Universidad Autónoma de Querétaro

Facultad de Ingeniería

Ingeniería Física

Implementación experimental y computacional del protocolo de Distribución Cuántica de Llaves Criptográficas BB84.

TESIS

Que como parte de los requisitos para obtener el grado de
Ingeniero Físico.

Presenta:

Andres Avila Perea

Dirigido por:

Dr. Aldrin Meliton Cervantes Contreras

SINODALES

Dr. Aldrin Meliton Cervantes Contreras Presidente	Firma
Dr. Adolfo Huet Soto Secretario	ADOLFO HUET SOTO Firma
Dra. María Lucero Gomez Herrera Vocal	Firma
Dr. José Mauricio López Romero Sinodal	Firma

Dr. Manuel Toledano Ayala
Director de la Facultad

Dra. María Lucero Gomez Herrera
Coordinadora de Ingeniería Física

Centro Universitario
Querétaro, QRO
México.
Junio 2019

Por su infinito apoyo y amor, a mis padres María Elena Perea Castro y Orlando Ávila Hernández.

Agradecimientos

En primer lugar agradezco a todos y cada uno de mis asesores, los cuales no solo mostraron su apoyo durante este trabajo de investigación, sino que formaron parte de mi desarrollo como profesionista. Al Dr. Aldrin M. Cervantes Contreras y al Dr. Adolfo Huet Soto, por los años de trabajo en aulas así como fuera de ellas, a ellos reconozco el trabajo de introducirme a la física desde temas básicos hasta tópicos avanzados en áreas de interés mutuo. De igual manera agradezco el apoyo dado por la Dra. María Lucero Gómez Herrera, que como docente y coordinadora de la Licenciatura en Ingeniería Física, siempre mostró una disposición absoluta de ayudar en pro de mejorar la calidad de educación que recibí junto a todos mis compañeros. Al Dr. José Mauricio López Romero agradezco su confianza y apoyo para poder desarrollar las estancias de investigación que permitieron realizar este trabajo, también por su interés en acercar jóvenes a temas en la investigación de frontera, lo cual reafirmo mi postura de continuar con mis estudios y me dio una visión sobre lo que quiero hacer en mi futuro. A todos y cada uno de ellos, así como decenas de personas que no menciono en este documentos, pero tanto ellas como yo sabemos todo el apoyo que me brindaron de manera desinteresada para crecer como persona e Ingeniero Físico. Quiero agradecer en especial a la Universidad Autónoma de Querétaro (UAQ) por la oportunidad de formar parte del gran número de estudiantes que se forman en sus instalaciones como profesionistas para hacer de nuestra sociedad y nuestro entorno, un mejor lugar; del mismo modo debo agradecer a la sociedad en general la oportunidad que me dieron de haber pertenecido a una institución de educación pública. A el Centro de Investigaciones y Estudios Avanzados del Instituto Politécnico Nacional (CINVESTAV) Unidad Querétaro y al Consejo de Ciencia y Tecnología del Estado de Querétaro (CONCYTEQ) por los apoyos de infraestructura y económicos para haber podido desarrollar con la mejor calidad y calidez mi estancia de investigación. Agradezco a mi familia, amigos y profesores por estar conmigo en mi proceso de formación, agradezco estar vivo.

Abstract

Quantum cryptography, usually referred to as Quantum Keys Distribution (QKD) is a methodology that collects phenomena of quantum physics to make it theoretically impossible to decipher and / or modify messages that are exchanged between an emitter (**A**) and a receiver (**B**), with the presence in the communication channel of a spy (**E**). The BB84 protocol proposed by C.H. Bennet and G. Brassard in 1984 was the first of its kind. This paper presents the implementation of a QKD system in the Cinvestav Unidad Queretaro for teaching purposes and as a precedent for the implementation of a technological research and development system related to QKD.

Resumen

La criptografía cuántica, usualmente referida como Distribución Llaves Cuánticas (QKD, por sus siglas en inglés) es una metodología que recoge fenómenos de la física cuántica para hacer teóricamente imposible descifrar y/o modificar los mensajes que se intercambián entre un emisor (**A**) y un receptor (**B**), con la presencia en el canal de comunicación de un espía (**E**). El protocolo BB84 propuesto por C.H. Bennet y G. Brassard en 1984 fue el primero de su tipo. En este trabajo se presenta la implementación de un sistema QKD en el Cinvestav Unidad Querétaro para propósitos de enseñanza y como antecedente de la implementación de un sistema de investigación y desarrollo tecnológico relacionado con QKD.

Índice general

CAPÍTULO 1

Introducción

En la actualidad el tráfico de datos es la espina dorsal de la comunicación, esta puede ser para correspondencia privada, la cual es usada mayormente para concebir transacciones comerciales. A lo largo de la historia humana, el hecho de establecer canales de comunicación segura ha representado una serie de problemas a resolver, esto ha dado lugar a la creación de todo un tema de investigación en el campo de las matemáticas y criptografía, la cual se encarga de establecer estos canales.

Para el entendimiento de la Criptografía Cuántica (QC, por sus siglas en inglés) es necesario tener conocimientos sobre óptica, mecánica cuántica y criptografía. Probablemente al hablar óptica el nombre de Sir Issac Newton (1642-1727) y su antagonista Christiaan Huygens (1629-1695) con sus dos teorías acerca de la naturaleza de la luz, la corpuscular y la ondulatoria respectivamente, así como los nombres de Albert Eistein (1879-1955) quien comprobó la naturaleza de partícula o corpúsculo con el efecto fotoeléctrico (desarrollo por el cual recibio el premio nobel en 1921) además Thomas Young (1773-1829) con su experimento de la doble rendija y Agustin Jean Fresnel (1788-1827) con su teoría de difracción comprobaron la naturaleza ondulatoria de la luz. Se atribuye a Jean Clerk Maxwell (1831-1879) el desarrollador de la teoría electromagnética actual a través de una recopilación de datos experimentales y desarrollos previos, estos hombres sentaron las bases de la óptica tal y como la conocemos hoy [1].

A pesar de que estos nombres sean los grandes exponentes de la óptica, el humano a lidiado con la pregunta acerca de la verdadera naturaleza de la luz o al menos se ha hecho de los medios para manipularla desde hace bastante tiempo [2], se data del siglo XV antes de nuestra era que en Egipto ya existían artilugios de vidrio y esmaltes. Además se han encontrado en expediciones arqueológicas lentes de distintos tipos procedentes de la antigua Mesopotamia aproximadamente 3000 años AC. También se tiene conocimiento de que en la antigua Grecia se generaron distintas teorías acerca de la naturaleza de la luz grandes filósofos de la época como Pitágoras, Demócrito, Empédocles, Pláton y Aristóteles. Más tarde en el Imperio Romano también se desarrollaron estudios sobre la luz como lo menciona el historiador Plinio o Séneca , también se ha encontrado una lente plano-convexa en las ruinas de Pompeya [1].

Queda claro entonces que el hombre ha tenido una larga historia con la luz y su interpretación. Ahora podemos mencionar de manera tan coloquial el hecho de que la luz tiene un carácter tanto de propagación ondulatoria como de partícula, un ente físico finito y medible, sin embargo no resulta

fácil ni intuitivo la comprensión de la naturaleza onda-partícula de la luz, dualidad que se extiende para cualquier otra partícula, como los electrones por mencionar una (la interacción entre estas dos partículas es el fundamento para comprender la física atómica). Esta dualidad fue descrita gracias a la mecánica cuántica, desarrollada durante el siglo pasado[3]. Y después de todo esto ¿Por qué es tan importante la luz, su naturaleza e interacción con la materia? La respuesta a esta pregunta no solo tiene un trasfondo filosófico, ni es mera física teórica, sino que esta presente en nuestra vida diaria, en la tecnología moderna, en las comunicaciones, en el desarrollo del laser y sus aplicaciones, en la espectrometría, en la electrónica [4], esta presente en los procesos tan comunes como prender un foco incandescente hasta la investigación de punta, hecho que nos llevo en el 2015 a ser el Äño Internacional de la Luz y las Tecnologías Basadas en la Luz"decretado por la Asamblea General de las Naciones Unidas, evento celebrado 100 años después de la formulación de la teoría del efecto fotoeléctrico.

En otro ámbito, el primer registro que se tenga sobre el uso de criptografía es probablemente una inscripción de 1900 AC en la cámara de la tumba de Khnumhotep II, donde se encuentran jerolíficos inusuales en lugar de los ordinarios que se tienen documentados [5]. El propósito no sería ocultar un mensaje, sino hacerlo más exótico para dignificarlo. Por lo que no es una forma secreta de escribir, pero incorpora una transformación del mensaje. Otro texto de las civilizaciones antiguas donde se tratan asuntos de criptografía es el *Arthshashtra*, un texto en sanscrito escrito por Kautalya acerca del arte de gobernar, la política económica y la estrategia militar. En éste se describe los servicios de espionaje de la India y su *escritura secreta*.

Pero no fue hasta el Renacimiento que el estudio de la criptografía es tratado de manera rigurosa. Un claro ejemplo de la necesidad de la criptografía es tal vez, las ciudades estado de hoy conforman Italia. Debido a su tráfico de comercio y los constantes conflictos bélicos, una comunicación segura era prioritaria[6].

Se tiene documentado que en 1467 Leon Battista Alberti [7] compositor, organista, poeta, filósofo, arquitecto y atleta renacentista, escribió un manuscrito llamado *De Cifris*. En el se describe un dispositivo mecánico para crifrar mensajes basado en sustitución polialfabética, el cual pretendía resolver el problema de la frecuencia del cifrado.

Durante los siglos XVI a XIX, varios cryptosistemas fueron creados de manera que fuera sencillo utilizarlos. El uso de maquinas complejas llegó después junto con la invención del telegrafó, para sentar las bases de la criptografía utilizada durante la Segunda Guerra Mundial. Es aquí donde la criptografía toma contacto con la computación. Máquinas como Enigma, Z40 y Z42 utilizadas por los alemanes o los laboratorios ingleses en Bletchley Park y los Alamos en EUA; son prescendetes de la creación de la computación actual[6]. Después de la SGM la criptología se combirtió en tema cetral de investigación para el gobierno de los EUA, la era de la electrónica y los ordenadores dio auge a esto.

La seguridad de datos es ahora menos importante en comercio y el mundo financiero, que en privacidad personal alrededor del mundo. Es aquí donde la creación de sistemas que sean totalmente indescifrable, aún para el proveedor del servicio de encriptación, presenta una oportunidad de unir la investigación de frontera con aplicaciones ingenieriles que mejoren la calidad de vida de las

personas, en este mundo globalizado y cada vez más inmerso con la tecnología como herramienta para la vida diaria.

Actualmente la criptografía tiene varios usos comerciales como tarjetas ATM, comtraseñas de computadoras y el comercio electrónico. El desarrollo moderno ha hecho que la criptografía no sea exclusivamente para mantener la privacidad de mesajes, sino puede resolver otros problemas como: integridad, autentificación y la no anulación de datos.

La criptografía es el estudio del envío recepción de mensajes secretos. Su objetivo principal es asegurar el intercambio de información entre dos entidades sin que nadie más pueda obtener dicha información[8]. Con el nacimiento de los ordenadores el siglo pasado esta rama de estudio tuvo un auge sin precedentes

En general la criptografía es aplicarle un tratamiento llamado criptosistema (e.g. algún algoritmo) para combinar un mensaje con información adicional llamada llave, de modo que se convierta en otra cosa lo más parecido a ruido, llamado criptograma. De ésta forma sólo **A** y **B** serían capaces de tener acceso al contenido original del mensaje. Esta técnica es conocida como encriptación. Para que la encriptación sea segura debe ser imposible obtener información sobre el criptograma sin la llave. Además la criptografía estudia los ataques sobre el criptograma, de parte de agentes externos a la comunicación **E**. Los sistemas criptográficos se clasifican en dos sistemas de acuerdo con el tipo de llave que utilizan, estas son llave pública y privadas [8].

Los de llaves públicas son un sistema donde la llave k es pública y **B** o cualquier **E** puede encriptar mensajes. Pero **A** ya conoce de antemano (k^{-1}), por lo que solo **A** puede desencriptar el mensaje que **B** le quiera comunicar. Durante los 70's, varios algoritmos criptográficos de llave pública han sido propuestos, el más famoso y utilizado es el RSA [9] el cual basa su seguridad en el pequeño teorema de Fermat. El punto débil de este algoritmo es el hecho de que basa su seguridad en la factorización de números primos, el cuál es un problema de complejidad computacional. Irresolvible en un tiempo aceptable (de orden exponencial, $\mathcal{O}(2^t)$) para las computadoras actuales. Pero ya se han planteado métodos para vencer este obstáculo, tal es el caso del algoritmo de Criba General del Cuerpo de Números (Number Field Sierve)[10] o con la aplicación del Algoritmo de Shor[11] en cómputo cuántico, el cual es capaz de hacer la factorización en un tiempo polinomial $\mathcal{O}(t^n)$. Una desventaja de este método es que cualquiera puede encriptar mensajes por lo que es necesario identificarse de algún modo. Esta desventaja puede puede ser explotada por **E** para obtener información de la llave k.

Las llaves privadas donde sólo él emisor y receptor conocen la llave, por lo que ambos pueden encriptar y desencriptar mensajes sin la necesidad de identificarse. El mayor reto de este tipo de sistemas es que la llave permanezca privada para evitar el espionaje, por lo que este sistema basa sus seguridad en la distribución de la llave[12].

Estos planteamientos, fueron los que inspiraron a una generación de físicos para generar formas de encriptación que basaran su seguridad en los fundamentos de mecánica cuántica, debido a que sería un sistema para generar criptogramas totalmente secretos. El primer registro se que tiene sobre criptografía cuántica fueron las ideas de Sthephen Wiesner durante la década de 1970 [13].

En contraste con la criptografía convencional, la QC como la conocemos actualmente es una rama basada en la mecánica cuántica, la teoría de información y la generación de estados cuánticos individuales. Por lo que es una rama multidisciplinaria que implica aspectos de física experimental y teórica, además de computacionales.

El primer protocolo de QC fue propuesto por Charles H. Bennett y Gilles Brassard en 1984 [14] en una conferencia de la IEEE en la India. El cuál planteaba una distribución cuántica de llaves (QKD, por sus siglas en inglés), a través de un canal clásico y uno cuántico. Es por eso que el protocolo es llamada BB84. Su comprensión teórica es sencilla, mientras que la implementación experimental ha sido um verdadero reto a lo largo de las últimas décadas.

En la actualidad la información cuántica representa un aspecto fundamental en el constante desarrollo de la tecnología relacionada con las comunicaciones. Resulta difícil imaginar un escenario en el que no se requiera mantener información oculta por razones de privacidad o de seguridad, desde los negocios hasta el ámbito académico. Tan sólo en México según cifras del INEGI [15]: 57.4 % de la población de seis años o más se declaró usuaria de internet, 39.2 % de los hogares tienen acceso a internet, 77.7 millones de personas usan celular y dos de cada tres cuentan con un teléfono inteligente. Todas estas cifras presentan la contundencia necesaria como para iniciar una discusión acerca de la necesidad de crear un sistema infalible de encriptación de datos.

En este trabajo se pretende implementar un experimento capaz de generar una QKD con la aplicación del protocolo BB84. Esto con tiene como finalidad generar una comunicación segura entre **A** y **B**, aun con la presencia de **E**. Probablemente la QC represente la primera aplicación comercial a un nivel puramente cuántico.

A diferencia de la criptografía clásica, la cual es usada actualmente para mantener las comunicaciones en todo el mundo, su análogo cuántico representa una innovación desde que la seguridad recae en postulados universales de la naturaleza. En otras palabras no es posible violar la seguridad de QC sin violar leyes físicas fundamentales. Mientras que la criptografía clásica preserva su seguridad a través de algoritmos matemáticos, misma seguridad que no puede ser probada. Ya que esta basada en suposiciones que no han sido probadas [16], además del desarrollo de algoritmos que minimizan la complejidad computacional tales como el algoritmo de Shor planteado en computación cuántica.

Es por esto que implementar un algoritmo de encriptamiento basado en principios de la mecánica cuántica, más que en matemáticos, nos permitirá estar seguros de intercambiar información confidencial sin preocupaciones sobre la intromisión de otros agentes externos.

Por otra parte protocolo BB84 utiliza los aspectos de la naturaleza onda-partícula de la luz, para cerciorarse de que los criptogramas enviados serán imposibles de desencriptar. El protocolo presenta un problema básicamente imposible de resolver si se quiere obtener la llave para desencriptar el mensaje por parte de **E**.

El objetivo general del proyecto es la implementación experimental del Kit de demostración de

Criptografía Cuántica DCL EDU-QCRY1_M de la empresa THOR Labs para probar el protocolo BB84, entender detalladamente los procesos físicos que generan durante todo el protocolo, hacer una simulación computacional como precedente de un estudio detallado de su aplicación real. Los objetivos específicos a resolver son:

- Entender el fundamento físico del protocolo BB84.
- Hacer la implementación experimental del sistema EDU-QCRY1_M.
- Diseñar un algoritmo que sea capaz de simular el protocolo.
- Analizar los aspectos a considerar para una aplicación real.

La estructura de la tesis consiste en una revisión literaria en el capítulo 2 para hacer el desarrollo de la teoría necesaria para entender el protocolo BB84 de manera teórica y experimental, en el capítulo 3 se discute la metodología utilizada para implementar el protocolo de manera experimental y el algoritmo para su simulación computacional. En el capítulo 4 se hace un análisis y discusión de los datos, para comparar los resultados obtenidos con los esperados, esto con la finalidad de desarrollar una conclusión del trabajo, así como plantear perspectivas de trabajos futuros sobre esta línea de investigación.

CAPÍTULO 2

Revisión Literaria

Es evidente notar que al paso de un análisis sobre un esquema de criptografía, se encuentra el problema de cómo tratar los ataques sobre el mensaje por parte de **E**. Por lo que utilizar esquemas como la sustitución alfanumérica presenta la cualidad que al interceptar varios mensajes cifrados, es posible comenzar a obtener información sobre la llave. Antes de la existencia de la probabilidad formal, desarrollada por Kolmogorov , era aún posible detectar patrones a través de un análisis repetitivo [17].

Existen dos tipos de criptosistemas: los simétricos y asimétricos. En los sistemas simétricos la misma llave es utilizada para encriptar y desencriptar el mensaje. Los sistemas asimétricos utilizan una llave pública para encriptar el mensaje y una llave privada para desencriptarlo [5] .Los sistemas simétricos son útiles para manipulación de datos de manera más rápida, mientras que los sistemas asimétricos mejora la seguridad de la comunicación.

Los criptosistemas simétricos son aquellos que utilizan una la misma llave para encriptar el texto plano como para desencriptar el cifer o criptograma, es por esto que también es llamado sistema de una sola llave [12]. El problema principal de este esquema reside en que **A** y **B** deben ponerse de acuerdo y comunicar la llave de manera totalmente secreta, esto por razones obvias, ya que toda la seguridad de este esquema esta basada en el completo desconocimiento de la llave, sin importar si se conoce el algoritmo utilizado por parte de un agente externo **E**. Los problemas principales asociados a éste son la distribución de la llave.

Los criptosistemas asimétricos, son también llamados de llave pública. Esto debido a que para su funcionamiento se utilizan dos llaves: una pública y otra privada, el esquema general de un algoritmo de este tipo, es que por ejemplo **A** tiene conocimiento de ambas, tanto la llave pública como la privada, mientras que a **B** (o cualquier otro **E**) se le comunica la llave pública únicamente. Debido a esto **B** podrá encriptar sus mensajes con esta llave pública, pero solo **A** con conocimiento de la llave privada podrá desencriptar este mensaje[16]. En este tipo de sistemas es posible crear lo que se conoce como *firmas electrónicas*, el proceso es que **A** encriptará un mensaje con la llave privada, que será enviado a **B**, éste haciendo uso de la llave pública podrá desencriptar el mensaje asegurando que su remitente contiene la llave privada necesaria para la comunicación, además que se cercioran que no haya una intromisión por parte de algún **E** en el canal de comunicación.

Como ejemplo de sismetas simétricos podemos mencionar AES (Advanced Encryption Standard) y DES (Data Encryption Standard). Mientras que un sistema asimétrico incluye al RSA (Rivest-Shamir-Adleman), y ECC (Elliptic Curve Cryptography).

2.1. Nota de un solo uso

Como se ha mencionado un criptosistema simétrico requiere el uso de una sola llave para la encriptación y la desencriptación, por lo que es un criptosistema de llave única. La *nota de un solo uso* propuesto por Gilbert Vernam en 1926 resolvía este problema en teoría [18].

Para que esto sea posible se deben cumplir al menos cuatro aspectos:

- Generación aleatoria de la llave.
- Una llave del mismo tamaño que el mensaje.
- Nunca reutilizar la llave.
- Mantener completamente la llave.

Siguiendo estos puntos, se podría mantener el mensaje cifrado en completo secreto y sería irrompible la encriptación. Vernam planteo el cifrado que lleva su nombre en 1919 [19], donde proponía un esquema electrónico con la implementación de una operación XOR. El nombre de "nota"se debe a que cuando se creo el protocolo se utilizaba una libreta con los códigos para encriptar.

El modelo de la nota de un solo uso, consiste en que un emisor **A** encriptará un mensaje m_1 que consiste en una cadena plana de bits con una cadena *aleatoria* k como llave ($s = m_1 \oplus k$, donde $\oplus$ denota la suma binaria modulo 2). Este mensaje encriptado s puede ser entonces enviado a un receptor **B** que aplicando la llave k desencriptaría el mensaje para obtener m_1 ($s \ominus k = m_1 \oplus k \ominus k = m_1$, donde $\ominus$ denota la operación inversa a $\oplus$).

Entonces, si esta llave no fuera usada una sola vez para la encriptación un agente **E** podría obtener información sobre la llave k. Si s_1 y s_2 son creados con una misma llave k, en criptografía clásica es posible copiar un bit el cual se podría encontrar como:

$$s_1 \oplus s_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \ominus k = m_1 \oplus m_2$$

2.2. Polarización

La luz puede ser analizada como una onda electromagnética transversal, dado su vector de campo electromagnético el cuál oscila en el tiempo y espacio. Sea un haz de luz que se propaga en el espacio, si la orientación del campo es constante aún cuando su magnitud y signo cambian, se dice que la luz es linealmente polarizada[20] [1].

Ahora si dos ondas oscilantes linealmente polarizadas con la misma dirección y frecuencia son coliniales, la onda resultante de la superposición de estas dos seguirá siendo una onda de luz linealmente polarizada. Pero cuando las componentes de éstas dos ondas son perpendiculares, la onda

resultante no será linealmente polarizada.

Otra consideración para una descripción más realista del fenómeno relacionado con el perfil del estado de polarización de la luz es el medio. En un medio isotrópico, la dirección de propagación siempre es perpendicular a la dirección en que se propaga la onda. Dando como resultado dos direcciones independientes que pueden ser escogidas de manera arbitraria, si las dos componentes son no correlacionadas la dirección resultante de la oscilación sera aleatoria y se dice que la onda de luz esta no polarizada o que presenta polarización aleatoriamente.

Las dos perturbaciones ópticas ortogonales pueden ser escritas como

$$\mathbf{E}_x = A_x \cos(\omega t - kz + \delta_x)\hat{x} \tag{2.1}$$
$$\mathbf{E}_y = A_y \cos(\omega t - kz + \delta_y)\hat{y} \tag{2.2}$$

donde A_x y A_y son dos amplitudes positivas e independientes y las fases quedan representadas por δ_x y δ_y las cuales son variables (toman valores entre $-\pi < \delta_{x,y} < -\pi$) que muestran la independencia entre las dos componentes del perfil de polarización. El estudio de este fenómeno de superponer dos ondas electromagnéticas es bien conocido desde mecánica clásica con el oscilador armónico bidimensional. La orbita general de este movimiento es una elipse. Por lo que para las ondas ópticas sería el estado más general es un perfil elíptico, los estados de polarización lineal y esféricos están contenidas en este modelo.

El estado de polarización lineal se da cuando la fase relativa $\delta = \delta_y - \delta_x$ es cero, en otras palabras hay un desfase de π entre una componente y otra

$$\mathbf{E} = (A_x\hat{x} + A_y\hat{y}) \cos(\omega t - kz) \tag{2.3}$$

La onda resultante oscilará en el plano ortogonal la dirección de propagación dada por el cociente de sus dos componentes

$$\frac{E_y}{E_x} = \frac{A_y}{A_x} \tag{2.4}$$

Como las amplitudes A_x y A_y son independientes, el vector de campo eléctrico de luz linealmente polarizada puede vibrar en cualquier dirección del plano xy.

Cuando el desfase entre ambas componentes sea de $\pi/2$ ocurrirá una oscilación del vector de campo eléctrico a lo largo del plano xy. Esto ocurre cuando $A_x = A_y$ y $\delta = \delta_y - \delta_x = \pm\pi/2$. Esto daría como resultado una onda con perfil

$$\mathbf{E} = A_x \cos(\omega t - kz)\hat{x} + A_y \sin(\omega t - kz)\hat{y} \tag{2.5}$$

Por convención de la regla de mano derecha, la polarización circular derecha ocurre cuando $\delta = -\pi/2$, la cual corresponde en rotación levógira del vector de campo en el plano xy. Lo contrario ocurre para $\delta = \pi/2$ con rotación dextrógira y un estado de polarización circular izquierda

Como se menciono el estado de polarización elíptica es el caso más general de un rayo de luz polarizada. Las ecuaciones (2.1) y (2.2) en un punto específico del espacio ($z = 0$) son la

parametrización de una elipse dado por el punto final del vector de de campo eléctrico. La ecuación de una elipse se puede obtener quitando la dependencia en (ωt) estas ecuaciones una vez que se ha tomado como referencia un punto el espacio donde $(z = 0)$. Obteniendo como resultado

$$\left(\frac{E_x}{A_x}\right)^2 + \left(\frac{E_y}{A_y}\right)^2 - 2\frac{\cos\delta}{A_x A_y}E_x E_y = \sin^2\delta \tag{2.6}$$

2.2.1. Birrefringencia

Es interesante realizar un estudio sobre el medio en que se transmite la luz. En un modelo más realista la luz podría interactuar con un medio óptico anisotrópico, donde el desplazamiento eléctrico $\mathbf{D}$ es proporcional al campo eléctrico $\mathbf{D} = \varepsilon\mathbf{E}$, pero debido a que estamos dentro de un medio anisotrópico la permitividad ε y el índice de refracción n serán ahora tensores. Entonces si consideramos la onda plana

$$\mathbf{E} = E_0 e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} \tag{2.7}$$

donde $\mathbf{r}$ es el vector de posición, $\mathbf{k}$ el vector de onda y ω la frecuencia angular. Ahora debemos encontrar los vectores de onda $\mathbf{k}$ permitidos. Para hacer esto combinamos las ecuaciones de Maxwell en la materia, suponiendo que no hay corrientes (cargas libres) y obtenemos la ecuación de onda

$$-\nabla\times(\nabla\times\mathbf{E}) = \mu_0\frac{\partial\mathbf{D}}{\partial t^2} \tag{2.8}$$

Ahora si sustituimos la ecuación (2.7) en ésta última ecuación obtenemos

$$(-\mathbf{k}\cdot\mathbf{k})\mathbf{E} + (\mathbf{k}\cdot\mathbf{E})\mathbf{k} = -\mu_0\omega^2(\varepsilon\mathbf{E}) \tag{2.9}$$

Para encontrar los valores de $\mathbf{k}$ dada una frecuencia ω es recomendable utilizar coordenadas cartesianas con los ejes x, y y z elegidos de tal manera que sean simétricos a los ejes del cristal, resultando en una matriz diagonal para el tensor de permitividad ε

$$\varepsilon = \varepsilon_0\begin{bmatrix} n_x^2 & 0 & 0 \\ 0 & n_y^2 & 0 \\ 0 & 0 & n_z^2 \end{bmatrix} \tag{2.10}$$

donde los valores de la diagonal son los cuadrados de los índices de refracción para una polarización a lo largo de los tres ejes principales. Ahora utilizando esta forma de ε y la definición $c^2 = \frac{1}{\mu_0\varepsilon_0}$ podemos escribir el sistema de ecuaciones

$$\left(-k_y^2 - k_z^2 + \frac{\omega^2 n_x^2}{c^2}\right)E_x + k_x k_y E_y + k_x k_z E_z = 0 \tag{2.11}$$

$$k_x k_y E_x + \left(-k_x^2 - k_z^2 + \frac{\omega^2 n_y^2}{c^2}\right)E_y + k_y k_z E_z = 0 \tag{2.12}$$

$$k_x k_z E_x + k_y k_z E_y + \left(-k_x^2 - k_y^2 + \frac{\omega^2 n_z^2}{c^2}\right)E_z = 0 \tag{2.13}$$

donde E_x, E_y, E_z y k_x, k_y, k_z son las componentes de E_0 y $\mathbf{k}$ respectivamente. Como obtuvimos un conjunto de ecuaciones lineales para E_x, E_y, E_z, significa que podemos obtener una solución no trivial mientras que el siguiente determinante sea cero

$$\begin{vmatrix} \left(-k_y^2 - k_z^2 + \frac{\omega^2 n_x^2}{c^2}\right) & k_x k_y & k_x k_z \\ k_x k_y & \left(-k_x^2 - k_z^2 + \frac{\omega^2 n_y^2}{c^2}\right) & k_y k_z \\ k_x k_z & k_y k_z & \left(-k_x^2 - k_y^2 + \frac{\omega^2 n_z^2}{c^2}\right) \end{vmatrix} = 0 \tag{2.14}$$

Evaluando el determinante y reordenando términos, obtenemos la ecuación

$$\frac{\omega^4}{c^4} - \frac{\omega^2}{c^2}\left(\frac{k_x^2+k_y^2}{n_z^2} + \frac{k_x^2+k_z^2}{n_y^2} + \frac{k_y^2+k_z^2}{n_x^2}\right) + \left(\frac{k_x^2}{n_y^2 n_z^2} + \frac{k_y^2}{n_x^2 n_z^2} + \frac{k_z^2}{n_x^2 n_y^2}\right)\left(k_x^2+k_y^2+k_z^2\right) = 0 \tag{2.15}$$

Para el caso de un material uniaxial, elegimos el eje óptico sobre la dirección del eje z por lo cual $n_x = n_y = n_o$ y $n_z = n_e$, por lo que podemos factorizar la ecuación anterior de la siguiente manera

$$\left(\frac{k_x^2}{n_{\mathrm{o}}^2} + \frac{k_y^2}{n_{\mathrm{o}}^2} + \frac{k_z^2}{n_{\mathrm{o}}^2} - \frac{\omega^2}{c^2}\right)\left(\frac{k_x^2}{n_{\mathrm{e}}^2} + \frac{k_y^2}{n_{\mathrm{e}}^2} + \frac{k_z^2}{n_{\mathrm{o}}^2} - \frac{\omega^2}{c^2}\right) = 0 \tag{2.16}$$

Eligiendo valores que hagan cualquiera de los factores de la ecuación anterior cero, dará como resultado una superficie elipsoidal en el espacio de los vectores de onda $\mathbf{k}$ permitidos para cierta frecuencia ω. El primer término de la ecuación igualado a cero define una esfera, ésta es la solución para los llamados rayos ordinarios asociados a n_o, independiente de la dirección de $\mathbf{k}$. Mientras que el segundo término igualado a cero define una elipse simétrica al rededor del eje z, esta solución corresponde a los llamados rayos extraordinarios asociados a n_e, y cuyo índice de refracción efectivo se encuentra entre n_o y n_e dependiendo de la dirección de $\mathbf{k}$ [21].

Podemos entonces entender el problema como el fenómeno que ocurre cuando la luz se propaga a través de una sustancia traslúcida lo hace excitando los átomos del medio. Los electrones son estimulados por el campo incidente $\mathbf{E}$, éstos radian; los frentes de onda secundarios se recombinan y da como resultado una onda refractada. La velocidad de la luz en el material y por lo tanto su índice de refracción, es determinada por la diferencia entre la frecuencia del campo incidente $\mathbf{E}$ y la frecuencia natural de los átomos. Por lo tanto una anisotropía en los enlaces del medio darán como resultado una anisotropía en el índice de refracción. Típicamente un material que presenta dos índices de refracción se dice que es birrefringente. Por ejemplo si suponemos un cristal cuyas fuerzas de enlace en la dirección y y z son idénticas, y las del eje x no, entonces éste definirá la dirección del eje óptico. El eje óptico es de hecho una dirección de propagación y no una línea recta.

Una de las aplicaciones prácticas de la birrefringencia son los elementos retardadores, los cuales sirven para cambiar la polarización de una onda incidente. Estos retardadores son de hecho, retardadores de fase relativa, su función es cambiar la fase de uno de las dos componentes ortogonales del vector de campo incidente. Estos retardadores siempre tendrán especificados dos ejes perpendiculares, uno rápido y uno lento, que corresponden a los ejes de los rayos ordinarios y extraordinarios.

2.3. Teorema de no clonación cuántica

En la década de los 80's se planteó el cuestionamiento si era posible comunicar información a velocidades mayores a las de la luz, este problema terminó planteándose de manera más simple, como si fuese posible copiar un estado cuántico desconocido [22]. Dentro de la QC y la información cuántica en general se espera que sea imposible poder obtener información de un estado cuántico a través de crear una copia exacta. Esta pregunta fue respondida de manera indirecta por Wootters y Zurek y Dieks en 1982, con su teorema de imposibilidad de la mecánica cuántica [23].

Matemáticamente el planteamiento para copiar un estado cuántico desconocido, sería que tengamos una máquina que toma un estado $|\psi\rangle$ hace una copia sobre un segundo estado $|\Xi\rangle$

$$|\psi\rangle|\Xi\rangle \rightarrow |\psi\rangle|\psi\rangle$$

Pero este tipo de máquina es imposible de ser creada [23]. Una manera simple de explicar esto es: si suponemos un estado como combinación $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$, entonces obtendríamos como salida al aplicar el tratamiento de esta "maquina"lo siguiente

$$|\psi\rangle|\Xi\rangle \rightarrow \alpha|\psi_1\rangle|\psi_1\rangle + \beta|\psi_2\rangle|\psi_2\rangle$$

Pero por lo que deberíamos obtener por linealidad del estado es una combinación de la siguiente manera

$$|\psi\rangle|\psi\rangle = \alpha^2|\psi_1\rangle|\psi_1\rangle + \beta^2|\psi_2\rangle|\psi_2\rangle + \alpha\beta[|\psi_1\rangle|\psi_2\rangle + |\psi_1\rangle|\psi_2\rangle]$$

Dicho de otra forma si suponemos que dos sistemas cuánticos A y B, cuyos espacios de Hilbert $\mathcal{H}_A$ y $\mathcal{H}_B$ son subespacios de $\mathcal{H}$ de manera que $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}$. Entonces se quiere copiar el estado desconocido $|\psi\rangle_A \in \mathcal{H}_A$ en un estado "vacío"$|e\rangle_B \in \mathcal{H}_B$, independiente de $|\psi\rangle_A$. Este estado compuesto esta descrito por el producto tensorial $\mathcal{H}_A \otimes \mathcal{H}_B$

$$|\psi\rangle_A \otimes |e\rangle_B \equiv |\psi\rangle_A |e\rangle_B \tag{2.17}$$

Por lo que para realizar una copia sería necesaria una transformación unitaria U que logre lo siguiente

$$U|\psi\rangle_A |e\rangle_B = |\psi\rangle_A |\psi\rangle_B \tag{2.18}$$

como el estado del sistema $\mathcal{H}_A$ es arbitrario y desconocido, debería cumplir también

$$U|\phi\rangle |e\rangle_B = |\phi\rangle_A |\phi\rangle_B \tag{2.19}$$

Por lo que si se toma el producto escalar

$$(\langle\phi|_A \langle e|_B U^\dagger)(U|\psi\rangle_A |e\rangle_B) = (\langle\phi|_A \langle\phi|_B)(|\psi\rangle_A |\psi\rangle_B) = (\langle\phi|\psi\rangle)^2 \tag{2.20}$$

Por otro lado dado que U es unitario, se tiene que $UU^\dagger = 1$ y que los estados están normalizados, entonces

$$(\langle\phi|_A \langle e|_B U^\dagger)(U|\psi\rangle_A |e\rangle_B) = \langle\phi|_A \langle e|_B |\psi\rangle_A |e\rangle_B = \langle\phi|\psi\rangle \tag{2.21}$$

Dado que siguiendo dos caminos posibles y válidos, se llega a la expresión

$$\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2 \tag{2.22}$$

Lo que implica que $|\psi\rangle = |\phi\rangle$ lo cual no se puede aplicar U a un estado arbitrario y obtener una copia; o que $\langle\phi|\psi\rangle = 0$ que es un caso particular en el que los estados son ortogonales y tampoco es válido para un estado arbitrario.

Entonces no existe operador unitario U actuando sobre $\mathcal{H}_A \otimes \mathcal{H}_B$ de forma que para todos los estados normalizados $|\psi\rangle_A$ y $|e\rangle_B$ en $\mathcal{H}$ cumplan que

$$U\,|\psi\rangle_A\,|e\rangle_B = |\psi\rangle_A\,|\psi\rangle_B$$

Por lo que teóricamente es demostrable que no existe la posibilidad sin romper las formulaciones fundamentales de la mecánica cuántica de que un intruso **E** pueda clonar estados cuánticos que sean utilizados en un protocolo de comunicación, para obtener información sobre el mensaje que se plantea enviar[24].

2.4. Protocolo BB84

La QC es hipotéticamente el único tratamiento que se tenga para mantener la privacidad entre dos interlocutores, a pesar de la intromisión de un tercer agente con capacidad de cómputo teóricamente ilimitado [25]. Además de que plantea la primera aplicación tecnológica a un verdadero nivel cuántico, hasta el día de hoy, esto se debe a que para funcionar se deberían enviar en únicamente estados cuánticos individuales.

Los principios de la QC se deben al trabajo de investigación de Stephen Wiesner en la década de los 70, tan solo unos años después de la creación del cifrado de Vermann, en el cual propone utilizar la polarización de un fotón para poder hacer una distribución de la llave [13].

Estos trabajos son retomados por Guilles Brassard y Wiesner a lo largo de la segunda mitad del siglo XX, donde comienzan a utilizar ideas de mecánica cuántica, para diseñar (*notas bancarias*) que fueran imposibles de decifrar sin violar leyes de la naturaleza [26].

Durante Octubre de 1979, Brassard y Bennet derivado de este trabaj, encontraron una manera de utilizar luz polarizada como nuevo paradigma de criptosistema de llave pública junto con un cifrado de Vermann (o nota de un solo uso), para generar una distribución de llaves. El término QKD nace en 1983 en el *IEEE Symposium on Onformation Theory* al exponer sus avances en el campo. Para 1984 se publican sus avances y son presentados en "Quantum cryptography: Public-key distribution and coin tossing"[14]. Tras 10 años de colaboración en Octubre de 1989 el protocolo BB84 es puesto a prueba de manera experimental [27].

La codificación cuántica por si misma garantiza una de las ventajas de la criptografía de llave pública al permitir una distribución de llaves aleatórias seguras entre dos interlocutores antes de compartir información secreta [14]. Aún con la presencia de un espía, es posible mantener la distribucón de la llave compleamente segura. Un punto clave es que a pesar de la actividad de un espía

y que éste cuente con un hipotético poder de cómputo ilimitado, el protocolo es lo suficientemente robusto en el tema de seguridad que es simplemente imposible de romper sin violar leyes fundamentales de la mecánica cuántica [**?**].

El espacio de Hilbert para un fotón polarizado es 2-dimensional; entonces el estado del fotón puede ser descrito como una convinación lineal de dos vectores base unitarios $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ y $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Los cuales representan la polarización horizontal y vertical respectivamente.

En general, un par de estados polarizados serán referidos como una *base* y dos bases son conjuadas si al medir una propiedad (cuántica) cambia aleatoriamente la otra. Por lo cual las bases utilizadas para enviar información codificada en estados cuánticos no ortogonales [28] serán

$$\mathcal{B}_1 = \{|0\rangle, |1\rangle\} \tag{2.23}$$

$$\mathcal{B}_2 = \{|+\rangle, |-\rangle\} \tag{2.24}$$

donde $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Los cuales representan una polarización a $-45°$ y $45°$.

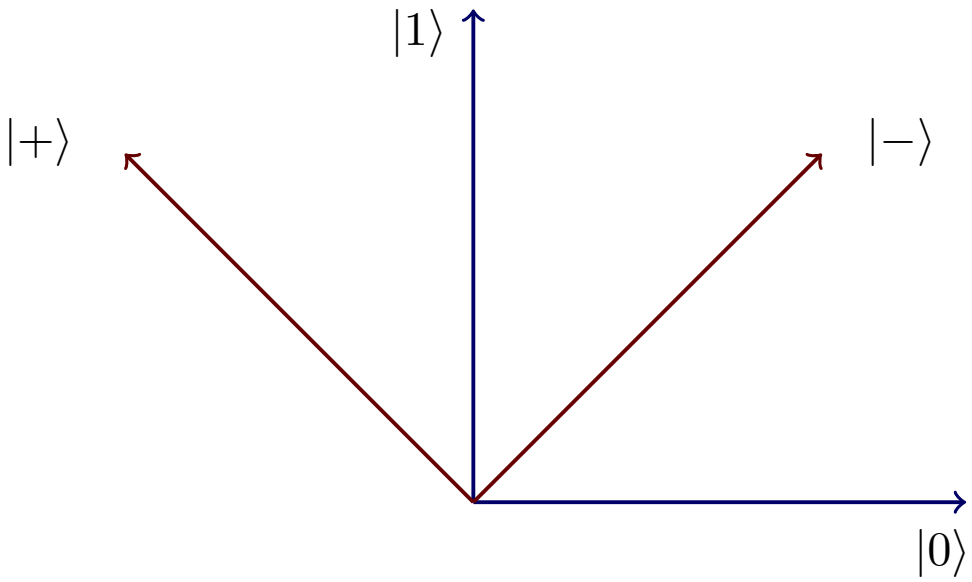


Figura 2.1: Bases mutuamente no ortogonales en el espacio de Hilbert

El protocolo BB84 debe llevarse a cabo con un solo fotón polarizado, esto es debido a que al hacer incidir el fotón sobre un polarizador con la misma orientación con la que fue preparado, que equivale a efectuar la medición en la misma base, éste conservará la orientación de la polarización. Si en cambio el fotón incide en un polarizador con una orientación distinta, es decir se realiza la medición con un abase distitnta con la que fue preparado, éste perderá toda la información sobre la orientación original y emergerá con una polarización correspondiente a la nueva base.

Para establecer una llave criptográfica Alice manda una cadena de N bits en bases elegidas de manera aleatoria. Por su parte, Bob recibirá los N estados, mismos que medirá con una elección

de bases aleatorias. Esta cadena de tamaño N es llamada llave en bruto. Bob anuncia a través de un canal de comunicaciópn clásico las bases que utilizó para efectuar las mediciones, pero no revela sus resultados. Alice decidirá que bits podrán ser utilizados por Bob para establecer la llave, estos serán los bits que hayan sido enviados por Alice y medidos por Bob en la misma base. De aquí se obtiene una cadena de n bits con $n \leq N$ que se llama llave filtrada.

Si hubiera una espía Eve en el canal de comunicación, comunmente referida como Eve, Alice y Bob la podrían detectar comunicando en el canal clásico una parte de la llave filtrada a efecto de encontrar inconsistencias entre los bits enviados y medidos con la misma base.

Esto se puede analizar cuantitativamente con la razón de error de bits cuánticos [29] ($QBER$, por sus siglas en inglés), el cual mide la probabilidad o porcentaje de errores en la distribución de la llave. El ruido dentro del canal cuántico contribuye al QBER, así la actividad la espía Eve en el canal cuántico. La manera de calcular la razón de error es

$$QBER = \frac{N - n}{N}$$

donde N es la Llave en Bruto y n es la Llave Filtrada.

CAPÍTULO 3

Metodología

En esta sección se muestra la metodología de investigación que se siguió para implementar el protocolo BB84 de manera computacional y experimental. El objetivo principal del trabajo es el entendimiento e implementación del protocolo, por lo cuál una vez que se tiene una base teórica sobre el funcionamiento de éste, se planteó utilizar un equipo analógico debido a la accesibilidad y su enfoque pedagógico para entender el fenómeno. Hecho que representó varios problemas técnicos, pero aún dadas estas condiciones es posible obtener resultados concretos. En la parte experimental se utilizó un Kit de Demostración EDU-QCRY1_M de la empresa Thor LABS, los detalles de este equipo y el estudió que se hizo con el se muestran a continuación. Para la implementación computacional se utilizó un algoritmo que sintetizara los procesos implicados en el protocolo, él cual presenta simplificaciones para hacer más factible el estudio, esto en aras del tiempo disponible.

El arreglo experiental utilizado para la implementación del protocolo BB84. Dicho arreglo experimental consta de dos diodos láser de clase 2 con emisión en 635 nm, 4 placas $\lambda/2$ de orden cero, 2 divisores de haz polarizados de 20mm$\times$20mm, 4 sensores, así como diversas componentes mecánicas a fin de fijar todos los elementos en una mesa óptica.

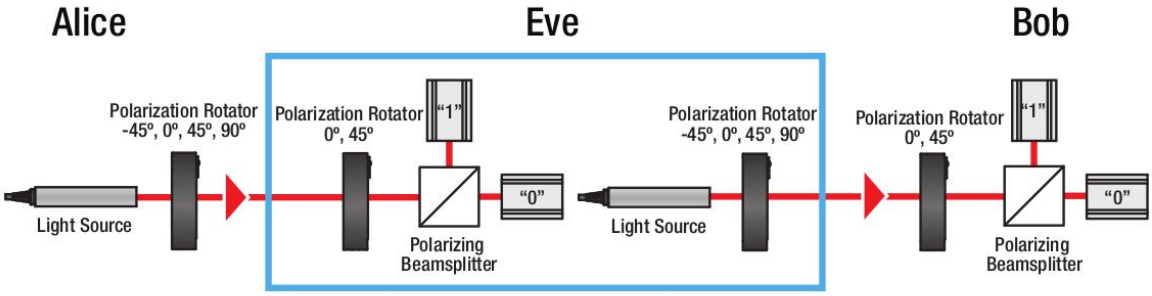


Figura 3.1: Arreglo experimental EDU-QCRY1_M Thor LABS

El láser es un dispositivo de Luz Amplificada por Emisión Estimulada de Radiación, la palabra es un anglisismo[1]. El funcionamiento de este tipo de dispositivos se puede simplificar de la siguiente

manera; la luz esta cuantizada

$$E = h\nu \tag{3.1}$$

donde h es la constante de Planck y ν es la frecuencia de la radiación incidente.

De manera clásica la probabilidad de distribución media de un número de átomos por unidad de volumen N_i obedece la distribución de Maxwell-Boltzmann

$$N_i = N_0 e^{-\varepsilon_i \beta} \tag{3.2}$$

donde β es la temperatura estadística definida en términos de la constante de Boltzmann k_B y la temperatura del sistema T como $\beta = \frac{1}{k_B T}$

Debido al argumento de la exponencial negativa podemos deducir que a mayor energía en el sistema, habrá una probabilidad menor de hallar átomos en este estado. Por lo cual los átomos tenderán a estar en el estado de menor energía del sistema (su probabilidad será mayor).

Si pensamos en dos niveles atómicos cuya transición de estado es permitida, con energías $\varepsilon_j > \varepsilon_i$ tendremos que la propoción de las poblaciones que ocupan los dos estados será la siguiente donde N_j presenta la misma constante de estados ocupados N_0, se dice que $N_j = N_0 e^{-\varepsilon_j \beta}$. Entonces

$$\frac{N_j}{N_i} = \frac{e^{-\varepsilon_i \beta}}{e^{-\varepsilon_j \beta}} \tag{3.3}$$

Por lo cual deducimos que para el estado con energía ε_j la distribución N_j toma la forma

$$N_j = N_i e^{-(\varepsilon_j - \varepsilon_i)\beta} = N_i e^{-h\nu_{ji}\beta} \tag{3.4}$$

en este caso la transición se dará cuando la diferencia de energía de estos $(\varepsilon_j - \varepsilon_i)$ que es igual a la energía de un fotón incidente o emitido con frecuencia ν_{ji}. Esto es $(\varepsilon_j - \varepsilon_i) = h\nu_{ji}$.

Es importante recalcar que la misma naturaleza de la transición de estados de la nube electrónica da como resultado distintos fenómenos que siguen el mismo comportamiento estos son: absorción estimulada, la emisión espontánea y la emisión estimulada. Cada uno de ellos juega un papel importante en la descripción del comportamiento de un láser [20].

Suponiendo el modelo de dos niveles monoatómico podemos describir coloquialmente estos fenómenos como

- Absorción estimulada: Ocurre cuando um fotón con energía $h\nu_{ji}$ es igual a la diferencia de energía $(\varepsilon_j - \varepsilon_i)$ por lo cual excita el sistema ocurriendo una transición de estado, del estado base a un estado excitado que no es estable.
- Emisión espontánea: Esta sucede como reacción a la absorción estimulada, al encontrarse el electrón en un estado excitado no estable, decae emitiendo un fotón con la misma energía $h\nu_{ji}$, correspondiente a la diferencia de estados.
- Emisión estimulada: Este fenómeno solo ocurrirá en procesos colectivos, debido a que hay un N número de electrones decayendo los cuales emiten fotones con energía $h\nu_{ji}$ correspondiente

a la diferencia entre el estado base y el excitado, es posible en una gas o en una red cristalina que algunos de estos fotones vuelvan a causar absorción estimulada sobre otros átomos del sistema dando lugar a un proceso de reemisión del sistema.

Es de hecho la emisión estimulada la que hace posible el funcionamiento del láser, éste está conformado por cuatro componentes; el mecánismo de excitación o bombeo es el componente que produce la absorción estimulada, esta puede ser inducida por bombeo óptico (una lámpara incandescente), colisión de electrones (un gas en presencia de una diferencia de potencial) o pro procesos químicos (creando y/o rompiendo enlaces). Por otra parte el medio de acción será el material donde se producirá la amplificación óptica, el mecanismo de retroalimentación (la cual creará la emisión estimulada) y la ventana de salida forman juntos la *cavidad* del láser. Como resultado de todo el proceso el láser emite un pulso de femtosegundos de luz polarizada. Para el estudio realizado suponemos que la polarización de salida del láser es lineal.

Por otro lado las placas $\lambda/2$ son dispositivos que nos permiten controlar la polarización de un haz de luz incidente[30]. Estas introducen una diferencia de fase relativa de π entre las ondas o y e. Si supones que el plano de vibración de un haz incidente de luz lineal con longitud de onda λ_0 (linealmente polarizada) forma un ángulo arbitrario θ con el eje rápido. Al salir las ondas de ésta placa, se producirá un desfase relativo de $\lambda_0/2$, esto dará resultado que el vector de onda incidente $\mathbf{E}$ habrá girado en un ángulo 2θ. Para el caso de un haz linealmente polarizado que incida a 45° con respecto al eje óptico cambiara su plano de vibración de tal manera que saldrá a -45° del eje óptico, en pocas palabras para polarización lineal cambia la dirección con respecto al eje, para luz elíptica o circularmente polarizada invertirá el sentido con el que incidan, pasándola de derechas a izquierdas o viceversa.

Un divisor de haz es es un dispositivo óptico, que como su nombre lo dice, divide un haz de luz en dos[30]. Comúnmente un divisor de haz es un objeto cúbico que resulta de unir dos prismas triangulares, fabricados a base de polímeros o vidrio. En principio un haz de luz incidente por una de las caras tendrá una distribución de 50:50, donde una mitad de éste será transmitido y la otra será reflejada.

El fenómeno que da como resultado la reflexión se conoce como reflexión total interna frustrada. Para explicarlo solo tenemos que imaginar que un haz de luz viaja dentro de un bloque de vidrio o polímero y éste se refleja internamente en una frontera (ocurre una reflexión interna total). Podemos entonces unir otra pieza de vidrio a la primera, desapareciendo la interfaz aire-vidrio, entonces el haz se transmitiría sin ser perturbado. Pero si existiera una película de aire pequeña, habría también una componente reflejada.

De manera general la onda evanescente se propaga con una amplitud apreciable a través de un medio menos denso hacia una región ocupada con un índice de reflexión más alto, la energía ahora puede fluir a través del espacio que los separa. Esto es, que si la onda evanescente, después de atravesar el espacio separador (una interfaz delgada de aire), es aún lo suficientemente fuerte (presenta una potencia apreciable) se podrá transmitir a través del segundo material.

Los divisores de haz polarizado utilizan el mismo funcionamiento, pero estos presentan el uso de materiales birrefringentes en la interfaz, para poder discernir la polarización del haz incidente

y de esta manera transmitir los haces con polarización horizontal y reflejar los que presenten una polarización vertical[1].

Mientras que los detectores son cajas negras en este estudio, debido a que el fabricante del equipo se reserva la información sobre su funcionamiento o el tipo de detectores que usan. Típicamente los más utilizados de manera comercial y en la investigación son los fotodiodos de avalancha (APD, por sus siglas en inglés) debido a su eficiencia cuántica[31]. Ya que están hechos de tres materiales semiconductores diferentes: los más usados son silicio, germanio o la unión InGAs (indio, germanio y arsénico). Los APDs operan usualmente en el llamado *modo Greiger*. En este modo, dando como resultado que un fotón absorbido desencadena una avalancha de electrones que consta de miles de portadores. Para restablecer el diodo, esta corriente macroscópica debe apagarse: la emisión de cargas debe detenerse y el diodo es recargado.

3.1. Implementación experimental.

Para calibrar el equipo se siguió el procedimiento del manual es cual consiste en alinear el plano de polarización del láser con la orientación de la placa $\lambda/2$. El láser presenta un modo de pulsos y uno continuo, al usar el modo continuo ajustamos que el láser estuviera paralelo a los divisores de haz. Se ajusto que la luz a 90° (verticalmente polarizada) fuera reflejada, para obtener esto se busco que la intensidad reflejada del láser fuera mínima, de esta manera nos aseguramos que la polarización del láser es horizontal. Ahora colocando la placa $\lambda/2$ entre el láser y el divisor de haz se utilizó el mismo criterio de intensidad para encontrar el eje rápido y el eje lento de la placa $\lambda/2$, se ajusto mecánicamente, de esta manera nos aseguramos que el equipo estuviera calibrado, para corroborarlo los detectores tienen una función de detención y otra de calibración, con esta ultima se puede verificar que el equipo esta alineado y bien calibrado.

Para la obtención de los resultados se tomaron en cuenta varias suposiciones [32] [33] [34]. En la sección anterior se detalla una introducción sobre el funcionamiento del láser, así como de los componentes ópticos que juegan un papel en el arreglo experimental, para el haz emitido por el láser, se toma como consideración que éste esta emitiendo un pulso que puede ser interpretado como un solo fotón aunque el sistema se encuentra emitiendo un paquete de fotones. También se toma como suposición que este pulso corresponde a un haz linealmente polarizado.

Tomando en cuenta que el láser emite un haz linealmente polarizado **A** puede hacer la elección de su base y el bit (0,1) que desea enviar, con el simple hecho de hacer una elección correcta del ángulo con el que hará incidir el haz sobre una placa $\lambda/2$. Como convención la base $\mathcal{B}_1$ estará representada por los ángulos a 0°, el cual corresponderá a un bit 0, y 90° que será un bit 1. Para la base $\mathcal{B}_2$ serán los ángulos $-45°$, 45° que representarán los bit 0 y 1 respectivamente. Ahora pues para generar una llave **A** solo tendrá que hacer una elección aleatoria de la base que utilizará y el bit que enviará, recordando que la llave deberá ser a lo menos del mismo tamaño que el mensaje en binario como texto plano.

Para esto se utilizó un algoritmo en el que se empleó el generador de números aleatorios de Octave, que permitiera generar ésta elección de bases. En este punto se hizo otra suposición sobre la

implementación experimental ya que como es sabido las computadoras no pueden generar números aleatorios, en su defecto utilizan algoritmos para generar números pseudoaleatorios. Pero confiando en que un ordenador nos proporciona mayor aleatoriedad que la elección que un humano podría hacer, se utilizó esta herramienta. Como se ha descrito para **B** bastará solo con la elección de la base en que desea medir el bit enviado por **A**, las cuales fueron elegidas del mismo modo que **A**. Por lo que este solo tiene que discriminar entre utilizar $\mathcal{B}_1$ o $\mathcal{B}_2$, los cuales por convención están representados por un ángulo a 0° y 45° respectivamente.

Analizando un caso específico del proceso en el que **A** envié un bit 0 en base $\mathcal{B}_2$ y **B** lo mida con la base $\mathcal{B}_1$ y con $\mathcal{B}_2$. Entonces tenemos que físicamente **A** enviará un fotón (un pulso del láser) y lo hará pasar por una placa $\lambda/2$ con un ángulo a $-45°$ ahora el haz de luz viajará a través del aire hasta llegar al módulo de **B**. Si al incidir, éste utiliza una la base $\mathcal{B}_1$, significa que pondrá su placa a un ángulo de 0° por lo que el haz seguirá su camino con una inclinación de $-45°$ respecto al eje óptico. Ahora ocurre el proceso más importante del arreglo experimental, el fotón incidente llegará hasta el divisor de haz polarizado con éste ángulo, el funcionamiento de éste dispositivo en pocas palabras es transmitir los haces incidentes con polarización vertical (esto es transmitir un haz de luz que incida con un ángulo de 90°) y reflejar aquellos que incidan con una polarización horizontal (los que presenten un ángulo de incidencia a 0°). Por lo que existirá la misma probabilidad de que el fotón sea reflejado o transmitido creando una indeterminación.

Ahora si **B** utiliza la misma base con la fue creado el estado del fotón, para medirlo. Esto es que utiliza $\mathcal{B}_2$ al usar su placa a 45° cambiando la polarización lineal del fotón de $-45°$ a 0° haciendo que este se refleje al interactuar con el divisor de haz polarizado, por lo que el fotón será detectado con una probabilidad del 100 % en el detector que por convención se ha elegido para la llegada de un bit 0.

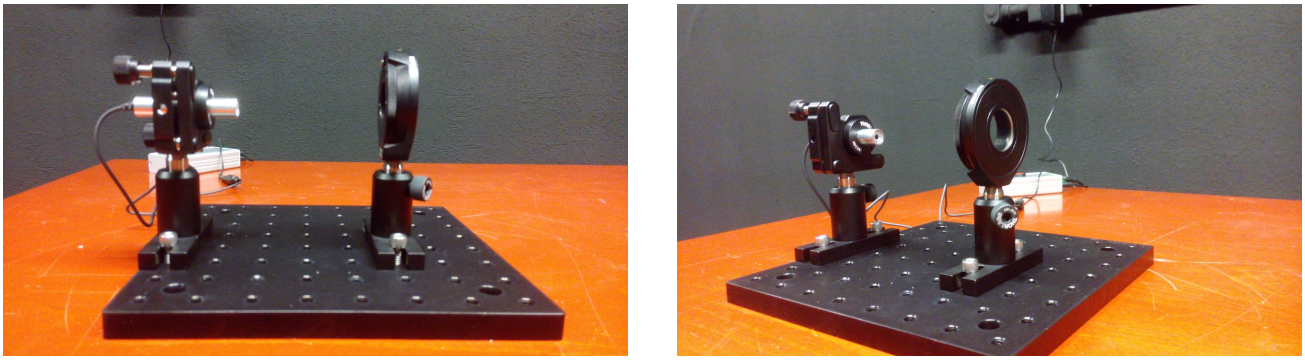


Figura 3.2: Modulo de **A**

Gracias al método de comunicación entre **A** y **B**, además de los principios físicos en que se basa como el teorema de no clonación cuántica o la tecnología de la nota de un solo uso, generan que el protocolo sea en teoría un sistema seguro e irrompible. Esto da como resultado la posibilidad de detectar la intromisión de un agente **E**, debido a que la única forma que tiene para espiar las comunicaciones es el esquema de recepción-envío. Las acciones de **E** en este esquema serán: cortar la línea de comunicaciones, recibir los bits enviados por **A**, generar un nuevo bit y como acto final

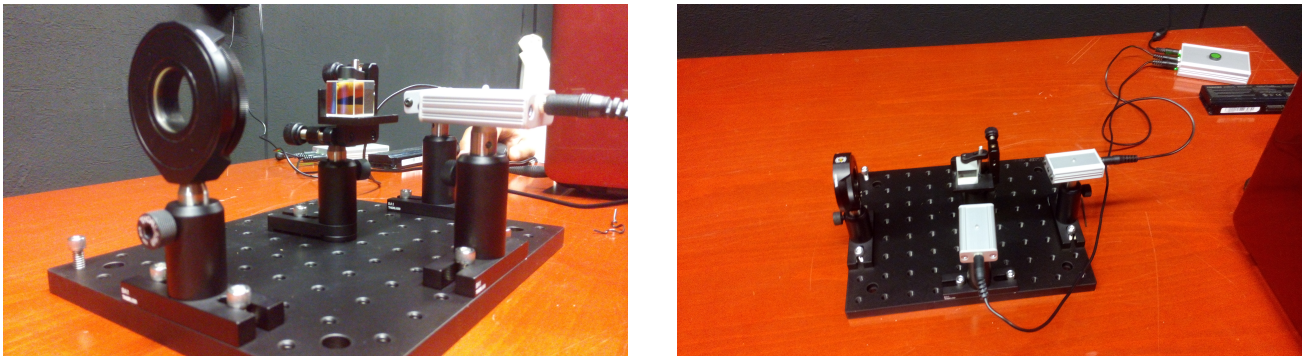


Figura 3.3: Modulo de **B**

Figura 3.4: Modulo de **E**

enviarlo a **B**. Su intromisión se constata cuando debido a que si **E** interviene las comunicaciones, el error en la distribución de los bits aumentara de manera notable por su injerencia en tratar de obtener información de la llave.

3.2. Algoritmo

La implementación computacional se dio una vez que el experimento había sido montado y se habían hecho varias pruebas. Entendiendo la teoría y la práctica se pretendió hacer un estudio simulado del $QBER$ para comparar la fiabilidad del equipo y su implementación realizada [35] [36] [37]. Debido a la forma en que se generó el algoritmo, se utilizo el software de licencia libre GNU Octave para realizar el código.

El protocolo BB84 si bien no puede ser simulado en un computador convencional debido a que no tenemos una forma de simular qbits, ya que esto implicaría simular un sistema cuántico completo, hecho que actualmente se plantea afrontar con la construcción de computadores cuánticos. Pero en cambio, simplificando el protocolo a un modelo que se basa en las decisiones, podemos tener un

aproximado de lo que sucedería, dado que la seguridad recae en la elección correcta de las bases para medir cada bit enviado. Entonces podemos esquematizar el protocolo para una simulación de la siguiente manera

1. Alice elige N bits aleatoriamente

2. Alice elige una cadena de bases aleatorias de tamaño N y codifica cada bit.

3. Alice envía la llave en bruto a Bob.

4. Bob recibe los N bits y los mide con una base aleatoria a cada uno.

5. Alice o Bob anuncian la cadena de bases utilizadas.

6. Los resultados de la medición no son anunciados.

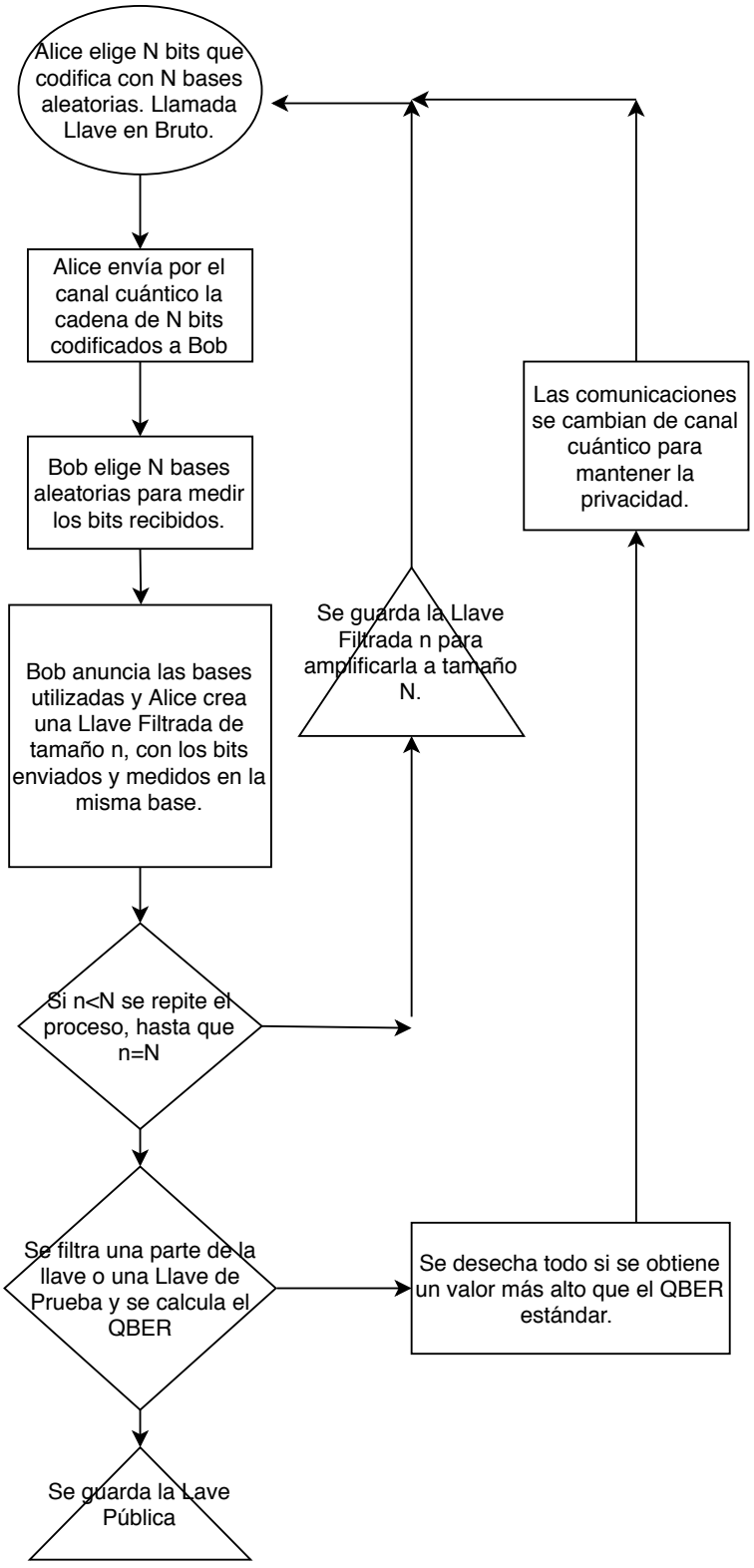
7. Alice y Bob descartan los bits que hayan sido medidos con bases, creando la llave filtrada de tamaño n.

8. Alice toma un conjunto de bits para checar la interferencia de Eve, y comunica con Bob los bits que utilizó.

9. Alice y Bob anuncian y comparan los valores de este conjunto. Si superan el QBER, abortan el protocolo.

10. Alice y Bob proceden a la reconciliación y la amplificación de privacidad para completar la llave.

Para visualizar este proceso en un computador convencional podemos hacer uso de un diagrama de flujo que nos ayude a entender cada uno de los procesos. En el siguiente diagrama los óvalos determinan los pasos de inicio y final, los rectángulos una acción, los rombos decisiones, los triángulos representan archivos si éste se encuentra boca arriba denota uno definido, de lo contrario se refiere a uno indefinido.


Alice elige N bits que codifica con N bases aleatorias. Llamada Llave en Bruto.
Alice envía por el canal cuántico la cadena de N bits codificados a Bob
Bob elige N bases aleatorias para medir los bits recibidos.
Bob anuncia las bases utilizadas y Alice crea una Llave Filtrada de tamaño n, con los bits enviados y medidos en la misma base.
Si n<N se repite el proceso, hasta que n=N
Se guarda la Llave Filtrada n para amplificarla a tamaño N.
Se filtra una parte de la llave o una Llave de Prueba y se calcula el QBER
Se desecha todo si se obtiene un valor más alto que el QBER estándar.
Las comunicaciones se cambian de canal cuántico para mantener la privacidad.
Se guarda la Lave Pública

Como se ha mencionado anteriormente, en una simulación no se podría generar una llave cuya seguridad fuera totalmente segura, de tal escenario se obtiene que no es objeto de estudio en una simulación generar una llave, pero se puede utilizar para estudiar el comportamiento del $QBER$ en un escenario real. Para esto se introdujo ruido en los procesos de comunicación de la llave para hacer más realista el estudio.

Dicho de otro modo, para asegurarnos que Bob y Alice comparten el mismo bit de la llave es necesario haber enviado y medido un fotón en la misma base, por lo que el problema en la simulación se reduce a tomar los casos en los que hayan medido el estado del qubit con la misma base que fue creado o preparado.

Utilizando entonces un código más básico cuya función sería generar "aleatoriamente" un vector con la elección de bases ($\{|0\rangle, |1\rangle\}$) de **A** y **B**, para después verificar que elementos habían sido creados con la misma base, las discrepancias en la elección nos darán entonces la distribución del error que puede ser interpretado como el $QBER$.

CAPÍTULO 4

Resultados y conclusiones

En esta sección se muestra un análisis de los resultados obtenidos tanto en la parte experimental como en la simulación computacional. Se hará un contraste entre los datos obtenidos, para así desarrollar las conclusiones pertinentes sobre el protocolo, su implementación real y hacer un planteamiento de las perspectivas para un estudio más detallado a futuro.

Se expone a continuación los datos obtenidos en la implementación experimental. Como ya se ha mencionado para generar estos datos se montó un Kit de Demostración EDU-QCRY1_M de la empresa Thor LABS. Para los resultados experimentales reportados en este trabajo se utilizaron 20 llaves diferentes generadas de manera aleatoria, las cuales tienen un tamaño de entre 10 y 100 bits. Para probar el efecto de la intromisión de Eve en una hipotética comunicación entre Alice y Bob, se utilizaron 10 llaves para calcular el $QBER$ sin la presencia de la atacante y otras 10 llaves con la presencia del mismo, lo anterior para medir el efecto en los valores numéricos de QBER.

Como resultado del experimento se obtuvo que en un escenario sin la presencia de **E** el $QBER$ era de 28 %, mientras que cuando hay presencia de éste en un esquema de recepción-envío el $QBER$ aumenta notablemente hasta un 40 %. Mientras tanto, como resultado de la simulación se obtuvo que el $QBER$ sin presencia de un atacante es de 48 % y con su presencia de 72 %, estos resultados coinciden con el cálculo teórico, ya que teniendo solo dos opciones a escoger **B** entre las bases que puede utilizar para efectuar la medida se espera que el $QBER$ sea de 50 % y de la misma manera si se tomara en cuenta a un agente **E** el error se duplicaría ya que habría un $QBER$ en su medición de 50 % que a su vez se sumaría con la de **B** dando como resultado un $QBER$ de 75 % o una probabilidad de elegir la misma base de 25 %. La discrepancia entre los resultados esperados y los obtenidos en el experimento se debe en cierta medida a la naturaleza del aparato, al ser un experimento analógico y cuyo funcionamiento depende en gran medida de la manipulación manual, se cree que esto aunado con un espacio no acondicionado en su totalidad provocó un sesgo. Dada la repetición múltiple del experimento y la cantidad de veces que se tuvo que ajustar para hacer cada medición (cerca de 1100) los resultados experimentales no concuerdan con los resultados esperados, pero muestran claramente la tendencia, este hecho es clave para la implementación del protocolo ya que es la referencia para poder poderlo a prueba en un ambiente real y cerciorarnos de que la privacidad de los mensajes estará intacta.

Se puede concluir entonces varias cosas sobre este trabajo. Como primer punto debemos abor-

dar la formulación teórica del protocolo BB84, la cual cambia el paradigma de criptografía clásica, ya que dejamos de confiar en los ordenadores para resguardar nuestra información y comenzamos a explotar los fenómenos físicos asociados a la dualidad onda-partícula de la luz, particularmente a fenómenos que conciernen a la mecánica cuántica. Si bien el BB84 no es como tal un algoritmo de criptografía, resuelve de manera práctica y sencilla (teoricamente) el problema más grande de los algoritmos clásicos, que es la distribución de la llave. Una vez que podamos intercambiar llaves criptográficas de manera real y atendiendo las condiciones de la comunicación moderna, el nuevo paradigma de QKD podrá ser mimetizado con los esquemas clásicos de criptografía, (así como la nueva tecnología cuántica que se desarrolle en función de controlar estados cuánticos individuales, el desarrollo de nuevos y mejores detectores, chips fotónicos o incluso computadores cuánticos); para de esta forma generar el hardware y software necesario que permita un nueva forma de comunicación donde la privacidad no volverá a ser un problema.

Ahora haciendo una conclusión realista con base en los resultados obtenidos en este trabajo podemos encontrar un panorama menos alentador para una implementación real, pero no imposible. En el ámbito experimental actualmente el grupo de investigación no cuenta con la tecnología necesaria para comenzar a hacer pruebas que se acerquen más a una implementación real, con fines comerciales o de investigación, pero éste trabajo nos da como antecedente los puntos que se deben de tomar en cuenta para lograrla. Puntos importantes como la calibración de la fuente de fotones, así como los elementos ópticos, que en este trabajo se ve reflejado de manera muy notoria dados los resultados obtenidos. Otro punto que ya se había mencionado pero vale la pena retomarlo y expandirlo, es que la QC al utilizar fenómenos cuánticos para asegurar la privacidad de las comunicaciones, no nos permite hacer una simulación de tales procesos con un ordenador clásico. Si bien esto es una limitante, no demerita el papel que pueden llegar a jugar éstos en una implementación real, ya que como se ha mencionado el protocolo BB84 resuelve el problema de la distribución de la llave, por lo que el uso de ambas tecnologías (cuántica-fotónica y electrónica) nos permitiría generar esquemas de criptografía híbrida, los cuales retomarían los aspectos importantes (los que provean una mayor seguridad) del paradigma de llave pública tanto como del de llave privada.

En este trabajo se hicieron varias aproximaciones para la implementación experimental y el análisis de los resultados. Como trabajo futuro se plantea el establecimiento de una fuente de fotones individuales a diferencia del laser pulsado que se utilizó en e sta ocación. También se plantea la automatización de los polarizadores a fin de enviar cadenas de bits más largas e introducir el ruido debido al medio (aire en este caso, pero el modelo puede extenderse a una implementación con fibra óptica) que presenta el canal cuántico en el cálculo del $QBER$. Asi mismo existe el interés de generar una simulación computacional que nos permita poder recrear casos en los que las limitaciones experimentales pueden ser ajustadas a diferentes escenarios.

Bibliografía

[1] E. Hetch, *Optics*. Edinburgh Gate Harlow Essex CM20 2JE England: Person Education, fifth ed., 2017.

[2] R. Loudon, "What is a photon?," *The Nature of Light Optical Science and Engineering*, p. 11–22, 2008.

[3] D. Finkelstein, "What is a photon?," *The Nature of Light Optical Science and Engineering*, p. 23–35, 2008.

[4] C. Rangacharyulu, "The nature of light: What is a photon?," *The Nature of Light Optical Science and Engineering*, p. 129–141, 2008.

[5] S. Waghmare, S. Sikhwal, S. Nimje, and T. Pawar, "History of cryptography," *International Journal For Technological Research In Engineering*, vol. 4, no. 8, 2017.

[6] S. Singh, *Codigos Secretos*. Debate, 2000.

[7] D. Davies, "A brief history of cryptography," *Information Security Technical Report*, vol. 2, no. 2, p. 14–17, 1997.

[8] T. W. Judson, *Abstract Algebra Theory and Applications*. Stephen F. Austin State University, 2011.

[9] A. S. R.L Rivest and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[10] M. M. A.K. Lenstra, H.W. Lenstra Jr. and J. Pollard, *The Development of the Number Field Sieve*, vol. 1554 of Lectures Notes in Mathematics. Springer-Verlag, 1993.

[11] P. Shor., "Presentation slides : Quantum error correcting codes and quantum cryptography.," in *Proceedings of the 35th Symposium on Fundations of Computer Science*, p. 124–134, IEEE Computer Society Press, Los Alamitos, 1994.

[12] N. K. Jawahar Thakur, "Des, aes and blowfish: Symmetric key cryptography algorithms simulation based performance analysis," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, pp. 6–12, dec 2011.

[13] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, p. 78–88, 1983.

[14] G. B. C.H. Bennett, "Quantum cryptography: Public-key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, p. 175–179, IEEE Press, Bangalore, India,1984.

[15] INEGI, "Comunicado de prensa num. 122/17."

[16] P. Singh and S. Kumar, "Study and analysis of cryptography algorithms : Rsa, aes, des, t-des, blowfish," *International Journal of Engineering and Technology*, vol. 7, no. 1.5, p. 221, 2017.

[17] R. L. Graham, D. E. Knuth, O. Patashnik, and S. Liu, "Concrete mathematics: a foundation for computer science," *Computers in Physics*, vol. 3, no. 5, pp. 106–107, 1989.

[18] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[19] G. S. Vernam, "Secret signaling system," July 22 1919. US1310719A.

[20] P. Y. Amnon Yariv, *Photonics Optical Electronics in Modern Communications*, vol. III of *IV*. 198 Madison Avenue, New York, New York 10016: Oxford University Press, sixth ed., 2007.

[21] M. Born and E. Wolf, "Principles of optics," 1999.

[22] W. K. Wootters and W. H. Zurek, "The no-cloning theorem," *Physics Today*, vol. 62, no. 2, p. 76–77, 2009.

[23] W. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802–803, 1982.

[24] D. J. Griffiths, *Introduction to Quantum Mechanics*. Pearson Education, Inc., 2005.

[25] "Brief history of quantum cryptography: a personal perspective," *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, Oct 2005.

[26] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Physical Review Letters*, vol. 69, no. 20, p. 2881–2884, 1992.

[27] C. H. Bennett and G. Brassard, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working]," *ACM SIGACT News*, vol. 20, no. 4, p. 78–80, 1989.

[28] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. University Press, Cambridge, 2010.

[29] O.-M. Foong, T. Low, and K. Hong, "Simulation study of single quantum channel bb84 quantum key distribution," pp. 159–167, 01 2018.

[30] J. V. S. Benito, *Manual de óptica geométrica*. Carretera de San Vicente del Raspeig, s/n, 03690 San Vicente del Raspeig, Alicante, España: Universidad de Alicante, first ed.

[31] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, p. 145–195, 2002.

[32] S. Arunachalam, "Quantum key distribution: A resource letter," *International Journal of Computer Applications*, vol. 37, no. 3, p. 11–17, 2012.

[33] T. Baignères, "Quantum cryptography : On the security of the bb84 key-exchange protocol," 07 2010.

[34] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, p. 43–43, 2002.

[35] O. K. Jasim, S. Abbas, E.-S. M. El-Horbaty, and A.-B. M. Salem, "Quantum key distribution: Simulation and characterizations," *Procedia Computer Science*, vol. 65, p. 701–710, 2015.

[36] M. Sharifi and H. Azizi, "A simulative comparison of bb84 protocol with its improved version," 01 2007.

[37] N. H. M. Halip, M. Mokhtar, and A. Buhari, "Simulation of bennet and brassard 84 protocol with eves attacks," *2014 IEEE 5th International Conference on Photonics (ICP)*, 2014.