Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Criptografía cuántica con fotones individuales

Tesis presentada al

Colegio de Física

como requisito parcial para la obtención del grado de

Licenciado en Física

por

Abril Vargas Cortés

Asesorado por

Dr. Luis Manuel Arévalo Aguilar

Puebla Pue.
Junio 2021

Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Criptografía cuántica con fotones individuales

Tesis presentada al

Colegio de Física

como requisito parcial para la obtención del grado de

Licenciado en Física

por

Abril Vargas Cortés

Asesorado por

Dr. Luis Manuel Arévalo Aguilar

Puebla Pue.
Junio 2021

Título: Criptografía cuántica con fotones individuales
Estudiante: Abril Vargas Cortés

COMITÉ

Dr. Carlos Ignacio Robledo Sánchez
Presidente

Dra. Marcela Maribel Méndez Otero
Secretario

Dr. Wuiyebaldo Fermín Guerrero Sánchez
Vocal

Dr. Martín Rodolfo Palomino Merino
Vocal

Dr. Luis Manuel Arévalo Aguilar
Asesor

Dedico este trabajo a mi amada madre Elia Cortés Hernández, a mi hermana y orgullo Jocelyn Vargas Cortés, y a mi profesor y amigo Julio Hernández Juárez

Agradecimientos

Quiero agradecer principalmente a mi madre Elia Cortés quien me inspira y es mi motivo para ser alguien mejor cada día, al igual que sin su apoyo, entendimiento y amor incondicional esto no podría haberse realizado, este trabajo sin duda alguna es también de ella y de su esfuerzo por ser la mejor madre.
Al igual agradezco, a mi hermana Jocelyn Vargas quien desde pequeñas fue mi primer modelo a seguir e inspiración para dar mis primeros grandes pasos en diversos ámbitos de mi vida.
También agradezco, a mi profesor y amigo Julio Hernández quien me introdujó por primera vez al ámbito de la investigación y de lo que enfrentaría a lo largo de mi carrera y vida profesional, sin sus enseñanzas no podría tener la seguridad y conocimientos que hoy tengo.
A mis amigos de la universidad,Luis Tuxtla, Alfonso de Jesus Correa, A. David Toriz,Jesus I. Morán, R. Eduardo Rodríguez y Jesus A. Arellano quienes fueron un apoyo invaluable durante la carrera y una compañia única.
Por último, agradezco al Dr. Luis Manuel Arévalo Aguilar, quien fue un gran guía y apoyo durante el proceso de este trabajo, y quien me proporcionó conocimientos invaluables.

Índice general

Índice de figuras

Índice de tablas

Resumen

La criptografía cuántica es una de las nuevas áreas sumamente investigadas que tiene como uno de sus objetivos principales aplicar los principios de la mecánica cuántica en nueva tecnología, por esto mismo es importante estudiar y entender los criptosistemas planteados por los cuales se puede realizar un intercambio de información seguro principalmente la parte de distribución de claves.
Todo inició desde la necesidad de establecer comunicación de forma segura, es decir, sin intervenciones de personas ajenas, dando así paso a la criptografía. Esta se ha sustentado en supuestos matemáticos no comprobables, por lo que avances tecnológicos podrían poner en riesgo la seguridad.
Ante esto, la criptografía cuántica se muestra invulnerable ante el posible robo de información, esto sustentado por la característica fundamental de los estados cuánticos: si se realiza una medición se perturba el sistema.
En la actualidad, se han realizado diversos esquemas para criptografía cuántica, donde se han usado estados enredados tipo Bell e incluso esquemas con estados enredados con un solo fotón. Estos últimos, presentan ciertas ventajas sobre los esquemas tradicionales.
En este trabajo se estudiará los postulados de la mecánica cuántica e información cuántica para así entender lo que son las compuertas lógico clásicas y lógico cuánticas, y poder realizar la construcción de una compuerta unitaria de dos qubits de un solo fotón.Finalmente, se explicará la definición de criptografía cuántica y se analizarán dos protocolos de distribución de claves: el BB84 y uno basado en criptografía cuántica con estados enredados con un solo fotón.
Palabras clave: *Criptografía cuántica, mecánica cuántica, distribución de claves,compuertas lógico cuánticas, estados enredados con un solo fotón.*

Introducción

La mecánica cuántica ha tenido un gran impacto en el desarrollo de la física, viéndose enfrentada a diversas opiniones y debates, sin embargo hoy en día sus aplicaciones auguran un gran avance tecnológico; siendo una de sus aplicaciones prácticas, la unión de esta misma y la teoría de la información (desarrollada por Shannon) conocida como Teoría de la información cuántica. La cual vió uno de sus inicios en 1970 con Stephen J. Wiesner, para posteriormente basándose en sus ideas, Bennet y Brassard propusieran el primer protocolo de criptografía cuántica haciendo uso de fotones.

En consecuencia, la criptografía cuántica ha visto diversas propuestas y protocolos de criptografía los cuales empiezan a comercializarse con el fin de una transmisión de información segura.

La criptografía cuántica con un solo fotón data de principios del nuevo siglo, cuando se entendió que los sistemas individuales también poseen enredamiento cuántico entre sus diversos grados de libertad. Esto permitió que se propusieran esquemas de criptografía con fotones individuales, los cuales presentan ventajas respecto a los esquemas tradicionales ya que en ellos es posible usar todos los fotones para realizar el envío de llaves seguras; de modo que se comenzó a idear para ello esquemas de medición cuántica apropiado para tales efectos.

En el primer capítulo, se presentan los postulados de la mecánica cuántica e información cuántica. Con esto, se llega al segundo capítulo, donde se explican los conceptos de compuertas lógico clásicas y lógico cuánticas, con sus respectivos ejemplos, para así llegar a la construcción de una compuerta lógica universal para estados de dos qubits de un solo fotón haciendo uso de los conceptos de divisor de haz cuántico y de la interferometría con un solo fotón. Finalmente, en el tercer capítulo, se analizaran dos esquemas de criptografía cuántica propuestos centrándonos en el criptosistema con fotones individuales y sus diferencias con un criptosistema cuántico tradicional.

Capítulo 1

Conceptos básicos

En este capítulo, se revisará de manera breve el espacio de Hilbert, los principios básicos de la mecánica cuántica y de la información cuántica.

1.1. Espacio de Hilbert

El espacio de Hilbert es una generalización del espacio vectorial euclidiano (espacio vectorial real de dimensión finita con un producto escalar), es decir, es un espacio vectorial real o complejo en el que se define un producto escalar y que es completo respecto a la norma inducida por el producto escalar.
El producto escalar en un espacio de Hilbert complejo H asocia a dos vectores cualesquiera θ, λ pertenecientes a H con un número complejo $\langle\theta|\lambda\rangle$ tal que [12]:

1. $\langle\theta|\lambda\rangle$ es lineal en λ, es decir, $\langle\theta|\chi + \lambda\rangle = \langle\theta|\chi\rangle + \langle\theta|\lambda\rangle$ y $\langle\theta|\beta\lambda\rangle = \beta\langle\theta|\lambda\rangle$ donde θ, λ, χ pertenecen a H y β es un complejo.
2. $\langle\theta|\lambda\rangle = \overline{\langle\lambda|\theta\rangle}$ donde la barra denota la conjugación compleja.
3. $\langle\lambda|\lambda\rangle \geq 0$ para todo $\lambda \in H$
4. $\langle\lambda|\lambda\rangle = 0$ si y solo si $\lambda = 0$

Como un ejemplo del espacio de Hilbert podemos mencionar al oscilador armónico que tiene como base los eigenvectores del hamiltoniano:

$$\Psi_n(x) = \left(\frac{m\omega}{\pi\hbar}\right)^{\frac{1}{4}} \frac{1}{\sqrt{2^n n!}} H_n(\xi) e^{\frac{-\xi^2}{2}} \tag{1.1}$$

donde $H_n(\xi)$ son los polinomios de Hermite, $\xi \equiv \sqrt{\frac{m\omega}{\hbar}}x$ y $n = 0, 1, 2, 3, ...$ siendo este un espacio de dimensión infinita.

También tenemos el espacio de Hilbert para el operador de spin $1/2$ S_z donde los eigenvectores ortonormales $|+\rangle$ y $|-\rangle$ forman la base para el espacio, siendo este el espacio de Hilbert más pequeño, con solo dos dimensiones.

1.2. Mecánica cuántica

La mecánica cuántica es la rama de la física (creada a finales del siglo XIX e inicios del siglo XX) que estudia el comportamiento de la naturaleza en escalas pequeñas, como el átomo, sin embargo actualmente se está aplicando al estudio de sistemas macroscópicos.

La mecánica cuántica ha contribuido al estudio de la estructura del átomo, la fusión nuclear de las estrellas, las partículas fundamentales, entre otros.

Podemos resumir la teoría cuántica en los siguientes postulados básicos los cuales nos permiten realizar diversos cálculos, como por ejemplo: la evolución del estado de un sistema.

1.2.1. Primer postulado

Asociado a cualquier sistema físico aislado hay un espacio vectorial complejo con un producto interno (es decir, un espacio de Hilbert) conocido como el espacio de estados del sistema. El sistema está completamente descrito por su vector de estado $|\Psi\rangle$, que es un vector unitario en el espacio de estado del sistema. La evolución temporal del estado, sin realizar ninguna medida, se rige por la ecuación de Schrödinger:

$$i\hbar\frac{\partial\,|\Psi(t)\rangle}{\partial t} = \hat{H}\,|\Psi(t)\rangle \tag{1.2}$$

donde $\hbar \equiv \frac{h}{2\pi}$, h conocida como la constante de Planck y $\hat{H}$ es un operador autoadjunto conocido como el hamiltoniano del sistema.

1.2.2. Segundo postulado

Asociamos con cualquier observable A un operador autoadjunto $\hat{A}$ en el espacio de Hilbert H_s. El único resultado posible de una medición de la observable A es uno de los valores propios de este operador. Si escribimos la ecuación de valor propio para el operador $\hat{A}$:

$$\hat{A}\,|a_i\rangle = a_i\,|a_i\rangle \tag{1.3}$$

donde $|a_i\rangle$ es una base ortonormal de eigenvectores del operador $\hat{A}$ y escribimos el vector de estado sobre la base ortogonal de eigenvectores:

$$|\Psi(t)\rangle = \Sigma_i c_i(t)\,|a_i\rangle \tag{1.4}$$

1.2.3. Tercer postulado

Si un sistema es descrito por el vector de estado $|\Psi\rangle$ y la observable A se mide obteniendo el eigenvalor a_1, inmediatamente después de la medición el estado del sistema corresponderá al eigenvector $|a_1\rangle$.

Partiendo de los postulados básicos anteriores podemos inferir el principio de incertidumbre.

1.2.4. Principio de incertidumbre de Heisenberg

Si $\hat{A}$ y $\hat{B}$ son operadores asociados con observables del mismo sistema cuántico y $|\Psi\rangle$ es el estado cuántico actual, se cumple la siguiente relación:

$$\Delta A \Delta B \geq \frac{|\,\langle\Psi|\,[\hat{A},\hat{B}]\,|\Psi\rangle\,|}{2} \tag{1.5}$$

donde $[\hat{A},\hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ es el conmutador entre ellos dos y $\Delta A(\Delta B)$ la desviación estándar correspondiente a la observable A(B) en el estado $|\Psi\rangle$. El principio de incertidumbre nos dice que si estos dos operadores no conmutan no podemos predecir con certeza las dos observables al mismo tiempo.

Así mismo, es conveniente resaltar las correlaciones cuánticas, y de entre de ellas el entrelazamiento cuántico.

1.2.5. Entrelazamiento

El espacio de Hilbert H_s asociado con un sistema compuesto es el producto tensorial de los espacios de Hilbert H_i asociados con los componentes del sistema i: $H_s = H_1 \otimes H_2$. Decimos que un estado no esta entrelazado si puede escribirse como un producto tensorial de un estado de H_1 ($|\alpha\rangle$) y un estado de H_2 ($|\beta\rangle$):

$$|\Psi\rangle = |\alpha\rangle \otimes |\beta\rangle \tag{1.6}$$

Cuando dos sistemas están entrelazados no es posible asignar un vector de estado en cada sistema.
Por ejemplo, para lo estados de Bell no es posible asociar un vector de estado con cada sistema físico, sino que se asocia un estado global que los sistemas comparten:

$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|1\rangle_1 |1\rangle_0 + |0\rangle_1 |0\rangle_0) \tag{1.7}$$

1.3. Información cuántica

La información cuántica es el estudio de las tareas de procesamiento de información (tareas en las cuales se recaban datos y procesan o manipulan para obtener información relevante y útil) que se pueden realizar utilizando sistemas de mecánica cuántica, es decir, involucra el estudio de la representación, el procesamiento y el acceso a la información mediante sistemas mecánicos cuánticos. Siendo uno de sus objetivos el desarrollar herramientas que fortalezcan el entendimiento de la mecánica cuántica.
Esta se desarrolló desde las investigaciones de los límites físicos hasta la computación iniciada por Charles Bennett, sin embargo, también se encontraba Richard Feynman quien demostró que la mecánica cuántica no limitaba a lo que podía hacer una computadora.

1.3.1. El qubit

La unidad básica de la información clásica es el bit que puede ser 0 o 1. En información cuántica su equivalente es el qubit que es un sistema cuántico de dos niveles. Estos niveles son denotados por $|1\rangle$ y $|0\rangle$, siendo equivalentes al 0 y 1 en el modelo clásico.
Estos sistemas pueden ser representados físicamente por los espines o la polarización de un fotón. La diferencia entre el bit y qubit es que este último puede existir en una superposición de estado:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1.8}$$

mientras que el bit es definitivamente 0 o 1(α y β son números complejos).
Desde otro punto de vista, un qubit es un vector en un espacio vectorial complejo bidimensional, donde los estados $|1\rangle$ y $|0\rangle$ son conocidos como estados de base computacional y forman una base ortonormal.
Estos dos estados pueden ser representados de forma matricial, de la siguiente manera:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.9}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{1.10}$$

1.3.2. Qubits múltiples

Supongamos que tenemos dos qubits, si estos fueran dos bits clásicos, entonces tendriamos cuatro estados posibles: 00, 01, 10 y 11. Por lo tanto, un sistema de dos qubit tiene cuatro estados

de base computacional:$|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Un par de qubits también pueden existir en superposiciones de estos cuatro estados, por lo que el estado cuántico de dos qubits implica asociar un coeficiente complejo, a veces llamado amplitud, con cada estado de base computacional, de tal manera que el vector de estado que describe los dos qubits es:

$$|\Psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{1.11}$$

Un estado importante de dos qubits es el estado de Bell o el par EPR:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.12}$$

este estado es responsable de muchas sopresas en computación cuántica e información cuántica. El estado de Bell tiene la propiedad de que al medir el primer qubit se obtienen dos resultados posibles: 0 con probabilidad de $\frac{1}{2}$, dejando el estado posterior a la medición $|\rho'\rangle = |00\rangle$, y 1 con probabilidad de $\frac{1}{2}$, dejando $|\rho'\rangle = |11\rangle$. Como resultado, una medición del segundo qubit siempre da el mismo resultado que la medición del primer qubit,es decir, los resultados de la medición están correlacionados. [7] [9]

Capítulo 2

Compuertas lógico clásicas y cuánticas

En este capítulo, se revisarán los conceptos de las compuertas lógico clásicas y de las compuertas lógico cuánticas con algunos ejemplos. Pasando así a la construcción de una compuerta cuántica unitaria para estados de dos qubits producidos por un solo fotón (basado en el desarrollo del artículo de Englert, et. al. [11]), revisando antes el funcionamiento del divisor de haz cuántico y del interferómetro de Mach- Zehnder

2.1. Compuertas lógico clásicas

En la computación clásica se puede realizar un procesamiento básico de la información haciendo uso de una compuerta lógica.
El propósito básico de una compuerta lógica es manipular o procesar información a nivel de bit de alguna manera,un ejemplo es la compuerta *NOT*.
La compuerta NOT es una compuerta de entrada única, esta compuerta invierte el valor del bit de entrada. Es decir, si entra un bit 1 sale un bit 0, y si entra un bit 0 sale un bit 1. Esquematicamente se puede escribir como:

$$1 \rightarrow 0 \tag{2.1}$$

$$0 \rightarrow 1 \tag{2.2}$$

En ocasiones es necesario una forma más sistemática para escribir la acción de una compuerta lógica, esto se puede hacer usando una tabla de verdad. Para la compuerta NOT, del lado izquierdo se colocan los valores de entrada y del lado derecho los valores de salida:

Entrada	**NOT**
1	0
0	1

Tabla 2.1: Tabla de verdad: Compuerta NOT

También se puede ver esquematizado por el siguiente diagrama, donde las interconexiones son cables ideales que llevan uno de los voltajes estándar que representan el 1 y el 0, y el los cables salientes se obtienen los valores lógicos resultantes.

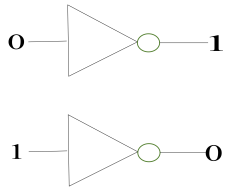

Figura 2.1: Compuerta NOT

También hay compuertas más complicadas que se aplican a pares de bits, como las compuertas: OR, AND y XOR.
La compuerta OR acepta dos bits como entrada (A y B), y la salida es 1 si A o B son 1, y es 0 en caso contrario.

A	B	A OR B
1	0	1
0	1	1
0	0	0
1	1	1

Tabla 2.2: Compuerta OR

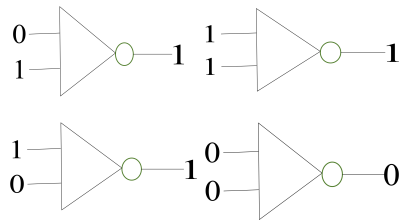

Figura 2.2: Compuerta OR

La compuerta AND acepta dos bits de entrada, A y B, y la salida es 1 siempre que ambos bits sean 1, en caso contrario es 0.

A	B	A AND B
1	0	0
0	1	0
0	0	0
1	1	1

Tabla 2.3: Compuerta AND

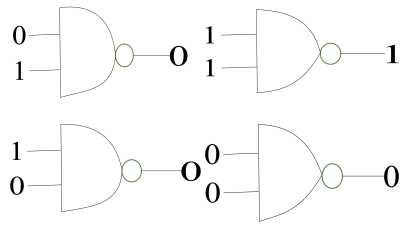

Figura 2.3: Compuerta AND

La compuerta XOR da como salida 1 cuando A o B son 1, pero no da 1 cuando ambos lo son. La operación XOR se indica con el simbolo $\oplus$.

A	B	A $\oplus$ B
1	0	1
0	1	1
0	0	0
1	1	0

Tabla 2.4: Compuerta XOR

La compuerta NAND o NOT-AND, es una unión entre las dos compuertas, primero se aplica la compuerta AND y al resultado se le aplica la compuerta NOT.

A	B	A NAND B
1	0	1
0	1	1
0	0	1
1	1	0

Tabla 2.5: Compuerta NAND

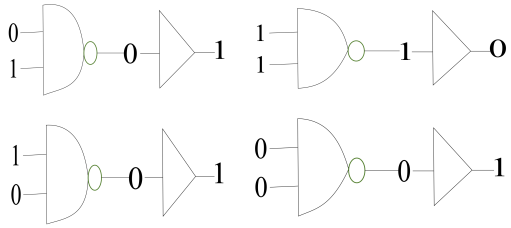

Figura 2.4: Compuerta NAND

Esta compuerta tiene la propiedad de ser universal, es decir, todas las operaciones informáticas se pueden completar usando solo compuertas NAND. [8]

2.2. Compuertas lógico cuánticas

En computación cuántica, la información también se procesa mediante compuertas, pero las compuertas ahora son " operadores".
Las compuertas cuánticas son operadores unitarios que actúan sobre uno o más qubits. Dado esto, las compuertas cuánticas deben ser reversibles, es decir, que si conocemos el estado de salida podemos inferir cuál es el estado de entrada. Esto mismo descarta la posibilidad de versiones cuánticas de algunas compuertas clásicas, por ejemplo: si de la compuerta AND obtenemos una salida de 0, esto puede ser producido por las entradas 00,01 o 10, por lo que no es reversible y no puede tener una versión cuántica. Pero la compuerta NOT si puede ser reversible por lo que puede existir una compuerta cuántica.
Analizando este caso, buscamos que:

$$\alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha\,|1\rangle + \beta\,|0\rangle$$

Si representamos el estado de qubits como un vector de columna de dos componentes:

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{2.3}$$

Así entonces, la compuerta cuántica NOT (representada por X) puede ser representada por la matriz:

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix} \tag{2.4}$$

donde

$$X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \tag{2.5}$$

Por lo tanto, aplicando la compuerta NOT a $|1\rangle$ y $|0\rangle$:

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{2.6}$$

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \tag{2.7}$$

Podemos representar la acción de una compuerta cuántica dibujando un diagrama de circuito. Cada operador unitario o compuerta está representado por un bloque con líneas (o "cables") que se utilizan para representar la entrada y la salida. El diagrama de circuito para la compuerta NOT es:

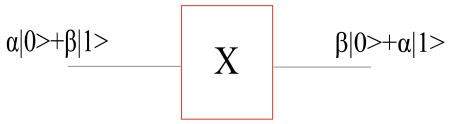

Figura 2.5: Circuito: Compuerta cuántica NOT o X

Como se sabe los operadores cuánticos se pueden representar con matrices. Por lo tanto, una compuerta con n entradas y salidas se puede representar con una matriz de grado 2^n. Por ejemplo, para un qubit necesitamos una matriz de grado $2^1 = 2$,así una compuerta cuántica que actúa sobre un solo qubit será una matriz unitaria de 2×2 , mientras que para una compuerta de dos qubits se necesita una matriz de grado $2^2 = 4$ o una matriz de 4×4.

Ahora pasemos al análisis de compuertas cuánticas de dos qubits. Considerando el caso de las compuertas controladas clásicas tenemos que si tenemos un bit de control de valor 0 entonces la compuerta no realiza nada, mientras que si el bit control es 1 entonces la compuerta realiza una acción.

Por consiguiente, las compuertas cuánticas controladas (o unitarias controladas) funcionan usando un qubit de control para determinar si una acción se ejecutará o no sobre un qubit objetivo [7][8][9].

2.2.1. Compuerta cuántica CNOT

La compuerta cuántica CNOT es una compuerta de dos qubits, representada por el siguiente circuito:

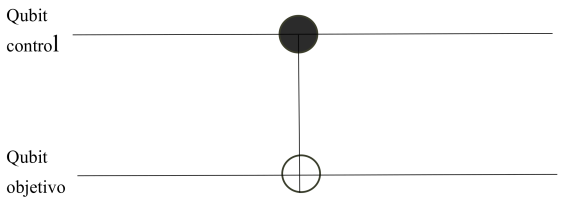

Figura 2.6: Circuito: Compuerta cuántica CNOT

El qubit superior se llama qubit de control y el inferior es el qubit objetivo. La compuerta no cambia el estado del qubit de control, y el cambio se da en el estado del qubit objetivo depende del estado del qubit de control. En particular, si el qubit de control es $|0\rangle$, no le sucede nada al qubit

objetivo, pero si el qubit de control es $|1\rangle$, el qubit objetivo se invierte. Por lo tanto, si el primer qubit es el control y el segundo el objetivo, tenemos [7]

$$\begin{aligned} |0\rangle\,|1\rangle &\longrightarrow |0\rangle\,|1\rangle \\ |0\rangle\,|0\rangle &\longrightarrow |0\rangle\,|0\rangle \\ |1\rangle\,|0\rangle &\longrightarrow |1\rangle\,|1\rangle \\ |1\rangle\,|1\rangle &\longrightarrow |1\rangle\,|0\rangle \end{aligned} \tag{2.8}$$

2.3. Compuerta unitaria para estados de dos qubits de un solo fotón

2.3.1. Divisor de haz cuántico

Un divisor de haz es aquel instrumento óptico que divide un rayo de luz en dos. Para los haces de luz clásicos, coherentes y térmicos, los tratamientos cuántico y clásico de los divisores de haz concuerdan. Pero a nivel de uno o pocos fotones, el enfoque del divisor de haz produce resultados incorrectos.
Para ver el error, consideremos un campo de luz clásico de amplitud compleja ε_1 incidente sobre un divisor de haz sin pérdidas, mientras que ε_2 y ε_3 son las amplitudes de los haces reflejado y transmitido.

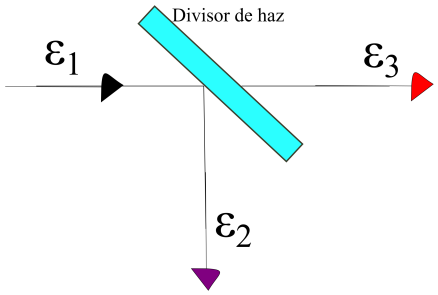

Figura 2.7: Divisor de haz clásico

Si r y t son la reflectancia y la transmitancia (ambos complejos) del divisor de haz, se deduce que:

$$\varepsilon_2 = r\varepsilon_1 \;\text{ y }\; \varepsilon_3 = t\varepsilon_1 \tag{2.9}$$

Para un divisor de haz 50:50, tendríamos:

$$|r| = |t| = \frac{1}{\sqrt{2}}$$

Dado que el divisor de haz no tiene pérdidas, la intensidad del haz de entrada y salida debe ser igual, por consiguiente debe ser igual a la suma de las intensidades de los haces de salida:

$$|\varepsilon_1|^2 = |\varepsilon_2|^2 + |\varepsilon_3|^2 \tag{2.10}$$

lo que requiere que $|r|^2 + |t|^2 = 1$

Para tratar un divisor de haz con la mecánica cuántica se podría reemplazar las amplitudes complejas de los campos ε_i por operadores de aniquilación $\hat{a}_i$ donde $(i = 1, 2, 3)$. De manera análoga

al tratamiento clásico, tenemos:

$$\hat{a}_2 = r\hat{a}_1 \tag{2.11}$$
$$\hat{a}_3 = t\hat{a}_1$$

estos operadores deben satisfacer las relaciones de conmutación:

$$[\hat{a}_i, \hat{a^\dagger}_j] = \delta_{ij}, [\hat{a}_i, \hat{a}_j] = 0 = [\hat{a^\dagger}_i, \hat{a^\dagger}_j]$$

Sin embargo, podemos ver que:

$$[\hat{a}_2, \hat{a^\dagger}_2] = |r|^2, \;\; [\hat{a}_3, \hat{a^\dagger}_3] = |t|^2, \;\; [\hat{a}_2, \hat{a^\dagger}_3] = rt^*$$

Dado que no preservan las relaciones de conmutación no pueden proporcionar una descripción cuántica correcta del divisor de haz.
Para ver qué sucede debemos considerar que en el tratamiento clásico hay un puerto de entrada que no se consideró y no afecta a los haces que emergen. Pero en mecánica cuántica el puerto de entrada no utilizado contiene un modo cuantizado que pertenece a las fluctuaciones del vacío y tiene importantes efectos físicos.
Así entonces, representaremos los modos de entrada con los operadores $\hat{a_0}$ que representa el modo correspondiente al vacío cuántico y el modo $\hat{a_1}$ el modo por donde entra el haz. Por ende, se tienen dos conjuntos de reflectancia y transmitancia , por lo que los operadores de salida que describen la salida de cada uno de los puertos es:

$$\hat{a_2} = r\hat{a_1} + t'\hat{a_0} \tag{2.12}$$
$$\hat{a_3} = t\hat{a_1} + r'\hat{a_0} \tag{2.13}$$

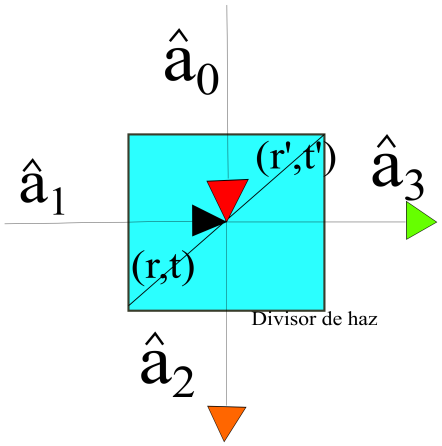

Figura 2.8: Divisor de haz cuántico

Para que las relaciones de conmutación se cumplan se deben satisfacer las siguientes relaciones:

$$|r'| = |r|, |t| = |t'|, |r|^2 + |t|^2 = 1$$
$$r^*t' + r't^* = 0, r^*t + r't'^* = 0$$

Dado que es un divisor de haz simétrico 50:50, los haces transmitidos y reflejados difieren por un factor de fase i , entonces los modos de salida son de la forma:

$$\hat{a}_2 = \frac{1}{\sqrt{2}} i\hat{a}_1 + \frac{1}{\sqrt{2}}\hat{a}_0 = \frac{1}{\sqrt{2}}(\hat{a}_0 + i\hat{a}_1) \tag{2.14}$$

$$\hat{a}_3 = \frac{1}{\sqrt{2}}\hat{a}_1 + \frac{1}{\sqrt{2}}i\hat{a}_0 = \frac{1}{\sqrt{2}}(i\hat{a}_0 + \hat{a}_1) \tag{2.15}$$

Veamos el siguiente ejemplo: si consideramos la entrada $|0\rangle_0 |1\rangle_1$, que puede ser escrita como $\hat{a}_1^\dagger |0\rangle_0 |0\rangle_1$, si la entrada del vacío en un divisor de haz se transforma de la forma: $|0\rangle_0 |0\rangle_1 \rightarrow |0\rangle_2 |0\rangle_3$. Y el operador $\hat{a}_1^\dagger$ se expresa:

$$\hat{a}_1^\dagger = \frac{1}{2}(i\hat{a}_2^\dagger + \hat{a}_3^\dagger)$$

Por lo tanto, el estado de entrada $|0\rangle_0 |1\rangle_1$ al pasar el divisor de haz toma la forma:

$$|0\rangle_0 |1\rangle_1 \rightarrow \frac{1}{\sqrt{2}}(i\hat{a}_2^\dagger + \hat{a}_3^\dagger) |0\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}}(i |1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3)$$

Lo que nos indica que el fotón único incidente en uno de los puertos de entrada del divisor de haz y el otro puerto que contiene solo el vacío, serán transmitidos o reflejados con la misma probabilidad. El estado anterior es un estado entrelazado, es decir que no puede escribirse como un simple producto de los estados de los modos individuales 2 y 3 [10].

2.3.2. Interferometría con un solo fotón

Para obtener efectos de interferencia con fotones individuales, debemos codificar las rutas hacia los detectores, ya que la interferencia ocurre por la falta de información sobre qué ruta. Una forma de lograrlo es a través de un interferómetro de Mach- Zehnder (MZI), que consta de dos divisores de haz, un conjunto de espejos y un desfasador. La interferencia ocurre ya que los detectores D1 y D2 no pueden distinguir entre el fotón que toma la trayectoria en sentido horario o antihorario.

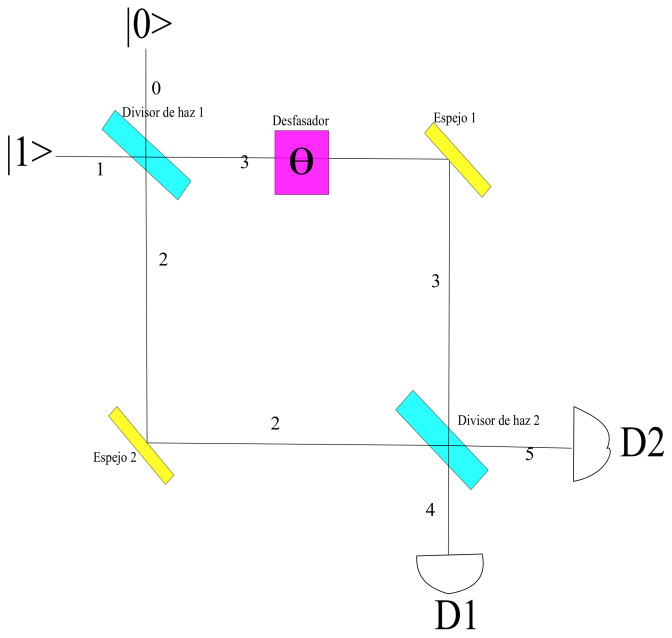

Figura 2.9: Interferómetro de Mach-Zehnder

Para ver como surge la interferencia de un solo fotón en el MZI, comenzamos con el estado de entrada $|0\rangle_0 |1\rangle_1$ como se puede ver en la figura 2.9.

Suponiendo que los divisores de haz están descritos por las ecuaciones 2.14 y 2.15, cuando el estado de entrada pasa por el primer divisor de haz(BS1) este se transforma de la forma:

$$|0\rangle_0 |1\rangle_1 \xrightarrow{BS1} \frac{1}{\sqrt{2}}(|0\rangle_2 |1\rangle_3 + i\,|1\rangle_2 |0\rangle_3) \tag{2.16}$$

Los espejos aportan un factor de $e^{i\pi/2}$ a cada término lo que equivale a una fase irrelevante que omitimos. El desfasador provoca un cambio de fase en el primer componente:

$$\frac{1}{\sqrt{2}}(|0\rangle_2 |1\rangle_3 + i\,|1\rangle_2 |0\rangle_3) \xrightarrow{\theta} \frac{1}{\sqrt{2}}(e^{i\theta}|0\rangle_2 |1\rangle_3 + i\,|1\rangle_2 |0\rangle_3) \tag{2.17}$$

Para el segundo divisor de haz (BS2) tenemos:

$$|0\rangle_2 |1\rangle_3 \xrightarrow{BS2} \frac{1}{\sqrt{2}}(|0\rangle_5 |1\rangle_4 + i\,|1\rangle_5 |0\rangle_4) \tag{2.18}$$

$$|1\rangle_2 |0\rangle_3 \xrightarrow{BS2} \frac{1}{\sqrt{2}}(|1\rangle_5 |0\rangle_4 + i\,|0\rangle_5 |1\rangle_4) \tag{2.19}$$

En consecuencia:

$$\frac{1}{\sqrt{2}}(e^{i\theta}|0\rangle_2 |1\rangle_3 + i\,|1\rangle_2 |0\rangle_3) \xrightarrow{BS2} \frac{1}{\sqrt{2}}\left(e^{i\theta}\left[\frac{1}{\sqrt{2}}(|0\rangle_5 |1\rangle_4 + i\,|1\rangle_5 |0\rangle_4)\right] + i\left[\frac{1}{\sqrt{2}}(|1\rangle_5 |0\rangle_4 + i\,|0\rangle_5 |1\rangle_4\right]\right) \tag{2.20}$$

Reduciendo la expresión obtenemos:

$$\frac{1}{\sqrt{2}}(e^{i\theta}|0\rangle_2 |1\rangle_3 + i\,|1\rangle_2 |0\rangle_3) \xrightarrow{BS2} \frac{1}{2}[(e^{i\theta}-1)|0\rangle_5 |1\rangle_4 + i(e^{i\theta}+1)|1\rangle_5 |0\rangle_4] \tag{2.21}$$

Siendo esta última expresión 2.21 el estado final del estado $|0\rangle_0 |1\rangle_1$ que paso por el interferómetro de Mach-Zehnder[10].

2.3.3. Construcción de compuerta unitaria para estados de dos qubits de un solo fotón

Cualquier alternativa binaria cuántica puede servir como qubit, por lo que podemos hacer uso de los diferentes grados de libertad de un objeto físico para representar varios qubits.
Para este esquema, ambos qubits de un par entrelazado se realizará físicamente mediante un solo fotón, donde la polarización será un qubit y la alternativa espacial será el otro qubit.
Para la realización de esta compuerta primero se obtendrá la compuerta espacial y la compuerta de polarización.

Compuerta para el qubit espacial

El qubit espacial consiste en la alternativa binaria $|0\rangle_0 |1\rangle_1$ y $|1\rangle_0 |0\rangle_1$, como se indica en los siguientes esquemas de MZI:

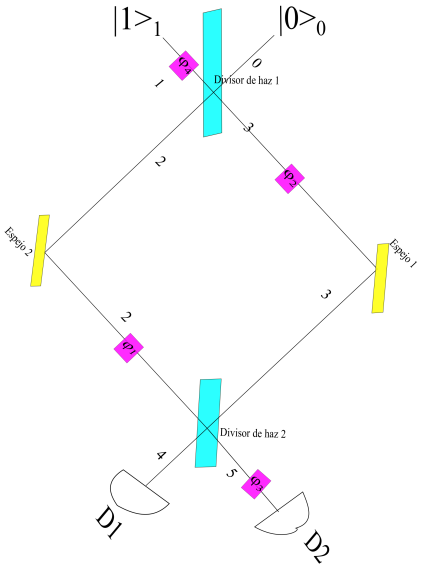

Figura 2.10: Interferómetro de Mach-Zehnder con entrada $|1\rangle_1 |0\rangle_0$

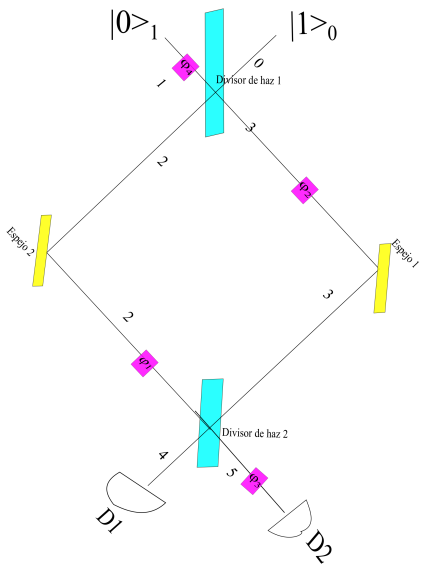

Figura 2.11: Interferómetro de Mach-Zehnder con entrada $|0\rangle_1 |1\rangle_0$

Considerando que φ_1, φ_2, φ_3 y φ_4 son cambios de fase y realizando un análisis similar al desarrollado en la sección anterior, tenemos que para el primer esquema de la figura 2.10:
Tenemos la entrada $e^{i\varphi_4} |0\rangle_0 |1\rangle_1$(el término $e^{i\varphi_4}$ es debido al primer cambio de fase):

1. Pasando el estado entrante por el primer divisor de haz (BS1), obtenemos:

$$e^{i\varphi_4} |0\rangle_0 |1\rangle_1 \overset{BS1}{\rightarrow} \frac{1}{\sqrt{2}}(e^{i\varphi_4} |0\rangle_2 |1\rangle_3 + ie^{i\varphi_4} |1\rangle_2 |0\rangle_3) \tag{2.22}$$

2. Pasando por los cambios de fase φ_1 y φ_2:

$$\frac{1}{\sqrt{2}}(e^{i\varphi_4} |0\rangle_2 |1\rangle_3 + ie^{i\varphi_4} |1\rangle_2 |0\rangle_3) \overset{\varphi_1,\varphi_2}{\rightarrow} \frac{1}{\sqrt{2}}(e^{i\varphi_4}e^{i\varphi_2} |0\rangle_2 |1\rangle_3 + ie^{i\varphi_4}e^{i\varphi_1} |1\rangle_2 |0\rangle_3) \tag{2.23}$$

3. Cuando el estado pasa por el segundo divisor de haz, tenemos que los estado toman la forma:

$$|0\rangle_2 |1\rangle_3 \overset{BS2}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle_5 |1\rangle_4 + i |1\rangle_5 |0\rangle_4) \tag{2.24}$$

$$|1\rangle_2 |0\rangle_3 \overset{BS2}{\longrightarrow} \frac{1}{\sqrt{2}}(|1\rangle_5 |0\rangle_4 + i |0\rangle_5 |1\rangle_4) \tag{2.25}$$

Sustituyendo las ecuaciones 2.24 y 2.25 en el estado resultante de la ecuación 2.23:

$$\frac{1}{\sqrt{2}}\left(e^{i\varphi_4}e^{i\varphi_2}\left\{\frac{1}{\sqrt{2}}(|0\rangle_5 |1\rangle_4 + i |1\rangle_5 |0\rangle_4)\right\} + ie^{i\varphi_4}e^{i\varphi_1}\left\{\frac{1}{\sqrt{2}}(|1\rangle_5 |0\rangle_4 + i |0\rangle_5 |1\rangle_4)\right\}\right) \tag{2.26}$$

4. Aplicando el cambio de fase de la salida por la ruta 5 (φ_3):

$$\frac{1}{\sqrt{2}}\left(e^{i\varphi_4}e^{i\varphi_2}\left\{\frac{1}{\sqrt{2}}(|0\rangle_5 |1\rangle_4 + i |1\rangle_5 |0\rangle_4)\right\} + ie^{i\varphi_4}e^{i\varphi_1}\left\{\frac{1}{\sqrt{2}}(|1\rangle_5 |0\rangle_4 + i |0\rangle_5 |1\rangle_4)\right\}\right) \overset{\varphi_3}{\rightarrow}$$
$$\frac{1}{\sqrt{2}}\left(e^{i\varphi_4}e^{i\varphi_2}\left\{\frac{1}{\sqrt{2}}(|0\rangle_5 |1\rangle_4 + ie^{i\varphi_3} |1\rangle_5 |0\rangle_4)\right\} + ie^{i\varphi_4}e^{i\varphi_1}\left\{\frac{1}{\sqrt{2}}(e^{i\varphi_3} |1\rangle_5 |0\rangle_4 + i |0\rangle_5 |1\rangle_4)\right\}\right)$$

Reduciendo la expresión del estado resultante anterior:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left(e^{i\varphi_4}e^{i\varphi_2}\left\{\frac{1}{\sqrt{2}}(|0\rangle_5|1\rangle_4+ie^{i\varphi_3}|1\rangle_5|0\rangle_4)\right\}+ie^{i\varphi_4}e^{i\varphi_1}\left\{\frac{1}{\sqrt{2}}(e^{i\varphi_3}|1\rangle_5|0\rangle_4+i|0\rangle_5|1\rangle_4)\right\}\right) = \\
&\qquad \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left[e^{i\varphi_4}e^{i\varphi_2}(|0\rangle_5|1\rangle_4+ie^{i\varphi_3}|1\rangle_5|0\rangle_4)+ie^{i\varphi_4}e^{i\varphi_1}(e^{i\varphi_3}|1\rangle_5|0\rangle_4+i|0\rangle_5|1\rangle_4)\right] \\
&=\frac{1}{2}\left[e^{i\varphi_4}e^{i\varphi_2}|0\rangle_5|1\rangle_4+ie^{i\varphi_4}e^{i\varphi_2}e^{i\varphi_3}|1\rangle_5|0\rangle_4+ie^{i\varphi_4}e^{i\varphi_1}e^{i\varphi_3}|1\rangle_5|0\rangle_4+i^2e^{i\varphi_4}e^{i\varphi_1}|0\rangle_5|1\rangle_4\right] \\
&=\frac{1}{2}\left[e^{i(\varphi_4+\varphi_2)}|0\rangle_5|1\rangle_4+ie^{i(\varphi_4+\varphi_2+\varphi_3)}|1\rangle_5|0\rangle_4+ie^{i(\varphi_4+\varphi_1+\varphi_3)}|1\rangle_5|0\rangle_4-e^{i(\varphi_4+\varphi_1)}|0\rangle_5|1\rangle_4\right] \\
&=\frac{1}{2}\left[(e^{i(\varphi_4+\varphi_2)}-e^{i(\varphi_4+\varphi_1)})|0\rangle_5|1\rangle_4+i(e^{i(\varphi_4+\varphi_2+\varphi_3)}+e^{i(\varphi_4+\varphi_1+\varphi_3)})|1\rangle_5|0\rangle_4\right] \\
&=\frac{1}{2}\left[e^{i\varphi_4}(e^{i\varphi_2}-e^{i\varphi_1})|0\rangle_5|1\rangle_4+ie^{i\varphi_3}e^{i\varphi_4}(e^{i\varphi_2}+e^{i\varphi_1})|1\rangle_5|0\rangle_4\right] \\
&=\frac{1}{2}\left[e^{i\varphi_4}(e^{i\varphi_2}-e^{i\varphi_1})|0\rangle_5|1\rangle_4+ie^{i(\varphi_3+\varphi_4)}(e^{i\varphi_2}+e^{i\varphi_1})|1\rangle_5|0\rangle_4\right] \qquad (2.27)
\end{aligned}$$

Realizando un procedimiento análogo para el esquema de la figura 2.11, obtenemos:

$$\frac{1}{2}\left[e^{i(\varphi_4+\varphi_3)}(e^{i\varphi_1}-e^{i\varphi_2})|0\rangle_4|1\rangle_5+ie^{i\varphi_4}(e^{i\varphi_1}+e^{i\varphi_2})|1\rangle_4|0\rangle_5\right] \qquad (2.28)$$

Compuerta para el qubit de polarización

El qubit de polarización consiste en la alternativa binaria $|v\rangle$ y $|h\rangle$. La polarización del fotón se manipula con placas de onda (placa de cuarto de onda y placa de media onda). Para la creación de esta compuerta se usarán dos placas de cuarto de onda y una de media onda las cuales permiten realizar cambios arbitrarios del estado de polarización del fotón.
El operador unitario de una placa de cuarto de onda QWP, con su eje mayor en un ángulo θ con la dirección vertical, es:

$$U_{QWP}(\theta)=e^{-i\theta\sigma_2}e^{-i(\frac{\pi}{4})\sigma_3}e^{i\theta\sigma_2}$$

Mientras que, la acción de una placa de media onda (HWP) esta dado por el operador unitario:

$$U_{QWP}(\theta)=e^{-i\theta\sigma_2}e^{-i(\frac{\pi}{2})\sigma_3}e^{i\theta\sigma_2}$$

Así entonces, el armado para esta compuerta esta dado por el siguiente esquema:

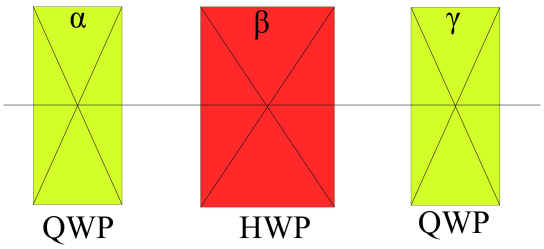

Figura 2.12: Esquema de placas de onda para la compuerta de polarización

Por consiguiente, expresando el operador unitario en término de los tres ángulos (eulerianos):

$$U_{pol}=U_{QWP}(\gamma)U_{HWP}(\beta)U_{QWP}(\alpha) \qquad (2.29)$$

Por lo tanto, la polarización dependiente de un desfasador es:

$$U_{pol} = |v\rangle\, e^{-i\vartheta}\, \langle v| + |h\rangle\, e^{i\vartheta}\, \langle h| \tag{2.30}$$

lo que se cumple con el ajuste $\alpha = \gamma = \frac{1}{4}\pi, \beta = \frac{1}{2}\vartheta - \frac{1}{4}\pi$.

Compuerta unitaria para estados de dos qubits

Una vez establecidos los operadores espacial y de polarización, podemos modificar el esquema 2.10 donde los desfasadores $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ son reemplazados cada uno por un desfasador y un conjunto de placas de onda (como el planteado en el esquema 2.12)nombrados V_R, V_L, V_2, V_1, tal sustitución actúa como el operador de la ecuación 2.30.

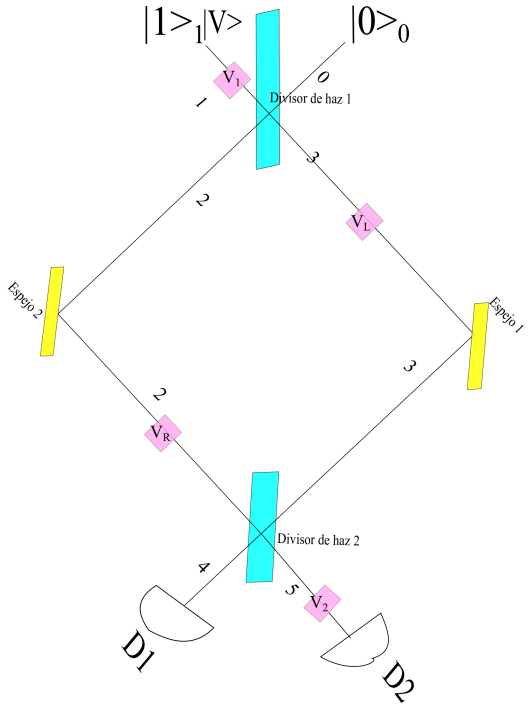

Figura 2.13: Interferómetro de Mach-Zehnder con entrada $|0\rangle_1 |1\rangle_0 |v\rangle$

Consideramos la entrada $|1\rangle_1 |0\rangle_0 |v\rangle$:

1. Pasando el estado por V_1, el cual esta definido de la forma:

$$V_1 = |v\rangle\, e^{-i\vartheta_1}\, \langle v| + |h\rangle\, e^{i\vartheta_1}\, \langle h| \tag{2.31}$$

Obtenemos:

$$\begin{aligned} |1\rangle_1 |0\rangle_0 |v\rangle &\overset{V_1}{\rightarrow} |1\rangle_1 |0\rangle_0 \left(|v\rangle\, e^{-i\vartheta_1}\, \langle v| + |h\rangle\, e^{i\vartheta_1}\, \langle h|\right) |v\rangle \\ &= |1\rangle_1 |0\rangle_0 |v\rangle\, e^{-i\vartheta_1} \end{aligned} \tag{2.32}$$

2. Ahora el estado de la ecuación 2.32 pasa por el primer divisor de haz (BS1):

$$|1\rangle_1 |0\rangle_0 |v\rangle\, e^{-i\vartheta_1} \overset{BS1}{\rightarrow} \frac{1}{\sqrt{2}}(e^{-i\vartheta_1} |1\rangle_3 |0\rangle_2 |v\rangle + ie^{-i\vartheta_1} |0\rangle_3 |1\rangle_2 |v\rangle) \tag{2.33}$$

3. Ahora el estado pasa por V_R y V_L, que tienen la forma:

$$V_R = |v\rangle e^{-i\vartheta_R} \langle v| + |h\rangle e^{i\vartheta_R} \langle h| \quad (2.34)$$
$$V_L = |v\rangle e^{-i\vartheta_L} \langle v| + |h\rangle e^{i\vartheta_L} \langle h| \quad (2.35)$$

Aplicándose las ecuaciones 2.34 y 2.35 en el estado resultante de la ecuación 2.33:

$$e^{-i\vartheta_1} |0\rangle_3 |1\rangle_2 |v\rangle \overset{V_R}{\rightarrow} e^{-i\vartheta_1} e^{-i\vartheta_R} |0\rangle_3 |1\rangle_2 |v\rangle \quad (2.36)$$
$$e^{-i\vartheta_1} |1\rangle_3 |0\rangle_2 |v\rangle \overset{V_L}{\rightarrow} e^{-i\vartheta_1} e^{-i\vartheta_L} |1\rangle_3 |0\rangle_2 |v\rangle \quad (2.37)$$

Por lo tanto, el estado ahora es:

$$\frac{1}{\sqrt{2}}(e^{-i\vartheta_1} e^{-i\vartheta_L} |1\rangle_3 |0\rangle_2 |v\rangle + ie^{-i\vartheta_1} e^{-i\vartheta_R} |0\rangle_3 |1\rangle_2 |v\rangle) \quad (2.38)$$

4. Pasando por el segundo divisor de haz (BS2), tenemos:

$$|1\rangle_3 |0\rangle_2 \overset{BS2}{\rightarrow} \frac{1}{\sqrt{2}}(|1\rangle_4 |0\rangle_5 + i |0\rangle_4 |1\rangle_5) \quad (2.39)$$
$$|0\rangle_3 |1\rangle_2 \overset{BS2}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle_4 |1\rangle_5 + i |1\rangle_4 |0\rangle_5) \quad (2.40)$$

Sustituyendo las ecuaciones 2.39 y 2.40 en la ecuación 2.38:

$$\frac{1}{\sqrt{2}} \left\{ e^{-i\vartheta_1} e^{-i\vartheta_L} \left[\frac{1}{\sqrt{2}}(|1\rangle_4 |0\rangle_5 + i |0\rangle_4 |1\rangle_5) \right] |v\rangle + ie^{-i\vartheta_1} e^{-i\vartheta_R} \left[\frac{1}{\sqrt{2}}(|0\rangle_4 |1\rangle_5 + i |1\rangle_4 |0\rangle_5) \right] |v\rangle \right\} \quad (2.41)$$

5. Finalmente en la salida 5 actúa V_2, que tiene la forma:

$$V_2 = |v\rangle e^{-i\vartheta_2} \langle v| + |h\rangle e^{i\vartheta_2} \langle h| \quad (2.42)$$

Lo que da como resultado:

$$\frac{1}{\sqrt{2}} \left\{ e^{-i\vartheta_1} e^{-i\vartheta_L} \left[\frac{1}{\sqrt{2}}(|1\rangle_4 |0\rangle_5 + ie^{-i\vartheta_2} |0\rangle_4 |1\rangle_5) \right] |v\rangle + ie^{-i\vartheta_1} e^{-i\vartheta_R} \left[\frac{1}{\sqrt{2}}(e^{-i\vartheta_2} |0\rangle_4 |1\rangle_5 + i |1\rangle_4 |0\rangle_5) \right] |v\rangle \right\} \quad (2.43)$$

Reduciendo la expresión de la ecuación 2.43:

$$\frac{1}{2} e^{-i\vartheta_1} \left\{ (e^{-i\vartheta_L} - e^{-i\vartheta_R}) |1\rangle_4 |0\rangle_5 |v\rangle + ie^{-i\vartheta_2} (e^{-i\vartheta_L} + e^{-i\vartheta_R}) |0\rangle_4 |1\rangle_5 |v\rangle \right\} \quad (2.44)$$

Realizando un proceso similar podemos obtener el resultado para las entradas $|1\rangle_1 |0\rangle_0 |h\rangle$, $|0\rangle_1 |1\rangle_0 |v\rangle$ y $|0\rangle_1 |1\rangle_0 |h\rangle$ [10][11].

Capítulo 3

Criptografía cuántica

En este capítulo, se revisará lo que es la criptografía cuántica y se analizará uno de sus criptosistemas más famosos el BB84, para finalmente, examinar el desarrollo de criptografía cuántica con un solo fotón propuesto por A. Beige, et.al. [5] y el armado de preparación y medición propuesto por Y. Kim [6].

3.1. Criptografía

La criptografía comenzó al menos hace 2500 años debido a la necesidad de desarrollar técnicas de cifrado para codificar información, como un mensaje, y así proteger la información de receptores no deseados, es decir, consiste en ocultar información a través de claves, las cuales codifican la información y permiten que el mensaje no sea entendido si no se cuenta con la clave empleada en tal mensaje.
Para lograrlo , se utiliza un algoritmo para combinar un mensaje con información adicional, conocida como "clave", para producir un criptograma, siendo conocida esta técnica como "cifrado".

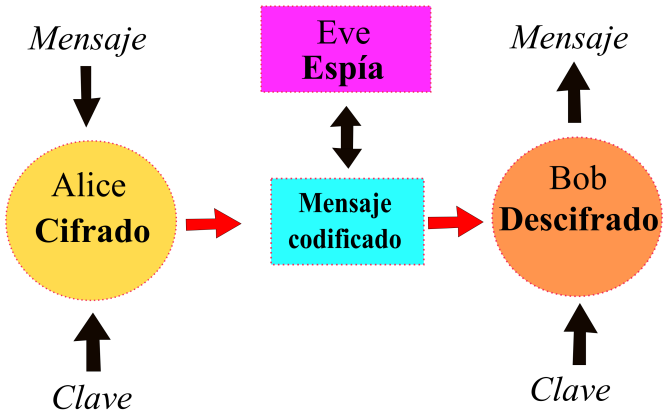

Figura 3.1: Esquema de criptografía [1]

La persona que encripta y envía el mensaje generalmente es conocida como Alice, el que lo recibe es llamado Bob y la persona que espía es nombrada Eve. Para garantizar la seguridad de un sistema criptográfico debe ser imposible desbloquear el criptograma sin la clave.

Los sistemas de cifrado se divide en dos clases: el secreto o simétrico y el público o asimétrico. Para el primer caso tenemos el ejemplo del sistema one-time pad, propuesto por Gilbert Vernam en 1935, en el cual se comparte una clave secreta siendo el único sistema criptográfico donde se da un secreto perfecto y probado. En este esquema, Alice cifra usando una clave generada aleatoriamente y luego simplemente agrega el bit correspondiente en la clave, el mensaje codificado se envía a Bob, quien lo descifra restando la misma clave. El problema con este sistema es que es indispensable que Alice y Bob compartan una clave secreta común, que debe ser al menos tan larga como el mensaje en sí (lo cual fue demostrado en la década de 1940 por Claude Shannon, pues si la clave es mas corta que el mensaje un espía suficientemente poderoso podría inferir cierta información del mensaje),la cual puede ser usada solo una vez y debe ser compartida por un medio extremadamente seguro, pues sino Eve podría empezar a formar una imagen de la clave[1][4].

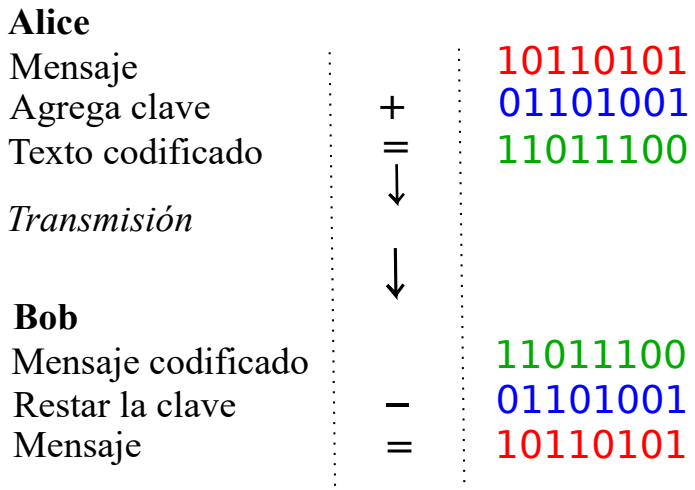

Figura 3.2: Esquema de one-time pad (las operaciones se realizan en módulo 2) [1]

Para el caso de los criptosistemas de cifrado público o de clave pública, los primeros fueron propuestos por Whitfield Diffie y Martin Hellman, en 1976, los cuales están basados en las funciones unidireccionales, donde es fácil calcular f(x) dada una variable x, pero es difícil es la dirección opuesta, esa dificultad es debida al tiempo ya que este incrementa para hacer una tarea con el número de bits de entrada. Factorizar números enteros grandes es un candado para este tipo de funciones.
Para la trsnmisión de un mensaje con un criptosistema de clave pública, Bob debe primero elegir una clave privada , la cual usa para calcular una clave pública, la cual divulga y Alice usa para cifrar su mensaje, para luego transmitirlo a Bob quien lo descifra con su clave privada.
Uno de estos sistemas criptográficos es el RSA, desarrollado por Ronald Rivest, Adi Shamir y Leonard Adleman en 1977, el cual basa su secreto en el hecho de que el tiempo para calcular factores primos de un número entero (clave privada) aumenta exponencialmente con el número de bits de entrada.
La criptografía tiene tres objetivos principales de seguridad: confidencialidad, integridad y autenticidad. Sin embargo, en la criptografía clásica uno de los principales problemas es el mantener el objetivo de la confidencialidad ya que las técnicas criptográficas actuales no permiten tal objetivo a largo plazo. Debido a este problema es donde entra la criptografía cuántica ya que esta a través de la distribución de claves cuánticas puede colaborar con la criptografía clásica para permitir tal confidencialidad a largo plazo.
Desde el punto de vista clásico, los canales privados pueden ser monitoreados de forma pasiva, por lo que el emisor o receptor no detectarían una posible escucha. Así entonces, la teoría de física clá-

sica, que permite medir las propiedades físicas sin alterarlas, deja abierta la posibilidad de escuchas pasivas[2].

3.2. Criptografía cuántica

Con el paso del tiempo, la criptografía ha buscado ir más allá con el fin de mejorar las técnicas de codificado fue entonces que dado el desarrollo de la mecánica cuántica se empezó a investigar una nueva rama: la Criptografía Cuántica (CC). La CC es vista como una unión entre la mecánica cuántica(MC) y la teoría de la información siendo considerada como una de las aplicaciones más prometedoras de la mecánica cuántica.
Todo surgió a través de las reglas "negativas" de la MC las cuales son: a)no se puede medir sin perturbar al sistema, b)no se puede determinar simultáneamente la posición y momento de una partícula, c)no se puede medir simultáneamente la polarización de un fotón, y, d)no se puede duplicar un estado cuántico desconocido; siendo precisamente estos puntos los que han permitido el desarrollo de la CC y la aplicación útil de la MC.
En 1970, Stephen J. Wiesner escribió un artículo titulado "Codificación conjugada" en donde hacía uso de la física cuántica para realizar dos tareas que no eran posibles con la física clásica, una consistía en crear billetes de banco imposibles de falsificar físicamente y el otro era un esquema para combinar dos mensajes clásicos en una única transmisión cuántica de la que el receptor podía extraer cualquiera de los mensajes, pero no ambos. Así, en 1979, Bennet y Brassard, basándose en las ideas de Wiesner, comenzaron a analizar cómo involucrar tales ideas con la criptografía de clave pública (CCP) dándose cuenta poco después que podían usarse como sustitutos de CCP. Tales esquemas criptográficos cuánticos, desarrollados en 1982 y 1984, no eran suficientemente prácticos pero las mejoras de estos en los años siguientes permitieron el desarrollo del prototipo de IBM Thomas J. Watson Research Center en 1989, donde John Smolin ayudó a la electrónica y óptica del aparato, y Francois Bessette y Louis Salvail asistieron en la escritura del software (para la creación del aparato de criptografía cuántica de IBM fue necesario modificar el protocolo BB84). Por los mismos tiempos, Artur K. Ekert, usando las ideas de David Deutsch, lo llevaron a idear un criptosistema ligeramente diferente basado en correlaciones cuánticas. A principios de 1991, John Rarity y Paul Tapster, usando las ideas de Massimo Palma, comenzaron a experimentar implementando el criptosistema de Ekert.
La criptografía cuántica se ha visto a prueba a través de diversos experimentos, entre ellos el de Paul Townsend en 1993, donde hace uso de la fase de los fotones en lugar de la polarización y de interferómetros de Mach-Zehnder[2].

3.2.1. Protocolo BB84

La criptografía cuántica dió un salto con la propuesta del protocolo BB84 creado por Bennett y Brassard en 1984, donde el emisor (Alice) y receptor (Bob) están conectados por dos canales: uno cuántico (el cual puede ser una fibra óptica) y uno público (una línea telefónica o incluso también una fibra óptica) por los cuales realizan su comunicación a través de fotones polarizados.
Para esto, el emisor Alice tiene la opción de 4 estados de polarización: horizontal (0^o), vertical (90^o) y en diagonal (45^o o 135^o), una vez polarizados aleatoriamente los fotones y registrando sus eleccciones, manda los fotones al receptor Bob, quien solo cuenta con dos analizadores que pueden distinguir: polarización vertical y horizontal y otro que distingue polarización diagonal.
Por consiguiente, el receptor Bob mide la polarización de los fotones con sus dos analizadores aleatoriamente y registra su elección y resultado.
Después de este proceso, el receptor Bob hace uso del canal público a través del cual publica la secuencia del analizador que usó para cada fotón (pero no publica su medición) lo que permite que el emisor Alice compare sus datos; dándole a conocer públicamente sus eleccciones correctas por lo que para los casos donde no coincidieron se descarta el bit.

Sin embargo, aún es necesario comprobar la privacidad de su comunicación, por esta razón el emisor Alice y receptor Bob comparten públicamente una sección de su clave y la comparan, si difieren en algunos casos es probable que hayan sido espiados [2][3].

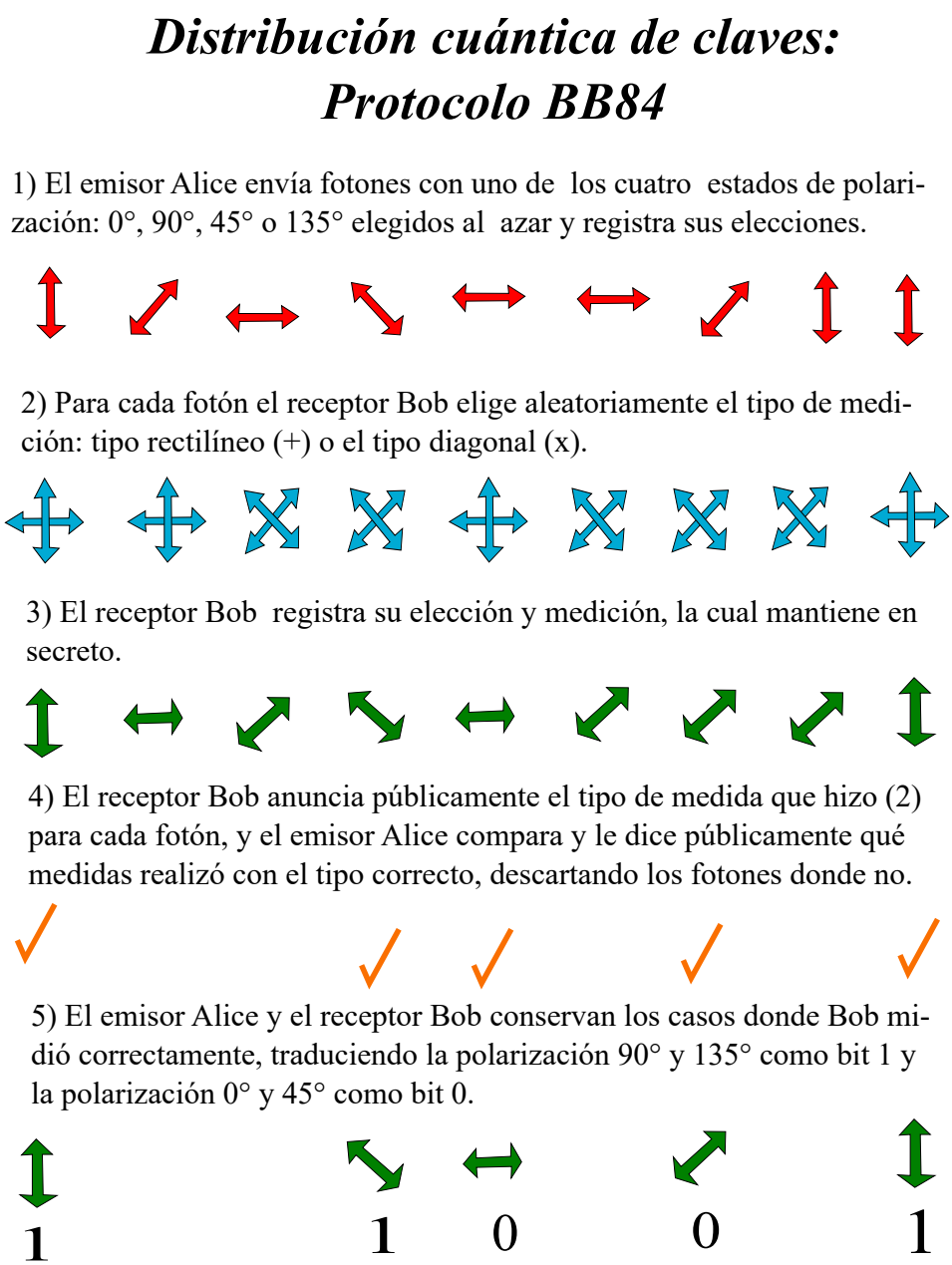

Figura 3.3: Distribución cuántica de claves: BB84 [2]

3.3. Criptografía cuántica: con un solo fotón

La mayoría de los esquemas de criptografía cuántica consisten en un par de qubit entrelazados sin embargo cualquier alternativa binaria cuántica puede servir como qubit, por lo que los diferentes grados de libertad de un objeto físico pueden representar varios qubits.
Para este esquema propuesto ambos qubits de un par entrelazado se realiza mediante un solo fotón, siendo la polarización del fotón un qubit y la alternativa espacial el otro.
Para este criptosistema el emisor Alice prepara cada fotón en estados de dos qubit, donde emplea la alternativa binaria espacial con los estados base $|1\rangle_1 |0\rangle_0$ y $|0\rangle_1 |1\rangle_0$ y los dos estados de polarización $|v\rangle$ y $|h\rangle$, para esto Alice hace uso de las compuertas unitarias de dos qubits para convertir los estados: $|1\rangle_1 |0\rangle_0 |v\rangle$, $|1\rangle_1 |0\rangle_0 |h\rangle$, $|0\rangle_1 |1\rangle_0 |v\rangle$ y $|0\rangle_1 |1\rangle_0 |h\rangle$ en cualquier superposición deseada del mismo, de manera que pueda enviar cada fotón en el estado de 2 qubits de solo un fotón de su elección.
Por otro lado, las medidas del receptor Bob de ciertos conjuntos de cuatro estados de dos qubits mutuamente ortogonales se logran mediante compuertas unitarias apropiadas, los cuales transforman los estados de la base de medición en cuestión en los cuatro estados básicos.

3.3.1. Distribución cuántica de clave

Para este esquema criptográfico Alice tiene dos pares de estado ortogonales (el par $|1+\rangle$ y $|2+\rangle$, y el par $|1-\rangle$ y $|2-\rangle$). Alice quiere enviar un bit "+" o "-", así entonces, Alice envía a Bob un fotón preparado en uno de los cuatro estados $|i\pm\rangle$ donde $(i = 1, 2)$. Para un bit + elige aleatoriamente entre $|1+\rangle$ y $|2+\rangle$ mientras que para un bit - elige entre $|1-\rangle$ y $|2-\rangle$.
Cuando el fotón llega a Bob, él elige al azar entre dos bases diferentes de dos qubits (base $|B_j\rangle$ y base $|B'_j\rangle$) para su ánalisis del estado del fotón (esto se logra experimentalmente enviando al fotón entrante por un divisor de haz y redirigiéndolo a diferentes dispositivos de medición). Bob mide los estados base $|B_1\rangle, ..., |B_4\rangle$ o $|B'_1\rangle, ..., |B'_4\rangle$, dependiendo de su resultado de medición, es posible que pueda deducir el bit entrante.

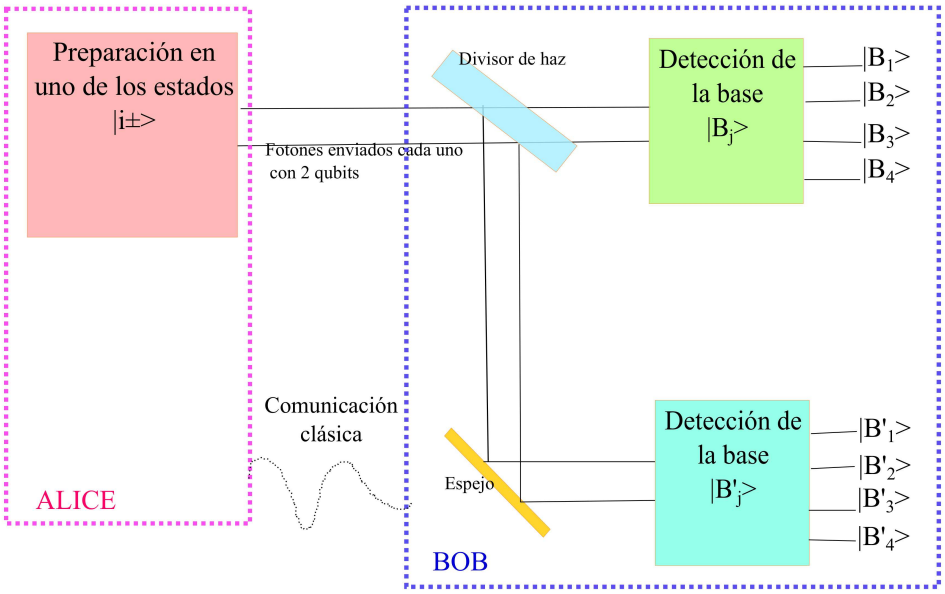

Figura 3.4: Esquema del criptosistema de distribución de clave cuántica con un sólo fotón

Para esto, debe distinguir los estados + de los estados - sin ambigüedades, lo cual es posible si para todos los pares de estado ($|i+\rangle$, $|i-\rangle$) cada medición posible solo puede ser causada por $|i+\rangle$ o $|i-\rangle$ pero no por ambos; este debe ser el caso de todas las bases medidas por Bob. Luego puede inferir el bit transmitido tan pronto Alice identifica el tipo de par utilizado (cuando le dice el valor de la etiqueta i). Cabe señalar, que es importante que los pares de estado $|1\pm\rangle$ y $|2\pm\rangle$ enviados por Alice no sean idénticos ni ortognales.

Consideramos el caso donde los estados enviados por Alice y los detectados por Bob son:

$$(|1+\rangle, |1-\rangle, |2+\rangle, |2-\rangle) = (|1\rangle_1 |0\rangle_0 |s\rangle, |0\rangle_1 |1\rangle_0 |a\rangle, |Sv\rangle, |Ah\rangle) \tag{3.1}$$

$$(|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle) = (|1\rangle_1 |0\rangle_0 |v\rangle, |1\rangle_1 |0\rangle_0 |h\rangle, |0\rangle_1 |1\rangle_0 |v\rangle, |0\rangle_1 |1\rangle_0 |h\rangle) \tag{3.2}$$

$$(|B'_1\rangle, |B'_2\rangle, |B'_3\rangle, |B'_4\rangle) = (|Ss\rangle, |As\rangle, |Sa\rangle, |Aa\rangle) \tag{3.3}$$

donde:

$$\left.\begin{matrix} |S\rangle \\ |A\rangle \end{matrix}\right\} = \quad \frac{1}{\sqrt{2}}(|1\rangle_1 |0\rangle_0 \pm |0\rangle_1 |1\rangle_0)$$

$$\left.\begin{matrix} |s\rangle \\ |a\rangle \end{matrix}\right\} = \quad \frac{1}{\sqrt{2}}(|v\rangle \pm |h\rangle)$$

Se puede observar que cada uno de los estados de Bob es ortogonal al estado + o al estado - de cada par.
Supongamos que Bob detecta el estado $|B_2\rangle = |1\rangle_1 |0\rangle_0 |h\rangle$, el cual es ortogonal a $|1-\rangle = |0\rangle_1 |1\rangle_0 |a\rangle$ y a $|2+\rangle = |Sv\rangle$, por lo tanto si se envio un + significa que se envió un tipo 1 y un - si se envió un tipo 2, este ánalisis se ve ejemplificado en la siguiente tabla:

Fotones enviados por Alice	Estados detectados por Bob			
	B_1 o B'_1	B_2 o B'_2	B_3 o B'_3	B_4 o B'_4
Tipo 1	+	+	-	-
Tipo 2	+	-	+	-

Tabla 3.1: Detección entre + o - según la medición de Bob

Por lo tanto, si Alice le dijera a Bob que para ese fotón envió un fotón de tipo 1 entonces sabrá Bob que Alice envió el estado $|1+\rangle = |1\rangle_1 |0\rangle_0 |s\rangle$.Es importante observar que en este criptosistema no se pierde ningún fotón por lo que cada fotón enviado te proporiciona un bit para la clave[5].

Distribución cuántica de claves para qubits de un solo fotón

1) El emisor Alice envía fotones con uno de los cuatro estados $|i\pm\rangle$ donde i=1,2, donde los pares de estado $|1\pm\rangle$ y $|2\pm\rangle$ no sean ortogonales ni idénticos.

|1+> |2-> |2-> |2+> |1-> |1->

2) Para cada fotón el receptor Bob elige aleatoriamente entre dos bases diferentes de dos qubits $|B_j\rangle=(|B_1\rangle,|B_2\rangle , |B_3\rangle, | B_4\rangle)$ o $|B'_j\rangle=|(B'_1\rangle,|B'_2\rangle,|B'_3\rangle,|B'_4\rangle)$, donde cada uno de los estados es ortogonal al estado + o al estado - de cada par.

	Bases de Bob			
Estados $\|i\pm\rangle$	B_1 o B'_1	B_2 o B'_2	B_3 o B'_3	B_4 o B'_4
|1+>			O	O
|2+>		O		O
|1->	O	O		
|2->	O		O	

3) El receptor Bob obtiene su medición y revisa con cuáles de los cuatro estados $|i\pm\rangle$ es ortogonal, y obtiene el signo + o - para cada tipo (1 o 2)..

B_1 B_2 B_2 B_3 B_4 B_4

Fotones enviados por Alice	Estados detectados por Bob			
	B_1 o B'_1	B_2 o B'_2	B_3 o B'_3	B_4 o B'_4
Tipo 1	+	+	−	−
Tipo 2	+	−	+	−

4) El emisor Alice hace público el tipo que envió 1 o 2 para cada fotón..

1 2 2 2 1 1

5) El receptor Bob puede estonces concluir qué estado envió el emisor Alice ,ya que conoce el signo para cada tipo.

|1+> |2-> |2-> |2+> |1-> |1->

6) Para comprobar la privacidad ,Alice y Bob comparten públicamente una sección aleatoria de la clave (aproximadamente el 10%) y la comparan, si difieren es probable que hayan sido espiados por lo que descartan la clave y vuelven a empezar, sino forman una clave con los bits restantes no publicados.

Figura 3.5: Distribución de clave cuántica con un sólo fotón

En las secciones siguientes se presentará un esquema experimental de preparación y uno de medición, basándose en el propuesto por Y. Kim [6]

3.3.2. Esquema experimental de preparación y medición

Esquema de preparación

Para este sistema de preparación de los estados, primero se tiene un cristal BBO de tipo II de 2 mm de espesor al cual se le incide un haz o láser, tal cristal nos generará fotones que se dirigen en una misma dirección y con polarización horizontal y vertical. Posteriormente, se encuentra un espejo dicroico el cual frena el láser y solo deja pasar los fotones. Así entonces, los fotones se encuentran con el primer divisor de haz polarizador (PBS) en el cual se transmite el fotón polarizado horizontalmente y se refleja el polarizado verticalmente, el cual llega a un detector T quien nos avisa que va un solo fotón polarizado horizontalmente por el otro camino.
Por consiguiente, llega a una placa de media onda (HWP) la cual será orientada a cierto ángulo que permitirá ir formando distintos estados. Para luego pasar por el divisor de haz polarizador que dará como resultado un estado en superposición y dependiendo de lo antes preparado y del estado que se desea se ajustan las placas de media onda giratorias de polarización θ_a y θ_b y los desfasadores ϕ_c y ϕ_b para obtener los estados deseados.

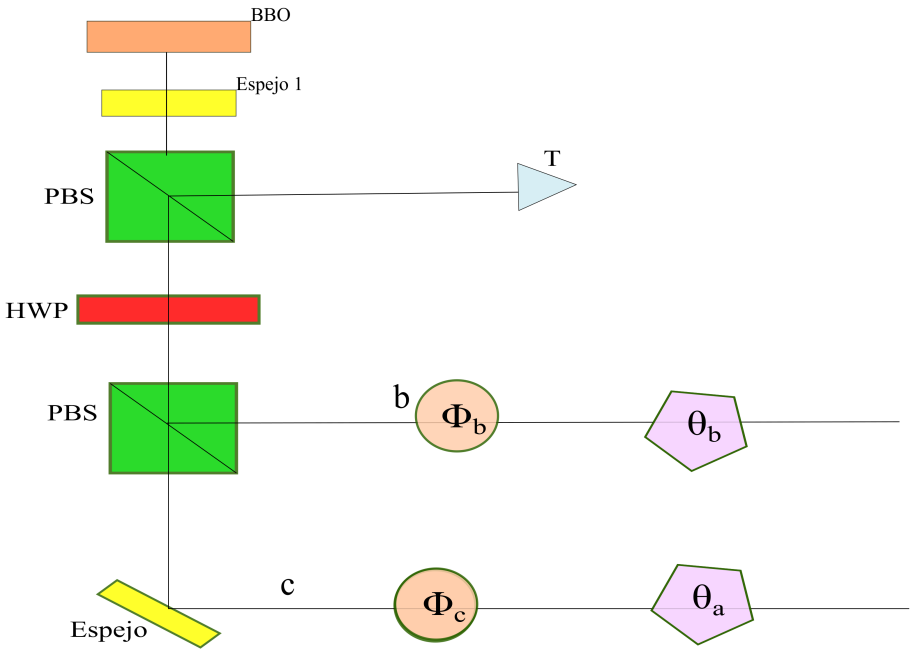

Figura 3.6: Esquema de la configuración experimental para la preparación de los estados[6]

Para este caso deseamos preparar los estados siguientes:

$$(|1+\rangle, |1-\rangle, |2+\rangle, |2-\rangle) = (|1\rangle_1 |0\rangle_0 |s\rangle, |0\rangle_1 |1\rangle_0 |a\rangle, |Sv\rangle, |Ah\rangle) \tag{3.4}$$

donde:

$$\left.\begin{matrix} |S\rangle \\ |A\rangle \end{matrix}\right\} = \frac{1}{\sqrt{2}}(|1\rangle_1 |0\rangle_0 \pm |0\rangle_1 |1\rangle_0) \tag{3.5}$$

$$\left.\begin{matrix}|s\rangle \\ |a\rangle\end{matrix}\right\} = \quad \frac{1}{\sqrt{2}}(|v\rangle \pm |h\rangle) \tag{3.6}$$

Si nombramos a $c = |1\rangle_1 |0\rangle_0$ y $b = |0\rangle_1 |1\rangle_0$, los estados de la ecuación 3.4 y de la ecuación 3.5, son:

$$(|1+\rangle, |1-\rangle, |2+\rangle, |2-\rangle) = (|cs\rangle, |ba\rangle, |Sv\rangle, |Ah\rangle) \tag{3.7}$$

$$\left.\begin{matrix}|S\rangle \\ |A\rangle\end{matrix}\right\} = \quad \frac{1}{\sqrt{2}}(|c\rangle \pm |b\rangle) \tag{3.8}$$

Por lo tanto, podemos ver que los ángulos a los que debe estar la placa de media onda (HWP), las placas de media onda giratorias de polarización θ_a y θ_b, y de los desfasadores ϕ_c y ϕ_b, son:

Estado	HWP	θ_a	θ_b	ϕ_b	ϕ_c
$\|cs\rangle$	0°	22,5°	0°	0°	0°
$\|ba\rangle$	45°	0°	−67,5°	0°	0°
$\|Sv\rangle$	22,5°	45°	0°	0°	0°
$\|Ah\rangle$	22,5°	0°	45°	π	o°

Tabla 3.2: Ángulos de la configuración del esquema de preparación

Analizando una de las construcciones anteriores tenemos que, si queremos formar el estado $|Sv\rangle = \frac{|cv\rangle+|bv\rangle}{\sqrt{2}}$ la placa de media onda a 22,5°nos formará el estado:

$$\frac{|ch\rangle + |bv\rangle}{\sqrt{2}} \tag{3.9}$$

Así entonces, el estado que va por el camino c lleva una polarización horizontal y como queremos que sea vertical la placa de media onda θ_a la debemos poner a 45° para pasar a una polarización vertical y así obtenemos el estado deseado.
Con un análisis similar podemos deducir los demás estados.

Esquema de medición

Para el esquema de medición,primero detallaremos la construcción de medición para la base $|B'_j\rangle$, la cual es:

$$(|B'_1\rangle, |B'_2\rangle, |B'_3\rangle, |B'_4\rangle) = (|Ss\rangle, |As\rangle, |Sa\rangle, |Aa\rangle) \tag{3.10}$$

Para este esquema, se introducen placas de media onda en cada puerto de entrada del divisor de haz polarizador (como se ve en el esquema de la figura 3.7), la placa de media onda en la ruta c debe estar orientada a 22,5° y la placa de media onda de la ruta b debe estar orientada a 67,5°, posteriormente mezclamos los modos de qubit espaciales, etiquetados como c y b en un divisor de haz polarizador y luego pasa el estado por uno de los divisores de haz polarizadores orientados a 45° (PBS45°) que están ubicados en los modos c' y b', los cuales separan los estados en cuatro modos espaciales distintos. Los cuatro detectores colocados en los puertos de salida de PBS45°, producen una señal inequívoca que corresponde al estado del fotón de entrada.

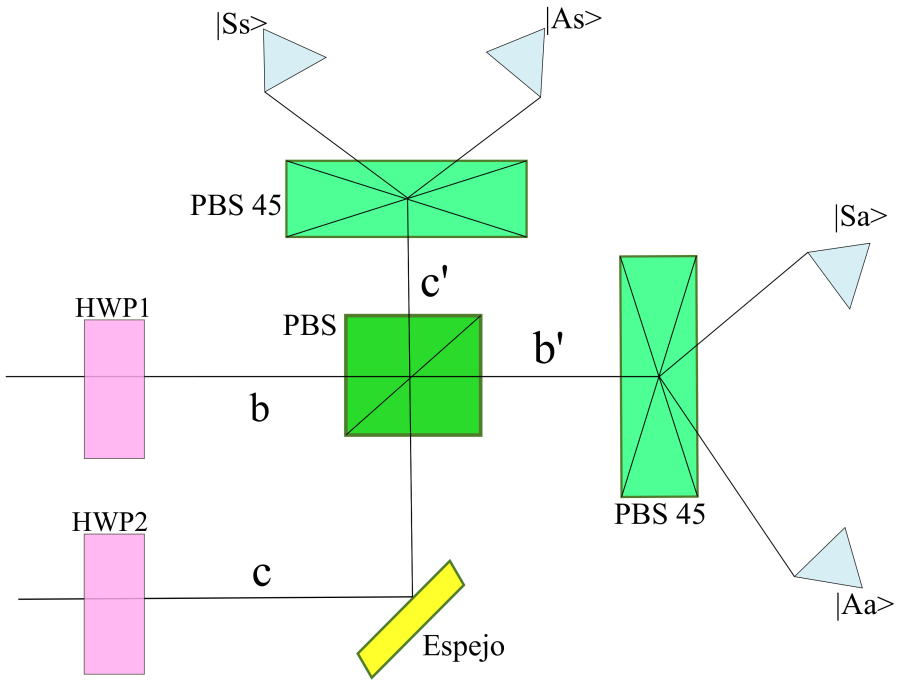

Figura 3.7: Esquema de la configuración experimental para la medición de los estados[6]

Así entonces, analizando el caso en el que se envía el estado $|1+\rangle = |cs\rangle = \frac{1}{\sqrt{2}}|c\rangle(|v\rangle + |h\rangle)$, este estado viene por el camino c, que al pasar por la placa de 22,5°, el estado se convierte en:

$$|ch\rangle \tag{3.11}$$

Por lo que, al llegar al divisor de haz el estado se va por el camino c', por lo que mediriamos en los estados B_1' o B_2' que es lo esperado; ya que si vemos la tabla 3.1 podemos ver que si mido el estado B_1' son ortogonales a el $|1-\rangle$ y $|2-\rangle$ por lo que si es del tipo 1 entonces es + y si es del tipo 2 es del signo +,por lo tanto puedo decir que el estado enviado por Alice pudó ser $|1+\rangle$ o $|2+\rangle$,así que cuando Alice informe que envió de tipo 1, confirmaría que se envió el estado $|1+\rangle$, de forma similar es si mido B_2' pues sus ortogonales son $|1-\rangle$ y $|2+\rangle$. De manera análoga podemos analizar para las demás mediciones.

El siguiente esquema nos muestra el esquema completo de preparación y medición, el cual nos muestra la estructura que nos indica el esquema 3.4.
Por ejemplo, si Alice envió el estado antes mencionado $|1+\rangle = |cs\rangle$, si lo medimos en la base B_j podríamos medir los estados B_1 o B_2 , que si verificamos en la tabla 3.1 podemos ver que si medimos B_1 y Alice nos dice que envió un tipo 1, entonces tendríamos el estado correcto.
Como podemos ver el divisor de haz realiza la acción de enviar los estados recibidos a dos bases distintas, de las cuales Bob eligirá al azar en cual medir.
Como se puede apreciar, en este criptosistema de criptografía cuántica no perdemos ningún fotón como en el criptosistema BB84 por lo que cada fotón enviado proporcionará un bit clave a lo que se le conoce como determinista [5] [6].

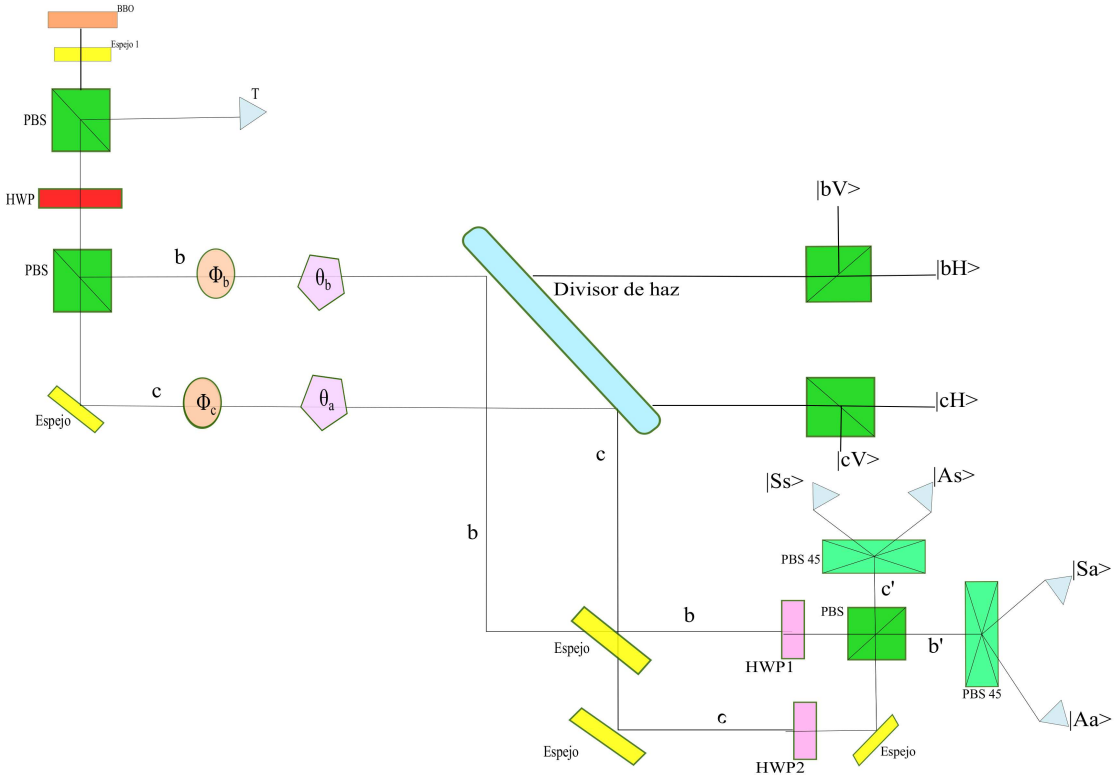

Figura 3.8: Esquema de la configuración experimental para la preparación y medición

Conclusión

En este trabajo se revisó y analizó un nuevo sistema de criptografía cuántica basado en el entrelazamiento con un solo fotón,en el cual se emplea que los sistemas individuales también presentan enredamiento cuántico entre sus diversos grados de libertad por lo que cualquier alternativa binaria cuántica puede servir como qubit, por consecuencia nos permitió mostrar que se puede usar este fenómeno para establecer un sistema en criptografía cuántica.
Igualmente, se pudó apreciar la diferencia del protocolo de distribución de claves de qubits de un solo fotón con el protocolo BB84, en el cual algunas mediciones realizadas por el receptor Bob no coinciden con la preparación de estados que realiza Alice, lo que lleva a que haya fotones perdidos ya que no forman parte de la clave, a diferencia del criptosistema con qubits de un solo fotón en el cual todos los fotones enviados proporcionan información para la clave, lo cual es llamado de acuerdo a los autores un sistema de criptografía cuántica "determinista".
Para el entendimiento y descripción general del criptosistema con un solo fotón fue importante revisar el funcionamiento del divisor de haz cuántico, así como el concepto de compuerta lógico cuántica.
Por otro lado, se reescribió tal criptosistema y el desarrollo de la compuerta unitaria para estados de dos qubits de un solo fotón en la nomenclatura que se ha establecido para etiquetar los estados que se generan cuando un fotón atraviesa un divisor de haz; lo que permite un entendimiento general si se conoce la nomenclatura antes mencionada.

Bibliografía

[1] Tittel, W. , Ribordy, G., and Gisin, N., *Quantum cryptography.* Physics world, 11(3), 41-45 (1998).

[2] Bennett,C. H., Brassard, G. and Ekert, A. K. , *Quantum cryptography.* Scientific American, 267(4), 50-57 (1992).

[3] Acín, A. y Navascués, M. , *Criptografía cuántica.* Revista Española de Física, 21(2), 5-9 (2008).

[4] Gisin,N., Ribordy,G., Tittel,W., and Zbinden,H., *Quantum cryptography.* Reviews of modern physics, 74(1), 145-195 (2002).

[5] Beige,A., Englert, B.G. , Kurtsiefer,C. and Weinfurter, H., *Secure communication with single-photon two-qubit states.* Journal of Physics A: Mathematical and General, 35(28), L407 (2002).

[6] Kim,Y. H. , *Single-photon two-qubit entangled states: Preparation and measurement.* Physical Review A, 67(4), 040301(2003).

[7] Bergou, J. A., and Hillery, M. (2013). *Introduction to the theory of quantum information processing.* Springer Science & Business Media.

[8] McMahon, D. (2007). *Quantum computing explained.* John Wiley & Sons.

[9] Nielsen, M. A., and Chuang, I. (2002). *Quantum computation and quantum information..* Cambridge University Press.

[10] Gerry, C., Knight, P. (2005). *Introductory quantum optics.* Cambridge university press.

[11] Englert, B. G., Kurtsiefer, C., & Weinfurter, H. *Universal unitary gate for single-photon two-qubit states.* Physical Review A, 63(3), 032303 (2001).

[12] Greenberger, D., Hentschel, K., & Weinert, F. (Eds.). *Compendium of quantum physics: concepts, experiments, history and philosophy.* Springer Science & Business Media.(2009)