonlocality beyond quantum mechanics.Nature Phys10,264–270 (2014).

[5] Scales, J. A. and Snieder, R. (1999). What is a wave?. Nature, 401(6755), 739-740.