



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Criptografía cuántica con estados coherentes

Tesis presentada al

Posgrado en Ciencias Física Aplicada

como requisito parcial para la obtención del grado de

Maestra en Ciencias (Física Aplicada)

por

Lic. Abril Vargas Cortés

Asesorada por

Dr. Luis Manuel Arévalo Aguilar

Puebla, Puebla

Julio 2023



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Criptografía cuántica con estados coherentes

Tesis presentada al

Posgrado en Ciencias Física Aplicada

como requisito parcial para la obtención del grado de

Maestra en Ciencias (Física Aplicada)

por

Lic. Abril Vargas Cortés

Asesorada por

Dr. Luis Manuel Arévalo Aguilar

Puebla, Puebla

Julio 2023

Criptografía cuántica con estados coherentes

ABRIL VARGAS CORTÉS

COMITÉ

Dra. Marcela Maribel Méndez Otero
Presidente

Dr. Carlos Ignacio Robledo Sánchez
Secretario

Dr. Victor Manuel Velázquez Aguilar
Vocal

Dr. Wuiyebaldo Fermín Guerrero Sánchez
Suplente

Dr. Luis Manuel Arévalo Aguilar
Asesor

Para mi familia y para mí

AGRADECIMIENTOS

Quiero agradecer principalmente a mi madre Elia Cortés quien siempre me ha dado su apoyo, entendimiento y amor incondicional.

Al igual agradezco, a mi hermana Jocelyn Vargas quien me apoya y escucha aunque no me haya preguntado pero se interesa y entiende mi propósito de esto.

También agradezco, a mi profesor y amigo Julio Hernández quien siempre muestra interés porque sea una mejor investigadora y crezca profesionalmente, así mismo como entiende esta fase en mi vida.

También agradezco al Dr. Luis Manuel Arévalo Aguilar, quien siempre ha mostrado interés en mi proceso para entender lo nuevo a lo que me enfrenté en la realización de este trabajo, quien supó guiarme y comprendió los problemas por los que pase mientras realizaba el trabajo de tesis.

Finalmente, agradezco al Conahcyt por el apoyo para la realización de este trabajo.

ÍNDICE GENERAL

1. CONCEPTOS BÁSICOS	1
1.1. Mecánica cuántica	1
1.1.1. Primer postulado	1
1.1.2. Segundo postulado	1
1.1.3. Tercer postulado	1
1.1.4. Cuarto postulado	2
1.1.5. Quinto postulado	2
1.1.6. Sexto postulado	2
1.2. Teoría de la información	2
1.2.1. Distribución cuántica de clave (QKD)	2
1.2.1.1. Fases	3
1.2.2. Elementos clásicos de la teoría de la información	4
1.2.2.1. Entropía	4
1.2.2.2. Entropía condicional	5
1.2.2.3. Información mutua	5
1.2.2.4. Entropía para variables continuas	5
1.2.2.5. Entropía condicional para variables continuas	5
1.2.2.6. Información mutua para variables continuas	5
1.2.2.7. Información de Holevo	5
1.3. Fundamentos de seguridad	6
1.3.1. Ataques	6
1.3.2. Fracción secreta de clave	7
1.3.3. Tasa de clave secreta	7
1.3.3.1. Tasa de clave sin procesar	8
2. PROTOCOLO CON ESTADOS COHERENTES	9
2.1. Protocolos basados en preparación y medición (PM)	9
2.2. Protocolos basados en enredamiento (EB)	9
2.3. Protocolos de preparación-medición a protocolos de enredamiento	10
2.4. Protocolo con estados coherentes : análisis de seguridad	11

2.4.1. Protocolo	11
2.4.2. Análisis de seguridad	12
3. ANÁLISIS DE SEGURIDAD DIRECTA	16
3.1. Análisis sin contemplar a Eve en los estados de Bob	16
3.2. Análisis contemplando a Eve en los estados de Bob	21
4. CONCLUSIONES	25
BIBLIOGRAFÍA	27

RESUMEN

La criptografía cuántica como bien se sabe comenzó con el estudio de la implementación de distribución cuántica de claves con variables discretas y los primeros esquemas experimentales se basaron en la realización de estos, sin embargo, con el tiempo se comenzó a ver que el uso de estados continuos (como estados coherentes) presentan ventajas respecto a los protocolos con variables discretas pues se necesitan de ciertos aparatos que complican su aplicación a gran escala.

En cuanto al análisis de seguridad de los protocolos de QKD, en criptografía cuántica, es común hacer el uso de esquemas basados en enredamiento (EB) ya que estos presentan ciertas facilidades matemáticas, pues no involucran un canal cuántico que intervenga en los estados analizados en cambio en los esquemas de preparación y medición (PM), el cálculo necesita involucrar todas las alteraciones que los estados puedan sufrir en el canal cuántico, de ahí que se realice la analogía para la revisión de seguridad de los esquemas PM con un esquema EB.

En esta tesis nos proponemos analizar aspectos relevantes de la criptografía cuántica, enfocándonos en la realización de criptografía cuántica con variables continuas (siendo para este caso con estados coherentes). Donde nuestro objetivo será revisar los aspectos de la seguridad del esquema criptográfico, las ventajas que este presenta y se realizarán los cálculos para analizar la seguridad partiendo desde lo planteado en el esquema PM (análisis directo) sin hacer uso de un análisis de seguridad de un protocolo EB.

INTRODUCCIÓN

La criptografía tiene como uno de sus objetivos principales el cifrado de mensajes, es decir, que estos no sean entendidos por alguien que desea interceptar la comunicación entre el remitente y el receptor, así mismo como la autenticación, que es la creación de mecanismos que permiten verificar la identidad entre los comunicantes.

Sin embargo, para poder conseguir un proceso criptográfico exitoso es sumamente importante que la *clave*, que es aquella serie de símbolos, signos o bits con los cuales se cifran los mensajes, sea totalmente secreta y que el posible espía no tenga información parcial de esta. Para esto el proceso por el cual se transmite la clave, *distribución de claves*, entre el remitente y receptor debe garantizar la seguridad. No obstante, si el remitente y el receptor se comunican a través de mensajes clásicos esta seguridad se enfrenta a problemas pues un espía muy posiblemente pueda obtener algún tipo de información de la clave lo que vulneraría el proceso de cifrado.

Con el paso del tiempo, el avance de la ciencia y tecnología, se dio el paso a la creación de la Teoría de la Información Cuántica, la cual es la unión de la teoría de la información (desarrollada por Shannon) y la mecánica cuántica, permitiendo la creación de la criptografía cuántica. Basándose esta última, en la inviolabilidad de las leyes de la mecánica cuántica y en los protocolos de manejo de datos de la teoría de la información.

De esta manera, la distribución cuántica de claves (QKD) presenta ventaja respecto a lo conocido clásicamente ya que cuando un espía desee interceptar la comunicación este se verá en la necesidad de medir los estados cuánticos enviados por lo que causará una perturbación que alterará al sistema originalmente enviado y generará una mayor tasa de error, permitiendo que el remitente y receptor detecten el intento de espionaje.

Siendo así el primer protocolo de criptografía cuántica: el *Protocolo BB84* publicado en 1984 por Charles Bennett y Gilles Brassard, que fue primeramente construido de forma experimental utilizando fotones individuales (variable discreta).

Pero con el avance del estudio de la criptografía cuántica y de los esquemas para QKD, se comenzó con el uso de variables continuas (como estados coherentes) y se observó la ventaja experimental de estos esquemas respecto a los esquemas con variables discretas puesto que estos últimos se enfrentan a problemas experimentales tales como la baja eficiencia de detección, los conteos oscuros del detector, la fiabilidad de los aparatos para la generación de pulsos de un fotón, entre otros.

No obstante, en los esquemas de criptografía cuántica con variables continuas se presentan problemas con la demostración de seguridad dado que para cada criptosistema propuesto se tienen demostraciones de seguridad ante ciertos ataques pero pueden presentar vulnerabilidad respecto a otros algo que en los criptosistemas con variables discretas ya no es así debido a que su seguridad ha sido totalmente demostrada.

CONCEPTOS BÁSICOS

En este capítulo se revisarán de manera breve los principios de la mecánica cuántica e información cuántica especialmente lo relacionado a la distribución cuántica de claves (QKD).

1.1. Mecánica cuántica

El estudio de la mecánica cuántica nos ha traído una nueva concepción de la naturaleza y la descripción de los sistemas físicos desde finales del siglo XIX e inicios del siglo XX, cuando fue creada.

Por lo que, fueron creados los postulados de la mecánica cuántica los cuales nos permiten entender los principios de esta.

1.1.1. Primer postulado

El estado de un sistema físico aislado está definido por un vector de estado o un ket en específico $|\Psi\rangle$ el cual describe totalmente el sistema.[1]

1.1.2. Segundo postulado

Las cantidades físicas medibles son representadas por operadores autoadjuntos A , que actúan en los vectores de estado en el espacio de Hilbert, estos operadores son conocidos como *observables*. [1, 2]

1.1.3. Tercer postulado

Los resultados posibles de una medición de una cantidad física son los eigenvalores de la observable correspondiente. [2]

1.1.4. Cuarto postulado

Sea un operador A con los eigenvalores λ_i y eigenvectores $|\alpha_i\rangle$ [2]:

$$A|\alpha_i\rangle = \lambda_i|\alpha_i\rangle \quad (1.1)$$

La probabilidad de obtener el resultado de la medición λ_i , el cual esta asociado al eigenvector $|\alpha_i\rangle$, esta dada por la regla de Born:

$$P(\lambda_i) = |\langle\alpha_i|\Psi\rangle|^2 \quad (1.2)$$

1.1.5. Quinto postulado

El estado de un sistema, después de una medición, está dado por el eigenvector correspondiente al eigenvalor que haya sido medido. Es decir, el estado del sistema inmediatamente después de la medición es la proyección normalizada de Ψ en el subespacio asociado a α_i [1, 2]:

$$\Psi \longrightarrow \frac{P_n}{\sqrt{\langle\Psi|P_n|\Psi\rangle}} \quad (1.3)$$

1.1.6. Sexto postulado

La evolución en el tiempo de un vector de estado esta gobernada por la ecuación de Schrödinger [2]:

$$i\hbar\frac{\partial}{\partial t}|\Psi\rangle = H|\Psi(t_0)\rangle \quad (1.4)$$

1.2. Teoría de la información

La teoría de la información fue creada por Claude E. Shannon en 1948, en donde a través del artículo titulado *Una teoría matemática de la comunicación* sentó las bases matemáticas de lo que sería la teoría de la información. Consigo trajo el estudio del proceso de codificación- transmisión-recepción-decodificado, por lo que el papel de la criptografía tomó un papel importante en lo que sería la seguridad de la información.

Con el paso del tiempo, el avance tecnológico y teórico dió paso a que el uso de la mecánica cuántica se considerará para las nuevas tecnologías de la comunicación de esta manera surge lo que es la teoría de la información cuántica y por ende la criptografía cuántica.

De este modo, en esta sección se revisará toda la teoría involucrada en el análisis de la seguridad de los esquemas criptográficos para el proceso de la *distribución cuántica de claves* (QKD).

1.2.1. Distribución cuántica de clave (QKD)

Toda comunicación en la actualidad debe constar de seguridad como el envío de un mensaje de texto, un correo electrónico o una transacción bancaria, por lo que para ello

se requiere del proceso de cifrar y descifrar los mensajes, procesos que requieren de una *clave* para reescribir y comprender el mensaje cifrado.

Por lo tanto, el primer paso para el poder cifrar un mensaje es tener una clave que tanto el emisor (Alice) y el receptor (Bob) compartan para poder hacer la transferencia segura de información. Sin embargo, este proceso no es tan fácil pues la creación de un dispositivo ideal no es realista hoy en día debido a las características que este necesitaría, pero si se reajustan tales características y haciendo uso de los principios de la mecánica cuántica podemos crear dispositivos o mecanismos por los cuales se pueda distribuir una clave segura a través del proceso de *Distribución cuántica de claves*, cumpliendo las siguientes características [3]

1. La probabilidad de que la clave de Bob y Alice difiera sea muy pequeña:

$$Pr(S_A \neq S_B) \leq \epsilon \tag{1.5}$$

2. Que la clave esté cerca de ser perfecta, es decir, sea casi una clave uniformemente aleatoria. Donde los bits de la clave no tengan ninguna correlación entre ellos.
3. Que los ataques puedan ser detectados.

1.2.1.1. Fases

Todo protocolo de distribución cuántica de claves se puede caracterizar por dos etapas:

1. Primera etapa: preparación - envío -medición

Esta consiste en la preparación, la transmisión y medición de los estados cuánticos entre Alice y Bob. En esta etapa se comunican a través de un canal cuántico del cual un posible espía, generalmente llamada Eve, tiene acceso. Al final de este paso, Alice y Bob tendrán dos cadenas de bits que serán llamadas *llaves sin procesar*. [3, 4]

2. Segunda etapa: posprocesamiento clásico

Esta etapa mejor conocida como posprocesamiento clásico se lleva a cabo a través de distintos pasos en los cuales las cadenas de bits sin procesar serán transformadas a dos claves secretas que compartirán tanto Alice y Bob. En esta etapa la comunicación se realiza a través de un canal clásico; siendo así los pasos de esta etapa los siguientes [3, 4]

(a) Sifting:

Este paso se realiza solo si Alice y Bob hicieron uso de bits aleatorios generados uniformemente e independientemente para seleccionar las bases de preparación y medición, de tal manera que habrá señales en las que se usó distintas bases de preparación y medición, por tanto en este paso se eliminan dichas señales.

- (b) Estimación de parámetro:
 Después de la transmisión de los estados Alice y Bob revelarán un conjunto aleatorio de los datos enviados y medidos (los cuales son descartados de la clave final) lo cual les permitirá estimar la transmisión total y el exceso de ruido del canal por tanto podrán calcular su información mutua I_{AB} y la información de Eve (espía) χ . Es importante mencionar que si χ es demasiado grande a comparación de I_{AB} se descarta el protocolo.
- (c) Reconciliación de la información o corrección de errores:
 Este paso se puede realizar de dos maneras diferentes por: *reconciliación directa* (Bob corrige sus bits de acuerdo a los datos de Alice) o por *reconciliación inversa* (Alice corrige sus bits de acuerdo a los datos de Bob). En este paso se busca borrar todos los errores posibles, obteniendo así dos cadenas de bits idénticas.
- (d) Confirmación:
 Alice y Bob realizar un paso de confirmación utilizando una familia de funciones hash universales para acotar la probabilidad de que la corrección de errores haya fallado: Alice o Bob eligen con probabilidad uniforme una función hash particular de la familia y transmiten la elección al otro. Ambos aplican esa función hash a su clave para obtener un valor hash. Posteriormente, Alice y Bob intercambian y comparan sus valores hash. Si los valores hash son diferentes, las claves deben ser diferentes y abortan; si los valores hash son iguales, continúan y saben que han obtenido un límite superior en la probabilidad de que las claves no sean idénticas.
- (e) Amplificación de la privacidad:
 Después de la confirmación exitosa Alice y Bob compartirá la misma cadena de bits con una probabilidad muy alta. Pero, Eve tiene cierta cantidad de información sobre la llave. Para reducir la probabilidad de que Eve adivine con éxito (una parte de) la clave, Alice y Bob realizarán un protocolo de amplificación de privacidad, eliminando la información que Eve pueda tener de la clave.
- (f) Autenticación:
 Para evitar un ataque de intermediario, Alice y Bob necesitan autenticar su comunicación clásica usando una familia de funciones hash fuertemente universales.

1.2.2. Elementos clásicos de la teoría de la información

1.2.2.1. Entropía

La entropía de $H(X)$ de una variable aleatoria discreta X esta definida por [5]:

$$H(X) = - \sum_{x \in X} p(x) \log p(x) \quad (1.6)$$

1.2.2.2. Entropía condicional

Si $(X, Y) \sim p(x, y)$, la entropía condicional $H(Y|X)$ esta definida por [5]:

$$H(Y|X) = \sum_{x \in X} p(x)H(Y|X = x) = - \sum_{x \in X} \sum_{y \in Y} p(x, y) \log p(y|x) \quad (1.7)$$

1.2.2.3. Información mutua

La información mutua entre dos variables esta definida por [5]:

$$I(X; Y) = H(X) - H(X|Y) \quad (1.8)$$

1.2.2.4. Entropía para variables continuas

La entropía para una variable aleatoria continua X o también llamada entropía diferencial $h(X)$ con una función de densidad de probabilidad $f(x)$, esta definida como [5]:

$$h(X) = - \int_S f(x) \log f(x) dx \quad (1.9)$$

1.2.2.5. Entropía condicional para variables continuas

Sean X, Y con una función de densidad conjunta $f(x, y)$, podemos definir la entropía diferencial condicional $h(X|Y)$ como [5]:

$$h(X|Y) = - \int f(x, y) \log f(x|y) dx dy \quad (1.10)$$

donde $f(x|y) = \frac{f(x,y)}{f(y)}$, o por otro lado:

$$h(X|Y) = h(X, Y) - h(Y) \quad (1.11)$$

1.2.2.6. Información mutua para variables continuas

La información mutua $I(X; Y)$ entre dos variables aleatorias continuas con densidad conjunta $f(x, y)$ se define como [5]:

$$I(X; Y) = \int f(x, y) \log \frac{f(x, y)}{f(x)f(y)} dx dy \quad (1.12)$$

o por otro lado:

$$I(X; Y) = h(X) - h(X|Y) \quad (1.13)$$

1.2.2.7. Información de Holevo

La información de Holevo es un límite superior a la cantidad de información que se pueda conocer sobre un estado cuántico [4].

1.3. Fundamentos de seguridad

1.3.1. Ataques

La seguridad de un esquema criptográfico depende de varios factores experimentales y de las capacidades tecnológicas que presente el posible espía (Eve), para esto los tipos de ataques que puede realizar un espía se dividen en tres tipos que son [4, 6]

1. **Ataque individual:**

Eve prepara estados auxiliares para cada señal enviada por Alice y los hace interactuar, los almacena y mide independientemente hasta después del paso sifting pero antes del paso de parámetro de estimación.

2. **Ataque colectivo:**

Eve prepara estados auxiliares para cada señal enviada por Alice y los hace interactuar, los almacena y realiza una medición colectiva en todos los estados cuánticos después de la fase de posprocesamiento.

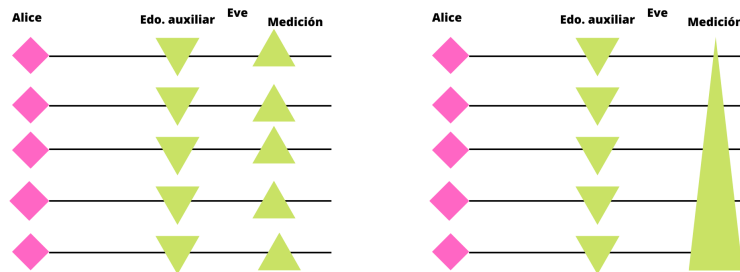


Figura 1.1: Ataque individual y colectivo

3. **Ataque coherente o general:**

Eve realiza un estado global auxiliar cuyos modos interactúan con las señales enviadas, los almacena y realiza una medición colectiva después de la fase de posprocesamiento.

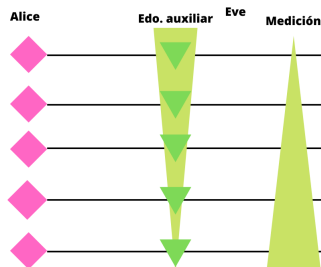


Figura 1.2: Ataque coherente

1.3.2. Fracción secreta de clave

Después del paso de parámetro de estimación, Alice y Bob comparten unas claves de una longitud de $n \leq N$ (siendo N la cantidad de señales enviadas en el paso de transmisión). Estas claves son solo parcialmente secretas y están parcialmente correlacionadas. Sin embargo, conforme se avanza con la etapa de posprocesamiento se transforma en una clave totalmente segura K de longitud $l \leq n$. La longitud l depende de la información que Eve tenga sobre las llaves sin procesar [6].

Por tanto, un elemento sumamente importante en los protocolos de criptografía es la fracción secreta asintótica (aunque en algunas referencias pueda encontrarse como tasa de clave secreta) la cual nos indica que si elegimos la longitud de la clave final de acuerdo al límite de esta tasa nuestra llave será completamente segura [6, 7].

Es importante mencionar que esta cantidad esta definida para el caso donde $N \rightarrow \infty$. es decir, para llaves infinitamente largas.

$$r = \lim_{N \rightarrow \infty} \frac{l}{n} \tag{1.14}$$

Siendo este elemento fundamental del cual se debe de obtener una expresión clara para cada revisión de seguridad de un protocolo. Así, la fracción secreta es el número de bits de clave segura que se pueden extraer por señal enviada, para la cual Devetak-Winter probaron una cota inferior para el caso de ataques colectivos y contemplando que la clave es infinita, el límite inferior viene dado por [3, 4, 6]:

$$r \geq I(A : B) - \chi \tag{1.15}$$

donde A y B son las llaves de Alice y Bob y χ es la información de Holevo (es un límite de la información que Eve tiene de las llaves ya sea de Alice o de Bob). La información de Holevo dependerá del protocolo de corrección de errores, si Bob corrige sus datos de acuerdo a la información de Alice se habla de una reconciliación directa donde χ_{EA} será la información que Eve tenga de Alice, por otro lado si Alice corrige sus datos de acuerdo a la información que recibió de Bob se realiza reconciliación inversa χ_{EB} .

Así pues, la fracción secreta se interpreta como la fracción de bits secretos generados por ronda de uso de protocolo es igual a la cantidad compartida entre Alice y Bob menos la cantidad de información que Eve tenga sobre la clave de Alice o de Bob (que tiene como unidades $\frac{\text{bits}}{\text{simbolo}}$).

1.3.3. Tasa de clave secreta

Otro de los elementos importantes es la tasa de clave secreta, la cual evalúa el rendimiento de los sistemas QKD prácticos, que se encuentra definida por [4, 6]:

$$K = f_{sym} r \tag{1.16}$$

donde f_{sym} es la tasa de clave sin procesar (en unidades de simbolos s^{-1}) y r que es la fracción secreta (razón de clave por simbolo).

1.3.3.1. Tasa de clave sin procesar

La tasa de clave sin procesar (f_{sym}) es un elemento que depende del protocolo desde el hardware, como pérdidas y detectores, es decir, se ven involucrados los elementos de: tiempo muerto de los detectores, la probabilidad de detección, la transmitividad del canal cuántico, las pérdidas en el dispositivo de Bob, la eficiencia del detector, entre otros elementos; por ende este elemento es analizado para cada caso en específico [6].

En este capítulo se revisaron conceptos fundamentales para el análisis de seguridad de los protocolos de QKD resaltando la variable de fracción secreta, dado que es un elemento fundamental para garantizar la seguridad de nuestra clave. Estos mismos nos permitirán que en los capítulos siguientes se realice el análisis de seguridad para protocolos de QKD con estados coherentes. Igualmente se revisaron los conceptos de mecánica cuántica que permiten entender la implementación de los protocolos QKD.

PROTOCOLO CON ESTADOS COHERENTES

En este capítulo, se revisará la analogía de los protocolos de preparación y medición con los protocolos basados en enredamiento, para así dar paso al análisis de seguridad del protocolo con estados coherentes descrito en [4].

2.1. Protocolos basados en preparación y medición (PM)

Para entender este tipo de protocolos solo basta con recordar el cómo se ejecuta QKD del protocolo BB84 con polarización.

En este protocolo, Alice cuenta con cuatro tipos de polarizaciones para preparar sus estados (polarizaciones de 0° , 90° , 45° y 135°). Ella elige arbitrariamente cualquiera de estas cuatro polarizaciones para preparar el estado y registra sus elecciones. Una vez preparados, los envía a Bob quien cuenta con dos tipos de base (aparato para medir polarización lineal y diagonal). Bob mide y registra el aparato usado para medir y su resultado de la medición.

Este tipo de protocolos son llamados *protocolos de preparación y medición (PM)*, en donde Alice elige arbitrariamente una secuencia S_n que ella va a enviar, prepara los estados y se los envía a Bob, quien realiza mediciones en cada uno de los estados recibidos. [3, 6]

2.2. Protocolos basados en enredamiento (EB)

En este tipo de protocolos, se hace uso de una fuente que provee estados entrelazados (a través de un canal cuántico) entre Alice y Bob, la cual puede ser controlada ya sea por Alice o por un tercero (Charlie) o incluso por Eve. Es importante mencionar que la comunicación se realiza a través de un canal clásico autenticado, al cual tiene acceso Eve pero no puede alterar ninguna de las comunicaciones. La seguridad de estos protocolos suele ser más fácil de analizar debido a que no hay presencia de un canal cuántico entre

Alice y Bob. [3]

2.3. Protocolos de preparación-medición a protocolos de enredamiento

Algo interesante entre este tipo de protocolos es que se puede pasar de un protocolo PM a un protocolo EB. Esto es sumamente útil ya que el poder traducir un protocolo PM a uno EB permite usar las técnicas de seguridad de este último en los protocolos PM. El poder transformar un protocolo PM a uno EB requiere de un análisis y suposiciones distintas debido a cada protocolo correspondiente. Sin embargo, se puede ver la generalidad de la transformación de la siguiente manera [3, 6]

PM:

1. Alice elige una secuencia de N símbolos que son eventos de una variable aleatoria X con una distribución de probabilidad $p_X(x)$ [3].
2. Luego codifica todos los símbolos en un estado cuántico de la forma

$$|\Phi_{X_1}\rangle \otimes \cdots \otimes |\Phi_{X_N}\rangle \quad (2.1)$$

Es importante mencionar que los estados deben ser no ortogonales para la codificación.

3. Bob recibe los estados y los mide.

EB

A continuación se presenta el cómo el esquema anterior se puede ver con el tipo de protocolo EB [3]

1. Alice prepara un estado enredado bipartito:

$$|\Phi_{AB}\rangle = \sum_x \sqrt{p_X(x)} |x\rangle_A \otimes |\phi_X\rangle_B \quad (2.2)$$

donde $|x\rangle_A$ es una base ortonormal del subsistema A .

2. Alice mide en esta base para obtener el valor clásico de X y le envía la otra mitad a Bob.
3. La probabilidad de obtener un valor y en el sistema de Alice es de:

$$P(y) = p_X(y) \quad (2.3)$$

mientras aún no se hace nada en el estado de Bob.

4. En el sistema de Bob, debe contener la codificación correcta de X, por lo que si Alice mide y entonces el sistema de Bob debe ser $|\phi_y\rangle$. Así el estado del sistema después de la medición de Alice es:

$$\frac{(|y\rangle_A \langle y| \otimes I_B) |\Phi\rangle_{AB}}{P(y)} = \frac{1}{\sqrt{p_X(y)}} \sqrt{p_X(y)} |y\rangle_A \otimes |\phi_y\rangle_B \quad (2.4)$$

$$= |y\rangle_A \otimes |\phi_y\rangle_B \quad (2.5)$$

siendo lo esperado. Así entonces, podemos ver que la prueba de seguridad de un protocolo EB se puede traducir a la prueba de seguridad PM, siendo esto conveniente pues el análisis de los protocolos EB son más fáciles aunque es importante mencionar que este hecho no significa que ambas realizaciones sean igual de prácticas o factibles con la tecnología actual [3, 6].

2.4. Protocolo con estados coherentes : análisis de seguridad

En esta sección se revisará lo presentado en el artículo [4], detallando los pasos en su análisis de seguridad.

2.4.1. Protocolo

1. Alice prepara estados coherentes desplazados con componentes de cuadratura q y p que son realizaciones de dos variables aleatorias Q y P . Estas dos variables aleatorias responden a la distribución normal [4]

$$Q \sim P \sim N(0, \widehat{V}_{mod}) \quad (2.6)$$

donde \widehat{V}_{mod} es la varianza de modulación. Alice prepara una secuencia de estados coherentes desplazados de la forma

$$|\alpha_j\rangle = |q_j + ip_j\rangle \quad (2.7)$$

que obedece a la ecuación de eigenvalor [8]

$$\widehat{a} |\alpha_j\rangle = \alpha_j |\alpha_j\rangle \quad (2.8)$$

2. Bob al recibir los estados realiza ya sea una detección homodina o una detección heterodina. En la detección homodina Bob mide un componente de cuadratura en un tiempo aleatorio seleccionando seleccionando una fase reactiva θ de 0 o de $\pi/2$. Mientras que en la detección heterodina Bob separa los estados entrantes con un divisor de haz balanceado y mide ambas cuadraturas, 0 si mide q y $\pi/2$ para p [4].

2.4.2. Análisis de seguridad

Los estados bosónicos multimodo pueden describirse mediante matrices de covarianza (las cuales son suficientes para dar una descripción completa del estado del sistema), de las cuales las entradas diagonales representan las varianzas de los operadores de cuadratura y los demás términos son las covarianzas entre las cuadraturas.

Para este protocolo se hará el análisis haciendo uso de un protocolo EB, es decir, se hará la equivalencia de protocolo con estados coherentes (PM) con el protocolo donde Alice prepara un estado de vacío comprimido de dos modos (TMSVS), donde realiza una medición de ambas cuadraturas de un modo y envía el otro modo a Bob.

En las unidades de ruido-disparo, TMSVS esta descrito por la matriz de covarianza:

$$\sum_{AB} = \begin{pmatrix} \langle q_A q_A \rangle & \langle q_A p_A \rangle & \langle q_A q_B \rangle & \langle q_A p_B \rangle \\ \langle p_A q_A \rangle & \langle p_A p_A \rangle & \langle p_A q_B \rangle & \langle p_A p_B \rangle \\ \langle q_B q_A \rangle & \langle q_B p_A \rangle & \langle q_B q_B \rangle & \langle q_B p_B \rangle \\ \langle p_B q_A \rangle & \langle p_B p_A \rangle & \langle p_B q_B \rangle & \langle p_B p_B \rangle \end{pmatrix} \quad (2.9)$$

Para ello es importante recordar que un elemento de la matriz de covarianza se define como [9]

$$\sum_{ij} = \frac{1}{2} \langle \{ \Delta \hat{p}_i, \Delta \hat{q}_j \} \rangle \quad (2.10)$$

o por otro lado,

$$\sum_{ij} = \frac{1}{2} [\langle p_i q_j \rangle + \langle q_j p_i \rangle] - \langle q_i \rangle \langle p_j \rangle \quad (2.11)$$

Calculando primero los elementos diagonales que son las varianzas, se tiene que:

$$\sum_{11} = \sum_{22} = \sum_{33} = \sum_{44} = V \quad (2.12)$$

Calculando ahora los elementos $\sum_{21} = \sum_{12}$ y $\sum_{34} = \sum_{43}$ tenemos que:

$$\sum_{21} = \sum_{12} = 0 \quad (2.13)$$

$$\sum_{34} = \sum_{43} = 0 \quad (2.14)$$

Calculando ahora los elementos $\sum_{31} = \sum_{13}$ y $\sum_{42} = \sum_{24}$ tenemos que:

$$\sum_{31} = \sum_{13} = \sqrt{V^2 - 1} \quad (2.15)$$

$$\sum_{24} = \sum_{42} = -\sqrt{V^2 - 1} \quad (2.16)$$

Calculando ahora los elementos $\sum_{14} = \sum_{41}$ y $\sum_{32} = \sum_{23}$ tenemos que:

$$\sum_{14} = \sum_{41} = 0 \quad (2.17)$$

$$\sum_{32} = \sum_{23} = 0 \quad (2.18)$$

Haciendo uso de las ecuaciones (2.12)-(2.18), obtenemos la matriz de covarianza:

$$\sum_{AB} = \begin{pmatrix} V & 0 & \sqrt{V^2 - 1} & 0 \\ 0 & V & 0 & -\sqrt{V^2 - 1} \\ \sqrt{V^2 - 1} & 0 & V & 0 \\ 0 & -\sqrt{V^2 - 1} & 0 & V \end{pmatrix} \quad (2.19)$$

Recordando que:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

se tiene que:

$$\sum_{AB} = \begin{pmatrix} VI_2 & \sqrt{V^2 - 1}\sigma_z \\ \sqrt{V^2 - 1}\sigma_z & VI_2 \end{pmatrix} \quad (2.20)$$

Esta varianza V se puede tomar como la suma de la varianza de modulación de Alice y la varianza shot-noise de vacío, así: $V = V_{mod} + 1$. Por tanto,

$$\sum_{AB} = \begin{pmatrix} (V_{mod} + 1)I_2 & \sqrt{V_{mod}^2 + 2V_{mod}}\sigma_z \\ \sqrt{V_{mod}^2 + 2V_{mod}}\sigma_z & (V_{mod} + 1)I_2 \end{pmatrix} \quad (2.21)$$

Debido al envío el estado de Bob se verá afectado debido a diversas fuentes de ruido, por lo que el modo de Bob se transforma de la siguiente manera:

$$\sum_{AB} = \begin{pmatrix} VI_2 & \sqrt{T(V^2 - 1)}\sigma_z \\ \sqrt{T(V^2 - 1)}\sigma_z & (T(V - 1) + 1 + \xi)I_2 \end{pmatrix} \quad (2.22)$$

o

$$\sum_{AB} = \begin{pmatrix} (V_{mod} + 1)I & \sqrt{T(V_{mod}^2 + 2V_{mod})}\sigma_z \\ \sqrt{T(V_{mod}^2 + 2V_{mod})}\sigma_z & (TV_{mod} + 1 + \xi)I \end{pmatrix} \quad (2.23)$$

donde T es la transmitancia y ξ el exceso de ruido.

Como ya se mencionó anteriormente, Bob puede realizar dos tipos de mediciones: homodina o heterodina. Si Bob realiza una medición heterodina, tendríamos que la matriz de covarianza entre el modo de Alice y uno de los modos de Bob, esta representado por

$$\sum_{AB_{1,2}} = \begin{pmatrix} (V_{mod} + 1)I_2 & \pm\sqrt{\frac{T}{2}(V_{mod}^2 + 2V_{mod})}\sigma_z \\ \pm\sqrt{\frac{T}{2}(V_{mod}^2 + 2V_{mod})}\sigma_z & (\frac{T}{2}V_{mod} + 1 + \frac{\xi}{2})I_2 \end{pmatrix} \quad (2.24)$$

donde $V = V_{mod} + 1$.

Debido a que buscamos la expresión para la fracción secreta:

$$r \geq I(A : B) - \chi$$

Se calcula primero la información mutua entre Alice y Bob, la cual es [9]:

$$I(A|B) = \frac{1}{2} \log \left(\frac{V + \xi}{\xi + 1} \right) \quad (2.25)$$

Por otro lado, se requiere del conocimiento de la información de Holevo, en este caso se trabaja con una reconciliación inversa, por lo que se necesita la información que Eve tiene de Bob y considerando que $\chi_{EB} = S_E - S_{E|B} = S_{AB} - S_{A|B}$, se puede obtener tal dato.

Primero calculando la entropía S_E , tenemos que:

$$S_E = \sum g(v_i) \quad (2.26)$$

donde $g(v_i) = \frac{v+1}{2} \log \left(\frac{v+1}{2} \right) - \frac{v-1}{2} \log \left(\frac{v-1}{2} \right)$. Para ello se hará uso de la matriz del subestado de Eve:

$$\sum_{E_1 E_2} = \begin{pmatrix} ((1-T)V + TW)I_2 & \sqrt{T(W^2 - 1)}\sigma_z \\ \sqrt{T(W^2 - 1)}\sigma_z & WI_2 \end{pmatrix} \quad (2.27)$$

Obteniendo los valores de v [4]

$$v_1 = \frac{1}{2} \left[\sqrt{V - TV + TW + W^2 - 4(TW^2 - T)} + W - V + TV - TW \right] \quad (2.28)$$

$$v_2 = \frac{1}{2} \left[\sqrt{V - TV + TW + W^2 - 4(TW^2 - T)} - W + V - TV + TW \right] \quad (2.29)$$

siendo W la varianza de los estados TMSVS creados por Eve. Ahora para la entropía condicional, se tienen que contemplar el tipo de medición que se realice para su obtención, así:

$$S_{E|B} = \sum g(x_i) \quad (2.30)$$

Para la obtención de x_i tomemos la matriz (2.22) y la renombramos como sigue:

$$\sum_{AB} = \begin{pmatrix} aI & c\sigma_z \\ c\sigma_z & bI \end{pmatrix} \quad (2.31)$$

Podemos hacer uso de ciertas relaciones que describen cada una de las posibles mediciones [4].

Si se realiza una medición homodina se usa la relación:

$$\sum_{A|B} = \sum_A - \frac{1}{V(q_B)} \sum_C \prod_q \sum_C^T \quad (2.32)$$

donde $\sum_A = aI$, $\sum_C = c\sigma_z$ y $V(q_B) = b = V_B$. Se obtiene:

$$\sum_{A|B} = \begin{pmatrix} a - \frac{c^2}{b} & 0 \\ 0 & a \end{pmatrix} \quad (2.33)$$

obteniendo los eigenvalores de esta matriz, tenemos:

$$x = \sqrt{a \left(a - \frac{c^2}{b} \right)} = \sqrt{V \left(V - \frac{T(V^2 - 1)}{T(V - 1) + 1 + \xi} \right)} \quad (2.34)$$

Mientras que para una detección heterodina se ocupa la relación:

$$\sum_{A|B} = \sum_A - \frac{a}{V_B + 1} \sum_C \sum_C^T \quad (2.35)$$

Obteniendo así:

$$x = a - \frac{c^2}{b + 1} = V - \frac{T(V^2 - 1)}{T(V - 1) + 2 + \xi} \quad (2.36)$$

Entonces, ya puede ser calculada cada una de las entropías para la información de Holevo. Una vez obtenida y conociendo la información mutua dada por la ecuación (2.25), podemos calcular la fracción secreta.

Es importante mencionar que en este análisis se encuentra finalmente que la fracción secreta depende únicamente de cuatro parámetros: la varianza de modulación (directamente relacionada con el número promedio de fotones por símbolo), la transmitancia, el exceso de ruido y la eficiencia de reconciliación [4].

ANÁLISIS DE SEGURIDAD DIRECTA

Como se ha mencionado en el capítulo anterior, se puede realizar el análisis de seguridad de un protocolo PM como si fuera un protocolo EB haciendo las consideraciones necesarias para que sean similares ambos protocolos. Tal, que se mostró en forma general el análisis de seguridad que se realizó en [4] en el que se hizo uso de estados comprimidos del vacío de dos modos en lugar de los estados coherentes que son los preparados experimentalmente para la implementación del protocolo. Por este motivo, en este capítulo se mostrará un primer análisis para la obtención de la variable de fracción secreta pero partiendo directamente de los estados coherentes.

3.1. Análisis sin contemplar a Eve en los estados de Bob

En este primer análisis, se contempla que Alice prepara estados coherentes que se definen por el número complejo α , el cual esta asociado con el número promedio de fotones en el pulso μ a través de la relación $\mu = |\alpha|^2$. De tal manera que, α está vinculado a la amplitud del campo eléctrico de la onda electromagnética. Igualmente como ya se mencionó cumple con la ecuación (2.8) y obedece para este caso una distribución normal (cada una de las cuadraturas q y p), de la forma:

$$f(q, p) = \frac{1}{\sqrt{2\pi V^2}} e^{-\frac{(q_{A,B}^2 + p_{A,B}^2)}{2V^2}} \quad (3.1)$$

$V = V_{mod}$ comparándolo al analisis anterior.

La comunicación entre Alice y Bob se contempla que es realizada por medio de una fibra óptica. Es importante mencionar que el uso de fibra óptica como canal cuántico tiene como ventajas: atenuación baja y constante, y que es un medio del cual ya se tiene infraestructura, por eso se considera este medio. Por otro lado, para este tipo de

canales hay diversas afectaciones posibles, entre ellas: la desalineación de polarización y la atenuación de la intensidad del haz de luz [10]. Esta última causa una disminución en la amplitud del estado coherente por un factor $e^{-\lambda L}$ siendo L la longitud del canal de transmisión y λ la atenuación o coeficiente de pérdida de la fibra [10, 11, 12].

Por tanto, tenemos que la distribución de probabilidad del estado que Alice prepara para la cuadratura q es:

$$f(q_A) = \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \quad (3.2)$$

Mientras que la distribución del estado de Bob para la cuadratura q es:

$$f(q_B) = e^{-\lambda L} \frac{1}{\sqrt{2\pi V^2}} e^{\frac{-q_B^2}{2V^2}} \quad (3.3)$$

Si se supone que Eve interviene con un divisor de haz 20/80 solo separando los haces, quedándose ella con 20 % del haz que envía Alice, entonces la distribución de su estado para la cuadratura q es:

$$\begin{aligned} f(q_E) &= 0.2e^{-\lambda \frac{L}{2}} f(q_A) \\ f(q_E) &= 0.2e^{-\lambda \frac{L}{2}} \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \end{aligned} \quad (3.4)$$

Para obtener la fracción secreta, de acuerdo a la ecuación (1.15), se necesita de la información mutua y la información de Holevo, entonces:

Sea

$$I(A|B) = h(q_A) - h(q_A|q_B) \quad (3.5)$$

Calculando $h(q_A)$:

$$\begin{aligned} h(q_A) &= - \int_S f(q_A) \log f(q_A) dq_A \\ &= - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \log \left[\frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \right] dq_A \\ &= - \frac{1}{\sqrt{2\pi V_{mod}^2}} \int_{-\infty}^{\infty} e^{\frac{-q_A^2}{2V_{mod}^2}} \left[\log e^{\frac{-q_A^2}{2V_{mod}^2}} - \log \sqrt{2\pi V_{mod}^2} \right] dq_A \\ &= - \frac{1}{\sqrt{2\pi V_{mod}^2}} \int_{-\infty}^{\infty} e^{\frac{-q_A^2}{2V_{mod}^2}} \left[\frac{-q_A^2}{2V_{mod}^2} - \log \sqrt{2\pi V_{mod}^2} \right] dq_A \end{aligned}$$

$$= -\frac{1}{\sqrt{2\pi V_{mod}^2}} \left[-\frac{1}{2V_{mod}^2} \int_{-\infty}^{\infty} q_A^2 e^{\frac{-q_A^2}{2V_{mod}^2}} dq_A - \log \sqrt{2\pi V_{mod}^2} \int_{-\infty}^{\infty} e^{\frac{-q_A^2}{2V_{mod}^2}} dq_A \right]$$

resolviendo las integrales usando el apéndice I de [13]:

$$\int_{-\infty}^{\infty} q_A^2 e^{\frac{-q_A^2}{2V_{mod}^2}} dq_A = \frac{1}{2} \sqrt{\pi} \left(\frac{1}{2V_{mod}^2} \right)^{\frac{-3}{2}}$$

$$\int_{-\infty}^{\infty} e^{\frac{-q_A^2}{2V_{mod}^2}} dq_A = \sqrt{2\pi V_{mod}^2}$$

$$= \frac{1}{\sqrt{2\pi V_{mod}^2}} \frac{1}{2V_{mod}^2} \frac{\sqrt{\pi}}{2} 2^{\frac{3}{2}} V_{mod}^3 + \frac{1}{\sqrt{2\pi V_{mod}^2}} \sqrt{2\pi V_{mod}^2} \log \left(\sqrt{2\pi V_{mod}^2} \right)$$

$$= \frac{1}{2} + \log(2\pi V_{mod}^2)^{\frac{1}{2}}$$

$$= \frac{1}{2} + \frac{1}{2} \log(2\pi V_{mod}^2)$$

$$h(q_A) = \frac{1}{2} \log(2\pi e V_{mod}^2) \tag{3.6}$$

Calculando ahora $h(q_B|q_A)$. Primero procedemos a recordar que:

$$h(q_A|q_B) = - \int f(q_B) f(q_A|q_B) \log f(q_A|q_B) dq_A dq_B \tag{3.7}$$

Para ello necesitamos encontrar la distribución de probabilidad de Bob obteniendo el resultado de la medición β condicionado a que Alice envíe un estado coherente con amplitud α está dado por la ecuación [8]

$$f(q_A|q_B) = \frac{1}{\pi} \langle \beta | \rho^\alpha | \beta \rangle \tag{3.8}$$

si $\langle \beta | \rho^\alpha | \beta \rangle = |\langle \beta | \alpha \rangle|^2 = e^{-|\beta-\alpha|^2}$, entonces:

$$f(q_A|q_B) = \frac{1}{\pi} e^{-(e^{-2\lambda L} - 2e^{-\lambda L} + 1)|\alpha|^2} \tag{3.9}$$

si $\varepsilon = e^{-2\lambda L} - 2e^{-\lambda L} + 1$, entonces:

$$f(q_A|q_B) = \frac{1}{\pi} e^{-\varepsilon|\alpha|^2} \tag{3.10}$$

pero como solo trabajamos con q :

$$f(q_A|q_B) = \frac{1}{\pi} e^{-\varepsilon q_A^2} \tag{3.11}$$

Por tanto:

$$\begin{aligned}
 h(q_A|q_B) &= - \int f(q_B)f(q_A|q_B) \log f(q_A|q_B) dq_A dq_B \\
 &= \int_{-\infty}^{\infty} \frac{1}{\pi} e^{-\varepsilon q_A^2} e^{-\lambda L} \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \log \left(\frac{1}{\pi} e^{-\varepsilon q_A^2} \right) dq_A \\
 &= \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \int_{-\infty}^{\infty} e^{-\varepsilon q_A^2} e^{\frac{-q_A^2}{2V_{mod}^2}} \log \left(\frac{1}{\pi} e^{-\varepsilon q_A^2} \right) dq_A \\
 &= \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \int_{-\infty}^{\infty} e^{-(\varepsilon + \frac{1}{2V_{mod}^2})q_A^2} \left[\log \left(\frac{1}{\pi} \right) + \log \left(e^{-\varepsilon q_A^2} \right) \right] dq_A \\
 &= \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \int_{-\infty}^{\infty} e^{-(\varepsilon + \frac{1}{2V_{mod}^2})q_A^2} dq_A - \varepsilon \int_{-\infty}^{\infty} q_A^2 e^{-(\varepsilon + \frac{1}{2V_{mod}^2})q_A^2} dq_A \right\} \\
 &\text{haciendo uso de los cálculos anteriores, se obtiene la solución de} \\
 &= \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{\pi}{\varepsilon + \frac{1}{2V_{mod}^2}}} - \frac{\varepsilon \sqrt{\pi}}{2} \frac{1}{\left(\varepsilon + \frac{1}{2V_{mod}^2} \right)^{\frac{3}{2}}} \right\} \\
 h(q_A|q_B) &= \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\varepsilon V_{mod}^2 + 1}} - \frac{\varepsilon \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\varepsilon V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \quad (3.12)
 \end{aligned}$$

Por lo tanto, de la ecuación (3.5):

$$\begin{aligned}
 I(A|B) &= h(q_A) - h(q_A|q_B) \quad (3.13) \\
 &= \frac{1}{2} \log(2\pi e V_{mod}^2) - \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\varepsilon V_{mod}^2 + 1}} - \frac{\varepsilon \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\varepsilon V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\}
 \end{aligned}$$

Ahora para obtener la información de Holevo χ_{EB} , se tiene que:

$$\chi_{E|B} = h(q_E) - h(q_E|q_B) \quad (3.14)$$

Primero calculamos $h(q_E)$. Si tomamos lo descrito en la ecuación (3.4), se tiene:

$$h(q_E) = - \int_{-\infty}^{\infty} 0.2e^{-\lambda \frac{L}{2}} f(q_A) \log\left(0.2e^{-\lambda \frac{L}{2}} f(q_A)\right) dq_A \quad (3.15)$$

$$= -0.2e^{-\lambda \frac{L}{2}} \int_{-\infty}^{\infty} f(q_A) (\log(-0.2e^{-\lambda \frac{L}{2}}) + \log(f(q_A))) dq_A$$

$$= -0.2e^{-\lambda \frac{L}{2}} \left[\int_{-\infty}^{\infty} \log(-0.2e^{-\lambda \frac{L}{2}}) f(q_A) dq_A + \int_{-\infty}^{\infty} f(q_A) \log(f(q_A)) dq_A \right]$$

contemplando lo ya calculado:

$$= -0.2e^{-\lambda \frac{L}{2}} \log\left(0.2e^{-\lambda \frac{L}{2}}\right) + 0.2e^{-\lambda \frac{L}{2}} \frac{\log(2\pi V_{mod}^2 e)}{2}$$

$$h(q_E) = \frac{-\log\left(0.2e^{-\lambda \frac{L}{2}}\right)}{5} e^{-\lambda \frac{L}{2}} + \frac{e^{-\lambda \frac{L}{2}}}{10} \log(2\pi V_{mod}^2 e) \quad (3.16)$$

Calculando el otro elemento de la información de Holevo $h(q_E|q_B)$:

$$h(q_E|q_B) = - \int_{-\infty}^{\infty} f(q_E) f(q_E|q_B) \log f(q_E|q_B) dq_E dq_B$$

realizando un análisis similar a lo anterior:

$$f(q_E|q_B) = \frac{1}{\pi} e^{-(0.04e^{-\lambda L} - 0.4e^{-\frac{3}{2}\lambda L} + e^{-2\lambda L})|\alpha|^2}$$

$$\text{si } \delta = 0.04e^{-\lambda L} - 0.4e^{-\frac{3}{2}\lambda L} + e^{-2\lambda L}$$

$$f(q_E|q_B) = \frac{1}{\pi} e^{-\delta q_A^2}$$

$$= \int_{-\infty}^{\infty} \frac{1}{\pi} e^{-\delta q_A^2} 0.2e^{-\lambda \frac{L}{2}} \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \log\left(\frac{1}{\pi} e^{-\delta q_A^2}\right) dq_A$$

realizando los calculos, se obtiene

$$h(q_E|q_B) = \frac{0.2}{\pi} \frac{e^{-\lambda L/2}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log\left(\frac{1}{\pi}\right) \sqrt{\frac{2\pi V_{mod}^2}{2\delta V_{mod}^2 + 1}} - \frac{\delta\sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\delta V_{mod}^2 + 1}\right)^{\frac{3}{2}} \right\} \quad (3.17)$$

Por consiguiente,

$$\begin{aligned} \chi_{E|B} &= \frac{-\log\left(0.2e^{-\lambda \frac{L}{2}}\right)}{5} e^{-\lambda \frac{L}{2}} + \frac{e^{-\lambda \frac{L}{2}}}{10} \log(2\pi V_{mod}^2 e) - \\ &\frac{0.2}{\pi} \frac{e^{-\lambda L/2}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log\left(\frac{1}{\pi}\right) \sqrt{\frac{2\pi V_{mod}^2}{2\delta V_{mod}^2 + 1}} - \frac{\delta\sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\delta V_{mod}^2 + 1}\right)^{\frac{3}{2}} \right\} \quad (3.18) \end{aligned}$$

Para concluir, la tasa secreta de clave, viene dada por:

$$\begin{aligned}
 r &\geq I(A : B) - \chi_{EB} \\
 &= \frac{1}{2} \log(2\pi e V_{mod}^2) - \frac{1}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log\left(\frac{1}{\pi}\right) \sqrt{\frac{2\pi V_{mod}^2}{2\epsilon V_{mod}^2 + 1}} - \frac{\epsilon\sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\epsilon V_{mod}^2 + 1}\right)^{\frac{3}{2}} \right\} \\
 &\quad + \frac{\log\left(0.2e^{-\lambda\frac{L}{2}}\right)}{5} e^{-\lambda\frac{L}{2}} - \frac{e^{-\lambda\frac{L}{2}}}{10} \log(2\pi V_{mod}^2 e) + \\
 &\quad \frac{0.2}{\pi} \frac{e^{-\lambda L/2}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log\left(\frac{1}{\pi}\right) \sqrt{\frac{2\pi V_{mod}^2}{2\delta V_{mod}^2 + 1}} - \frac{\delta\sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\delta V_{mod}^2 + 1}\right)^{\frac{3}{2}} \right\} \tag{3.19}
 \end{aligned}$$

Como se puede notar en la ecuación anterior (3.19), la fracción secreta depende en este caso de el coeficiente de pérdida de la fibra, de la varianza de modulación y de la distancia o longitud del canal.

3.2. Análisis contemplando a Eve en los estados de Bob

Haciendo las mismas consideraciones anteriores pero ahora contemplando la intervención de Eve en el camino que afecta el estado de Bob, tenemos que las distribuciones para cada uno son:

$$f(q_A) = \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \tag{3.20}$$

$$f(q_B) = 0.8e^{-\lambda L} f(q_A) \tag{3.21}$$

$$f(q_E) = 0.2e^{-\lambda\frac{L}{2}} f(q_A) \tag{3.22}$$

De nuevo se busca obtener una expresión para la tasa secreta. Primero se calculará la información mutua entre Alice y Bob:

$$I(A|B) = h(q_A) - h(q_A|q_B) \tag{3.23}$$

Como la distribución de Alice no cambio entonces su entropía tampoco, así que:

$$h(q_A) = \frac{1}{2} \log(2\pi V_{mod}^2 e) \tag{3.24}$$

Calculando $h(q_A|q_B)$:

$$\begin{aligned}
 h(q_A|q_B) &= - \int f(q_B) f(q_A|q_B) \log f(q_A|q_B) dq_A dq_B \\
 &= \int_{-\infty}^{\infty} \frac{1}{\pi} e^{-\varepsilon' q_A^2} e^{-\lambda L} \frac{0.8}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \log \left(\frac{1}{\pi} e^{-\varepsilon' q_A^2} \right) dq_A \\
 &= \frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \int_{-\infty}^{\infty} e^{-\varepsilon' q_A^2} e^{\frac{-q_A^2}{2V_{mod}^2}} \log \left(\frac{1}{\pi} e^{-\varepsilon' q_A^2} \right) dq_A \\
 &= \frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \int_{-\infty}^{\infty} e^{-(\varepsilon' + \frac{1}{2V_{mod}^2}) q_A^2} \left[\log \left(\frac{1}{\pi} \right) + \log \left(e^{-\varepsilon' q_A^2} \right) \right] dq_A \\
 &= \frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \int_{-\infty}^{\infty} e^{-(\varepsilon' + \frac{1}{2V_{mod}^2}) q_A^2} dq_A - \varepsilon' \int_{-\infty}^{\infty} q_A^2 e^{-(\varepsilon' + \frac{1}{2V_{mod}^2}) q_A^2} dq_A \right\} \\
 &\text{haciendo uso de los cálculos anteriores, se obtiene la solución de} \\
 &= \frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{\pi}{\varepsilon' + \frac{1}{2V_{mod}^2}}} - \frac{\varepsilon' \sqrt{\pi}}{2} \frac{1}{\left(\varepsilon' + \frac{1}{2V_{mod}^2} \right)^{\frac{3}{2}}} \right\} \\
 h(q_A|q_B) &= \frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\varepsilon' V_{mod}^2 + 1}} - \frac{\varepsilon' \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\varepsilon' V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \quad (3.25)
 \end{aligned}$$

donde $\varepsilon' = 0.64e^{-2\lambda L} - 1.6e^{-\lambda L} + 1$.

Siendo la información mutua:

$$\begin{aligned}
 I(A|B) &= h(q_A) - h(q_A|q_B) \\
 I(A|B) &= \frac{1}{2} \log(2\pi V_{mod}^2 e) - \\
 &\quad \frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\varepsilon' V_{mod}^2 + 1}} - \frac{\varepsilon' \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\varepsilon' V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \quad (3.26)
 \end{aligned}$$

Por otro lado, para la información de Holevo, ya se tiene el valor de $h(q_E)$:

$$h(q_E) = \frac{-\log(0.2e^{-\lambda \frac{L}{2}})}{5} e^{-\lambda \frac{L}{2}} + \frac{e^{-\lambda \frac{L}{2}}}{10} \log(2\pi V_{mod}^2 e) \quad (3.27)$$

Calculando la entropía condicional:

$$\begin{aligned}
 h(q_E|q_B) &= - \int_{-\infty}^{\infty} f(q_E)f(q_E|q_B) \log f(q_E|q_B) dq_E dq_B \\
 &\text{realizando un análisis similar a lo anterior:} \\
 f(q_E|q_B) &= \frac{1}{\pi} e^{-(0.04e^{-\lambda L} - 0.32e^{-\frac{3}{2}\lambda L} + 0.64e^{-2\lambda L})|q|^2} \\
 \text{si } \delta' &= 0.04e^{-\lambda L} - 0.32e^{-\frac{3}{2}\lambda L} + 0.64e^{-2\lambda L} \\
 f(q_E|q_B) &= \frac{1}{\pi} e^{-\delta' q_A^2} \\
 &= \int_{-\infty}^{\infty} \frac{1}{\pi} e^{-\delta' q_A^2} 0.2 e^{-\lambda \frac{L}{2}} \frac{1}{\sqrt{2\pi V_{mod}^2}} e^{\frac{-q_A^2}{2V_{mod}^2}} \log \left(\frac{1}{\pi} e^{-\delta' q_A^2} \right) dq_A \\
 &\text{realizando los calculos, se obtiene} \\
 h(q_E|q_B) &= \frac{0.2}{\pi} \frac{e^{-\lambda L/2}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\delta' V_{mod}^2 + 1}} - \frac{\delta' \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\delta' V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \quad (3.28)
 \end{aligned}$$

Por consiguiente:

$$\begin{aligned}
 \chi_{EB} &= \frac{-\log(0.2e^{-\lambda \frac{L}{2}})}{5} e^{-\lambda \frac{L}{2}} + \frac{e^{-\lambda \frac{L}{2}}}{10} \log(2\pi V_{mod}^2 e) - \\
 &\frac{0.2}{\pi} \frac{e^{-\lambda L/2}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\delta' V_{mod}^2 + 1}} - \frac{\delta' \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\delta' V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \quad (3.29)
 \end{aligned}$$

Ya conocidos los valores de la información mutua de Alice y Bob, y el valor de la información de Holevo, tenemos que la fracción secreta es:

$$\begin{aligned}
 r &\geq \frac{1}{2} \log(2\pi V_{mod}^2 e) - \\
 &\frac{0.8}{\pi} \frac{e^{-\lambda L}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\varepsilon' V_{mod}^2 + 1}} - \frac{\varepsilon' \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\varepsilon' V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \\
 &+ \frac{\log(0.2e^{-\lambda \frac{L}{2}})}{5} e^{-\lambda \frac{L}{2}} - \frac{e^{-\lambda \frac{L}{2}}}{10} \log(2\pi V_{mod}^2 e) + \\
 &\frac{0.2}{\pi} \frac{e^{-\lambda L/2}}{\sqrt{2\pi V_{mod}^2}} \left\{ \log \left(\frac{1}{\pi} \right) \sqrt{\frac{2\pi V_{mod}^2}{2\delta' V_{mod}^2 + 1}} - \frac{\delta' \sqrt{\pi}}{2} \left(\frac{2V_{mod}^2}{2\delta' V_{mod}^2 + 1} \right)^{\frac{3}{2}} \right\} \quad (3.30)
 \end{aligned}$$

Similarmente a la ecuación (3.19), la tasa secreta de la ecuación (3.30) depende de las variables de el coeficiente de pérdida de la fibra, la varianza de modulación y la longitud del canal. Sin embargo, se puede observar la diferencia que estas presentan solo debido al cambio del estado que Bob recibe considerando que este ya se ve afectado por la

intervención de Eve.

Cabe recalcar que este análisis solo contempló que Eve usó un divisor de haz que dividió el estado enviado por Alice mientras que en el análisis anterior (capítulo dos) Eve realiza un ataque de clonador enredador en donde se ven involucrados otros elementos que influyen en la obtención de la fracción secreta.

CONCLUSIONES

En este trabajo se revisaron los fundamentos básicos de la teoría de la información y cómo estos se ven involucrados en los análisis de seguridad de los protocolos de distribución cuántica de claves (QKD). Así mismo, se analizaron las características que debe cumplir una QKD y las dos fases que se ejecutan al hacer un protocolo de QKD: preparación-envío- medición y el posprocesamiento clásico.

Entre los conceptos importantes para el análisis de seguridad encontramos que la fracción secreta es una variable de suma importancia en todo protocolo de QKD pues esta variable debe ser calculada explícitamente en cada protocolo. Además, esta variable dependerá del tipo de esquema experimental que se planteó y de los tipos de ataques en los que se revise la seguridad del protocolo.

En el capítulo dos, se revisó como la seguridad de los protocolos llamados de preparación y medición (PM), puede ser examinada por medio del análisis de la seguridad de un protocolo basado en enredamiento (EB) análogo.

Siendo así, se revisó el protocolo de QKD haciendo uso de estados coherentes ya que este tipo de protocolos presentan ciertas ventajas experimentales comparadas con los protocolos de variable discreta en donde estos presentan problemas desde la fabricación de los estados a enviar hasta en los dispositivos actuales para la medición. Considerando este tipo de protocolo se realizó el análisis de seguridad haciendo la analogía de PM a EB, de acuerdo a [4], se implementó una analogía con un protocolo en donde se preparan estados de vacío comprimidos de dos modos, obteniendo una fracción secreta que depende de la varianza de modulación, la transmitancia, el exceso de ruido y la eficiencia de reconciliación.

De igual forma, se realizó la propuesta del cálculo de la variable de fracción secreta pero sin realizar la analogía PM a EB, por lo que se partió directamente de los estados coherentes y considerando que son variables continuas, se usó las entropías denominadas entropía diferencial, entropía diferencial condicional y la información mutua para variables continuas (definidas en el capítulo 1), resultando una fracción secreta que solo depende de la varianza de modulación, del coeficiente de pérdida de la fibra óptica y de la longitud del canal. Es importante mencionar que para este último análisis se consideró que el canal

de envío es una fibra óptica en donde solo se contempló que afecta al estado a través de la atenuación de la amplitud y que Eve interviene solo dividiendo los estados de Alice con un divisor de haz 20/80. Por tanto, se puede observar que las expresiones del análisis de seguridad usando un protocolo EB y sin usarlo (como en la propuesta del capítulo anterior) serán considerablemente diferentes aparte que las consideraciones de ambos análisis son distintas e involucran distintos factores que pueden cambiar su forma.

Así esto da paso a que en un futuro se pueda realizar un análisis cuantitativo de las expresiones obtenidas para la fracción secreta haciendo uso de los datos de protocolos ya realizados experimentalmente, y comparando los resultados que se pudieran obtener. También se pueden implementar otras consideraciones que afecten a los estados en el envío como la desalineación de polarización o incluso cambiar el medio de envío siendo este el aire. Incluso se podría diseñar un armado experimental en donde se realice un análisis de ambas maneras y comparar ambos resultados.

BIBLIOGRAFÍA

- [1] COHEN-TANNOUJDI, C., DIU, B., & LALOË, F. (2020). Quantum mechanics, volume 1: Basic Concepts, Tools, and Applications. John Wiley & Sons.
- [2] MCMAHON, D. (2013). Quantum mechanics demystified. McGraw-Hill Education.
- [3] WOLF, R. (2021). Quantum Key Distribution : An Introduction with Exercises. Springer.
- [4] LAUDENBACH, F., PACHER, C., FUNG, C. H. F., POPPE, A., PEEV, M., SCHRENK, B., ... & HÜBEL, H. (2018). Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1), 1800011. <https://doi.org/10.1002/qute.201800011>
- [5] COVER, T. M. (1999). Elements of information theory. John Wiley & Sons.
- [6] SCARANI, V., BECHMANN-PASQUINUCCI, H., CERF, N. J., DUŠEK, M., LÜTKENHAUS, N., & PEEV, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics*, 81(3), 1301. <https://doi.org/10.1103/RevModPhys.81.1301>
- [7] KRONBERG, D. A. (2021). Vulnerabilities of quantum cryptography on geometrically uniform coherent states. *Quantum Electronics*, 51(10), 928. <https://dx.doi.org/10.1070/QEL17625>
- [8] GERRY, C., & KNIGHT, P. L. (2005). Introductory quantum optics. Cambridge university press.
- [9] WEEDBROOK, C., PIRANDOLA, S., GARCÍA-PATRÓN, R., CERF, N. J., RALPH, T. C., SHAPIRO, J. H., & LLOYD, S. (2012). Gaussian quantum information. *Reviews of Modern Physics*, 84(2), 621. <https://doi.org/10.1103/RevModPhys.84.621>
- [10] CAPUTO, C., SIMONI, M., CIRILLO, G. A., TURVANI, G., & ZAMBONI, M. (2022). A simulator of optical coherent-state evolution in quantum key distribution systems. *Optical and Quantum Electronics*, 54(11), 689. <https://doi.org/10.1007/s11082-022-04041-8>

- [11] GLANCY, S., VASCONCELOS, H. M., & RALPH, T. C. (2004). Transmission of optical coherent-state qubits. *Physical Review A*, 70(2), 022317. <https://doi.org/10.1103/PhysRevA.70.022317>
- [12] GROSSHANS, F., & GRANGIER, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5), 057902. <https://doi.org/10.1103/PhysRevLett.88.057902>
- [13] SAXON, D. S. (2013). *Elementary quantum mechanics*. Courier Corporation.