Sistema de comunicación óptica basado en la modulación de coherencia y el momento angular orbital de la luz

Paula Andrea López Higuera

Informe final del trabajo de investigación para optar por el título de
Magister en Ingeniería de Telecomunicaciones

Director
Ernesto Aguilera Bermúdez
Ph.D. en Ingeniería

Codirector
Yezid Torres Moreno
Dr. Óptica y procesamiento de la señal

Universidad Industrial de Santander

Facultad de Ingenierías Fisicomecánicas

Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones

Maestría en Ingeniería de Telecomunicaciones

Bucaramanga

2019

Agradecimientos

Agradezco a Dios por haber sido mi guía a lo largo de este nuevo logro en mi carrera profesional, a mis directores por su tiempo, apoyo y dedicación a la realización del presente trabajo de investigación, a mis compañeros de la escuela y del grupo de investigación de óptica y tratamiento de señales por todos sus consejos y compañía, a mis padres Rosario del pilar Higuera Acacio y Carlos Julio López Sanabria por ser junto con mi hermano Juan Carlos mi más grande apoyo y motivación y a mi amore Anderson Atuesta por su apoyo incondicional.

Tabla de contenido

Pág.

Lista de Tablas

Pág.

Lista de Figuras

Pág.

Lista de Apéndices

Pág.

Resumen

TITULO: SISTEMA DE COMUNICACIÓN ÓPTICA BASADO EN LA MODULACIÓN DE COHERENCIA Y EL MOMENTO ANGULAR ORBITAL DE LA LUZ [*]

AUTOR: PAULA ANDREA LÓPEZ HIGUERA[**]

PALABRAS CLAVE: SISTEMA COMUNICACIÓN, SISTEMA DISTRIBUCIÓN CLAVE CUÁNTICA, MODULACIÓN DE COHERENCIA, MOMENTO ANGULAR ORBITAL, CODIFICACIÓN, SEGURIDAD, CONTEO DE FOTONES.

DESCRIPCIÓN:
Las redes ópticas con capacidades del orden de los terabits por segundo permiten brindar múltiples servicios a los usuarios, por lo cual se han convertido en la columna vertebral de los sistemas de telecomunicaciones modernos y deben garantizar y preservar la confidencialidad, disponibilidad e integridad de los datos, es decir, la seguridad, ya que soportan un gran flujo de información, en su mayoría de carácter personal y privado. En lo referente a la confidencialidad se ha encontrado que gran parte de los esquemas convencionales de cifrado pueden ser bastante vulnerables ante los avances en computación cuántica, en consecuencia se da la aparición de nuevos métodos y esquemas basados en las potencialidades del mundo cuántico.

Con base al nuevo enfoque en la seguridad de los sistemas, este trabajo de investigación considera la descripción de un sistema de distribución de clave cuántica basado en la codificación en dos bases mutuamente imparciales utilizando la coherencia temporal de una fuente de luz, introduciendo un retardo óptico τ_n mayor que el tiempo de coherencia de la fuente, entre los trenes de ondas emitidos y los modos de momento angular orbital descritos por el término de fase $e^{il\varphi}$, de modo que se logra una mayor capacidad de bits por fotón frente a esquemas convencionales y se obtiene una mayor resistencia contra los ataques por interceptación de canal por parte del sistema como se evidencia en los resultados obtenidos en simulación mediante el método de Montecarlo. Adicionalmente, se presentan los resultados experimentales asociados a algunos de los principales componentes del sistema de comunicación propuesto como punto de partida para una futura implementación.

---

[*] Trabajo de maestría.

[**] Facultad de ingeniería Físico-Mecánicas. Escuela de Eléctrica, Electrónica y de Telecomunicaciones. Maestría en Ingeniería de Telecomunicaciones. Director: Ernesto Aguilera Bermúdez, Ph.D. en Ingeniería. Co-director: Yezid Torres Moreno, Dr. Óptica y procesamiento de señal.

Abstract

TITLE: OPTICAL COMMUNICATION BASED ON COHERENCE MODULATION AND ORBITAL ANGULAR MOMENTUM OF LIGHT[*]

AUTHOR: PAULA ANDREA LÓPEZ HIGUERA[**]

KEYWORDS: COMMUNICATION SYSTEM, QUANTUM KEY DISTRIBUTION, COHERENCE MODULATION, ORBITAL ANGULAR MOMENTUM, ENCODING, SECURITY, PHOTON COUNTING.

DESCRIPTION:
Optical networks with terabits per second capabilities allow to provide multiple services to users, which have become the backbone of modern telecommunication systems and must ensure and preserve the confidentiality, availability and integrity of data, i.e., security, since they support a large flow of information, mostly of a personal and private nature. Regarding confidentiality, it has been found that a large part of conventional encryption schemes can be quite vulnerable to advances in quantum computing, as a result of which new methods and schemes based on the potentialities of the quantum world appear.

Taking account the new focus on systems security, this research considers the description of a quantum key distribution system based on encoding on two mutually unbiased basis using the temporal coherence of a light source, introducing an optical delay τ_n greater than their coherence time, between the wave trains emitted and the orbital angular momentum modes described by the phase term $e^{il\varphi}$, so that a higher bit capacity per photon is achieved in front of to conventional schemes and, greater resistance against attacks by channel interception is obtained as evidenced by simulation results obtained using the Monte Carlo method. Additionally, the experimental results associated with some of the main components of the communication system proposed as a starting point for a future implementation are presented.

---

[*] Master thesis.

[**] Facultad de ingeniería Físico-Mecánicas. Escuela de Eléctrica, Electrónica y de Telecomunicaciones. Maestría en ingeniería de Telecomunicaciones. Advisor: Ernesto Aguilera Bermúdez, Ph.D. in engineering. Co-advisor: Yezid Torres Moreno, Dr. Optics and signal processing.

Introducción

La evolución de las tecnologías de la información y las comunicaciones y la visión del internet de las cosas han ocasionado en los últimos tiempos un drástico aumento en el flujo de información a través de las redes de comunicación, generando la necesidad de contar con sistemas de mayor ancho de banda y mayor tasa de transmisión, como por ejemplo las redes ópticas las cuales se han destacado frente a las redes convencionales de cobre, convirtiéndose en el futuro de las telecomunicaciones (Saleh & Simmons, 2012). Sin embargo, al igual que las demás tecnologías de red, estas son objeto de varios tipos de infracciones o ataques a la seguridad, como por ejemplo el acceso no autorizado a los datos transportados (Furdek, Skorin-Kapov, Zsigmond, & Wosinska, 2014; Rejeb, Leeson, & Green, 2006), lo cual ha motivado la presente investigación, hacia el desarrollo de sistemas de comunicación seguros.

De forma convencional la seguridad en los sistemas de comunicación depende de supuestos matemáticos no probados y la complejidad computacional de los algoritmos de cifrado. Sin embargo se ha encontrado que son vulnerables ante el progreso tecnológico (Schneier, 1996; Sergienko, 2006), por esta razón surge un nuevo enfoque para el cifrado de datos basado en la mecánica cuántica (Raymer, 2017), la cual nos permite a partir de un partícula como el fotón trabajar con sistemas probabilísticos, que dadas sus propiedades impide la escucha a escondidas sobre un canal de comunicación por parte de un espía sin que este perturbe el sistema y sea probablemente detectado (Gisin, Ribordy, Tittel, & Zbinden, 2002; Phoenix & Townsend, 1995; Sergienko, 2006). La seguridad de esta clase de sistemas de distribución de clave cuántica

generalmente depende de fuentes de fotones individuales para su correcto funcionamiento, sin embargo, se analiza la posibilidad de utilizar un sistema de comunicación a nivel de conteo de fotones basado en la propuesta de W. Rhodes et al. donde un esquema de comunicación basado en la modulación de coherencia en un interferómetro que opera al nivel de conteo de fotones, puede evitar mediante las leyes de la física que un tercero acceda a una fracción del texto cifrado y por ende no pueda descifrar el mensaje (Boughanmi, 2017; Rhodes, Boughanmi, & Torres Moreno, 2016).

Como una extensión a esta nueva metodología de seguridad y con la idea de contar con sistemas completamente seguros y más eficientes, se considera utilizar esquemas de codificación de información alternos a los basados en polarización, dado que esta propiedad limita a un bit la cantidad de información transportada por cada fotón. En el presente trabajo de investigación se obtiene una idea teóricamente fundamentada y prácticamente relevante que permite abordar parte de los desafíos de asegurar las redes, a partir de un sistema de comunicación basado en la modulación de coherencia y una propiedad espacial que ha sido recientemente de gran interés como el momento angular orbital (MAO) (Andrews & Babiker, 2013; Allen, Beijersbergen & Woerdman, 1992; Padgett, 2014; Padgett, Courtial, & Allen, 2004; Yao & Padgett, 2011), logrando mejoras en la seguridad del sistema y la eficiencia del fotón, además de permitir contar con sistemas de seguridad en la capa física del sistema en conjunción con sistemas de seguridad en la capa de datos ya existentes, para asegurar la red.

El documento se estructura de la siguiente manera: En el primer capítulo se establece y recopila la terminología, el estado actual y el marco en el que se desarrollan conceptos como interferómetro de Mach-Zehnder, modulación de coherencia, momento angular orbital, sistemas de distribución de clave cuántica y el método de Monte Carlo, necesarios para la interpretación y

comprensión de la investigación que se aborda. En el segundo capítulo se presenta una explicación del funcionamiento de un sistema de comunicación basado en la modulación de coherencia cuando opera al nivel de conteo de fotones y su correspondiente análisis de ataques a la seguridad mediante un modelado estocástico a partir de una herramienta de simulación como el método de Monte Carlo. En el tercer capítulo se presenta la descripción y explicación del sistema de comunicación basado en la modulación de coherencia y el momento angular orbital, su correspondiente análisis de ataques a la seguridad mediante simulación y un análisis de la candencia del sistema, con base en este sistema se presenta en el cuarto capítulo una descripción y caracterización de algunos de los dispositivos, componentes y tecnología disponible en el laboratorio de óptica de la Escuela de Física de la Universidad Industrial de Santander para la futura implementación y finalmente se presenta la producción académica y las conclusiones derivadas de esta investigación.

1 Marco conceptual y estado del arte

Este trabajo de investigación es el resultado del trabajo colaborativo entre la Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones y la Escuela de Física, bajo el grupo de investigación RadioGIS y el grupo de investigación de Óptica y Tratamiento de señales (GOTS) respectivamente, razón por la cual es pertinente establecer una misma terminología, conocer el estado actual y el marco en el que se desarrollan dichos conceptos, realizando un análisis y

revisión bibliográfica, que permiten recopilar en este capítulo los conceptos e ideas principales que se utilizan para analizar el problema de investigación que se aborda.

1.1 Interferómetro de Mach-Zehnder

Un interferómetro es un dispositivo óptico que utiliza el fenómeno de superposición de dos o más ondas de luz para formar un patrón de interferencia sobre una pantalla y realizar mediciones de precisión del orden de la longitud de onda de la luz o aún mucho más pequeñas. Para obtener patrones de interferencia se deben cumplir ciertas condiciones en la coherencia espacial, coherencia temporal y la polarización de los haces, por ejemplo, una fuente puede producir franjas siempre que la diferencia de camino óptico (OPD por sus siglas en inglés Optical Path Difference) entre los dos haces sea menor que la longitud de coherencia (Goodwin & Wyant, 2000).

Existe una gran variedad de tipos de interferómetros, en particular este documento se centra en el conocido interferómetro de Mach– Zehnder, el cual fue desarrollado en 1892 por los físicos Ludwig Mach y Ludwig Zehnder y es el dispositivo base en algunos sistemas basados en modulación de coherencia (Rhodes et al., 2016; Wacogne & Jackson, 1996b). Como se observa en la **Figura 1**, consiste en una lámina divisora de haz (BS1) que divide el haz de entrada en dos haces, los cuales por medio de un par de espejos (M1 y M2) son redirigidos hacia una segunda lámina divisora de haz (BS2) donde se recombinan. Las trayectorias separadas de los haces (l_1 y l_2) en cada uno de los brazos superior e inferior respectivamente del interferómetro pueden ser ajustadas para ser iguales o diferentes. Dependiendo de la fase relativa adquirida por el haz a lo

largo de las dos trayectorias en los dos puertos de salida de la lámina divisora BS2 se presentara interferencia constructiva, destructiva o ninguna de las dos (Zetie, Adams, & Tocknell, 2000).

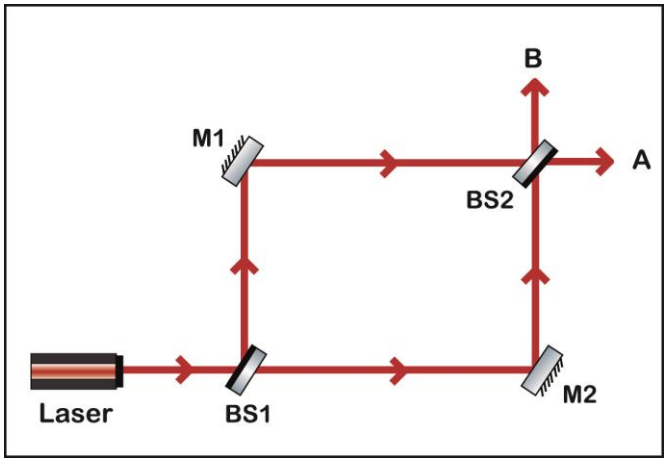

Figura 1. *Esquema de un interferómetro de Mach- Zehnder.*

Para comprender su funcionamiento es necesario tener en cuenta los cambios de fase por reflexión que se presentan, ya que de acuerdo a la física una onda que se transmite no adquiere ningún cambio de fase, mientras que una onda reflejada adquiere un desfase igual a π, sin embargo este último solo se da para el caso cuando el haz se refleja en un medio con índice de refracción menor a uno mayor. Generalmente una lámina divisora es vidrio con un recubrimiento dieléctrico en la superficie frontal, dado que el dieléctrico tiene un valor intermedio de índice de refracción entre el del vidrio y el del aire, el haz no presentará un desfase al incidir por la parte de atrás de la lámina (Zetie et al., 2000).

En la **Figura 1**, de acuerdo al posicionamiento de la segunda lámina y la diferencia de camino óptico en el puerto de salida A en la Ecuación 1 y en el puerto de salida B en la Ecuación 2, se encuentra que existe una interferencia constructiva en el camino hacia el puerto A y destructiva en el camino hacia el puerto B, donde λ es la longitud de onda de la fuente (Zetie et al., 2000).

$$OPD_A = 2\pi\left(\frac{l_1 - l_2}{\lambda}\right) \quad (1)$$

$$OPD_B = \pi + 2\pi\left(\frac{l_1 - l_2}{\lambda}\right) \quad (2)$$

1.2 Modulación de coherencia

La coherencia temporal considera la correlación en la fase entre puntos temporalmente distintos del campo de radiación de una fuente a lo largo de su propagación. Comúnmente se habla de haces incoherentes cuando las relaciones de fase son aleatorias y de haces coherentes cuando la relación de fase es constante y bien conocida. Debido a que en la realidad no existen fuentes de luz perfectamente monocromáticas, las fuentes se pueden caracterizar por un tren de onda promedio con tiempo de vida τ_c, denominado tiempo de coherencia, el cual está directamente relacionado con el ancho de banda de la fuente $\Delta w = 2\pi/\tau_c$. Para producir patrones de franjas de interferencia observables se requiere que los haces interferentes sean coherentes (Pedrotti & Pedrotti, 1993).

La modulación de coherencia es una técnica que se basa en las propiedades de coherencia temporal de las fuentes de luz y consiste en introducir un retraso de tiempo óptico variable entre los grupos de onda emitidos por una fuente con un tiempo de coherencia τ_c, con el objetivo de controlar la interferencia entre los paquetes de onda (Goedgebuer, Porte, & Mollier, 1993; Gutiérrez Martinez, Porte, & Goedgebuer, 1995; Rhodes et al., 2016). En la **Figura 2**, se presenta un esquema general de un sistema de modulación de coherencia donde se hace incidir un haz de luz de una fuente policromática con un tiempo de coherencia más corto que la diferencia de camino óptico de un interferómetro de Mach-Zehnder (codificador), generándose dos paquetes de onda $S(t)$ y $S(t-\tau)$ a la salida (τ es el retraso de tiempo dado por el

interferómetro) que se propagan hacia un segundo interferómetro de Mach-Zehnder (decodificador) con la misma diferencia de camino óptico del codificador, donde cada uno produce dos nuevos paquetes y la interferencia de estos paquetes solo ocurrirá si han sido propagados sobre la misma distancia, es decir, camino 1-4 igual a camino 2-3. Los datos son transmitidos modulando la diferencia de camino óptico del codificador, por medio de un modulador de fase controlado por la señal a transmitir, debido a que la diferencia de camino de los interferómetros siempre es mayor al tiempo de coherencia de la fuente, durante la transmisión no ocurrirá interferencia y solo a la salida del decodificador se obtendrá la señal original, siendo un esquema seguro en la transmisión (Wacogne & Jackson, 1996b).

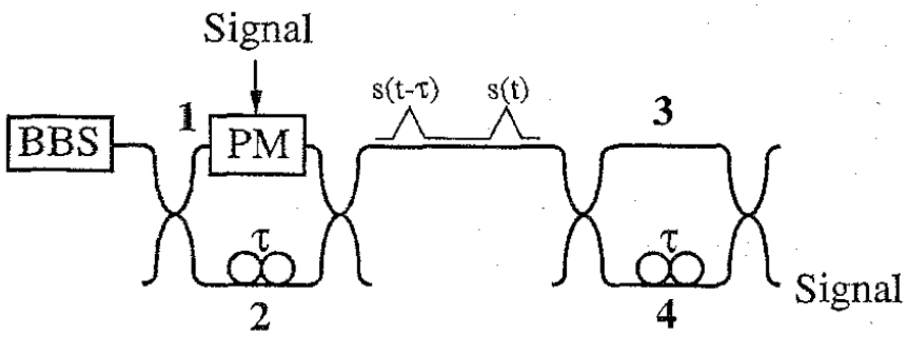

Figura 2. *Esquema clásico de modulación de coherencia, Nota. Tomada de (B. Wacogne & Jackson, 1996b).*

Sin embargo en 1996 Wacogne y Jackson encontraron un método para detectar la señal codificada por modulación de coherencia sin un interferómetro como decodificador, por medio de un análisis espectral y filtrado de longitud de onda (Wacogne & Jackson, 1996b). Para superar dicha vulnerabilidad se han propuesto nuevos arreglos de modulación de coherencia como: primero un esquema en el que la codificación de la información se basa en cambios de fase relativos entre los intervalos de tiempo consecutivos de la luz emitida desde una fuente altamente coherente, logrando una mejora en la seguridad debido a la potencia óptica constante en el enlace

de transmisión y por utilizar una fuente de baja coherencia para enviar datos falsos por el enlace de transmisión (Wacogne, Jackson, Fisher, Podoleanu, & Jackson, 1996); segundo, un esquema en el que la diferencia de camino óptico del codificador y decodificador se modula no sólo con la señal a transmitir, sino también con una señal clave, logrando corromper el espectro acanalado para cualquier intruso (Wacogne & Jackson, 1996a); tercero, un esquema mejorando al anterior donde se hace uso de una clave de cifrado compuesta por una parte de gran amplitud - baja frecuencia y una parte de baja amplitud - alta frecuencia, ya que esto permite que se corrompan tanto el espectro como la señal captada por el intruso (Wacogne et al., 1998) y por último un esquema donde la modulación de coherencia se especifica por clave y al operar en el régimen de conteo de fotones con una fuente de banda ancha, puede proporcionar un nivel cuantificablemente elevado de seguridad física garantizada para la transmisión de señales binarias (Rhodes et al., 2016).

1.3 Momento angular orbital

El momento angular orbital de la luz (MAO) es una propiedad física que se caracteriza por un frente de onda helicoidal en la dirección de propagación, el interés en las características y el comportamiento de haces con esta propiedad ha aumentado desde 1992 cuando L. Allen et al. en la aproximación paraxial relacionaron los modos Laguerre-Gauss con haces con MAO bien definido (Allen, Beijersbergen & Woerdman, 1992).

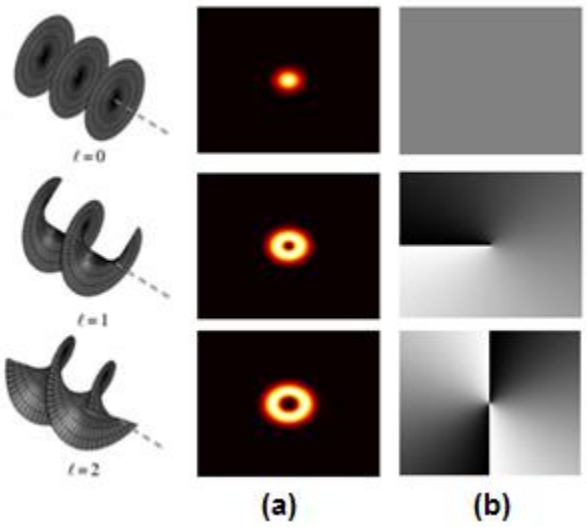

Figura 3. *Representación del MAO para diferentes valores de carga topológica a) Intensidad y b) fase.*

Los haces con MAO están descritos por un término de fase acimutal $e^{il\varphi}$ y poseen un MAO de $l\hbar$ por fotón (donde l es la carga topológica, φ es el ángulo acimutal, y $\hbar$ es la constante de Plank dividida por 2π) donde para valores enteros de l el frente de onda sufre una rotación de $2\pi l$ respecto a su eje de propagación, formándose una discontinuidad en la fase y una sección transversal de intensidad anular como se observa en la **Figura 3**, que se le denomina vórtice óptico de carga topológica entera l (Andrews & Babiker, 2013; Allen, Beijersbergen & Woerdman, 1992; Padgett, 2014; Padgett et al., 2004; Yao & Padgett, 2011), estos vórtices ópticos son modos de la luz que son comúnmente asociados a campos con MAO, como por ejemplo los haces Laguerre-Gauss (Allen, Beijersbergen & Woerdman, 1992) y los haces Bessel-Gauss (Schulze, Dudley, Brüning, Duparré, & Forbes, 2014).

Para estimar la calidad de una red de comunicación óptica dos de los índices más relevantes son la capacidad de transmisión de información y la seguridad. Con el fin de mejorar la capacidad de transmisión de un único canal de comunicación, se utiliza la multiplexación de los diferentes grados de libertad de la luz, como la multiplexación de tiempo, la multiplexación de

longitud de onda y la multiplexación de polarización (Salamon et al., 2003). Adicionalmente, como l es un parámetro de los haces con MAO que puede tomar cualquier valor entero, se reconoce como un nuevo grado de libertad para la creación de múltiples estados, característica que ha sido de gran interés en el ámbito de las comunicaciones ópticas, dando paso a estudios como: el de Gibson et al. quienes presentaron en 2004 un sistema de comunicación óptica utilizando MAO para crear ocho estados espaciales distintos dentro de un único haz óptico, siendo resistente a la escucha debido a una incertidumbre inherente en la medición (Gibson et al., 2004), en 2010 se propusieron unos esquemas de modulación de MAO basados en códigos de comprobación de paridad de baja densidad capaces de operar sobre el régimen de turbulencia atmosférica fuerte y lograr una transmisión óptica de 100 Gb/s (Djordjevic & Arabaci, 2010), en 2011 un esquema óptico para codificar y decodificar 2 bits de información en diferentes estados de MAO de un haz óptico paraxial (Slussarenko, Karimi, Piccirillo, Marrucci, & Santamato, 2011), para el 2012 se continuó con el enfoque de aumentar la capacidad de información en los sistemas de comunicación, llegando a la multiplexación/demultiplexación de haces MAO portadores de información para la transmisión de datos en el orden de los Terabits (Wang, 2016; Wang et al., 2012), para el caso de comunicaciones por fibra también se han reportado estudios como el uso de MAO dentro de fibras multimodo especialmente diseñadas (Bozinovic et al., 2013). Más recientemente se han estudiado los problemas de seguridad de los enlaces de comunicación por espacio libre para lograr una comunicación segura entre dos pares mediante la multiplexación por MAO (Sun & Djordjevic, 2016).

1.4 Sistema distribución de clave cuántica

Una técnica generalmente utilizada para las comunicaciones seguras es la criptografía, la cual consiste en ocultar la información transmitida para que el contenido del mensaje no pueda ser leído por una persona no autorizada. Para lograr este objetivo se basa en el proceso de encriptación o cifrado presentado en la **Figura 4**, el cual inicia con Alice (transmisor) quien cifra el mensaje o texto claro m mediante un algoritmo criptográfico (criptosistema) especifico el cual se encarga de transformar junto con una información adicional denominada clave k, el texto plano en texto cifrado c (criptograma), el cual posteriormente es enviado a Bob (receptor) quien emplea el algoritmo inverso junto con una clave d para descifrar y recuperar el mensaje m (Gisin et al., 2002; Phoenix & Townsend, 1995). A su vez durante la transmisión se encuentra Eve (intruso) quien escucha a escondidas y trata a partir del texto cifrado romper el algoritmo para determinar el mensaje de texto claro. De acuerdo a lo anterior, la idea es que sin la clave debe ser imposible recuperar el mensaje original desde el texto cifrado, por lo tanto la seguridad radica en dos factores principales: la fiabilidad del algoritmo y el secreto de la clave (Phoenix & Townsend, 1995).

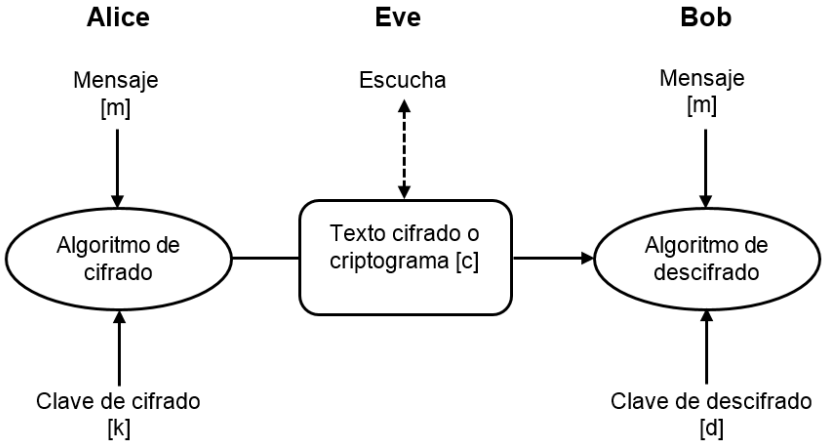

Figura 4. *Elementos básicos de un algoritmo de cifrado o criptosistema.*

Según la clave de cifrado y descifrado a utilizar existen dos tipos de criptosistemas, los sistemas asimétricos que consisten en el uso de una clave diferente para el cifrado y descifrado $(k \neq d)$ y los sistemas simétricos que consisten en el uso de una misma clave para el cifrado y descifrado $(k = d)$. La seguridad de este tipo de sistemas radica en supuestos no comprobados sobre la fortaleza de problemas matemáticos y la complejidad computacional, en consecuencia este tipo de sistemas pueden ser vulnerables a avances teóricos o prácticos, como por ejemplo la computación cuántica (Shor, 1994). No obstante, teóricamente un sistema de este tipo totalmente seguro es el "one time pad" propuesto en 1926 por Gilbert Vernam, que consiste en utilizar la clave para un solo cifrado y descifrado, donde la clave debe ser al menos tan larga como el mensaje de texto plano a transmitir (Gisin et al., 2002; Lo, Curty, & Tamaki, 2014; Phoenix & Townsend, 1995).

En vista de lo anterior la criptografía clásica aunque es ampliamente utilizada para la seguridad de los sistemas, presenta diversas vulnerabilidades, lo cual dio origen al estudio de la criptografía cuántica, la cual se basa en las leyes inalterables de la mecánica cuántica, principalmente en el principio de incertidumbre de Heisenberg (establece que no es posible medir el estado cuántico de ningún sistema sin perturbarlo) y en el teorema de no clonación (prohíbe la creación de copias idénticas de un estado cuántico desconocido) (Gisin et al., 2002; Phoenix & Townsend, 1995; Sergienko, 2006).

La criptografía cuántica en conjunción con la criptografía clásica permitiría obtener criptosistemas donde su seguridad resida únicamente en el secreto de la clave. Para este objetivo un paso importante es la distribución de la clave, ya que en el caso clásico se hace por medio de mensajeros de confianza, sin embargo estos pueden ser comprometidos sin que los usuarios lo

perciban, por esta razón aparece la criptografía cuántica, que utiliza fotones para formar la clave (Gisin et al., 2002; Lo et al., 2014; Phoenix & Townsend, 1995).

El primer protocolo para el intercambio o distribución de clave cuántica (QKD por sus siglas en inglés Quantum key Distribution) se propuso en 1984 por Charles H. Bennett de IBM y Gilles Brassard de la Universidad de Montreal; se denominó BB84. Este protocolo permite establecer una secuencia aleatoria de bits idéntica y secreta entre dos personas en lugares remotos (Bennett & Brassard, 1984). En la **Figura 5** se observa un ejemplo de realización del protocolo para la transmisión de una secuencia de 8 bits, en general el proceso para compartir la clave consta de los siguientes pasos:

1. Alice tiene una secuencia de bits para enviar y elige aleatoriamente una base de polarización para codificar cada uno de los bits como una secuencia de fotones en estados cuánticos de la base seleccionada de acuerdo con el esquema de codificación que se presenta en la **Tabla 1**, posteriormente envía a Bob a través del canal cuántico la secuencia de fotones preparados en los diferentes estados de polarización. Cabe resaltar que las bases empleadas son un parte fundamental para el protocolo dado que cumplen con la propiedad de ser conjugadas o mutuamente imparciales, lo cual permite que si un sistema es preparado en un estado específico de una base se comporte de forma totalmente aleatoria y pierda toda su información almacenada cuando se someta a una medición correspondiente a la otra base (Bennett & Brassard, 1984).

Tabla 1.
Esquema codificación de bits.

Bases	Bit 0	Bit 1
Rectilínea		
			
Diagonal		
		

2. Bob selecciona de forma independiente y al azar una de las dos bases para medir cada fotón entrante, almacena la elección de base y el bit detectado para cada caso. Si Bob mide de la misma manera que Alice codifica, puede determinar perfectamente el estado y si Bob mide de manera incorrecta, obtiene un valor aleatorio para el estado. Debido a las pérdidas en sus detectores y en el canal de transmisión, es posible que algunos de los fotones no se reciban en absoluto, lo que da como resultado espacios en blanco en sus tablas. Hasta este punto Bob cuenta con una secuencia de bits denominada Raw key (clave en bruto) (Bennett & Brassard, 1984; Phoenix & Townsend, 1995).

3. Alice y Bob intercambian la secuencia de bases utilizada entre ellos a través del canal público autenticado, el bit resultante del envío y medición con la misma base se mantiene intacto mientras que el bit resultante de diferentes bases y los espacios de tiempo donde Bob no recibió un fotón se descartan, logrando conformar secuencia de bits denominada Sifted key (clave tamizada) (Bennett & Brassard, 1984; Phoenix & Townsend, 1995).

4. Debido a errores causados por imperfecciones técnicas, o posiblemente por la intervención de Eve, esta clave puede presentar errores, por esta razón se utiliza un subconjunto adecuado de datos seleccionados al azar para estimar la tasa de error de bits cuánticos. Si la tasa de error se encuentra por debajo de un cierto valor umbral, Alice y Bob pueden continuar usando los datos

restantes para establecer una clave secreta mediante algoritmos clásicos para la corrección de errores y la amplificación de la privacidad. De lo contrario, decidirán que los datos no son seguros y comenzarán una nueva transmisión de datos (Phoenix & Townsend, 1995).

Alice Secuencia de bits	0	1	0	1	-	1	0	1
Alice secuencia de bases	⤫	⤫	+	+		⤫	⤫	+
Alice estados	↗	↖	→	↑		↖	↗	↑
Bob Secuencia bases	+	⤫		+	⤫	⤫	⤫	⤫
Bob estados medidos	↑	↖		↑	↗	↖	↗	↖
Clave tamizada o sifted key	-	1	-	1	-	1	0	-

Figura 5. *Ejemplo de una transmisión de 8 bits mediante el protocolo BB84.*

El aspecto principal en la seguridad de este protocolo es la selección aleatoria de las bases, ya que significa que cualquier espía, y de hecho el mismo Bob, deben adivinar la base correcta para recibir una clave. Eve en principio está forzada a realizar una medición o perturbar el sistema para poder obtener información, con una probabilidad a su vez de ser detectada (Phoenix & Townsend, 1995).

Desde la aparición del protocolo BB84 se han propuesto extensiones y variaciones de este, así como nuevos esquemas con el fin de mejorar la seguridad, la eficiencia o la implementación (Lo et al., 2014). A partir del uso de diferentes grados de libertad para la codificación de información en pulsos de luz, se han desarrollado esquemas como por ejemplo, el protocolo de cambio de fase diferencial (DPS por sus siglas en inglés Differential Phase Shift) en donde Alice envía un tren de pulsos y modula en cada pulso la fase de forma aleatoria por 0 y π, de tal forma que la

información es codificada entre la diferencia de fase de pulsos adyacentes, lo cual es medido por Bob con la ayuda de un interferómetro (Inoue, Waks, & Yamamoto, 2003; Inoue, Waks, & Yamamoto, 2002). Bechmann-Pasquinucci et al. propusieron a partir de una configuración interferométrica un esquema de QKD basado en cuatro estados y dos bases, encontrando ventajas significativas respecto a la cantidad de transferencia de información y baja tasa de errores introducidos por ataques de tipo de interceptación y reenvió en comparación con el protocolo BB84 (Bechmann-Pasquinucci & Tittel, 2000), lo cual motivó la generalización de los anteriores resultados para la codificación en N dimensiones usando M bases abriendo la posibilidad a nuevos sistemas multidimensionales (Bourennane, Karlsson, & Björk, 2001).

En 2012 se presenta un protocolo de distribución de clave de alta dimensión, con mayor tolerancia a errores y una mayor tasa de bits para la creación de la clave a partir de la codificación de polarización, fase y tiempo en un fotón (Buttler, Lamoreaux, & Torgerson, 2012). En 2014 proponen una extensión del protocolo BB84 para transmitir dos bits en un solo fotón a partir de la codificación en la polarización y los modos transversales de la luz (Luda, Larotonda, Paz, & Schmiegelow, 2014).

Djordjevic propone la codificación a partir del momento angular de un fotón teniendo en cuenta que se compone de dos partes principales el momento angular de spin asociado a la polarización y el momento angular orbital (MAO) asociado a la fase acimutal del campo electromagnético complejo, logrando aumentar la tasa de bits que se pueden transmitir en el sistema (Djordjevic, 2013), un año después se presenta un esquema experimental de comunicación en el espacio libre a una distancia de 210 metros donde se utliza un tipo de combinación particular del MAO y la polarización, de tal forma que se logra la independencia de marcos de referencia en la comunicación entre transmisor y receptor, ya que generan estados

invariantes por rotación (Vallone et al., 2014) y más recientemente en el campus de la universidad de Ottawa realizaron un sistema QKD considerando la turbulencia del medio y codificando sobre estos mismos dos grados de libertad (Sit et al., 2017).

En 2016 Bacco et al. presentaron el protocolo denominado corrimiento diferencial fase-tiempo (DPTS por sus siglas en inglés Differential Phase Time Shifting) el cual emplea el tiempo y la fase para codificar información en un alfabeto cuaternario (Bacco et al., 2016), en ese mismo año se presenta un método para la distribución de clave a partir del envío de dos señales, donde se establece la clave mediante la codificación entre el estado de polarización o fase de la primera señal y el tiempo de retardo entre las dos señales, logrando un aumento en la longitud de la clave compartida entre dos entidades (Ali, 2016).

En el dominio espacial se ha demostrado la codificación de información a través del perfil transversal de luz discretizado a partir de ranuras, donde se generan estados cuánticos de 16 dimensiones que aumentan la capacidad de información del sistema (Etcheverry et al., 2013) y para el 2015 Mirhosseini et al. utilizan la distribución espacial de fase del campo electromagnético, al demostrar experimentalmente un sistema QKD de siete dimensiones utilizando modos MAO y la correspondiente base conjugada de la posición angular acimutal (ANG), logrando la codificación de más de un bit de información en un fotón (Mirhosseini et al., 2015).

1.5 El método de Monte Carlo

El método de Monte Carlo es un tipo de simulación numérica que combina el uso de números aleatorios y el cálculo de probabilidades mediante inferencia estadística para la resolución de

problemas en áreas como la ingeniería, las ciencias físicas, la estadística, las finanzas, la informática, entre otras. Fue utilizado por primera vez durante la segunda guerra mundial por científicos que trabajaban en la bomba atómica y su nombre fue sugerido por el físico Nicholas Metropolis en 1949 por la ciudad turística de Mónaco famosa por sus casinos, debido a la similitud del tipo de simulación con los juegos de azar (Metropolis, 1987; Metropolis & Ulam, 1949).

La simulación de Monte Carlo se usa a menudo cuando el modelo de un sistema es complejo, no lineal o implica más que un par de parámetros inciertos, ya que es una técnica que se basa en el muestreo aleatorio repetitivo y el análisis estadístico para calcular resultados en aplicaciones como por ejemplo integración numérica, optimización y la simulación de sistemas físicos, químicos y biológicos (Cahill, 2013). Por lo general como se observa en la **Figura 6** este método consta de cuatro pasos principales (Harrison, 2010):

- Generación del modelo: Se desarrolla un modelo computarizado que represente el sistema a analizar, aplicando relaciones matemáticas que usan los valores de las variables de entrada y las transforman en la salida deseada.
- Generación de variables aleatorias: Consiste en generar un conjunto de n variables aleatorias distribuidas uniformemente entre 0 y 1, cuyos valores serán transformados en los valores de las variables aleatorias que siguen las distribuciones estadísticas identificadas para cada uno de los n parámetros de entrada del sistema a analizar.
- Experimentación numérica: Se toma un conjunto de variables aleatorias resultantes del paso anterior como entradas del modelo computarizado previamente generado el cual producirá un conjunto de valores de salida. El procedimiento anterior se ejecuta N veces con el fin de recolectar diferentes escenarios de resultado.

- Análisis de resultados: Se realiza un análisis estadístico de los experimentos (resultados del modelo), a partir de medidas comunes como el valor medio, la varianza, la distribución de los valores de salida y el valor de salida mínimo o máximo. Finalmente se extraen conclusiones sobre los resultados del modelo en función de los experimentos estadísticos.

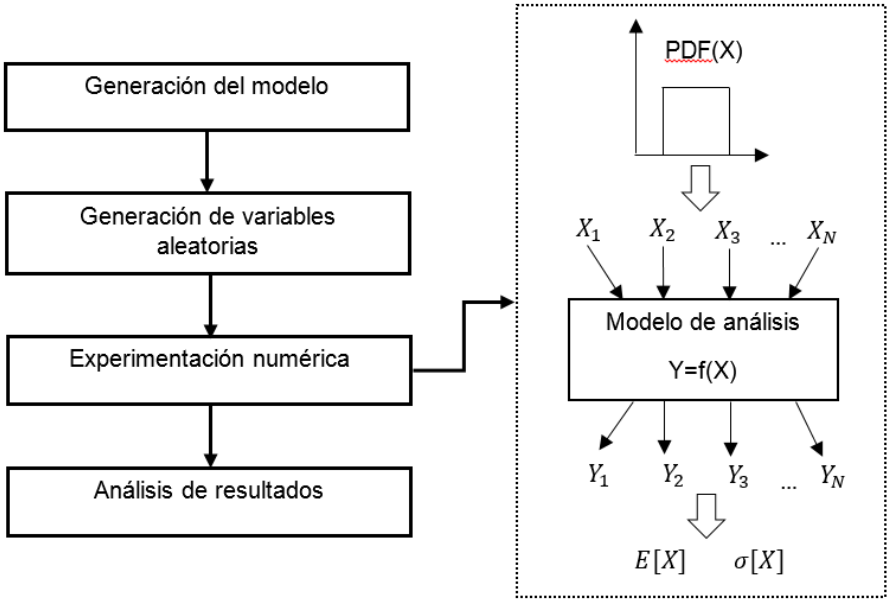

Figura 6. *Metodología de la simulación de Monte Carlo.*

Dado que el procedimiento de simulación se repite varias veces y se toma el promedio de los resultados como la solución, la precisión en dicha solución dependerá del número de simulaciones o experimentos N a realizar, ya que a medida que el número de simulaciones se acerca al infinito la solución de la simulación convergerá a la verdadera probabilidad que está bajo estimación (Teorema central del límite). Por lo tanto es necesario llegar a un equilibrio entre el esfuerzo computacional (cantidad de simulaciones) y la precisión de la solución.

Generalmente el nivel de precisión se mide por el intervalo de confianza, es decir, un intervalo de confianza más pequeño indica una estimación del valor más robusta y viceversa. Igualmente al ser un método estocástico presenta errores estadísticos resultado de las variaciones

aleatorias en el sistema de una medición a otra. Basado en el teorema del límite central y la ley de los grandes números se encuentra el error en la estimación y un intervalo de confianza en la Ecuación 3 y Ecuación 4 respectivamente (Lapeyre, 2007).

$$|\epsilon_n| = z_{\alpha/2}\frac{\sigma}{\sqrt{N}} \tag{3}$$

$$\left[\bar{X}_N - z_{\alpha/2}\frac{\sigma}{\sqrt{N}}, \bar{X}_N + z_{\alpha/2}\frac{\sigma}{\sqrt{N}}\right] \tag{4}$$

$$\bar{X}_N = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

Donde $z_{\alpha/2}$ es el error en valor critico de una distribución normal para un nivel de confianza $1-\alpha$ = 95% o 99% siendo 1,96 y 2,576 respectivamente, σ la desviación estándar, N la cantidad de experimentos y $\bar{X}_N$ el valor medio de los experimentos dado por la Ecuación 5. Mediante este intervalo de confianza se enuncia que con una probabilidad cercana a $1-\alpha$, el valor real de la probabilidad estimada pertenece a dicho intervalo.

2 Sistema de comunicación basado en la modulación de coherencia

Una comunicación es segura o confidencial cuando el mensaje transmitido solo puede ser decodificado e interpretado por la entidad a quien va dirigido, para esto desde 1949, cuando Shannon desarrolló una métrica para la teoría de la información para sistemas secretos (Shannon,

1949), la seguridad en las comunicaciones comúnmente se ha logrado a través de una técnica como la criptografía, donde un mensaje es cifrado por medio de una clave para ocultarlo de un intruso, quien escucha a escondidas en la transmisión, sin embargo como una variante a esta forma de seguridad aparece en 2016, un sistema de comunicación basado en la modulación de coherencia que cuando opera al nivel de conteo de fotones, puede evitar por medio de procesos físicos que un tercero acceda a una fracción del texto cifrado y por ende no pueda descifrarlo (Boughanmi, 2017; Rhodes et al., 2016), el cual es la base del esquema obtenido en el presente trabajo de investigación, por esta razón enseguida se proporciona una explicación del funcionamiento del sistema y un análisis de ataques a la seguridad del mismo a partir de una herramienta de simulación como el método de Monte Carlo.

2.1 Esquema y funcionamiento del sistema de comunicación

El sistema de comunicación propuesto en (Rhodes et al., 2016) se muestra en la **Figura 7**, donde se observa un interferómetro de Mach-Zehnder, en el cual un primer divisor de haz parte el haz de entrada de una fuente de luz en dos haces. Cada brazo del interferómetro está controlado por una de las entidades que busca confidencialidad para comunicar la información, en este caso Alice el brazo superior y Bob el brazo inferior.

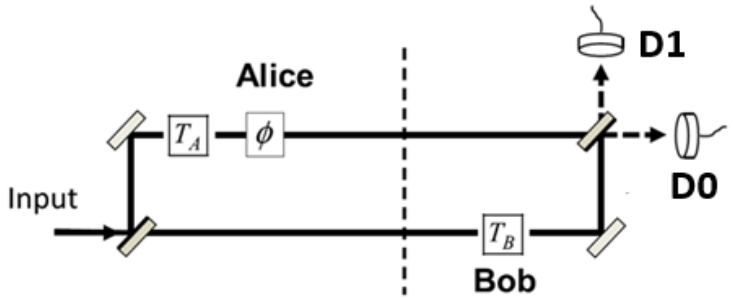

Figura 7. *Esquema básico de un sistema de comunicación basado en modulación de coherencia.*

En el brazo superior controlado por Alice se encuentra un modulador de fase acromático (funciona para todas las longitudes de onda) denotado por ϕ, el cual permite variar la fase del haz entre dos posibles valores 0 y π radianes. Con la variación de fase se logra codificar el valor de bit a transmitir de acuerdo a como se muestra en la **Tabla 2**.

Tabla 2.
Codificación por variación de fase.

Fase ϕ	**Valor de bit**
0	1
π	0

Para la seguridad del sistema se añade en cada brazo del interferómetro un retraso de tiempo configurable τ_A controlado por Alice y τ_B controlado por Bob, por medio de los cuales en el sistema se realiza una modulación de coherencia especificada por clave, ya que solo si la diferencia entre los retrasos de tiempo $|\tau_A - \tau_B|$ es igual a cero se logra que los dos haces interfieran y se recombinen en un segundo divisor de haz dando como resultado una interferencia constructiva en uno de sus puertos de salida, permitiendo determinar el valor del bit transmitido. Por el contrario si $|\tau_A - \tau_B|$ es mucho mayor al tiempo de coherencia τ_c de la fuente, los dos haces son mutuamente incoherentes y no interfieren, por ende generan salida por ambos puertos del segundo divisor de haz, quedando ambiguo para el receptor el valor del bit transmitido. Por lo tanto, la clave de transmisión consiste en una secuencia aleatoria de un subconjunto de M retrasos de tiempo que satisfacen la condición $|\tau_i - \tau_j| \gg \tau_c$, cuando $i \neq j$.

En general para la transmisión del mensaje mediante el sistema basado en la modulación de coherencia, primero, Alice y Bob acuerdan una secuencia de retrasos de tiempo entre un subconjunto de M posibles tiempos, que son la clave secreta, segundo, Alice posee una secuencia de bits a transmitir, la cual codifica mediante el modulador de fase ϕ y la envía a Bob ajustando su retraso de tiempo de acuerdo a la clave establecida previamente y finalmente Bob en sincronización con Alice ajusta su retraso de tiempo de acuerdo a la clave establecida, posiciona un detector D0 y D1 en el puerto de salida horizontal y vertical del segundo divisor de haz respectivamente. Si D0 hace click el valor del bit es 1 y si D1 hace click el valor del bit es 0.

En la **Tabla 3**, se presenta un ejemplo de la transmisión entre Alice y Bob de un mensaje de 5 bits y con M=3 posibles retrasos de tiempo para la clave.

Tabla 3.
Ejemplo de transmisión de una secuencia de 5 bits con M=3 posibles retrasos de tiempo en un sistema de comunicación basado en modulación de coherencia.

Secuencia de bits de Alice	1	0	1	1	0
Clave secreta	τ_1	τ_3	τ_2	τ_1	τ_2
Secuencia de bits codificada por Alice	0	π	0	0	π
Detector que hace click	D0	D1	D0	D0	D1
Secuencia de bits decodificada por Bob	1	0	1	1	0

La seguridad en el sistema depende de mantener secreta la secuencia de retrasos de tiempo (clave), pero también del funcionamiento del sistema al nivel de conteo de fotones, ya que se demuestra que si el sistema es interceptado por una tercera persona que desconoce la clave de transmisión, su detección será una sucesión aleatoria de unos y ceros, que no presentan relación con el mensaje cifrado (Rhodes et al., 2016).

2.2 Modelo estocástico y simulación de Monte Carlo

Como se observa en la **Figura 8**, cuando el sistema de comunicación es operado con un número elevado de fotones (luz clásica), Eve desvía una parte o la totalidad de la intensidad de luz transmitida por Alice I_{tot} y la divide en M cantidades iguales que funcionan como entrada a un conjunto de M interferómetros en paralelo cada uno configurado con uno de los posibles retrasos de tiempo utilizados por Alice y Bob. En (M-1) interferómetros se obtiene luz en cantidades iguales en ambos puertos de salida, debido a que la diferencia de retrasos de tiempo es mayor al tiempo de coherencia de la fuente, sin embargo en el interferómetro donde el retraso de tiempo de Eve coincide con el utilizado por Alice T_A, toda la luz sale por solo uno de los puertos de salida según la codificación por variación de fase empleada. Por lo cual, Eve puede determinar con facilidad el retraso de tiempo utilizado por Alice, junto con el valor de bit asociado (Rhodes et al., 2016).

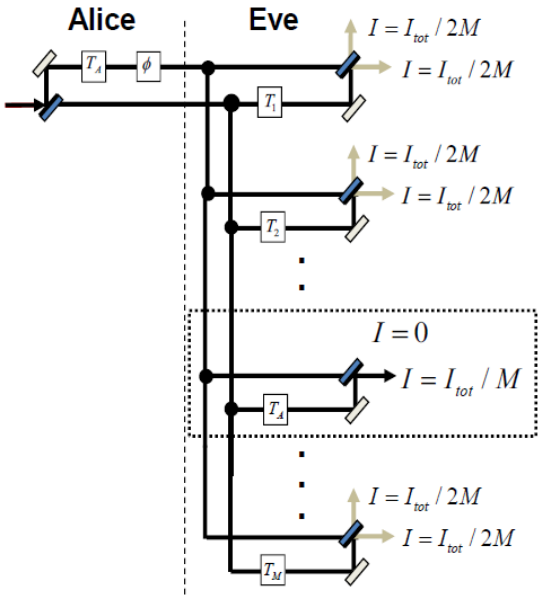

Figura 8. *Esquema del ataque por interceptación del canal al sistema de comunicación operado*

con un número elevado de fotones, Nota. Tomada de (Rhodes et al., 2016).

En la medida en que el sistema de comunicación por clave secreta opera al nivel de conteo de fotones, se encuentra que un intruso (Eve) utilizando toda la tecnología a su alcance con dispositivos ideales puede aplicar un ataque por interceptación en el canal, pero dado que desconoce la clave desde su punto de vista la detección de fotones será un proceso aleatorio, lo cual permite considerar un modelo estocástico para el sistema bajo este tipo de ataque.

El modelo estocástico se define de acuerdo a las siguientes consideraciones (Rhodes et al., 2016):

- La detección de fotones en los puertos de salida de un interferómetro son gobernados por procesos aleatorios de Poisson (Fox, 2006).
- La detección de fotones son procesos independientes de un puerto de salida a otro puerto de salida del interferómetro.
- La media de conteo de fotones o la probabilidad de detectar un fotón en un puerto de salida particular es proporcional a la intensidad clásica de la luz que se observaría en ese puerto, es decir, la intensidad total se convierte en la probabilidad total que es igual a 1.

Dado que se tiene un modelo estocástico, se analiza por medio de una herramienta de simulación como el método de Monte Carlo, el cual a partir de un muestreo aleatorio repetitivo sobre todos los eventos posibles que pueden suceder en el sistema y un análisis estadístico permite calcular resultados y extraer conclusiones. En la **Figura 9**, se observa el método desarrollado en MATLAB, que consta de los siguientes pasos principales aplicados al sistema de interés:

1. Generación del modelo: Considerando el modelo estocástico definido, se desarrolla un modelo computarizado que representa el sistema de comunicación bajo un ataque por interceptación del canal.

2. Generación de variables aleatorias: Se genera un conjunto de N variables aleatorias distribuidas uniformemente entre 0 y 1, las cuales corresponden a los fotones que se envían. Estos fotones son distribuidos en los 2M puertos de salida de los interferómetros del atacante, a partir de una distribución de probabilidad donde cada puerto de salida tiene una probabilidad igual 1/2M, excepto el puerto de salida del valor del bit y el retraso de tiempo correcto que tiene probabilidad igual a 1/M y el puerto de salida complementario a este que tiene probabilidad igual a cero, donde M es la cantidad de retrasos de tiempo posibles entre Alice y Bob para la clave. Mediante esta distribución de los fotones en los diferentes puertos de salida se transforman las variables aleatorias uniformes en una variable aleatoria bajo la distribución de Poisson, acorde con la estadística que se asume para el conteo de fotones.

3. Experimentación numérica: Con N como la variable de entrada se ejecuta el modelo computarizado trial cantidad de veces, el cual genera como salida la probabilidad p de ocurrencia de un evento de interés. El procedimiento anterior se ejecuta Ns cantidad de veces.

4. Análisis de resultados: La simulación se repite Ns cantidad de veces, por lo cual se obtienen Ns cantidad de probabilidades de ocurrencia del evento, por medio de las cuales se realiza un análisis estadístico a partir de medidas comunes como el valor medio y la varianza. Finalmente se extraen conclusiones sobre los resultados del modelo en función de los experimentos estadísticos.

```
function p=photonSim(N,trial,M)

count=0;
for j=1:1:trial
outcomes=rand(1, N);

ports=2*M;    %Cantidad de puertos
complement_port=4; %Puerto complemento
right_port=3;    %Puerto correcto

%%-- Definición probabilidades --%%
pnull=1/1e10;
a(1)=0;
for ka=2:1:ports+1
if ka==right_port+1
    a(ka)=a(ka-1)+((2/ports)-pnull);
elseif ka==complement_port+1
    a(ka)=a(ka-1)+pnull;
else
    a(ka)=a(ka-1)+(1/ports);
end
end
```

```
%%-- Distribución de fotones --%
for i=1:length(outcomes)
    for ik=1:ports
    if (a(ik) < outcomes(1,i)) &&
(outcomes(1,i)<= a(ik+1))
        O(j,i)=ik;
    end
    end
end
%%-- Conteo de fotones --%%
for k = 1:ports
y(j,k) = sum(O(j,:)==k);
end
%%-- Conteo de puertos vacíos --%%
Nc(j,:)=sum(y(j,:)==0);
end
end
```

Figura 9. *Código de MATLAB para simulación del método de Monte Carlo del sistema de comunicación ante un ataque por interceptación del canal.*

Dado que la simulación se debe repetir varias veces, la precisión en la solución dependerá del número de ensayos (trial) y el número de iteraciones (Ns) a realizar, ya que a medida que el número de simulaciones es mayor la solución de la simulación converge a la verdadera probabilidad que está bajo estimación. Con el fin de llegar a un equilibrio entre el esfuerzo computacional (cantidad de simulaciones) y la precisión de la solución se decide definir un intervalo con un nivel de confianza del 95% dado por la Ecuación 6 válida para una distribución normal de los datos, donde σ es la desviación estándar, Ns es la cantidad de iteraciones y $\bar{X}_N$ el valor medio de los experimentos calculado de acuerdo a la Ecuación 7. Con este intervalo es posible enunciar que a partir de los resultados de simulación con una probabilidad al menos del 95%, el valor real de la probabilidad de ocurrencia del evento se encuentra en dicho intervalo.

$$\left[\bar{X}_N - 1.96\frac{\sigma}{\sqrt{N_s}}, \bar{X}_N + 1.96\frac{\sigma}{\sqrt{N_s}}\right] \tag{6}$$

$$\bar{X}_N = \frac{1}{N_s}\sum_{i=1}^{N_s} x_i \tag{7}$$

En la **Figura 10**, se observan los histogramas obtenidos para una simulación con 100, 500 y 1000 iteraciones cada una con 1000 experimentos, encontrando que a medida que el número de iteraciones aumenta por el teorema del límite central la distribución se acerca a una distribución normal, sin embargo demanda mayor cantidad de tiempo computacional, por lo tanto se decide trabajar con una cantidad de iteraciones Ns=500, donde la forma de los datos logra ser una distribución normal y la Ecuación 6 y Ecuación 7 se satisfacen.

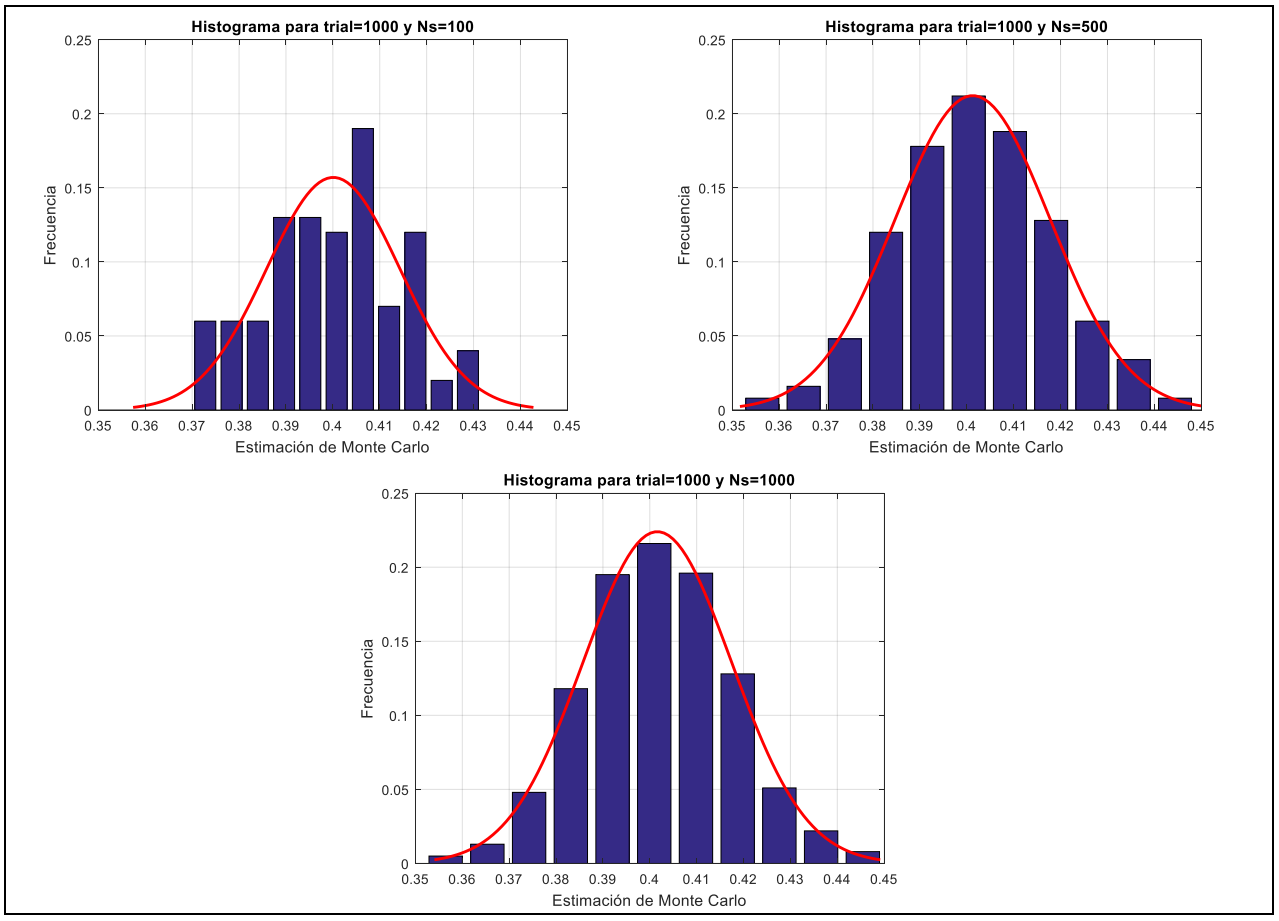

Figura 10. *Histogramas obtenidos para una simulación de Monte Carlo con Ns=100, 500 y 1000 cada una con trial=1000, para un caso de conteo promedio de fotones igual a 60 y M=10.*

En la **Figura 11**, se presentan los histogramas obtenidos para 100, 500 y 1000 experimentos cada uno con 500 iteraciones, donde se observa que a medida que se aumenta el número de experimentos la varianza del resultado disminuye. En la **Tabla 4**, se resumen los resultados obtenidos para cada simulación, de tal forma que se decide trabajar la simulación de Monte Carlo con una cantidad de experimentos igual a 1000, dado que ofrece una menor desviación y no afecta de manera significativa el tiempo de simulación en comparación con una cantidad de experimentos igual a 500.

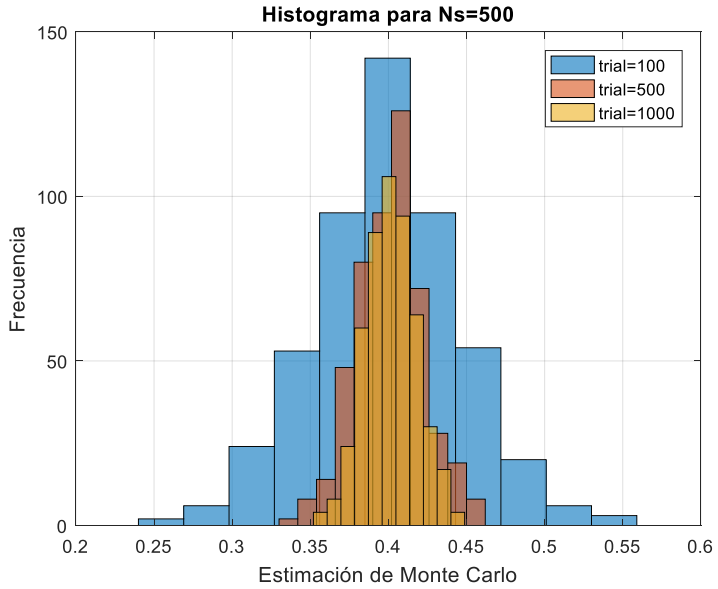

Figura 11. *Histogramas obtenidos para una simulación de Monte Carlo para trial=100, 500 y 1000 cada una con Ns= 500, para un caso de conteo promedio de fotones igual a 60 y M=10.*

Tabla 4.
Especificaciones de la simulación obtenidas para el caso de un conteo promedio de fotones de igual a 60, para diferente número de experimentos (trial) y Ns=500.

Trial	**Media $\bar{X}_N$**	**Desviación estándar σ**
100	0.39954	0.048649
500	0.40061	0.021916
1000	0.40120	0.016278

Con el fin de evaluar el desempeño de la simulación de Monte Carlo realizada, en la siguiente sección se comparan los resultados obtenidos con los resultados de las expresiones analíticas para los diferentes ataques que fueron desarrolladas en (Boughanmi, 2017; Rhodes et al., 2016).

2.3 Análisis de ataques a la seguridad del sistema

Teniendo en cuenta que Eve conoce el algoritmo de encriptación, posee dispositivos ideales y cuenta con la tecnología necesaria para un ataque, se analizan aspectos importantes de la seguridad del sistema ante un ataque por interceptación del canal como el que se muestra en la **Figura 12**, donde Eve desvía parte del haz de luz transmitido por Alice y lo divide en cantidades iguales que dirige a M interferómetros en cascada, donde cada uno corresponde a uno de los posibles retrasos de tiempo entre Alice y Bob. El objetivo de Eve es determinar el valor del retraso de tiempo utilizado en un determinado instante de la transmisión y por ende el valor de bit correcto, el cual corresponde al interferómetro encerrado en línea punteada.

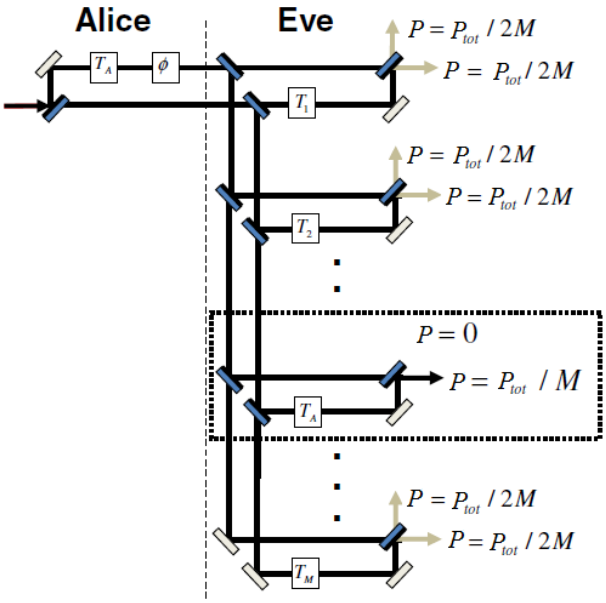

Figura 12. *Esquema del ataque por interceptación del canal al sistema de comunicación operado a nivel de conteo de fotones, Nota. Adaptado de (Rhodes et al., 2016).*

En los diferentes puertos de salida de los M interferómetros empleados por Eve para el ataque, se encuentra que los fotones se reparten de manera aleatoria, razón por la cual se analizan los diferentes eventos que se pueden presentar, donde se identifican tres eventos principales que se denominan como ataque 1, ataque 2_k y ataque 3_k, ya que mediante la ocurrencia de estos eventos Eve puede deducir con certeza el retraso de tiempo correcto, y por lo tanto, el valor del bit, lo cual le permite enviar un haz de luz con las propiedades correctas a Bob y ocultar así su presencia. Para analizar cada uno de los eventos se asume que Alice transmite un bit igual a 0 durante el tiempo para el cual su sistema está configurado para un retraso de tiempo específico T_A.

2.3.1 Ataque 1. Como se muestra en la **Figura 13**, este ataque consiste en la ocurrencia del evento donde todos los puertos de salida de los M interferómetros del atacante presentan al menos un fotón, excepto el puerto de salida correspondiente al bit igual a 1 del interferómetro ajustado al retraso de tiempo $\boldsymbol{T_A}$ que muestra cero fotones.

Figura 13. *Ejemplo del evento del ataque 1 para Eve, para M=10 posibles retrasos de tiempo junto con el conteo de fotones recibido por Bob, para un envío de un bit 0 con 22 fotones por parte de Alice. Cada bola azul es una representación pictórica de un fotón.*

La probabilidad de éxito de Eve para el ataque 1 en función de la media de conteo de fotones $\bar{n}_{tot}$ y la cantidad de interferómetros M está dada por la Ecuación 8 (Rhodes et al., 2016), y es calculada en la simulación de Monte Carlo mediante el código presentado en la **Figura 14**.

$$P_{succes}^{\#1} = \left(1 - e^{-\frac{\bar{n}_{tot}}{2M}}\right)^{2(M-1)} \times \left(1 - e^{-\frac{\bar{n}_{tot}}{M}}\right) \tag{8}$$

```
%%-- Condición de éxito para el evento --%
if (y(j,complement_port)==0)&&(Nc(j)==1)
    count=count+1;
end
```

Figura 14. *Código de MATLAB para determinar el evento del ataque 1 de Eve.*

En la **Figura 15** y **Figura 16**, se presentan los resultados del cálculo de la probabilidad de Eve de identificar correctamente el retraso de tiempo junto con el valor del bit para 10 posibles retrasos de tiempo, mediante la expresión analítica y la simulación de Monte Carlo para el ataque 1. Se observa que para el caso de 10 posibles retrasos de tiempo Eve requerirá al menos 66 fotones en promedio para lograr una probabilidad superior a 0.5. En al menos en uno de dos intentos logrará determinar el tiempo de retraso y el valor de bit correctos.

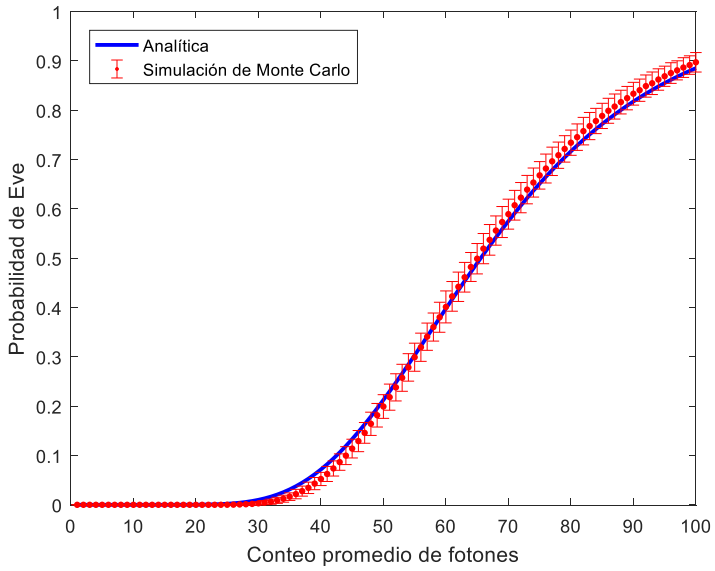

Figura 15. *Resultados del cálculo de la probabilidad de Eve mediante el ataque 1, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

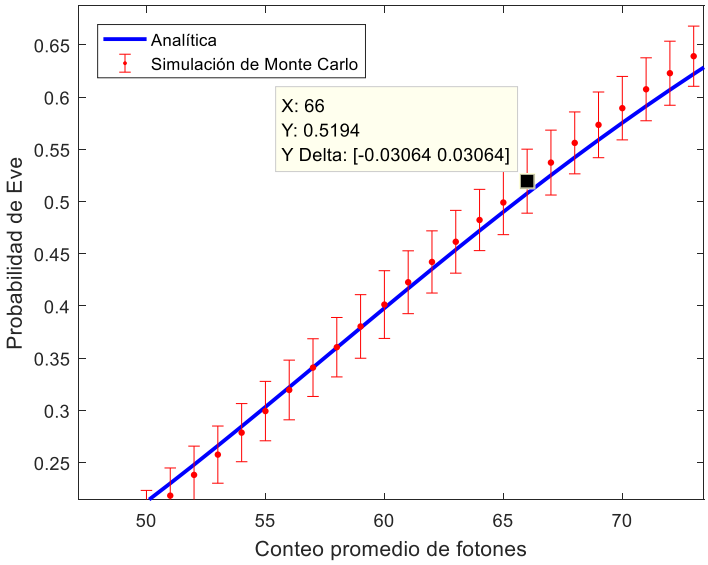

Figura 16. *Zoom para resultados del cálculo de la probabilidad de Eve mediante el ataque 1, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

En la **Figura 17**, se presenta la gráfica del error cuadrático medio entre los resultados y los resultados de la simulación de Monte Carlo para el ataque 1 con 10 posibles retrasos de tiempo,

donde se puede observar que el error es máximo del orden de 10^{-4}, lo que permite concluir que ambos resultados concuerdan con tal precisión.

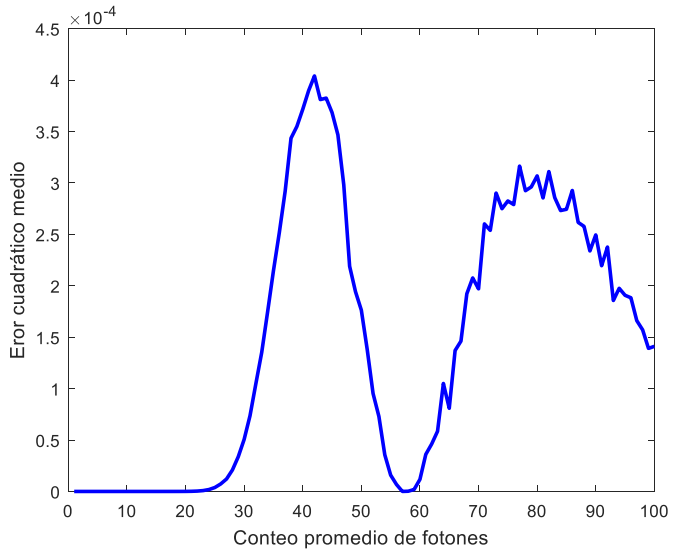

Figura 17. *Error cuadrático medio entre los resultados analíticos y los resultados de simulación para el ataque 1 y M = 10.*

2.3.2 Ataque 2_k. Como se muestra en la **Figura 18**, este ataque consiste en la ocurrencia del evento donde se presentan k+1 interferómetros de los M interferómetros del atacante con cero fotones en uno de sus puertos de salida, de tal forma que Eve revisa la cantidad de fotones en los puertos no vacíos de esos k+1 interferómetros y deduce que el retraso de tiempo correcto corresponde al interferómetro con mayor cantidad de fotones en su puerto de salida.

Figura 18. *Ejemplo del evento del ataque 2_1 para Eve, para M=10 posibles retardos de tiempo junto con el conteo de fotones recibido por Bob, para un envío de un bit 0 con 22 fotones por parte de Alice. Cada bola azul es una representación pictórica de un fotón.*

La probabilidad de éxito de Eve para el ataque 2_k en función de la media de conteo de fotones $\bar{n}_{tot}$ y la cantidad de interferómetros M está dada por la Ecuación 9 (Boughanmi, 2017) y es calculada en la simulación de Monte Carlo mediante el código presentado en la **Figura 19**.

$$P_{succes}^{\#2\_k} = \left\{ C_k^{M-1} \times [C_1^2]^k \times \left[\left(1 - e^{-\frac{\bar{n}_{tot}}{2M}}\right)^{2(M-(k+1))} \times \left(e^{-\frac{\bar{n}_{tot}}{2M}}\right)^k \right] \right\} \times \sum_{i_1,\ldots,i_k=1}^{\infty} \left\{ \left[\frac{\left(\frac{\bar{n}_{tot}}{2M}\right)^{i_1}}{i_1!} e^{-\frac{\bar{n}_{tot}}{2M}} \right] \times \ldots \times \left[\frac{\left(\frac{\bar{n}_{tot}}{2M}\right)^{i_k}}{i_k!} e^{-\frac{\bar{n}_{tot}}{2M}} \right] \times \sum_{j>i_1,\ldots,i_k}^{\infty} \left[\frac{\left(\frac{\bar{n}_{tot}}{M}\right)^{j}}{j!} e^{-\frac{\bar{n}_{tot}}{M}} \right] \right\} \quad (9)$$

```
%%-- Condición de éxito para el evento ---%%
if (y(j,complement_port)==0)&&(Nc(j)==(kports+1))
cont2=cont2+1;
A2(cont2,:)=y(j,:);
a2(cont2,:)=find(A2(cont2,:)==0);
end

if (cont2~=0)
      for j2=1:cont2
            for i2=1:((kports+1)-1)
                  if ((mod(a2(j2,i2),2)~=0)&&(a2(j2,i2+1)==a2(j2,i2)+1))
                  check(j2,i2)=1;
                  else
                  check(j2,i2)=0;
                  end
                  check(j2,(kports+1))=0;
            end
            if (sum(check(j2,:))==0)
            index2=index2+1;
            Afinal(index2,:)=A2(j2,:);
            a2final(index2,:)=a2(j2,:);
            end
      end

     for j3=1:size(a2final,1)
            for i3=1:size(a2final,2)
                  if (a2final(j3,i3)==complement_port)
                  CR(j3,:)=Afinal(j3,right_port);
                  else
                        if (mod(a2final(j3,i3),2)==0)
                        CW(j3,i3)=Afinal(j3,a2final(j3,i3)-1);
                        else
                        CW(j3,i3)=Afinal(j3,a2final(j3,i3)+1);
                        end
                  end
            end
    end
    count2=sum(CR>max(CW,[],2));
end
```

Figura 19. *Código de MATLAB para determinar el evento del ataque 2_k de Eve.*

En la **Figura 20** y **Figura 21**, se presentan los resultados del cálculo de la probabilidad de Eve de identificar correctamente el retardo de tiempo junto con el valor del bit para 10 posibles retrasos de tiempo, mediante la expresión analítica y resultados de la simulación de Monte Carlo para el ataque 2_1. Se observa que para el caso de 10 posibles retrasos de tiempo Eve requerirá al menos de 58 fotones en promedio para lograr una probabilidad de 0.3222 de determinar el tiempo de retraso y el valor de bit correctos mediante esta técnica, siendo el mayor valor de probabilidad resultante para este evento.

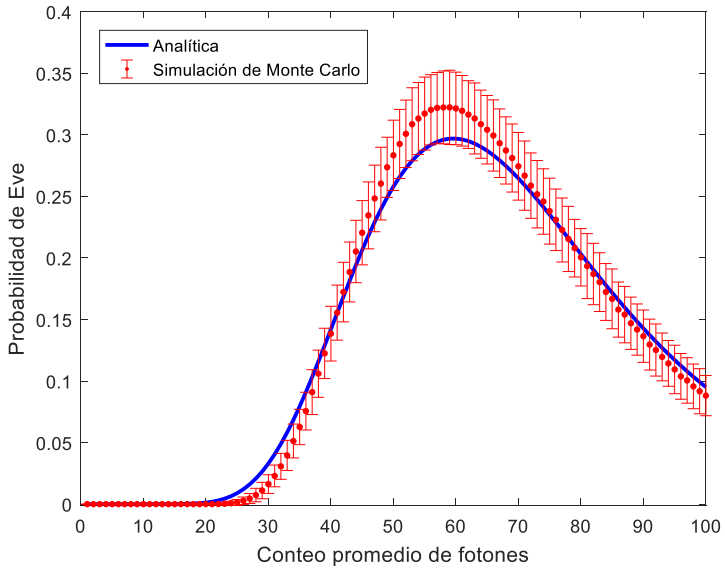

Figura 20. *Resultados del cálculo de la probabilidad de Eve mediante el ataque 2_1, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

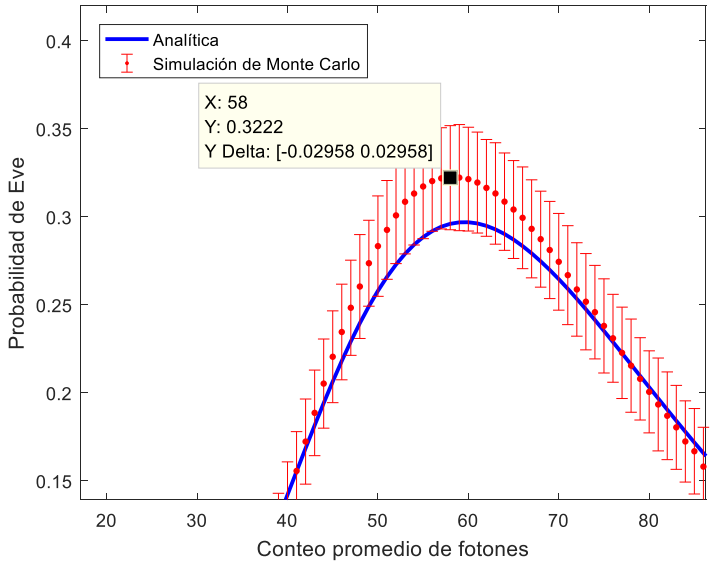

Figura 21. *Zoom para resultados del cálculo de la probabilidad de Eve mediante el ataque 2_1, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

En la **Figura 22**, se presenta la gráfica del error cuadrático medio entre los resultados analíticos y los resultados de la simulación de Monte Carlo para el ataque 2_1 con 10 posibles

retrasos de tiempo, donde se puede observar que el error es máximo del orden de 10^{-4}, lo que permite concluir que ambos resultados concuerdan con tal precisión.

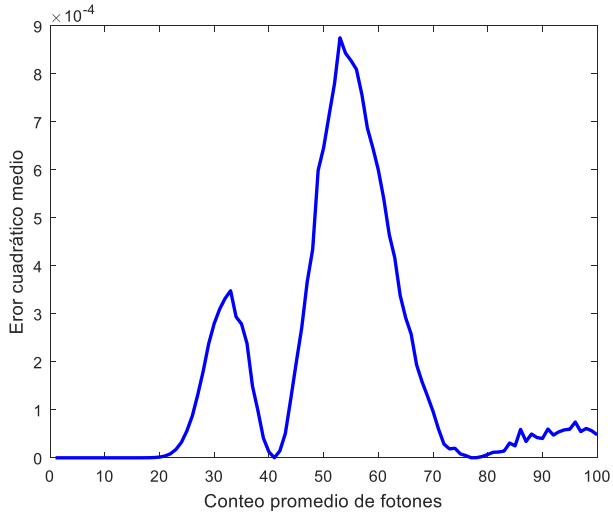

Figura 22. *Error cuadrático medio entre los resultados analíticos y los resultados de simulación para el ataque 2_1 y M = 10.*

2.3.3 Ataque 3_k. Como se muestra en la **Figura 23**, este ataque consiste en la ocurrencia del evento donde se presentan k interferómetros de los M interferómetros con cero fotones en sus dos puertos de salida y el puerto de salida correspondiente al bit igual a 1 del interferómetro ajustado al retraso de tiempo $\boldsymbol{T_A}$ que muestra cero fotones, de tal forma que Eve deduce que el retraso de tiempo correcto corresponde al interferómetro con solo un puerto de salida en cero.

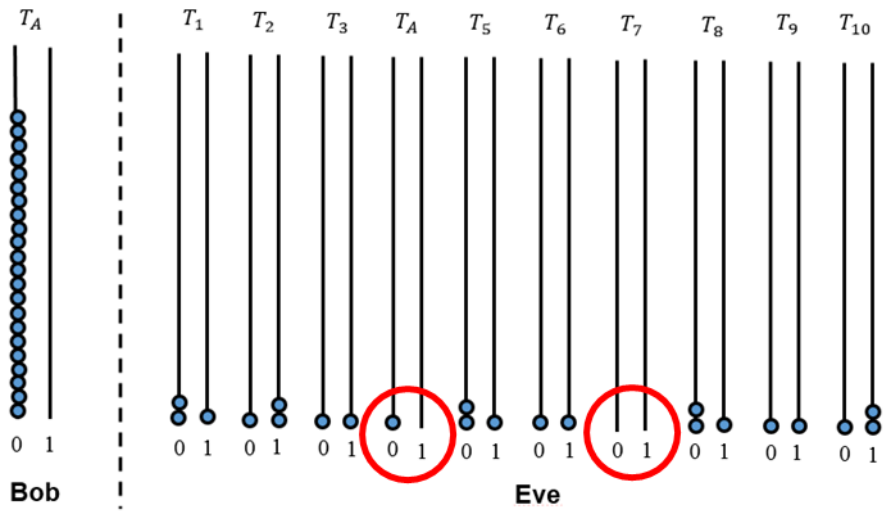

Figura 23. *Ejemplo del evento del ataque 3_1 para Eve, para M=10 posibles retardos de tiempo junto con el conteo de fotones recibido por Bob, para un envío de un bit 0 con 22 fotones por parte de Alice. Cada bola azul es una representación pictórica de un fotón.*

La probabilidad de éxito de Eve para el ataque 3_k en función de la media de conteo de fotones $\bar{n}_{tot}$ y la cantidad de interferómetros M está dada por la Ecuación 10 (Boughanmi, 2017) y es calculada en la simulación de Monte Carlo mediante el código presentado en la **Figura 24**.

$$P_{succes}^{\#3\_k} = \left\{ C_k^{M-1} \times \left[\left(1 - e^{-\frac{\bar{n}_{tot}}{2M}}\right)^{2(M-(k+1))} \times \left(e^{-\frac{\bar{n}_{tot}}{2M}}\right)^{2k} \right] \times \sum_{n\geq 1}^{\infty} \left[\frac{\left(\frac{\bar{n}_{tot}}{M}\right)^n}{n!} e^{-\frac{\bar{n}_{tot}}{M}} \right] \right\} \quad (10)$$

```
%%-- Condición de éxito para el evento --%
if
(y(j,complement_port)==0)&&(y(j,right_port)>=1)&&(Nc(j)==(2*kports+1))
cont2=cont2+1;
A2(cont2,:)=y(j,:);
a2(cont2,:)=find(A2(cont2,:)==0);
end

end

if (cont2~=0)
    for j2=1:cont2
           for i2=1:(2*kports)
                if ((mod(a2(j2,i2),2)~=0)&&(a2(j2,i2+1)==a2(j2,i2)+1))
                check(j2,i2)=1;
                else
                check(j2,i2)=0;
                end
                check(j2,(2*kports+1))=0;
           end
     if (sum(check(j2,:))==kports)
     count3=count3+1;
     end
    end
end
```

Figura 24. *Código de MATLAB para determinar el evento del ataque 3_k de Eve.*

En la **Figura 25** y **Figura 26**, se presentan los resultados del cálculo de la probabilidad de Eve de identificar correctamente el retraso de tiempo junto con el valor del bit para 10 posibles retrasos de tiempo, mediante la expresión analítica y la simulación de Monte Carlo para el ataque 3_1. Se observa que para el caso de 10 posibles retrasos de tiempo Eve requerirá al menos de 44 fotones en promedio para lograr una probabilidad de 0.01947 de seleccionar el tiempo de retraso y el valor de bit correctos mediante esta técnica, siendo el mayor valor de probabilidad resultante para este evento.

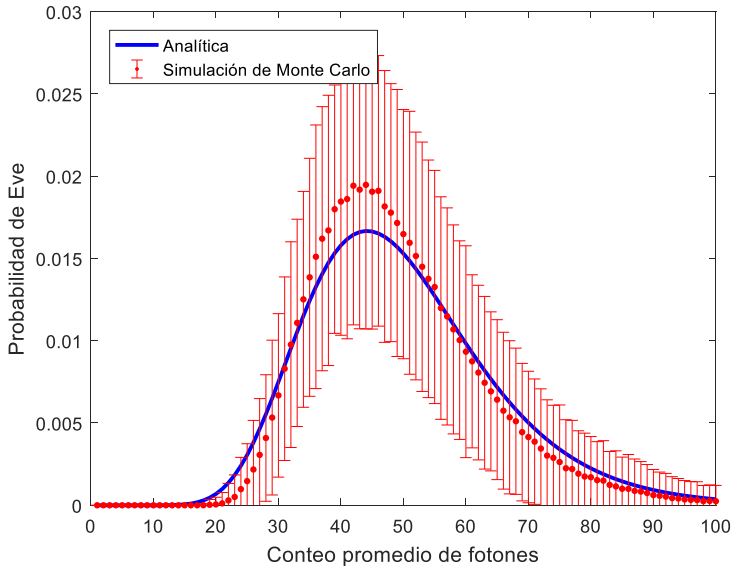

Figura 25. *Resultados del cálculo de la probabilidad de Eve mediante el ataque 3_1, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

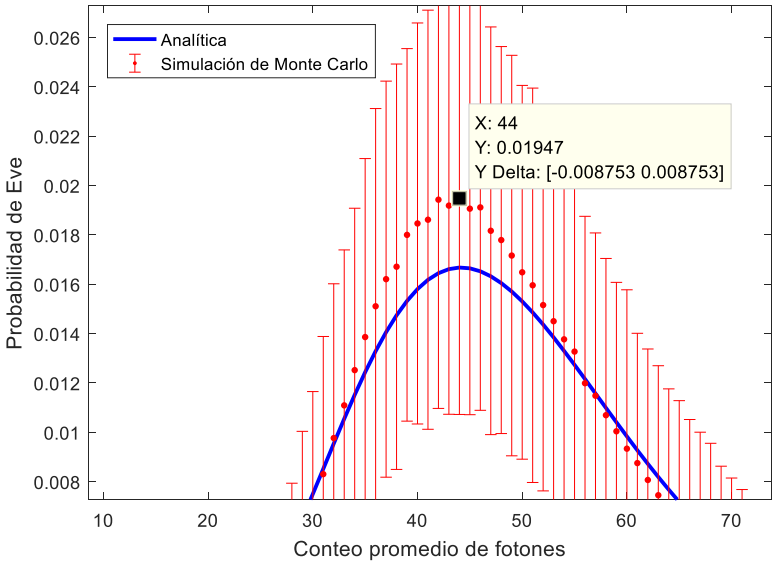

Figura 26. *Zoom para resultados del cálculo de la probabilidad de Eve mediante el ataque 3_1, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

En la **Figura 27**, se presenta la gráfica del error cuadrático medio entre los resultados analíticos y los resultados de la simulación de Monte Carlo para el ataque 3_1 con 10 posibles

retrasos de tiempo, donde se puede observar que el error es máximo del orden de 10^{-6}, lo que permite concluir que ambos resultados concuerdan con tal precisión.

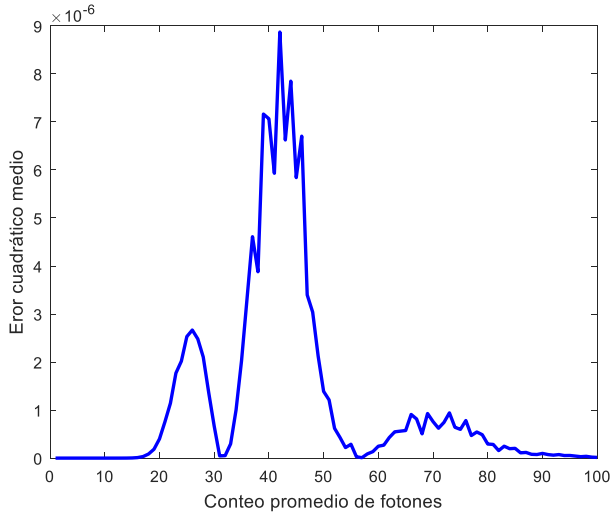

Figura 27. *Error cuadrático medio entre los resultados analíticos y los resultados de simulación para el ataque 3_1 y M = 10.*

2.3.4 Combinación de ataque 1, 2_k y 3_k. En particular para el caso de M=10 retrasos de tiempo posibles, se identifica la probabilidad de Eve de determinar el retraso de tiempo y el valor del bit correcto a partir de la combinación de todos los tipos de ataques analizados anteriormente, teniendo en cuenta que cada uno de los eventos o ataques son eventos independientes, lo que permite obtener la probabilidad de Eve total como la suma de cada una de las probabilidades.

En la **Figura 28**, se presentan los resultados del cálculo de la probabilidad de Eve de identificar correctamente el retraso de tiempo junto con el valor del bit para 10 posibles retrasos de tiempo, mediante la expresión analítica y la simulación de Monte Carlo para la combinación de ataques 1, 2_1 hasta 2_8 y 3_1 hasta 3_9. Se observa que para el caso de 10 posibles retrasos

de tiempo Eve requerirá al menos 39 fotones en promedio para lograr una probabilidad superior a 0.5 de seleccionar el tiempo de retraso y el valor de bit correctos.

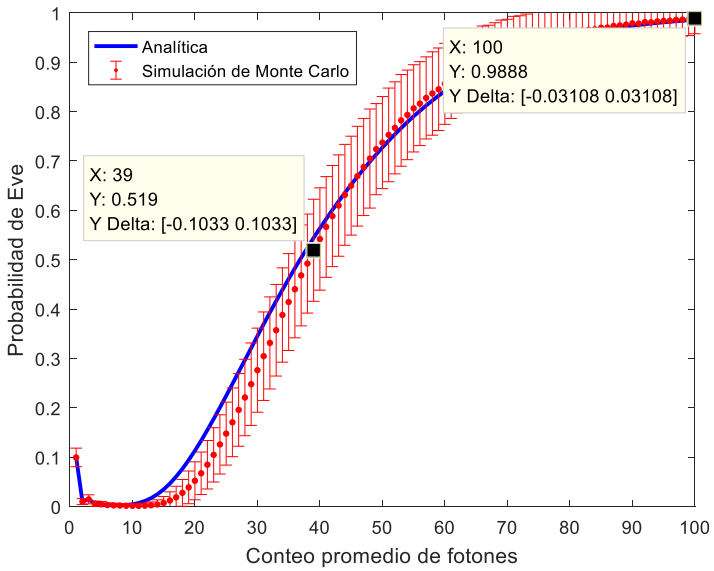

Figura 28. *Resultados del cálculo de la probabilidad de Eve mediante la combinación de ataques 1, 2_1 hasta 2_8 y 3_1 hasta 3_9, en función del conteo promedio total de fotones para M= 10. Resultados de la expresión analítica (azul) y resultados de la simulación de Monte Carlo (rojo) con trial=1000 y Ns=500.*

3 Sistema de comunicación basado en la modulación de coherencia y el momento angular orbital

Con la proliferación de Internet en la última década la cantidad de tráfico de información a través de las redes de telecomunicaciones ha aumentado drásticamente y con ello aumenta las posibilidades de recepción no autorizada, lo cual ha motivado un nuevo enfoque para el cifrado

de datos basado en la mecánica cuántica, que nos permite a partir de un partícula como el fotón, trabajar con sistemas probabilísticos como el que se presenta en este capítulo.

3.1 Descripción del sistema de comunicación

Con base en la aplicación de la mecánica cuántica para la seguridad en los sistemas de comunicación, se da el desarrollo de sistemas para distribución de clave cuántica (QKD), los cuales permiten la comunicación segura entre dos entidades, empleando propiedades individuales de los fotones. El sistema más conocido es el protocolo BB84, el cual permite establecer una secuencia aleatoria de bits idéntica y secreta entre dos personas en lugares remotos, a partir del uso de la polarización de la luz para codificar los valores de bit, sin embargo esto limita a un bit la cantidad de información transmitida por cada fotón e impone límites sobre las tasas de error toleradas por el sistema, por lo cual se desarrolló un sistema de comunicación basado en la metodología del protocolo BB84, donde se usan dos bases mutuamente imparciales que explotan la estructura transversal y las propiedades de coherencia del campo de luz.

3.1.1 Bases de la codificación. Las bases se definen a partir de la codificación de información en los grados de libertad de un fotón. El primer grado de libertad considerado es la coherencia temporal de una fuente de luz, donde a partir de introducir un retraso de tiempo $\boldsymbol{\tau_n}$ al interior del tren de onda emitido por una fuente, que sea mucho mayor al tiempo de coherencia de la fuente $\boldsymbol{\tau_c}$ permite la no interferencia de los paquetes de onda obteniendo un par de pulsos o trenes separados por un tiempo $\boldsymbol{\tau_n}$ como se muestra en la **Figura 29**, los cuales interferirán constructivamente solo cuando se propaguen sobre la misma longitud de camino óptico, siendo esto la aplicación de la técnica que se denomina como modulación de coherencia.

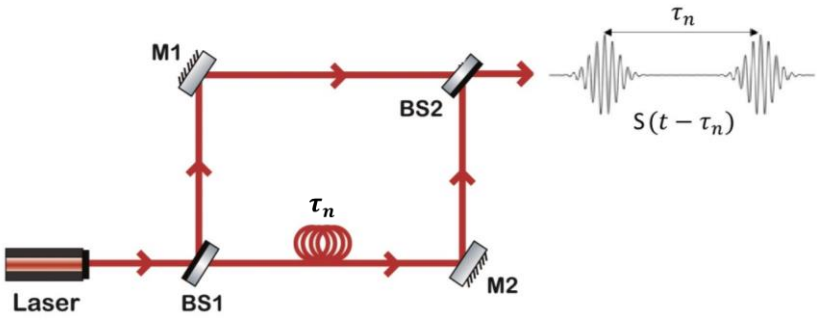

Figura 29. *Modulación de coherencia en un interferómetro de Mach-Zehnder.*

En la propagación del haz por un interferómetro de Mach-Zehnder se establece la señal $S(t-\tau_n)$ de salida como la convolución entre la señal de luz de entrada y dos pulsos distanciados τ_n, como se muestra en la Ecuación 11 y Ecuación 12.

$$S(t-\tau_n) = \left[\frac{1}{2} sinc(\pi t)\cos(2\pi f_o t)\right] * \left[\delta\left(t-\frac{\tau_n}{2}\right) + \delta\left(t+\frac{\tau_n}{2}\right)\right] \tag{11}$$

$$S(t-\tau_n) = \frac{1}{2}\left[sinc\left(\pi\left(t-\frac{\tau_n}{2}\right)\right) cos\left(2\pi f_o\left(t-\frac{\tau_n}{2}\right)\right) + sinc\left(\pi\left(t+\frac{\tau_n}{2}\right)\right) cos\left(2\pi f_o\left(t+\frac{\tau_n}{2}\right)\right)\right] \tag{12}$$

El conjunto de señales $S(t-\tau_n)$ constituyen una base ortonormal de retrasos de tiempo como se verifica de la Ecuación 13 a la Ecuación 18.

$$I1 = \int_{-\infty}^{\infty} S(t-\tau_k)\bar{S}(t-\tau_k)\,dt \tag{13}$$

$$I1 = \int_{-\infty}^{\infty} \left[sinc\left(\pi\left(t-\frac{\tau_k}{2}\right)\right) cos\left(2\pi f_o\left(t-\frac{\tau_k}{2}\right)\right) + sinc\left(\pi\left(t+\frac{\tau_k}{2}\right)\right) cos\left(2\pi f_o\left(t+\frac{\tau_k}{2}\right)\right)\right]^2 dt = 1 \tag{14}$$

$$I2 = \int_{-\infty}^{\infty} S(t-\tau_q)\bar{S}(t-\tau_q)\,dt \tag{15}$$

$$I2 = \int_{-\infty}^{\infty} \left[sinc\left(\pi\left(t-\frac{\tau_q}{2}\right)\right) cos\left(2\pi f_o\left(t-\frac{\tau_q}{2}\right)\right) + sinc\left(\pi\left(t+\frac{\tau_q}{2}\right)\right) cos\left(2\pi f_o\left(t+\frac{\tau_q}{2}\right)\right)\right]^2 dt = 1 \tag{16}$$

$$I12 = \int_{-\infty}^{\infty} S(t-\tau_k)\bar{S}(t-\tau_q)\,dt = I21 = \int_{-\infty}^{\infty} S(t-\tau_q)\bar{S}(t-\tau_k)\,dt \tag{17}$$

$$I12 = \int_{-\infty}^{\infty} \left[sinc\left(\pi\left(t-\frac{\tau_k}{2}\right)\right) cos\left(2\pi f_o\left(t-\frac{\tau_k}{2}\right)\right) + sinc\left(\pi\left(t+\frac{\tau_k}{2}\right)\right) cos\left(2\pi f_o\left(t+\frac{\tau_k}{2}\right)\right)\right] \left[sinc\left(\pi\left(t-\frac{\tau_q}{2}\right)\right) cos\left(2\pi f_o\left(t-\frac{\tau_q}{2}\right)\right) + sinc\left(\pi\left(t+\frac{\tau_q}{2}\right)\right) cos\left(2\pi f_o\left(t+\frac{\tau_q}{2}\right)\right)\right] dt = 0 \tag{18}$$

El otro grado de libertad considerado es el momento angular orbital, esta propiedad espacial se define a partir de algunos modos MAO como se observa en la **Figura 30**, caracterizados por

una intensidad de sección transversal anular y un perfil de fase helicoidal $e^{il\varphi}$ donde l es un número entero, conocido como carga topológica del modo.

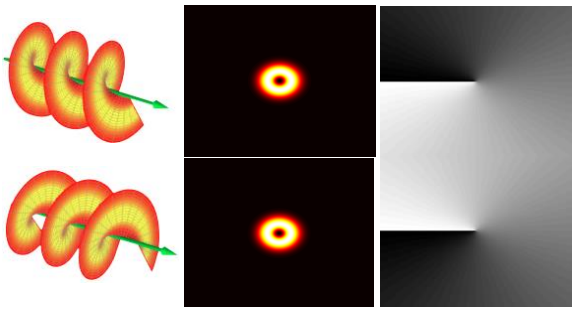

Figura 30. *De izquierda a derecha representación pictórica del MAO, intensidad y fase de un modo MAO con carga topológica* $l = -1$ *y* 1.

El conjunto de modos MAO $e^{il\varphi}$ se define como una base ortonormal como se verifica de la Ecuación 19 a la Ecuación 22.

$$I3 = \frac{1}{2\pi}\int_0^{2\pi} e^{il_a\varphi} * e^{-il_a\varphi}\, d\varphi = 1 \tag{19}$$

$$I4 = \frac{1}{2\pi}\int_0^{2\pi} e^{il_b\varphi} * e^{-il_b\varphi}\, d\varphi = 1 \tag{20}$$

$$I34 = \frac{1}{2\pi}\int_0^{2\pi} e^{il_a\varphi} * e^{-il_b\varphi}\, d\varphi = 0 \tag{21}$$

$$I43 = \frac{1}{2\pi}\int_0^{2\pi} e^{il_b\varphi} * e^{-il_a\varphi}\, d\varphi = 0 \tag{22}$$

A partir de la superposición de estas dos propiedades se define como el ejemplo más simple un conjunto de cuatro estados del fotón que conforman la primera base denotada por $\psi = [\psi_1 \ldots \quad \psi_4]^T$, como se muestra de la Ecuación 23 a la Ecuación 26.

$$\psi_1 = S(t - \tau_k)e^{il_a\varphi} \tag{23}$$

$$\psi_2 = S(t - \tau_k)e^{il_b\varphi} \tag{24}$$

$$\psi_3 = S(t-\tau_q)e^{il_a\varphi} \tag{25}$$

$$\psi_4 = S(t-\tau_q)e^{il_b\varphi} \tag{26}$$

Mediante una combinación lineal de los estados de la primera base se genera los estados del fotón que conforman la segunda base denotada por $\xi = [\xi_1 \ldots \ \xi_4]^T$, como se muestra de la Ecuación 27 a la Ecuación 34.

$$\xi_1 = \frac{1}{\sqrt{2}}\left(\frac{\psi_1+\psi_2}{\sqrt{2}} + \frac{\psi_3+\psi_4}{\sqrt{2}}\right) \tag{27}$$

$$\xi_1 = \frac{1}{2}\left(S(t-\tau_k)\left[e^{il_a\varphi} + e^{il_b\varphi}\right] + S\left(t-\tau_q\right)\left[e^{il_a\varphi} + e^{il_b\varphi}\right]\right) \tag{28}$$

$$\xi_2 = \frac{1}{\sqrt{2}}\left(\frac{\psi_1+\psi_2}{\sqrt{2}} - \frac{\psi_3+\psi_4}{\sqrt{2}}\right) \tag{29}$$

$$\xi_2 = \frac{1}{2}\left(S(t-\tau_k)\left[e^{il_a\varphi} + e^{il_b\varphi}\right] - S\left(t-\tau_q\right)\left[e^{il_a\varphi} + e^{il_b\varphi}\right]\right) \tag{30}$$

$$\xi_3 = \frac{1}{\sqrt{2}}\left(\frac{\psi_1-\psi_2}{\sqrt{2}} + \frac{\psi_3-\psi_4}{\sqrt{2}}\right) \tag{31}$$

$$\xi_3 = \frac{1}{2}\left(S(t-\tau_k)\left[e^{il_a\varphi} - e^{il_b\varphi}\right] + S\left(t-\tau_q\right)\left[e^{il_a\varphi} - e^{il_b\varphi}\right]\right) \tag{32}$$

$$\xi_4 = \frac{1}{\sqrt{2}}\left(\frac{\psi_1-\psi_2}{\sqrt{2}} - \frac{\psi_3-\psi_4}{\sqrt{2}}\right) \tag{33}$$

$$\xi_4 = \frac{1}{2}\left(S(t-\tau_k)\left[e^{il_a\varphi} - e^{il_b\varphi}\right] - S\left(t-\tau_q\right)\left[e^{il_a\varphi} - e^{il_b\varphi}\right]\right) \tag{34}$$

De acuerdo a la Ecuación 35, se verifica la ortonormalidad de cada una de las bases, es decir, que el producto interno entre dos estados diferentes de la misma base sea igual a cero y el producto interno de un estado con si mismo sea igual a la unidad.

$$\int_0^{2\pi}\int_{-\infty}^{\infty}\psi_j\overline{\psi_k}dtd\varphi=\int_0^{2\pi}\int_{-\infty}^{\infty}\xi_j\overline{\xi_k}dtd\varphi=\delta_{jk} \quad (35)$$

Adicionalmente las bases deben ser mutuamente imparciales (MUB) del inglés, como en la Ecuación 36, donde el cuadrado de la magnitud del producto interno entre cualquier estado es igual a $\frac{1}{N_e}$; donde N_e corresponde a la cantidad de estados por base, para este caso igual a 4. Esta propiedad permite que, al realizar una medición del estado del fotón en una base diferente a la utilizada para su preparación, el resultado obtenido sea aleatorio, es decir, si el fotón está preparado en un estado de la primera base, entonces todos los resultados son igualmente probables cuando se realiza una medición que sondea para los estados de la segunda base.

$$\left|\int_0^{2\pi}\int_{-\infty}^{\infty}\psi_j\overline{\xi_k}\,dtd\varphi\right|^2=\left|\int_0^{2\pi}\int_{-\infty}^{\infty}\xi_j\overline{\psi_k}\,dtd\varphi\right|^2=\frac{1}{4};\forall\, i\neq j \quad (36)$$

Considerando un conjunto de M posibles retrasos de tiempo $TD=\{\tau_1,\tau_2,\tau_3,\dots,\tau_M\}$ que satisfacen la condición $\left|\tau_i-\tau_j\right|\gg\tau_c$, el tiempo de coherencia de la fuente, cuando $i\neq j$ y un conjunto de N posibles modos MAO $SLM=\{l_1,l_2,l_3,\dots,l_N\}$, para el caso más simple, Alice selecciona de estos dos conjuntos y acuerda con Bob un par de retrasos de tiempo $\{\tau_k,\tau_q\}$ y un par de modos MAO $\{l_a,l_b\}$, donde $\{(k,q,a,b)\in\mathbb{Z};(k\neq q)\wedge(a\neq b)\}$, estos parámetros componen la clave que permite definir las bases de codificación para el esquema de distribución cuántica de clave propuesto.

Con las bases definidas con sus estados correspondientes, se inicia la comunicación con Alice quien selecciona al azar y con la misma probabilidad una de las bases $\{\psi,\xi\}$ para codificar la información que se enviará. Una vez selecciona la base prepara un número de fotones en el estado seleccionado, que se envían a Bob, quien selecciona de forma independiente y aleatoria

una de las dos bases para medir los fotones entrantes y almacenar la selección de base y el estado detectado, dado que solo si selecciona la misma base que Alice, obtendrá información.

3.1.2 Generación de estados (Alice). Una vez que las dos bases se han definido con sus estados correspondientes, se determina un esquema experimental para la generación, transporte y detección de estos estados de fotones. Dado que en los estados de la segunda base hay una superposición de dos pares de pulsos con retrasos de tiempo $\{\boldsymbol{\tau_k}, \boldsymbol{\tau_q}\}$, una técnica para preparar los estados se modela con la óptica de la **Figura 31**, que incluye un par de interferómetros Mach-Zehnder (MZ) simétricos en paralelo, donde cada brazo del interferómetro está controlado por una de las entidades que requieren confidencialidad en la comunicación, en este caso Alice y Bob.

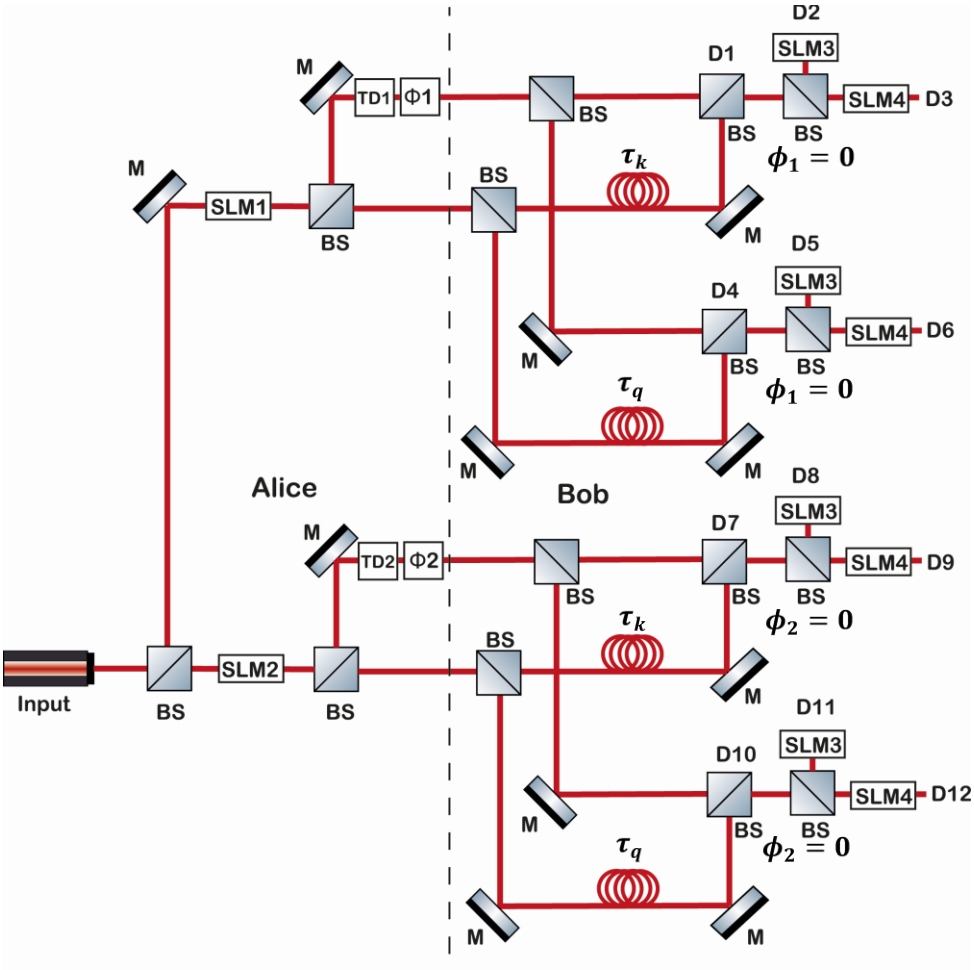

Figura 31. *Esquema óptico del sistema de comunicación con las bases ψ y ξ.*

En la **Figura 31**, en el lado izquierdo delimitado por la línea punteada se presenta la etapa de generación controlada por Alice, conformada por una fuente (input) para la generación de pulsos de luz con pocos fotones que inciden en un divisor de haz (BS), el cual divide el haz en dos haces, uno que se transmite al primer MZ (abajo) y otro que se refleja hacia un espejo que redirige este haz al segundo MZ (arriba). Antes de incidir sobre el siguiente divisor de haz, cada haz pasa a través de un modulador espacial de luz (SLM) donde se despliega el holograma tenedor correspondiente al modo MAO que requiere codificar Alice en los pares de pulsos, es decir, en el caso de la base ψ se proyecta un holograma del conjunto $SLM = \{l_a, l_b\}$ y en el caso de la base ξ se proyecta un holograma del conjunto $SLM = \{l_a \oplus l_b, l_a \ominus l_b\}$ para la base ξ,

donde $\oplus$ y $\ominus$ significa la suma y la resta de exponenciales complejos (modos MAO) respectivamente. Adicionalmente, Alice controla un par de moduladores de fase acromáticos indicados por ϕ, que permiten seleccionar la fase del haz entre dos posibles valores, 0 y π radianes. Hasta este punto de la descripción del sistema la señal enviada por Alice a Bob la componen dos pares de pulsos, como se muestran en la **Figura 32** y **Figura 33**.

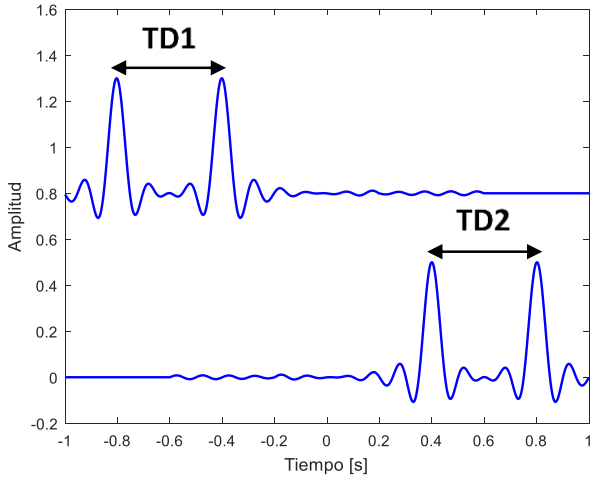

Figura 32. *Representación en el dominio del tiempo de la señal transmitida por Alice a Bob.*

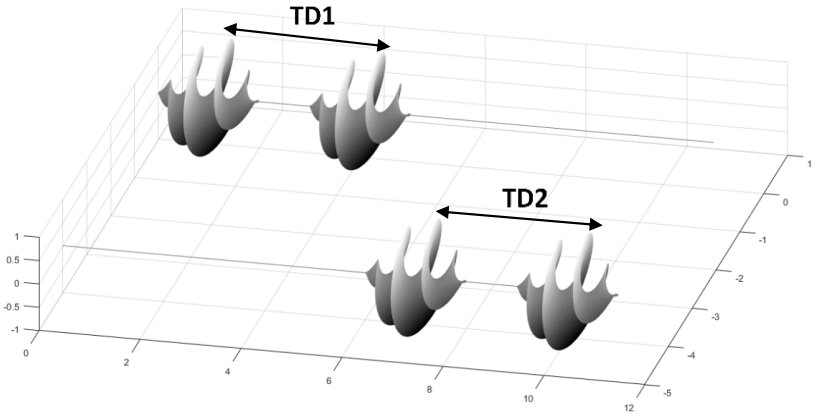

Figura 33. *Representación pictórica espacial y temporal de la señal transmitida por Alice a Bob.*

Para generar la señal de estado, Alice requiere inicialmente definir una clave de transmisión, para la cual tiene el conjunto de M posibles retrasos de tiempo, de los cuales selecciona un par y

posteriormente selecciona un par de modos MAO de un conjunto de N posibles, para lo cual tiene $\frac{M!L!}{(M-2)!(L-2)!}$ posibles maneras de seleccionar dicha clave como se muestra en la **Figura 34**.

Si Alice selecciona la 4-tupla $[\tau_k, \tau_q, l_a, l_b]$ como la clave, para el caso de la base ξ, los posibles retrasos de tiempo a considerar son τ_k y τ_q, donde debe establecer el primer retraso de tiempo TD1 en uno de estos dos posibles valores y configurar el otro, TD2, con el valor de retraso de tiempo no utilizado en TD1, cada uno con la superposición de modos MAO correspondiente y el modulador de fase.

Para cualquiera de los estados de segunda base ξ, Alice tiene dos posibles formas de implementar el estado a partir de la configuración de todos los pares de retrasos de tiempo con su correspondiente modo MAO, como se muestra en la **Figura 35**.

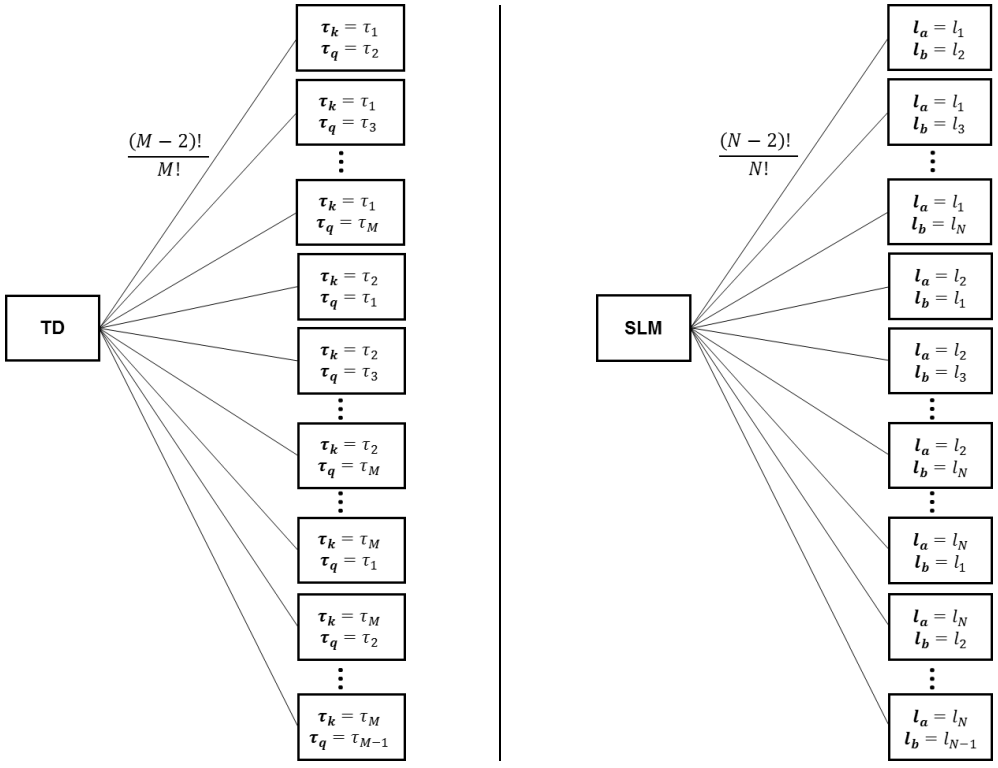

Figura 34. *Árbol de probabilidad para la especificación de la clave.*

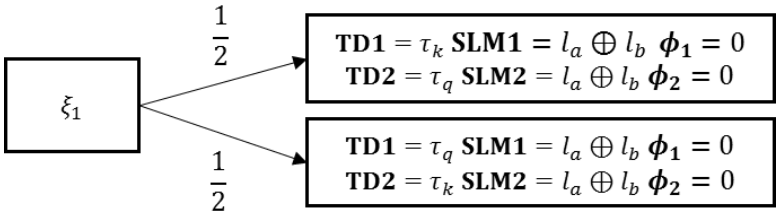

Figura 35. *Árbol de probabilidad para la implementación del estado* ξ_1.

Para el caso de la base ψ, los posibles retrasos a considerar son τ_k o τ_q dependiendo del estado a enviar, sin embargo, debido a que las características de la señal transmitida por Alice se deben preservar como en la **Figura 33**, independientemente de la base seleccionada, Alice debe usar dos retrasos de tiempo simultáneamente, es decir, en uno de los interferómetros envía el estado deseado y en el otro envía un estado que se usa como señuelo, ya que no transporta información. Alicia debe establecer el primer retraso de tiempo TD1 en uno de los dos posibles valores con su correspondiente modo MAO y establecer el otro retraso de tiempo TD2 en cualquiera de los M retrasos de tiempo posibles con cualquiera de los N posibles modos MAO. Se excluyen los casos en los que Alice asigna a ambos interferómetros los mismos valores de retraso de tiempo, ya que si Eve logra detectar que Alice envía el mismo retraso de tiempo en los dos interferómetros, puede identificar o deducir fácilmente la base que Alice está usando para preparar el estado.

Para cualquiera de los estados de la primera base ψ, Alice tiene $\frac{N![(N-1)!+(N-2)!(M-2)]}{(N-2)!(N-1)!}$ posibles formas de implementar el estado a partir de la configuración del par de retrasos de tiempo y todos los modos MAO, como se muestra en la **Figura 36**.

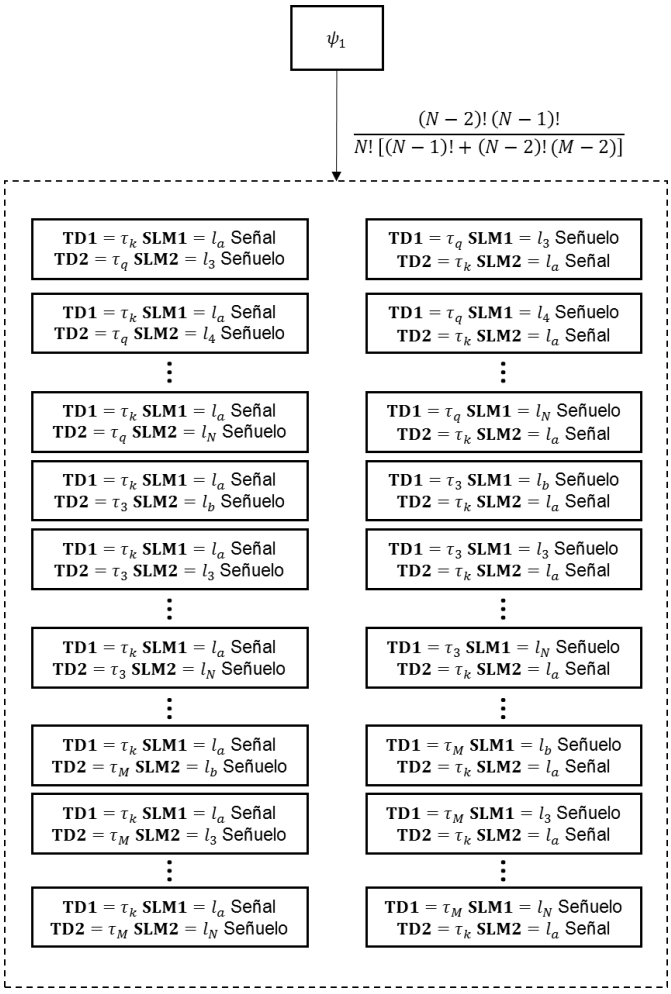

Figura 36. *Árbol de probabilidad para la implementación del estado* ψ_1.

Para generar cada uno de los estados de las dos bases con $[\tau_k, \tau_q, l_a, l_b]$ como la clave, Alice debe usar las configuraciones resumidas en la **Tabla 5**.

Tabla 5.

Configuraciones de Alice para la generación de un estado particular. $l_a \oplus l_b = e^{il_a\varphi} + e^{il_b\varphi}$; $l_a \ominus l_b = e^{il_a\varphi} - e^{il_b\varphi}$.

Base	Estado	TD1	TD2	ϕ_1	ϕ_2	SLM1	SLM2
ψ	ψ_1	τ_k	$\tau_{m\ m=q\leftrightarrow l_n\neq l_b}^{m\neq k}$	0	0	l_a	$l_{n\ n=b\leftrightarrow\tau_m\neq\tau_q}^{n\neq a}$
	ψ_1	$\tau_{m\ m=q\leftrightarrow l_n\neq l_b}^{m\neq k}$	τ_k	0	0	$l_{n\ n=b\leftrightarrow\tau_m\neq\tau_q}^{n\neq a}$	l_a
	ψ_2	τ_k	$\tau_{m\ m=q\leftrightarrow l_n\neq l_a}^{m\neq k}$	0	0	l_b	$l_{n\ n=a\leftrightarrow\tau_m\neq\tau_q}^{n\neq b}$
	ψ_2	$\tau_{m\ m=q\leftrightarrow l_n\neq l_a}^{m\neq k}$	τ_k	0	0	$l_{n\ n=a\leftrightarrow\tau_m\neq\tau_q}^{n\neq b}$	l_b
	ψ_3	τ_q	$\tau_{m\ m=k\leftrightarrow l_n\neq l_b}^{m\neq q}$	0	0	l_a	$l_{n\ n=b\leftrightarrow\tau_m\neq\tau_k}^{n\neq a}$
	ψ_3	$\tau_{m\ m=k\leftrightarrow l_n\neq l_b}^{m\neq q}$	τ_q	0	0	$l_{n\ n=b\leftrightarrow\tau_m\neq\tau_k}^{n\neq a}$	l_a
	ψ_4	τ_q	$\tau_{m\ m=k\leftrightarrow l_n\neq l_a}^{m\neq q}$	0	0	l_b	$l_{n\ n=a\leftrightarrow\tau_m\neq\tau_k}^{n\neq b}$
	ψ_4	$\tau_{m\ m=k\leftrightarrow l_n\neq l_a}^{m\neq q}$	τ_q	0	0	$l_{n\ n=a\leftrightarrow\tau_m\neq\tau_k}^{n\neq b}$	l_b
ξ	ξ_1	τ_k	τ_q	0	0	$l_a \oplus l_b$	$l_a \oplus l_b$
	ξ_1	τ_q	τ_k	0	0	$l_a \oplus l_b$	$l_a \oplus l_b$
	ξ_2	τ_k	τ_q	0	π	$l_a \oplus l_b$	$l_a \oplus l_b$
	ξ_2	τ_q	τ_k	π	0	$l_a \oplus l_b$	$l_a \oplus l_b$
	ξ_3	τ_k	τ_q	0	0	$l_a \ominus l_b$	$l_a \ominus l_b$
	ξ_3	τ_q	τ_k	0	0	$l_a \ominus l_b$	$l_a \ominus l_b$
	ξ_4	τ_k	τ_q	0	π	$l_a \ominus l_b$	$l_a \ominus l_b$
	ξ_4	τ_q	τ_k	π	0	$l_a \ominus l_b$	$l_a \ominus l_b$

3.1.3 Detección y medición del estado (Bob). Para detectar la información enviada por Alice en los dos pares de impulsos que se muestran en la **Figura 33**, Bob utiliza dos pares de interferómetros de Mach-Zehnder (MZ) simétricos en paralelo cada uno con los dos retrasos de tiempo acordados con Alice para la clave (es decir, $\boldsymbol{\tau_k}$ y $\boldsymbol{\tau_q}$) como se indica en la **Figura 31**. En cada uno de los interferómetros se divide el haz en dos haces para hacer que cada uno de ellos impacte sobre un modulador espacial de luz (SLM) configurado de acuerdo con la base que se utiliza para la medición. Como se observa en la **Figura 37**, para lograr la detección de un estado, se debe obtener una concentración de energía en el centro (haz gaussiano) en el primer orden del patrón de difracción resultante para solo uno de los estados, para el caso del holograma del modo MAO sucede solo cuando se mide con el mismo holograma con el que se genera el estado y en el caso de la superposición de modos de MAO cuando se mide con el holograma de operación opuesta al que se genera, es decir, si se genera un estado con la suma de modos MAO se detectara un único haz gaussiano con el holograma de la resta de modos MAO. Para la medición del estado en cada una de las bases, Bob debe configurar sus dispositivos de acuerdo a como se presenta en la **Tabla 6**.

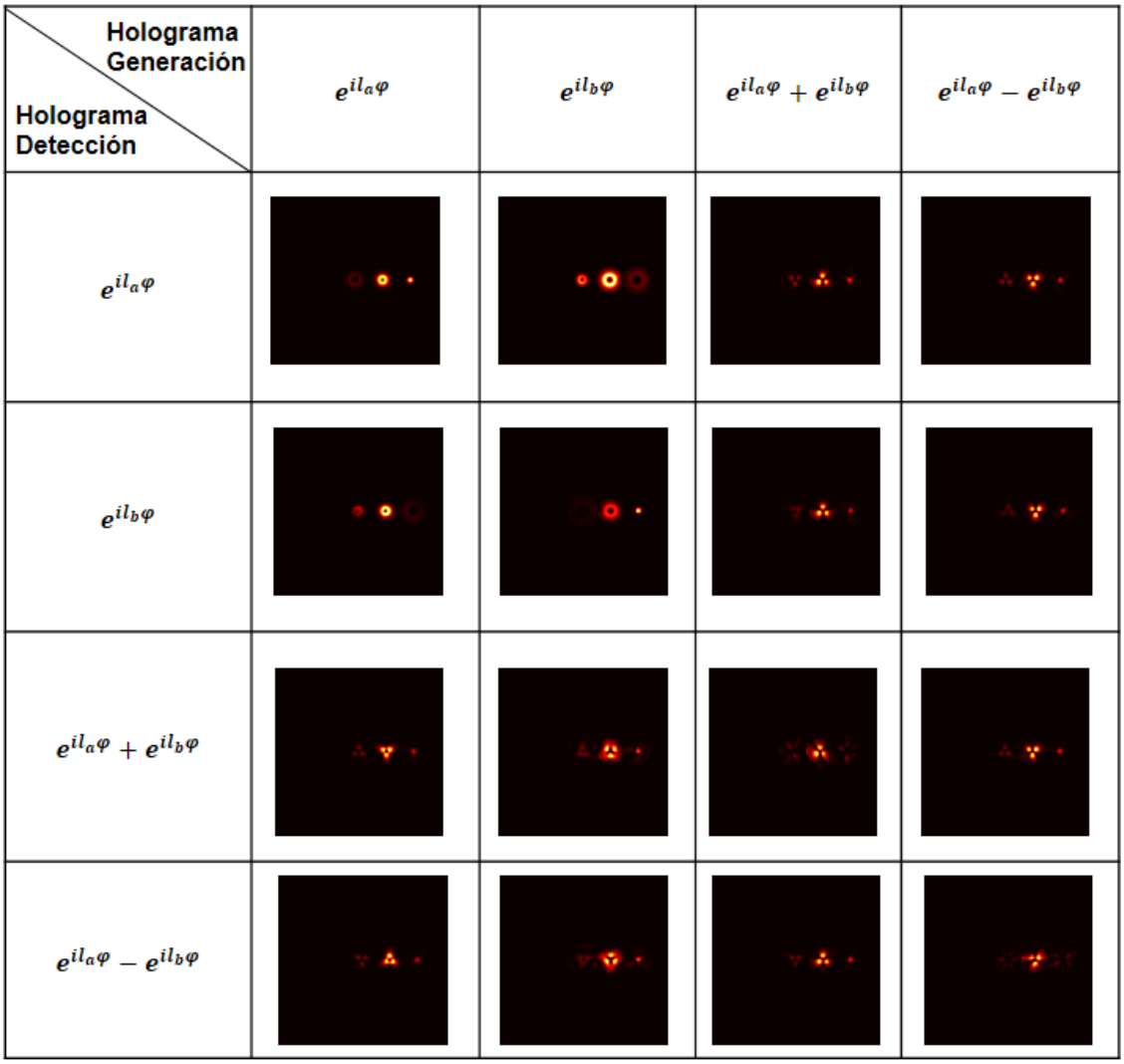

Figura 37. *Resultado de la difracción para el caso cuando $l_a = l_1 = 1$ y $l_b = l_2 = -2$. Los hologramas con los que se genera el estado (columnas) y los hologramas con los que se mide el estado (filas).*

Tabla 6.
Configuraciones de Bob para la medición de estados.

Base	SLM3	SLM4
ψ	l_a	l_b
ξ	$l_a \oplus l_b$	$l_a \ominus l_b$

Como se muestra en la **Figura 31**, el sistema de medición de Bob consta de cuatro interferómetros en paralelo, configurados por pares, cada uno de ellos con tres salidas, por ejemplo, la primera salida al detector D1 corresponde al puerto de salida vertical del primer

interferómetro, un divisor de haz está posicionado en el puerto de salida horizontal donde su salida vertical está acoplada al detector D2 y la salida horizontal al detector D3.

Para determinar un estado en la base ψ, se debe presentar el evento de un único interferómetro donde en sus puertos de salida se muestre un conteo de fotones igual a cero excepto en su segundo o tercer puerto de salida, D2 o D3, el cual muestra al menos un fotón, como se puede observar el bit en color azul en la **Tabla 7**. Para determinar un estado en la base ξ, dos eventos son posibles dependiendo del estado enviado por Alice: 1) dos interferómetros cuyos puertos de salida muestran un conteo de fotones igual a cero excepto por su segundo o tercer puerto de salida donde se muestra al menos un fotón 2) un solo interferómetro cuyos puertos de salida muestran un conteo de fotones igual a cero excepto en su segundo o tercer puerto de salida que muestra al menos un fotón y otro interferómetro en cuyos puertos de salida se muestra un conteo de fotones igual a cero excepto en su primer puerto de salida donde muestra al menos un fotón, como se puede observar el bit en color rojo en la **Tabla 7**.

De acuerdo a lo anterior, Bob en el proceso de medición solo puede determinar el estado enviado por Alice cuando elige la misma base que ella, de acuerdo con el click de cada uno de los detectores posicionados en los doce puertos de salida del sistema de detección. En el caso de que Bob no mida con la misma base, permanece en la incertidumbre entre dos estados posibles, es decir, puede descartar la medición.

Tabla 7.
Sistema de medición según los diferentes estados para una configuración de retrasos de tiempo de Alice TD1=τ_k TD2=τ_q.

Base de Alice	Estado	Base de Bob	D 1	D 2	D 3	D 4	D 5	D 6	D 7	D 8	D 9	D 10	D 11	D 12
ψ	ψ_1	ψ	**0**	**1**	**0**	1	1	0	1	0	0	0	0	0
	ψ_2		**0**	**0**	**1**	1	0	1	1	0	0	0	0	0
	ψ_3		0	0	0	1	0	0	1	1	0	**0**	**1**	**0**
	ψ_4		0	0	0	1	0	0	1	0	1	**0**	**0**	**1**
ξ	ξ_1	ψ	0	1	1	1	1	1	1	1	1	0	1	1
	ξ_2		0	1	1	1	1	1	1	1	1	1	0	0
	ξ_3		0	1	1	1	1	1	1	1	1	0	1	1
	ξ_4		0	1	1	1	1	1	1	1	1	1	0	0
ξ	ξ_1	ξ	**0**	**0**	**1**	1	0	1	1	0	1	**0**	**0**	**1**
	ξ_2		**0**	**0**	**1**	1	0	1	1	0	1	**1**	**0**	**0**
	ξ_3		**0**	**1**	**0**	1	1	0	1	1	0	**0**	**1**	**0**
	ξ_4		**0**	**1**	**0**	1	1	0	1	1	0	**1**	**0**	**0**
ψ	ψ_1	ξ	0	1	1	1	1	1	1	0	0	0	0	0
	ψ_2		0	1	1	1	1	1	1	0	0	0	0	0
	ψ_3		0	0	0	1	0	0	1	1	1	0	1	1
	ψ_4		0	0	0	1	0	0	1	1	1	0	1	1

3.2 Análisis de ataques a la seguridad del sistema (Eve).

Al igual que en el protocolo B884 se considera que un intruso (Eve) y Bob deben adivinar la base correcta para recibir información, sin embargo, esta selección aleatoria de la base permite con un 50% de probabilidad que Eve pueda obtener información al igual que Bob, por esta razón en el sistema propuesto se agrega una clave de transmisión entre Alice y Bob conformada por un par de retrasos de tiempo seleccionados de un subconjunto de M posibles retrasos de tiempo $TD = \{\tau_1, \tau_2, \tau_3, \dots, \tau_M\}$ y un par de modos MAO seleccionados de un subconjunto de N posibles modos MAO $OAM = \{l_1, l_2, l_3, \dots, l_N\}$. En consecuencia, se asume que Eve conoce el algoritmo de encriptación o funcionamiento general del sistema de comunicación, es decir, conoce los M

posibles retrasos y los N posibles modos MAO, pero no el par de retrasos de tiempo y el par de modos MAO acordados por Alice y Bob $[\tau_k, \tau_q, l_a, l_b]$ como semilla para la ejecución del protocolo.

Debido a que Eve posee dispositivos ideales y cuenta con toda la tecnología necesaria para toda variedad de posibles ataques, en este trabajo se analiza la seguridad del sistema ante un ataque por interceptación del canal que consta de dos etapas, donde en cada una de ellas el objetivo es determinar el estado del fotón, es decir, la clave, para así obtener información y ocultar su presencia. En la **Figura 38**, se observa que en la primera etapa del ataque para la medición en cualquier base, Eve utiliza interferómetros de Mach-Zehnder simétricos en paralelo configurados con uno de los M posibles retrasos de tiempo que componen la clave de transmisión entre Alice y Bob, una vez que ella determina el primer retraso de tiempo correcto τ_k, procede a realizar mediciones del modo MAO con un conjunto de N posibles modos, de acuerdo al resultado de esta medición Eve puede determinar en qué base fue preparado el estado. Si Eve obtiene solo un posible modo MAO corresponde al caso de la primera base ψ (a la izquierda de la línea punteada) y si Eve obtiene dos posibles modos MAO corresponde a la base ξ (a la derecha de la línea punteada), logrando determinar el modo MAO correcto l_a para el primer caso y los modos MAO correctos l_a y l_b en el otro caso.

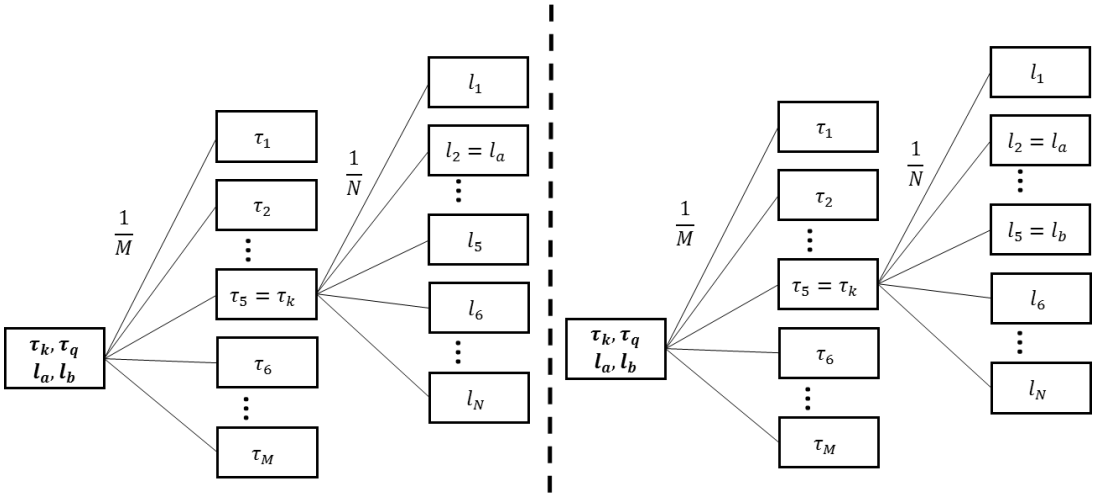

Figura 38. *Árbol de probabilidad de la primera etapa del ataque de Eve.*

Dado que Eve sabe que la clave está conformada por un par de retrasos de tiempo diferentes y un par de modos MAO diferentes, en la segunda etapa del ataque descarta el interferómetro asociado al retraso de tiempo determinado en la primera etapa τ_k, por lo cual utiliza solo (M-1) interferómetros de Mach-Zehnder simétricos en paralelo. Una vez que determina el segundo retraso de tiempo correcto τ_q, procede a realizar mediciones del modo MAO, como se muestra en la **Figura 39**, para la base ψ Eve utiliza un subconjunto de (N-1) modos posibles, descartando el modo MAO l_a determinado en la primera etapa (a la izquierda de la línea punteada) y para la base ξ utiliza un subconjunto de las tres posibles superposiciones del par de modos MAO determinados en la primera etapa (a la derecha de la línea punteada).

En consecuencia para las dos bases Eve logra determinar el par de retrasos de tiempo y el par de modos MAO y a partir de esta información para el caso de la base ξ ella puede detectar correctamente el estado, sin embargo para el caso de la base ψ ella tiene dos posibles valores de estado, por lo cual, debe decidir al azar, es decir, tiene un 50% de probabilidad de detectar el estado correcto.

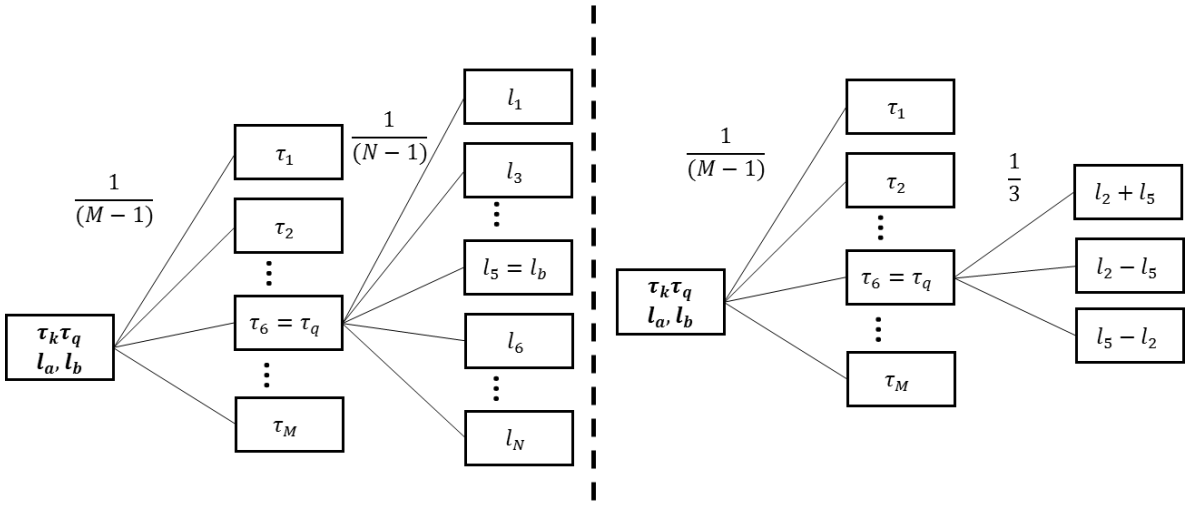

Figura 39. *Árbol de probabilidad de la segunda etapa del ataque de Eve.*

En la **Figura 40** se presenta el esquema de medición para la implementación de este tipo de ataque, el cual se analiza considerando el modelo estocástico utilizado para el sistema de comunicación basado en la modulación de coherencia al nivel de conteo de fotones, teniendo en cuenta que para este caso Eve presenta M interferómetros, un interferómetro para cada uno de los M posibles retrasos de tiempo para Alice y Bob, donde cada puerto de salida tiene una probabilidad de conteo de fotones igual a $\frac{1}{2M}$ excepto el puerto de salida del interferómetro donde el retraso coincide con el utilizado por Alice en la clave que tiene una probabilidad asociada igual a $\frac{1}{M}$ y el puerto de salida complementario a este que tiene una probabilidad igual a cero. Para el modelo, se consideran los interferómetros con dos puertos de salida. En el puerto de salida correcto, Eve utiliza una cascada de divisores de haz para realizar mediciones del modo MAO.

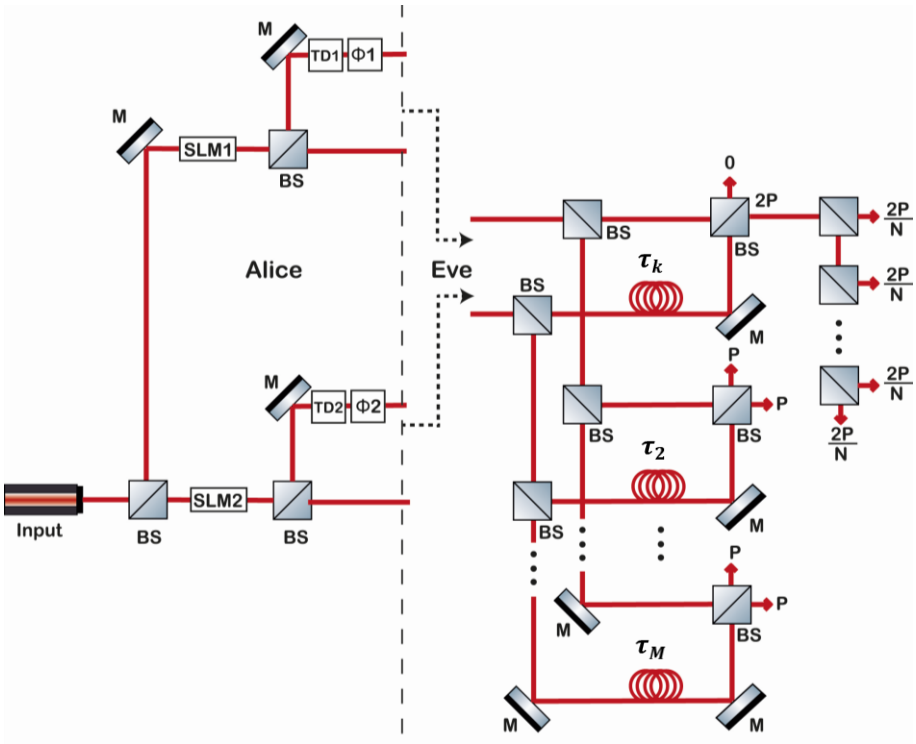

Figura 40. *Esquema óptico de Eve para atacar el sistema.*

Del modelo anterior, se analiza el ataque más simple que corresponde al evento mostrado en la **Figura 41**, donde en la primera etapa Eve obtiene al menos un fotón en cada uno de los puertos de salida excepto en un puerto del interferómetro con el retraso de tiempo τ_k donde se obtiene un conteo de fotones igual a cero y en el puerto complementario al realizar la medición de modos MAO, se obtiene al menos un fotón en la salida l_a.

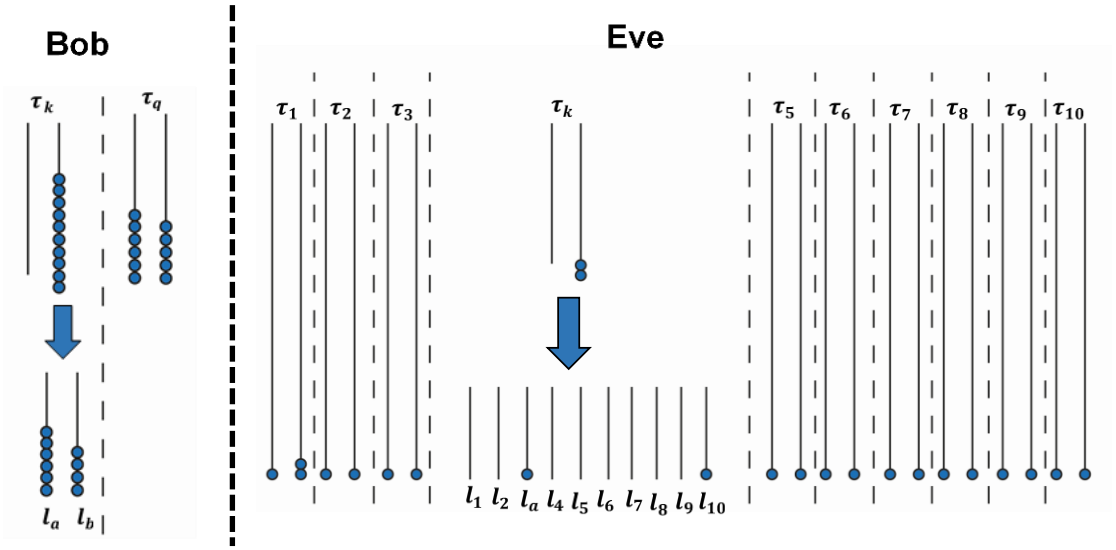

Figura 41. *Ejemplo de una realización para Bob e Eve del evento de la primera etapa del ataque, para M = 10 posibles retrasos de tiempo y N = 10 modos OAM posibles, para el envío de un elemento con 21 fotones por Alice. Cada bola azul es una representación gráfica de un fotón.*

En la segunda etapa el evento de interés corresponde a obtener al menos un fotón en cada uno de los puertos de salida excepto en un puerto del interferómetro con el retraso de tiempo τ_q donde se obtiene un conteo de fotones igual a cero, sin embargo para este caso se tienen 2(M -1) puertos, ya que el interferómetro asociado con el retraso de tiempo τ_k encontrado en la primera etapa se descarta, además el número de puertos para la medición de modos MAO también se reduce a (N-1) para el caso de la base ψ como se observa en la **Figura 42** y se reduce a solo tres para el caso de la base ξ como se observa en la **Figura 43**.

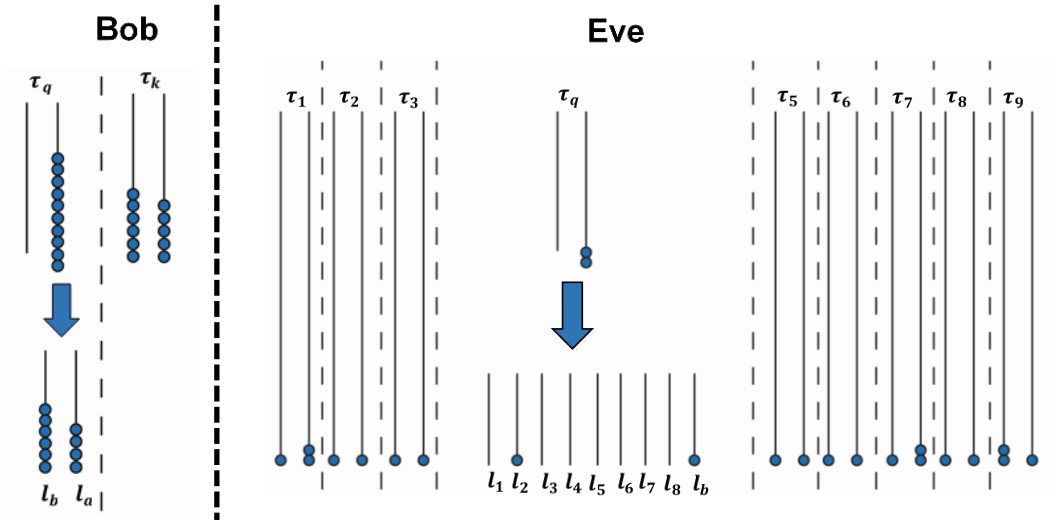

Figura 42. *Ejemplo de una realización para Bob e Eve del evento de la segunda etapa del ataque para el caso de la base ψ, con $M = 9$ posibles retrasos de tiempo y $N = 9$ posibles modos MAO, para el envío de un elemento con 21 fotones por Alice. Cada bola azul es una representación gráfica de un fotón.*

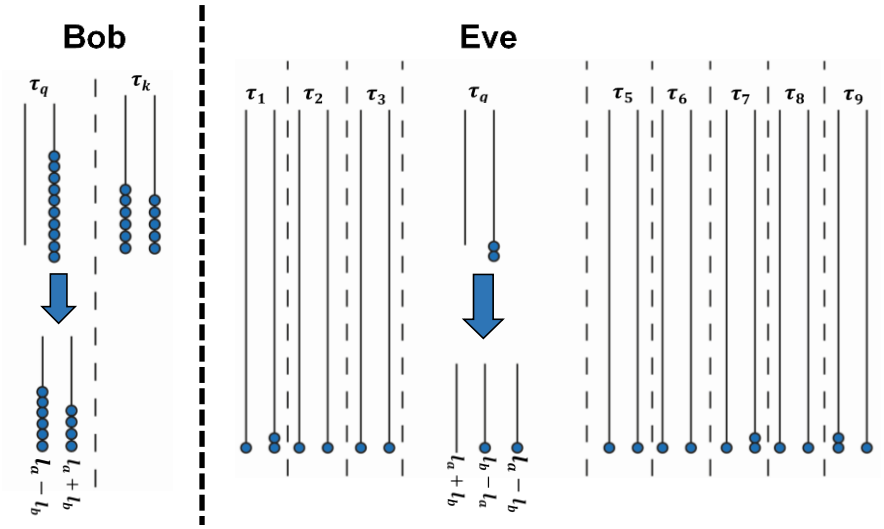

Figura 43. *Ejemplo de una realización para Bob e Eve del evento de la segunda etapa del ataque para el caso de la base ξ, con $M = 9$ posibles retrasos de tiempo y $N = 3$ posibles modos MAO, para el envío de un elemento con 21 fotones por Alice. Cada bola azul es una representación gráfica de un fotón.*

Debido a que la ocurrencia del evento en la segunda etapa del ataque se encuentra condicionado a la ocurrencia del evento en la primera etapa, se considera el ataque resultante como la ocurrencia de ambos eventos (intersección). En la **Figura 44** se presentan los resultados del cálculo de la probabilidad de Eve de identificar correctamente el par de retrasos de tiempo y

el par de modos MAO para el caso de un estado de la base ψ con 10 posibles retrasos de tiempo y 10 posible modos MAO, mediante la simulación de Monte Carlo del modelo estocástico propuesto. Se observa que Eve requiere al menos 200 fotones en promedio para lograr una probabilidad igual a 0.3147 de determinar la clave. Adicionalmente a medida que aumenta el número de fotones su probabilidad nunca supera el 50%.

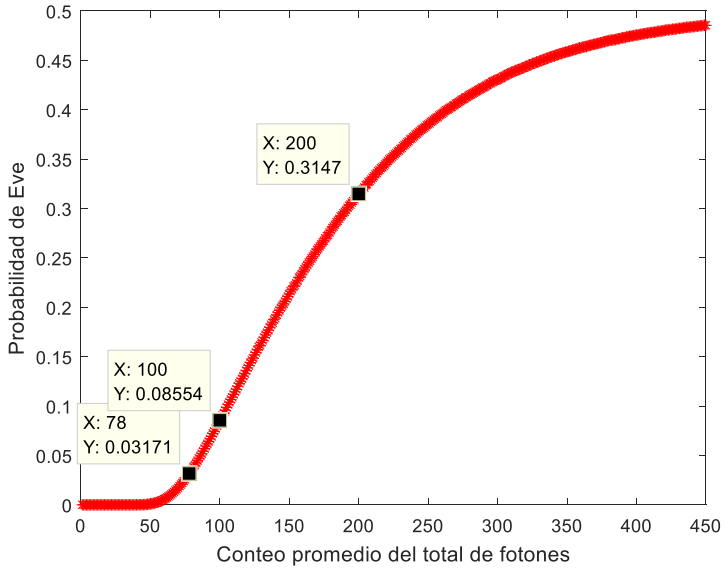

Figura 44. *Resultados del cálculo de la probabilidad de Eve mediante el ataque por interceptación del canal para el caso de la base ψ, en función del conteo promedio total de fotones para M= 10 y N=10, a partir de la simulación de Monte Carlo con trial=1000 y Ns=500.*

En la **Figura 45** se presentan los resultados del cálculo de la probabilidad de Eve de identificar correctamente el par de retrasos de tiempo y el par de modos MAO para el caso de un estado de la base ξ con 10 posibles retrasos de tiempo y 10 posible modos MAO, mediante la simulación de Monte Carlo del modelo estocástico propuesto. Se observa que Eve requiere al menos 130 fotones en promedio para lograr una probabilidad mayor al 50% de determinar la clave y el estado enviado por Alice.

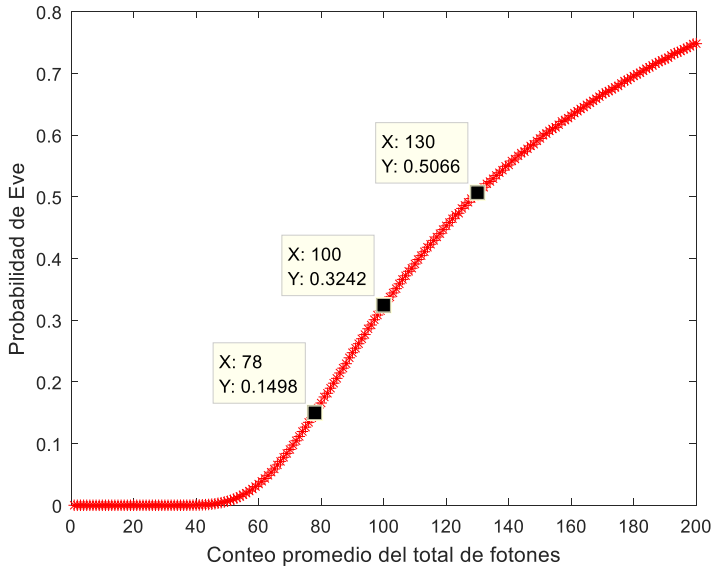

Figura 45. *Resultados del cálculo de la probabilidad de Eve mediante el ataque por interceptación del canal para el caso de la base ξ, en función del conteo promedio total de fotones para M= 10 y N=10, a partir de la simulación de Monte Carlo con trial=1000 y Ns=500.*

De acuerdo a lo anterior, 32.42% es la mayor probabilidad de éxito que presenta Eve al operar el sistema de comunicación con una fuente de 100 fotones en promedio, 10 posibles retrasos de tiempo y 10 posibles modos MAO, lo cual evidencia la mejora en la seguridad del sistema en comparación con un sistema de comunicación basado en modulación de coherencia al funcionar bajo las mismas condiciones, ya que para este caso Eve presenta 98.88% de probabilidad de éxito.

Con base en el esquema de detección de la **Figura 31** y siguiendo el protocolo BB84, para determinar el estado enviado por Alice, Bob requiere la ocurrencia del evento, donde se obtiene al menos un fotón en cada uno de los puertos de salida de los interferómetros excepto en un puerto del interferómetro con el retraso de tiempo correcto donde se obtiene un conteo de fotones igual a cero, por lo cual se analiza la probabilidad de ocurrencia de este evento en función del conteo de fotones promedio, para 2 posibles retrasos de tiempo y 2 posibles modos MAO como se muestra en la **Figura 46**. Se observa que Bob requerirá al menos 39 fotones en promedio para

lograr una probabilidad igual a 1 de detectar siempre los retrasos de tiempo correctos y los modos MAO enviados por Alice, es decir, el estado cuando selecciona la base correcta.

Finalmente se encuentra que Alice y Bob requieren operar el sistema con una fuente con un promedio de 78 fotones para un correcto funcionamiento y una baja amenaza a la seguridad, ya que con este nivel de fotones, Eve máximo presenta una probabilidad de éxito con un ataque por interceptación del canal de 14.98%.

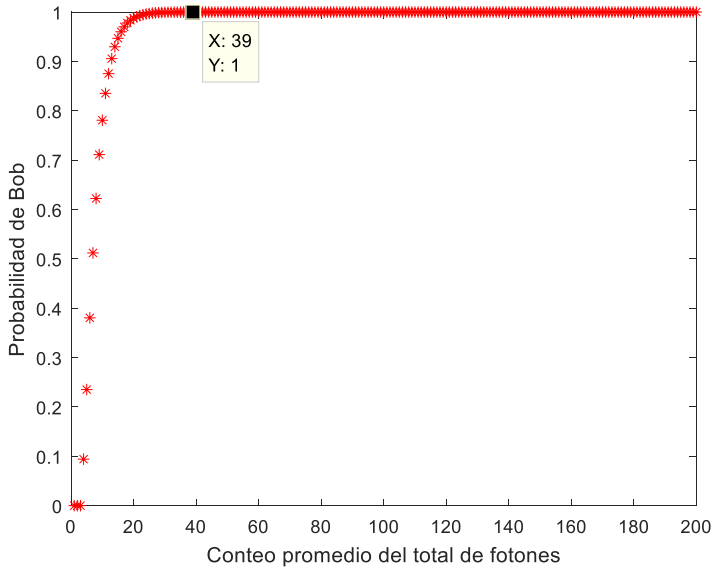

Figura 46. *Resultados del cálculo de la probabilidad de Bob en función del conteo promedio total de fotones para M= 2 y N=2, a partir de la simulación de Monte Carlo con trial=1000 y Ns=500.*

3.3 Cadencia del sistema

Ignorando errores causados por las pérdidas debidas a las eficiencias ópticas y de detección en el sistema es posible analizar la cantidad de información para el caso ideal, de acuerdo a la teoría de la información de Shannon (Thomas & Joy, 2006) en la que: Se tiene un sistema donde la fuente

o el destino cuentan con un rango de estados posibles $x_1, \dots, x_N$ para el alfabeto, cuyas probabilidades de ocurrencia respectivas son $p(x_1), \dots, p(x_N)$, y donde la cantidad de información generada en la fuente o detectada en el destino por la aparición de x_k esta dada por la Ecuación 37 en términos de bits. A su vez estos producen una secuencia de estados (mensaje), donde la cantidad promedio de información producida en la fuente o recibida en el destino denominada como la entropía está dada por la Ecuación 38 (Thomas & Joy, 2006).

$$I(x_k) = -\log_2(p(x_k)) \tag{37}$$

$$H(X) = H(Y) = -\sum_{k=1}^{N} p_k \log_2(p_k) \tag{38}$$

La cantidad promedio de información generada en la fuente X y recibida en el destino Y, denominada información mutua está dada por la Ecuación 39, donde $p(x,y)$ es la probabilidad conjunta de que x sea transmitido y y sea recibido, $p(x)$ es la probabilidad de que la fuente seleccione el símbolo x para transmitir, $p(y)$ es la probabilidad de que el símbolo y haya sido recibido en el destino y N_e la cantidad de estados por base. El máximo valor de información mutua cuando se consideran todas las posibles distribuciones de la probabilidad de la variable x se define como la capacidad del canal como se muestra en la Ecuación 40 (Thomas & Joy, 2006).

$$I(X;Y) = \sum_{x,y} p(x,y)\, log_2\left(\frac{p(x,y)}{p(x)p(y)}\right) = log_2(N_e) \tag{39}$$

$$C = \max_{p(x)} I(X;Y) \tag{40}$$

En vista de lo anterior y como se muestra en el esquema de codificación de la **Tabla 8**, el sistema propuesto de cuatro estados (N_e=4) utilizado para codificar la información presenta una

cantidad de información máxima transferida igual a 2 bits siendo mayor al caso del sistema BB84 clásico donde se tiene una cantidad de información máxima de 1 bit, dado que cada portador de este nuevo sistema contiene más información y por lo tanto aumenta el flujo de información correspondiente a una mayor tasa de creación de claves o mayor capacidad en el canal.

Tabla 8.
Esquema de codificación de bits.

Base	Estado	Bits
ψ	ψ_1	00
	ψ_2	01
	ψ_3	10
	ψ_4	11
ξ	ξ_1	00
	ξ_2	01
	ξ_3	10
	ξ_4	11

4 Principios para la implementación del sistema de comunicación basado en la modulación de coherencia y el momento angular orbital.

Un sistema de comunicación está conformado por tres partes principales: un transmisor (encargado de enviar y codificar el mensaje), un canal (medio utilizado para transmitir la señal del transmisor al receptor) y un receptor (encargado de recibir y reconstruir el mensaje), donde para el caso del esquema de comunicación propuesto basado en modulación de coherencia y

momento angular orbital corresponden a un módulo denominado Alice, el espacio libre y un módulo denominado Bob respectivamente. Para la implementación del sistema propuesto estos módulos requieren de una óptica que permita la generación de haces con bajo número de fotones, la interferometría, la modulación de fase, la generación y detección de haces con momento angular orbital y la detección o conteo de fotones. Por esta razón este capítulo proporciona una descripción y caracterización de los dispositivos ópticos y la tecnología disponible en el laboratorio de óptica de la escuela de Física para una futura implementación del esquema de comunicación propuesto.

4.1 Detección y conteo de fotones

Para las pruebas experimentales se acondiciona el laboratorio de óptica de la Escuela de Física de la UIS para trabajar en un espacio suficientemente oscuro con el mayor control posible de fuentes de luz no deseadas (LED, filtración de luz por orificios de ventanas y puertas, etc.), en una mesa óptica y en horas de la noche, con el fin de tener la menor incidencia de ruido tanto óptico como mecánico en el sistema.

Los contadores de fotones individuales se utilizan para aplicaciones donde los detectores tradicionales como el medidor de potencia óptica, no pueden discernir la diferencia entre la señal y el ruido. Estos módulos funcionan convirtiendo un fotón incidente en un pulso eléctrico y se caracterizan por propiedades como (Chunnilall, Degiovanni, Kück, Müller, & Sinclair, 2014; Stipčević, Wang, & Ursin, 2013):

- El tiempo muerto (Dead time): es el tiempo que tarda el detector en estar listo para detectar el próximo fotón. Está principalmente determinado por la electrónica empleada. El par

de detectores COUNT 1000-S del fabricante Laser Components utilizados presentan un tiempo muerto igual a 1.12 [ns] y 1.5 [ns].

- Tasa de conteo en la oscuridad (Dark count rate): es la tasa promedio de cuentas, ocasionadas por avalanchas o pulsos que aparecen en ausencia de cualquier luz incidente en el fotodiodo de avalancha SPAD. El par de detectores utilizados presentan una tasa de 846 [c/s] y 910 [c/s].
- Eficiencia de detección de fotones (Photon detection efficiency): es la probabilidad de que el detector genere un pulso de salida digital correspondiente a un solo fotón entrante. El par de detectores utilizados presentan una eficiencia de detección del 70% y 51% a 405 [nm] y al 55% y 52% a 670 [nm].

En la **Figura 47**, se presenta una forma de pulso típica de la señal de salida TTL del módulo contador de fotones de aproximadamente 2 [V] de amplitud como se observa en la gráfica en amarillo, la cual se convierte en la señal de salida de 5 [V] de amplitud en azul verdoso, como resultado de la amplificación de la misma mediante un circuito como el que se muestra en la **Figura 48**. Posteriormente la señal de pulsos amplificada se conecta a un contador externo implementado mediante Arduino y Python, para realizar la adquisición y almacenamiento de la tasa de conteo del detector.

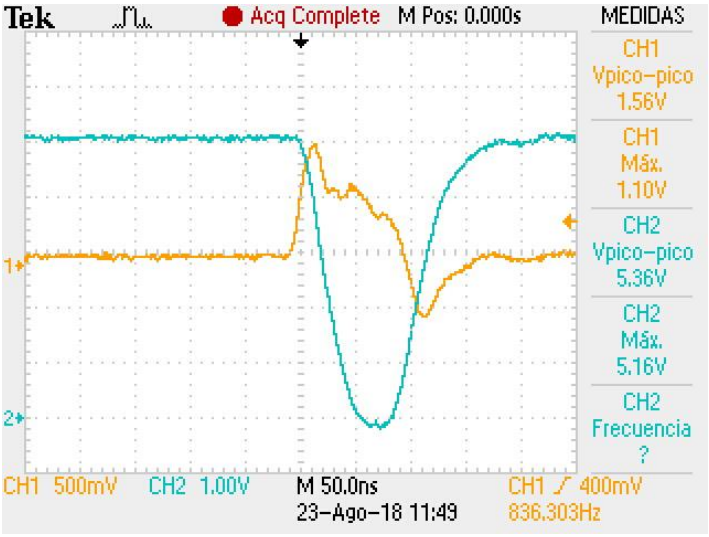

Figura 47. *Pulso señal TTL salida del contador de fotones (amarillo) y amplificado (azul verdoso).*

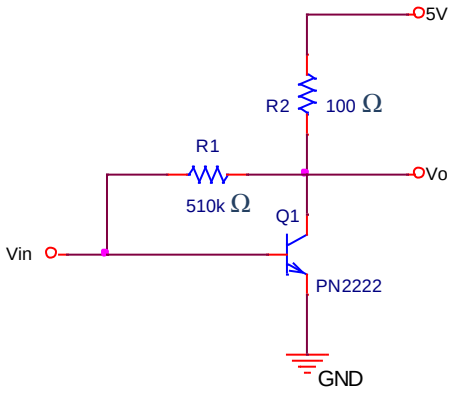

Figura 48. *Circuito amplificador para la señal TTL del contador de fotones.*

Previamente al proceso de adquisición de los datos se toma en cuenta que la estadística de detección de los fotones corresponde a una distribución de Poisson (Fox, 2006), lo cual se verifica mediante la prueba de bondad de ajuste de Chi-cuadrado que se puede aplicar a distribuciones discretas (Douglas C. & George C., 2003; NIST/SEMATECH, 2012). Para determinar si la tasa de conteo de fotones sigue una distribución de Poisson, las hipótesis nula y alternativa planteadas son:

H0: la tasa de conteo de fotones sigue una distribución de Poisson

H1: la tasa de conteo de fotones no sigue una distribución de Poisson

Dado que el parámetro lambda (media) de la distribución de Poisson asumida es desconocido, se estima a partir de los datos de muestra y con este valor, mediante MATLAB se genera una distribución de Poisson teórica. Esta distribución junto con el conjunto de datos experimentales se utilizan como parámetros de entrada de la función chi2gof() que permite llevar a cabo la prueba de Chi-cuadrado, donde se encuentra que para un nivel de significancia de 0.01 la tasa de conteo de fotones se ajusta bien a una distribución de Poisson para cada uno de los casos, ya que no se rechaza la hipótesis nula, a su vez este resultado permite definir que la cantidad de muestras mínima necesaria es igual a 100 para el análisis estadístico en cada uno de los experimentos. En la **Figura 49** se muestra el histograma comparado con la distribución de Poisson teórica para uno de los experimentos realizados.

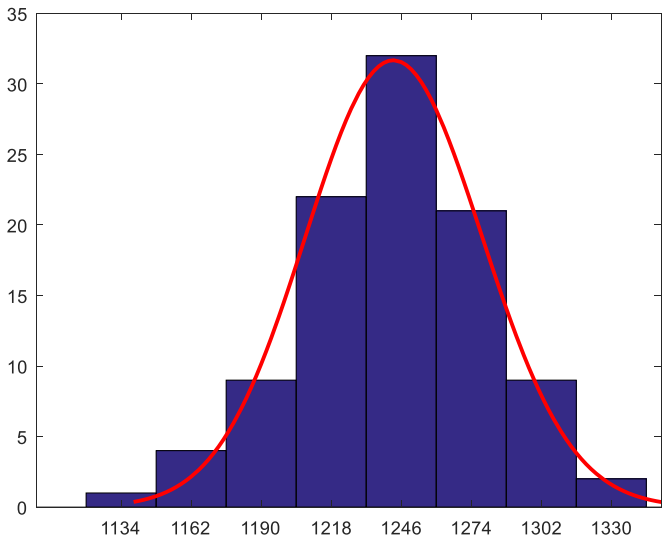

Figura 49. *Histograma y curva de probabilidad de la tasa de conteo con el contador de fotones H0490 en operación y abierto.*

Se realizan pruebas con el contador de fotones en operación y cerrado, es decir, en ausencia de cualquier luz incidente para verificar la tasa de conteo en la oscuridad asociada a ruido térmico y electrónico del sistema. En la **Figura 50**, se observan los resultados obtenidos, donde

para el contador H0490 la media es 876 [fotones/s] con un desviación estándar de 28 [fotones/s] y para el contador H0491 la media es 972 [fotones/s] con un desviación estándar de 32 [fotones/s], lo cual evidencia que en comparación a la tasa de conteo en la oscuridad dada por el fabricante se tienen aproximadamente 30 [fotones/s] y 62 [fotones/s] más en promedio respectivamente, lo cual se debe a variaciones en las condiciones del ambiente de medida. Adicionalmente estas tasas de conteo corresponden a la tasa de conteo mínima a la cual la señal es causada predominantemente por fotones reales en el contador.

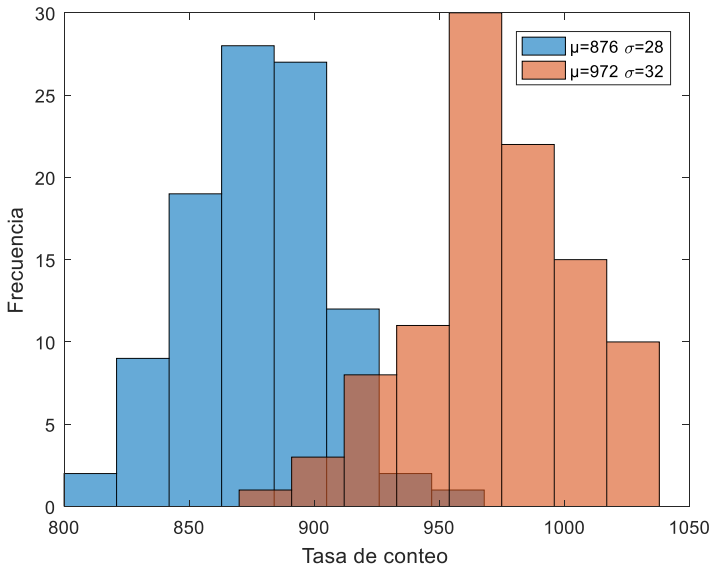

Figura 50. *Histograma de la tasa de conteo con el contador de fotones H0490 (azul) y H0491 (rojo) en operación y cerrado.*

En la **Figura 51**, se observan los resultados obtenidos cuando el contador de fotones se encuentra en operación y abierto bajo la incidencia de cualquier luz del ambiente, donde para el contador H0490 la media es 1243 [fotones/s] con una desviación estándar de 38 [fotones/s] y para el contador H0491 la media es 1603 [fotones/s] con una desviación estándar de 41 [fotones/s], lo cual permite determinar el ruido asociado al ambiente del laboratorio, siendo en promedio 367 y 631 [fotones/s] mayor al caso cuando el contador se encuentra en operación y cerrado.

Adicionalmente se encuentra que el detector es estable a través del tiempo a partir de 4 realizaciones, para el caso cuando el detector está en operación y cerrado como se muestra en la **Figura 52** y para el caso cuando el detector está en operación y abierto en la **Figura 53**, ya que para ambos casos la media de los datos no varía en gran medida y se mantiene en un mismo rango.

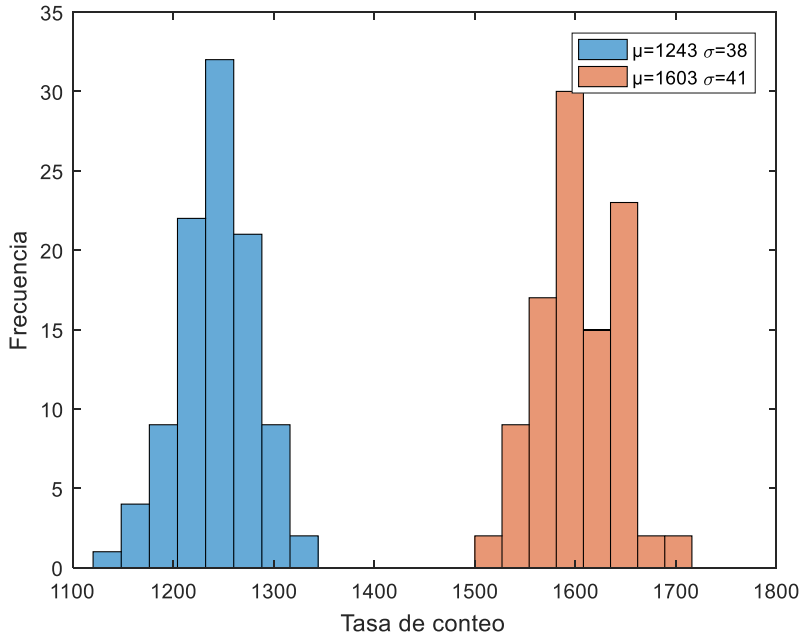

Figura 51. *Histograma de la tasa de conteo con el contador de fotones H0490 (azul) y H0491 (rojo) en operación y abierto.*

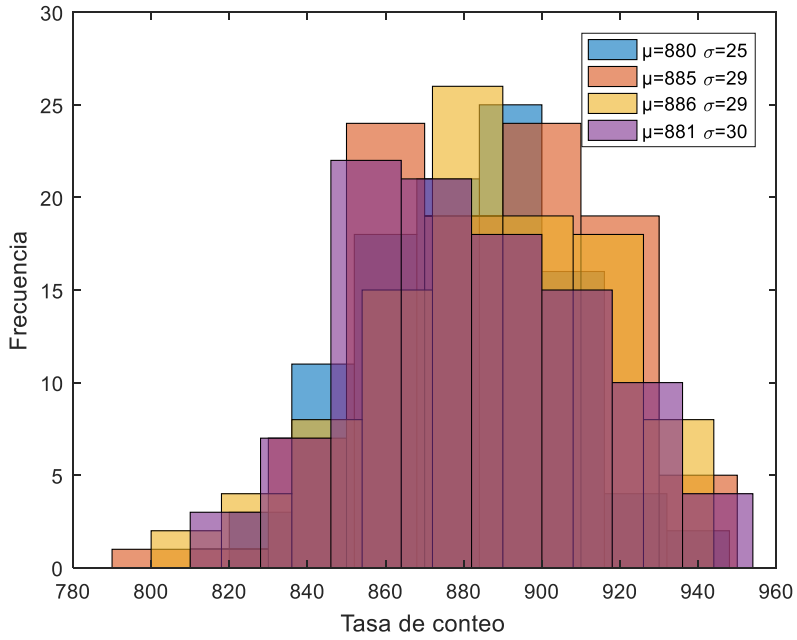

Figura 52. *Histograma de 4 realizaciones experimentales de la tasa de conteo con el contador de fotones H0490 en operación y cerrado.*

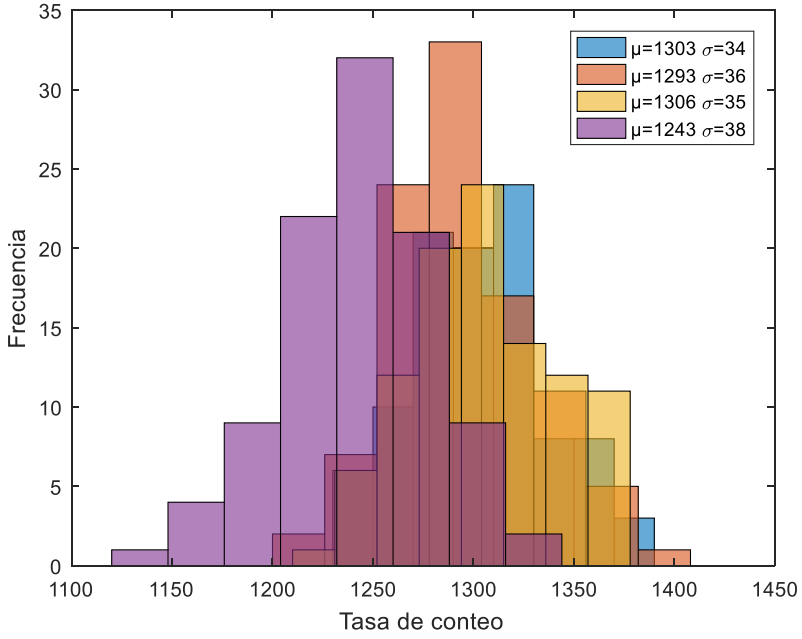

Figura 53. *Histograma de 4 realizaciones experimentales de la tasa de conteo con el contador de fotones H0490 en operación y abierto.*

4.2 Generación de bajo número de fotones

Se procede a realizar la caracterización a nivel de conteo de fotones de cada uno de los dispositivos ópticos que conforman un interferómetro de Mach- Zehnder, primero se analiza la fuente láser, después un divisor de haz y finalmente un espejo, a partir del montaje experimental que se presenta en la **Figura 54**.

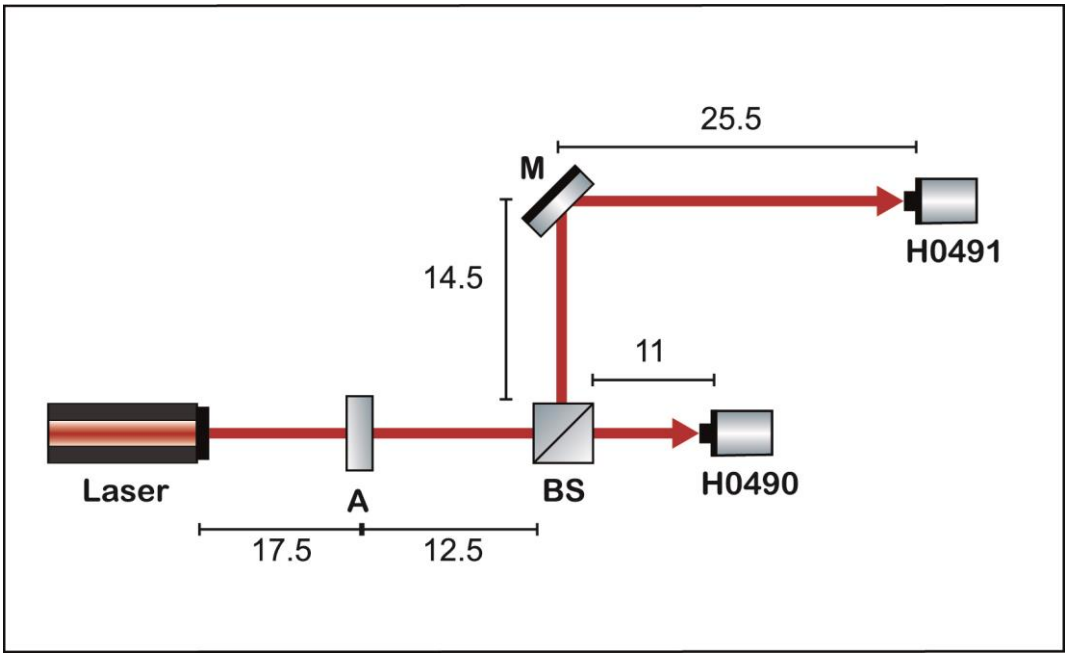

Figura 54. *Esquema del montaje experimental para la caracterización de los dispositivos que conforman un interferómetro de Mach-Zehnder. Unidades en centímetros.*

4.2.1 Caracterización de la fuente láser. Se hace incidir un haz láser He-Ne de 632,8 [nm] sobre un fotodetector, por medio del cual se obtienen las medidas de potencia óptica del haz láser que se resumen en la **Tabla 9**.

Tabla 9.
Datos de potencia óptica promedio y su desviación estándar para el haz láser.

Potencia [mW]	Desviación [nW]
1,698	138
1,698	70,7
1,698	28,6
1,698	99,9
1,698	100

De acuerdo a lo anterior se encuentra que la potencia promedio del láser a utilizar es igual a 1,698 [mW] para una área de detección de 1 [cm^2], por lo cual la cantidad de fotones por segundo que corresponde a dicho valor de potencia óptica es $5{,}406x10^{15}$ [fotones/s], de acuerdo a la Ecuación 41, donde P es la potencia óptica en vatios y λ es la longitud de onda en nanómetros. En la **Figura 55**, se observa la gráfica del número de fotones en función de la potencia óptica para una longitud de onda de 632,8 [nm] (Fox, 2006; Hodges & Grabher, 2014).

$$N(\lambda) = 5{,}03x10^{15} * \lambda * P \tag{41}$$

Un haz gaussiano es un haz de radiación electromagnética monocromática cuyo perfil en intensidad transversal se puede describir con una función de Gauss, es decir, el diámetro nominal del haz no incluye el 100% de la potencia, por lo tanto se tiene que la potencia P que pasa a través de un círculo de radio r en el plano transversal en la posición z está dada por la Ecuación 42, donde P_0 corresponde a la potencia total transmitida por el haz, r es el radio de la apertura y w(z) es el radio del haz a la distancia z, que a su vez corresponde en la curva de intensidad a la distancia desde el eje del haz donde la intensidad cae a 1 / e^2 (≈ 13.5%) del valor máximo como se observa en la **Figura 56** (CVI Melles Griot, 2009; Kogelnik & Li, 1966).

$$P(r,z) = P_0\left[1 - \exp\left(\frac{-2r^2}{w^2(z)}\right)\right] \tag{42}$$

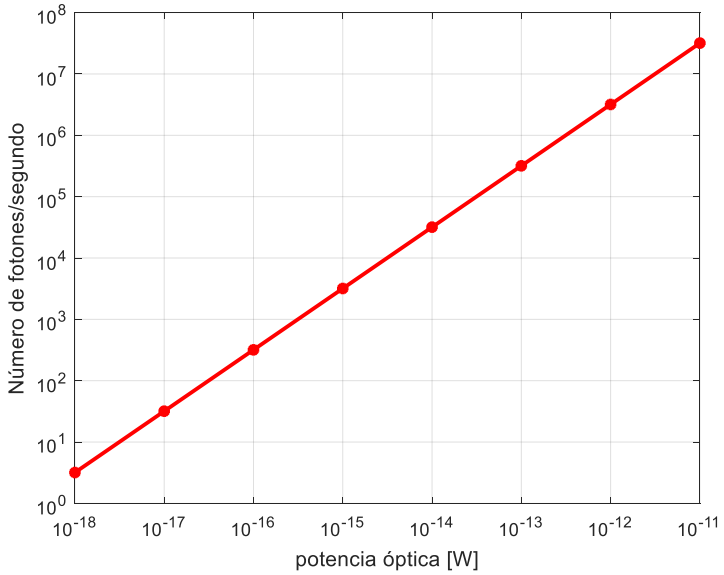

Figura 55. *Curva del número de fotones incidentes en función de la potencia óptica para una longitud de onda de 632,8 [nm].*

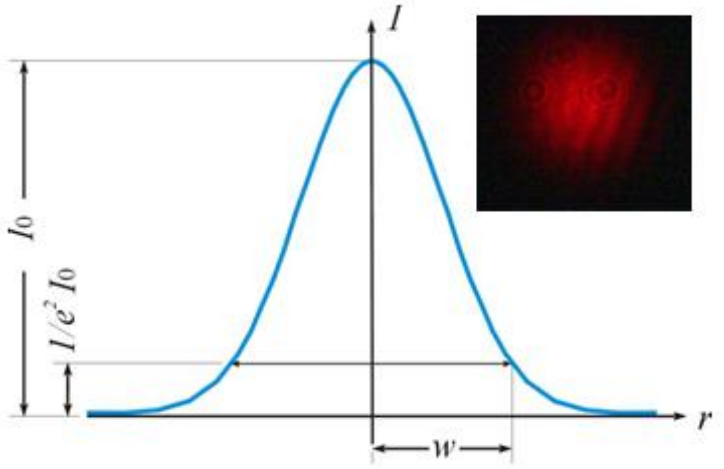

Figura 56. *Perfil de intensidad transversal de un haz gaussiano.*

Teniendo en cuenta que el contador de fotones presenta un diámetro de área activa de 0,5 [mm] y el haz láser presenta una potencia total transmitida igual a 1,698 [mW] y un radio aproximadamente igual a 0,75 [mm], a partir de la ecuación 42 se obtiene que la potencia vista por el contador de fotones a una distancia de 41 [cm] es igual a 0,338[mW].

Los filtros de densidad neutra (ND) están diseñados para reducir la transmisión de manera uniforme en una porción del espectro. Los filtros ND normalmente se definen por su densidad

óptica (OD) que describe la cantidad de energía bloqueada por el filtro (Edmund Optics, 2012). Para este trabajo se apilaron tres filtros con densidades ópticas de 4, 2.5 y 4, para lograr una densidad óptica final del sistema igual a 10,5, la cual de acuerdo a la ecuación 43 permite obtener una transmitancia igual a $3{,}16x10^{-9}$%.

$$T = 10^{-OD} x\, 100 \tag{43}$$

Se hace incidir el láser sobre el conjunto de atenuadores y se mide la tasa de conteo en diferentes posiciones horizontales con el contador H0491 y se mantiene al contador H0490 realizando medición del ambiente como se muestra en la **Figura 57** y **Figura 58** respectivamente, donde se puede observar que las condiciones del ambiente fueron bastantes estables. Adicionalmente a partir del promedio de cada uno de los histogramas se obtiene el perfil de intensidad del haz que se presenta en la **Figura 59**, el cual se ajusta con un parámetro R^2=0,9884 a una función gaussiana cuadrática $ae^{-2\left(\frac{x-b}{c}\right)^2}$ con a=35700, b=0,008105 y $c=0{,}6146x10^{-3}$.

De acuerdo al valor de potencia obtenido para el área del contador y la atenuación aplicada se encuentra a partir de la ecuación 41 que la cantidad de fotones por segundo teórica para el haz láser es igual a 34067 [fotones/s] y la cantidad de fotones obtenida experimental es igual a 36388 como se observa en la **Figura 59**. Conviene señalar que la señal generalmente se acompaña de ruido aleatorio térmico de promedio no nulo.

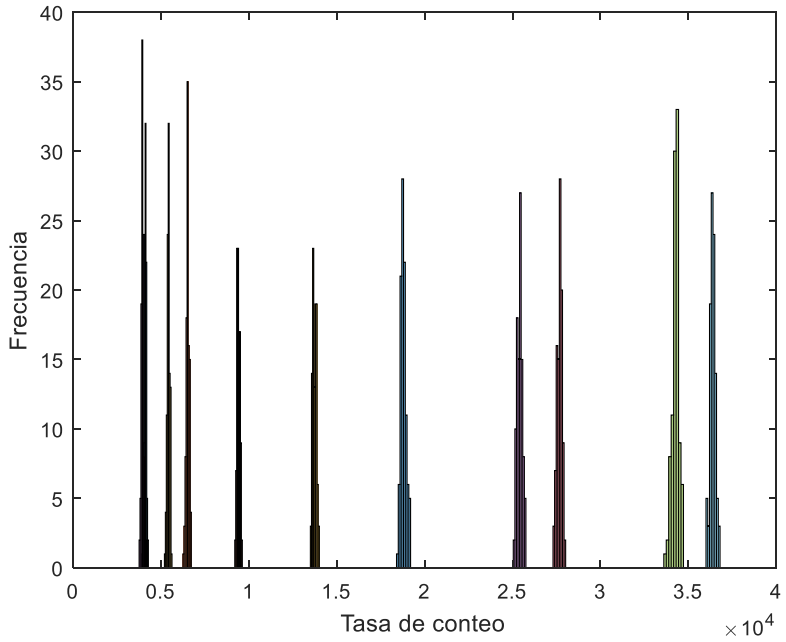

Figura 57. *Histograma de la tasa de conteo con el contador de fotones H0491 bajo la incidencia del haz láser a diferentes posiciones horizontales.*

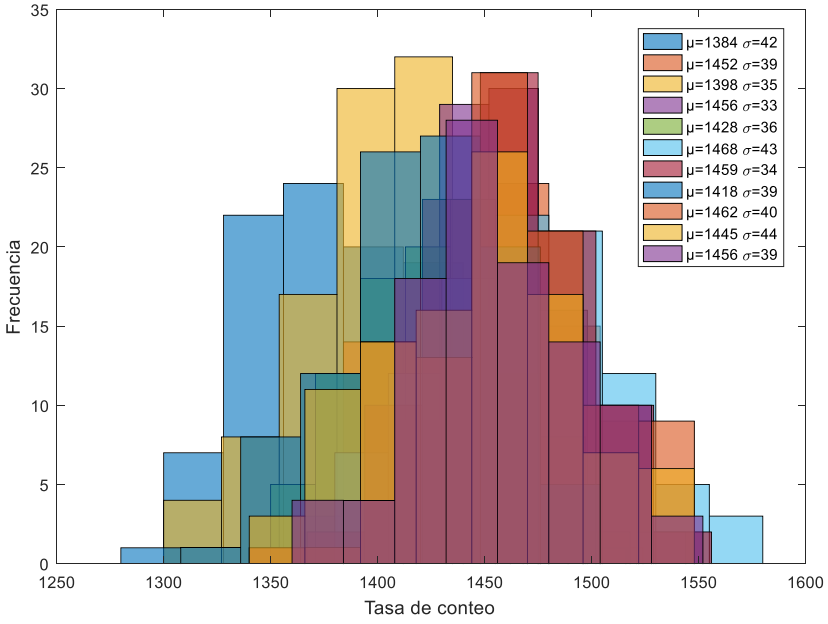

Figura 58. *Histograma de la tasa de conteo con el contador de fotones H0490 bajo la incidencia del haz láser.*

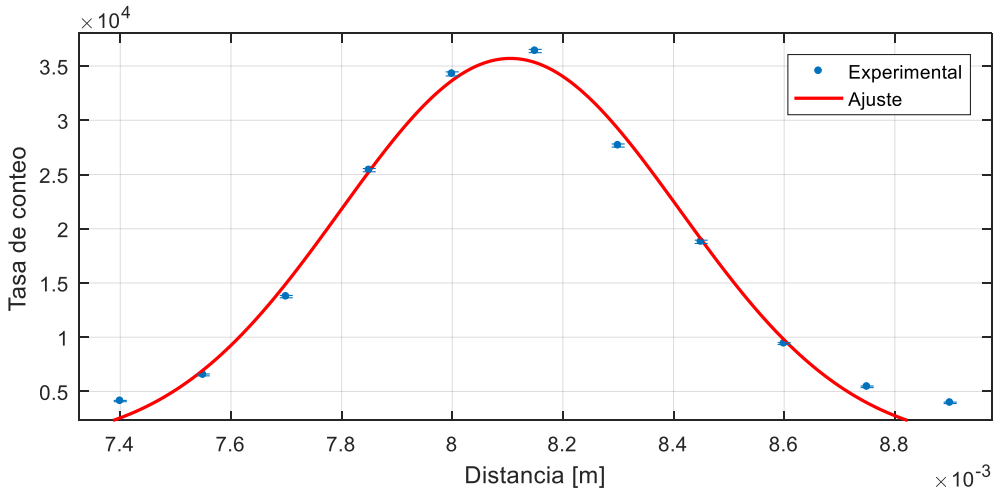

Figura 59. *Perfil del haz a partir de la detección con el contador de fotones H0491.*

4.2.2 Caracterización del divisor de haz. Se hace incidir el haz láser sobre un cubo divisor de haz no polarizador, por medio del cual se obtiene la tasa de conteo en diferentes posiciones transversales horizontales para cada uno de los puertos de salida como se observa en la **Figura 60** y **Figura 62** y el perfil de haz obtenido a partir del promedio de cada uno de los histogramas, como se observa en la **Figura 61** el cual se ajusta con un parámetro R2=0,9525 a una función gaussiana cuadrática con a=16560, b=0,008204 y c=0,6966x10-3 para el caso del puerto de salida horizontal y en la **Figura 63** con un parámetro R2=0,9674 a una función gaussiana cuadrática con a=12370, b=0,01942 y c=0,6853x10-3 para el caso del puerto de salida vertical. A partir de los resultados obtenidos se encuentra que el haz se divide, para cuando incide el mayor número de fotones, en 17178 y 12936 [fotones/segundo] en los puertos de salida, por lo cual no es exactamente a la mitad y en igual proporción, debido a la respuesta diferente de los dos contadores y a su vez se observa una reducción de la tasa de conteo máximo, debido a la absorción del material del divisor de haz y las múltiples reflexiones.

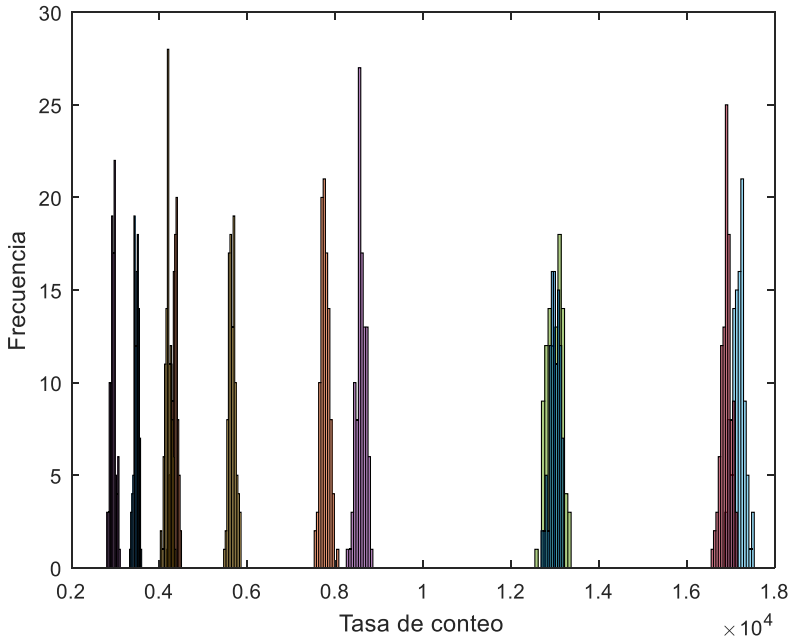

Figura 60. *Histograma de la tasa de conteo con el contador de fotones H0491 en el puerto de salida horizontal del divisor de haz a diferentes posiciones transversales horizontales.*

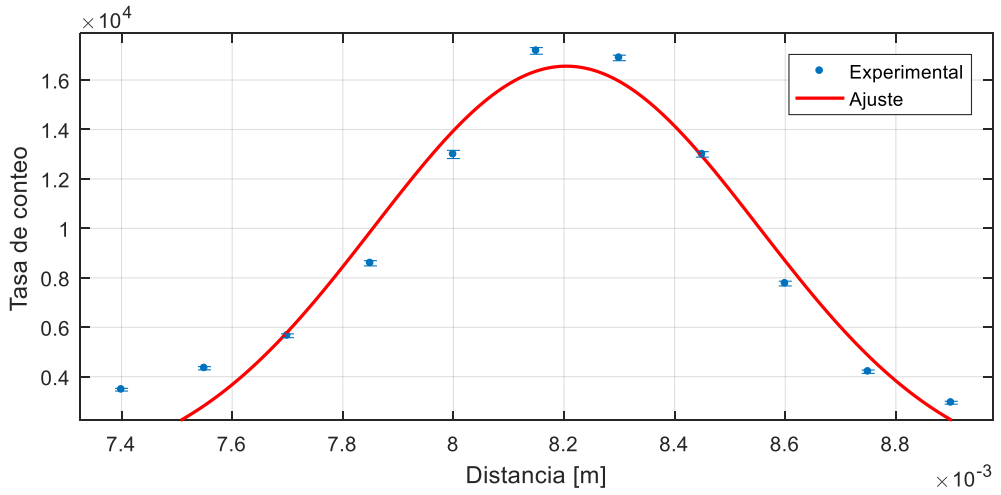

Figura 61. *Perfil del haz a partir de la detección con el contador de fotones H0491 en el puerto de salida horizontal del divisor de haz.*

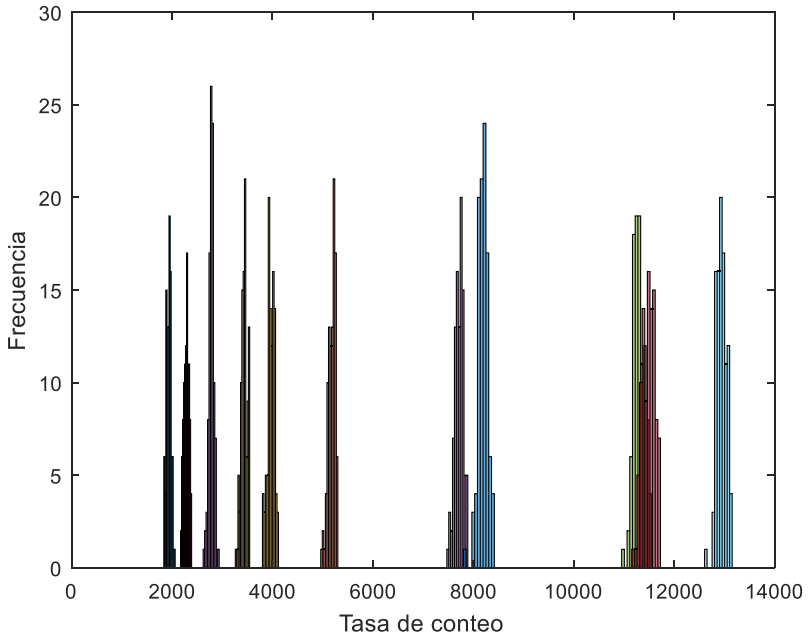

Figura 62. *Histograma de la tasa de conteo con el contador de fotones H0490 en el puerto de salida vertical del divisor de haz a diferentes posiciones transversales horizontales.*

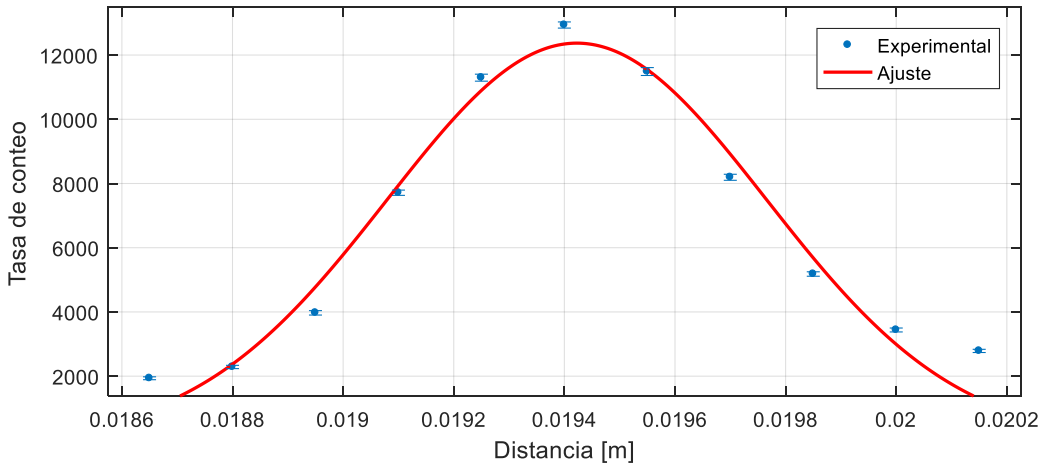

Figura 63. *Perfil del haz a partir de la detección con el contador de fotones H0490 en el puerto de salida vertical del divisor de haz.*

4.2.3 Caracterización del espejo. Se hace incidir el haz láser resultante del puerto de salida vertical del divisor de haz sobre un espejo metálico de λ/20, por medio del cual se obtiene la tasa de conteo en diferentes posiciones transversales horizontales como se observa en la **Figura 64** y el perfil de haz obtenido a partir del promedio de cada uno de los histogramas, como se observa en la **Figura 65** el cual se ajusta con un parámetro R2=0,9619 a una función gaussiana cuadrática con a=11760, b=0,01861 y c=0,88x10-3. De acuerdo a los resultados obtenidos se observa la forma del perfil del haz con una tasa de conteo máximo de 12015 [fotones/segundo].

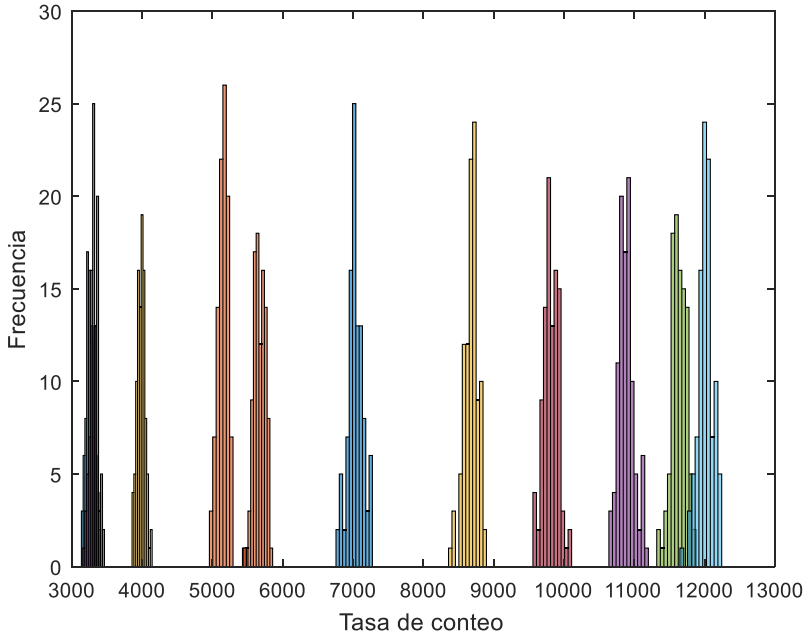

Figura 64. *Histograma de la tasa de conteo con el contador de fotones H0491 a diferentes posiciones transversales horizontales.*

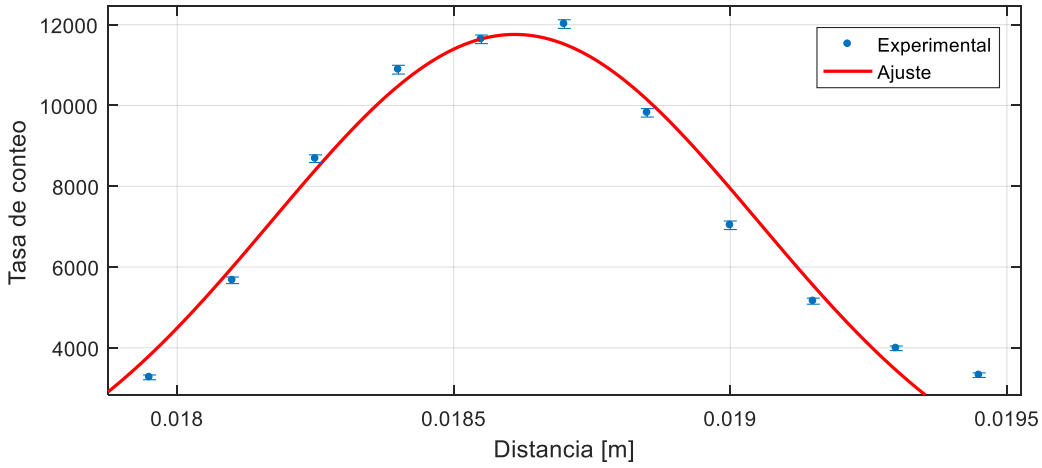

Figura 65. *Perfil del haz a partir de la detección con el contador de fotones H0491.*

4.3 Interferómetro de Mach-Zehnder

Se realiza el montaje de un interferómetro de Mach-Zehnder como el que se muestra en la **Figura 66**. Mediante una adecuada alineación del sistema con el haz láser sin atenuación se obtiene a la salida del segundo divisor de haz la interferencia de los haces, es decir, un patrón de franjas.

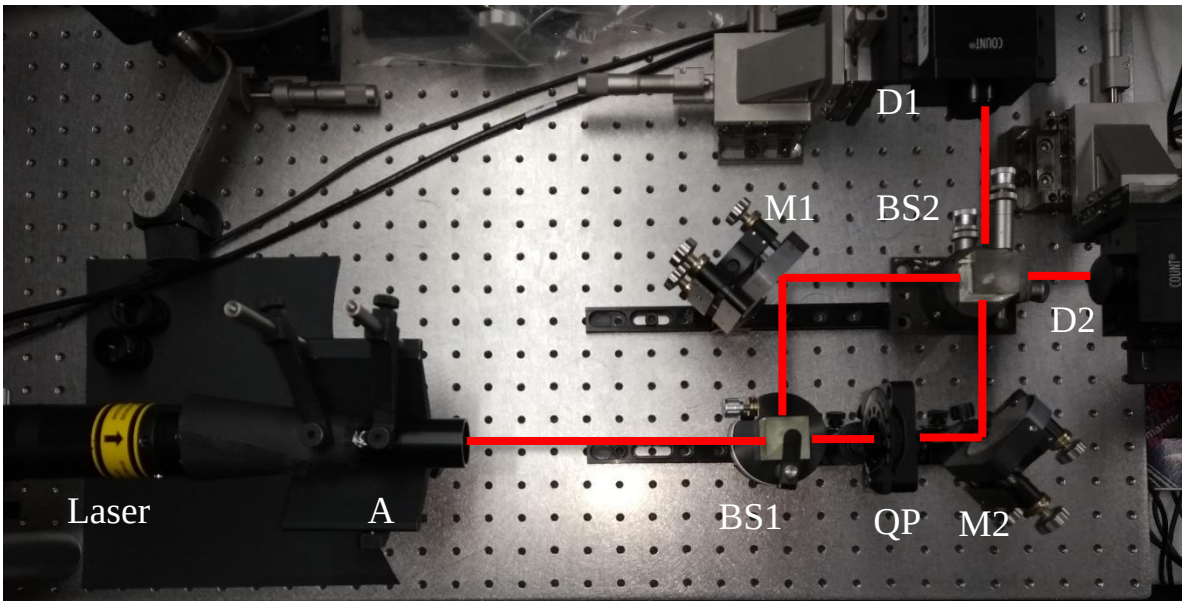

Figura 66. *Montaje experimental interferómetro de Mach-Zehnder. A=atenuador, BS=divisor de haz, M=espejo, QP=par de láminas λ/4 y D=detector o contador de fotones.*

A partir de una cámara CMOS y con un número muy elevado de fotones en el puerto de salida horizontal del segundo divisor de haz se captura la imagen del patrón de franjas verticales como se observa en la **Figura 67** y se verifica mediante un perfil transversal de las imágenes un desplazamiento equivalente a π en las franjas debido a la ubicación de dos láminas λ/4 en el brazo inferior del interferómetro como se muestra en la **Figura 68**.

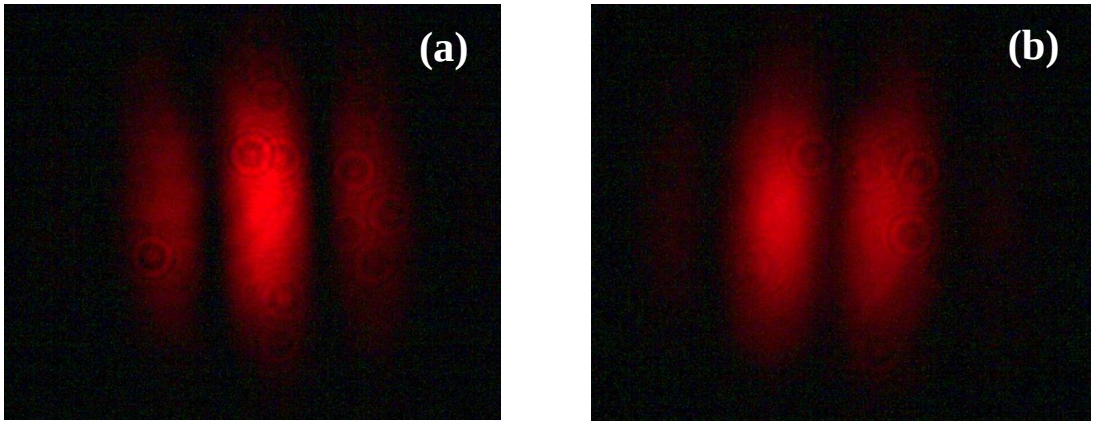

Figura 67. *Patrón de franjas (a) sin y (b) con el par de láminas λ/4 en serie en el brazo inferior del interferómetro. Aquí, el número de fotones es muy elevado y se tiene el régimen clásico.*

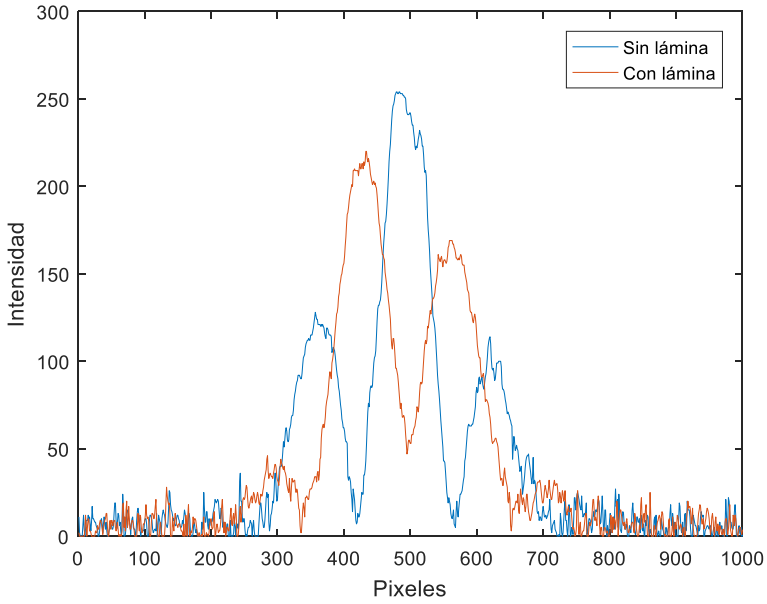

Figura 68. *Perfil transversal del patrón de franjas sin (azul) y con (rojo) el par de láminas λ/4 en el brazo inferior del interferómetro.*

Se procede a ajustar mediante la alineación de los dispositivos del sistema un patrón de franjas con un grosor por franja de mínimo 500 [µm], ya que este es el diámetro del área activa correspondiente a los contadores de fotones. En la **Figura 69** se presenta la franja donde se encuentra un grosor de 166 pixeles lo cual equivale a 531[µm] debido a que la cámara presenta un tamaño pixel de 3,2 x 3,2 [µm].

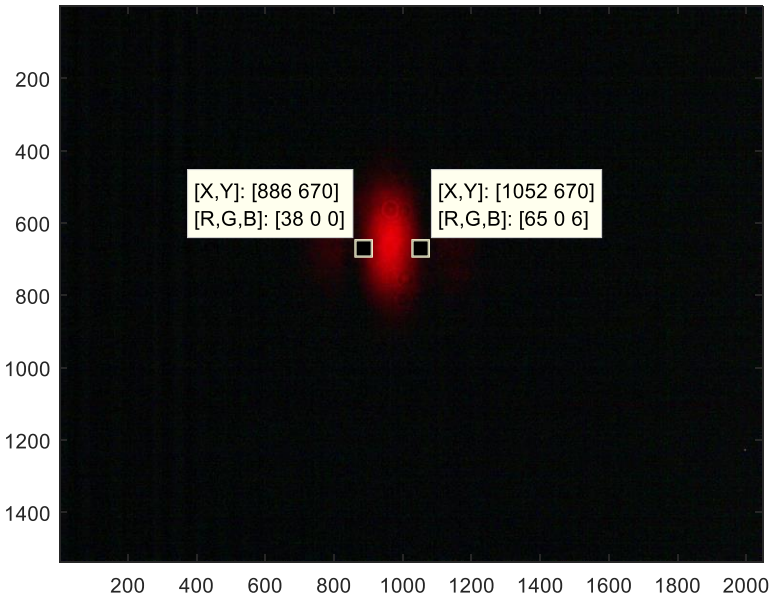

Figura 69. *Patrón de franjas a medir con los contadores de fotones.*

Finalmente se procede a atenuar el haz láser y se ubican los contadores en los puertos de salida del segundo divisor de haz, donde se ubica el máximo (la mayor tasa de conteo) en uno de los contadores de fotones y luego de hacer las mediciones, se colocan el par de láminas en el brazo inferior con el fin de ubicar el máximo en el otro contador, de tal forma que se obtiene la tasa de conteo de la **Figura 70** para cuando no se tiene el par de láminas y la tasa de conteo de la **Figura 71** una vez se pone el par de láminas, logrando observar el cambio entre un máximo y un mínimo entre los dos contadores.

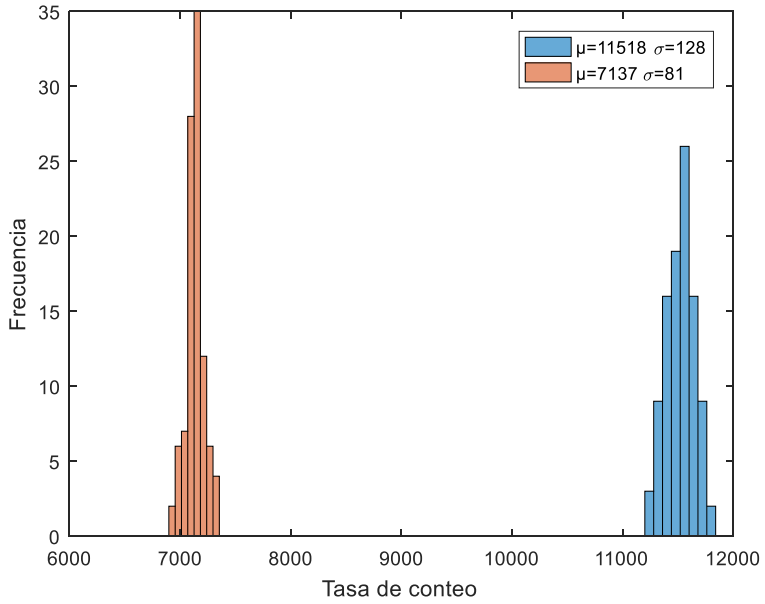

Figura 70. *Histograma tasa de conteo de fotones con el contador de fotones H0490 (azul) y H0491 (rojo).*

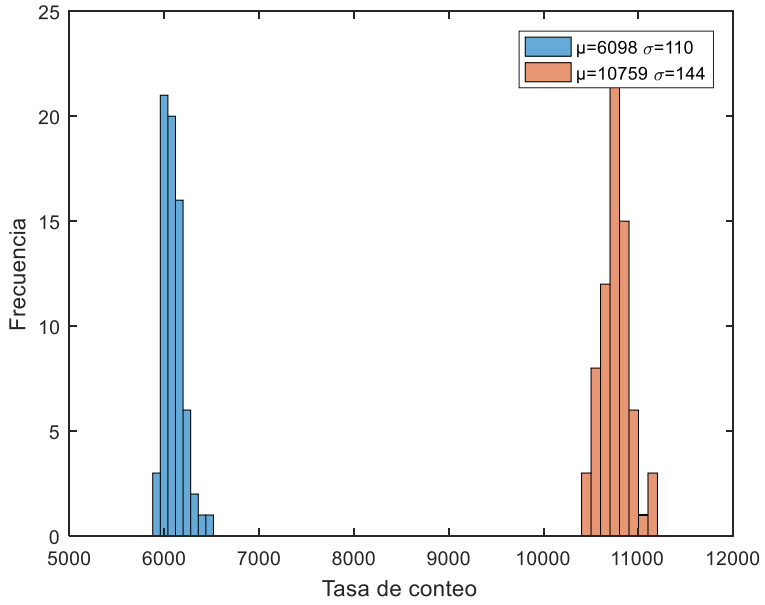

Figura 71. *Histograma tasa de conteo de fotones con el contador de fotones H0490 (azul) y H0491 (rojo) cuando se ubica un par de láminas λ/4 en serie en el brazo inferior del interferómetro.*

5 Conclusiones

El ataque a la seguridad del sistema de comunicación por interceptación del canal se describe como un modelo estocástico que permite el análisis numérico mediante una herramienta de simulación como el método de Monte Carlo, el cual en comparación con la expresión analítica permite considerar la ocurrencia de todos los posibles eventos en el sistema y analizar esta probabilidad como el experimento de lanzar un dado o una moneda.

Los resultados obtenidos mediante la simulación de Monte Carlo para el análisis de ataques al sistema de comunicación basado en modulación de coherencia concuerdan con los resultados analíticos obtenidos en (Boughanmi, 2017), dado que el error cuadrático medio entre las dos graficas resultantes es máximo del orden de 10^{-4}, lo que a su vez permite corroborar el correcto desempeño de la simulación realizada para la implementación en el análisis de la seguridad para el sistema de comunicación basado en modulación de coherencia y momento angular orbital propuesto.

En la curva de probabilidad de éxito de Eve para el ataque combinado resultante de la unión de los eventos del ataque 1, 2_1 hasta 2_8 y 3_1 hasta 3_9, se observa que Eve puede determinar el retraso de tiempo correcto con una probabilidad mayor al 50%, con 39 fotones en promedio en lugar de los 66 que requiere con solo el ataque No.1, lo que permite concluir que la combinación de eventos disminuye la cantidad de fotones necesarios para un atacante en un sistema de comunicación basado en modulación de coherencia.

A partir de la modulación de coherencia y el momento angular orbital, fue posible obtener, para el ejemplo más simple, un protocolo basado en cuatro estados ortogonales en dos bases

diferentes, ampliando la dimensión de la distribución de clave cuántica para un sistema óptico de comunicación en comparación con el protocolo BB84.

Desde el punto de vista teórico, extender el ejemplo más simple expuesto en este documento a N estados ortogonales en dos diferentes bases mutuamente imparciales es factible, por lo cual se logra ampliar la dimensión de la distribución de clave cuántica para un sistema óptico de comunicación.

Para el método propuesto, el uso de fuentes de fotones individuales o fotones entrelazados no es obligatorio, dado que la codificación que usa la modulación de coherencia permite un correcto funcionamiento al nivel de conteo de fotones, y a su vez no presentaría problemas de seguridad debido a los pulsos multifotónicos.

Teniendo en cuenta la tecnología actual, se expone una configuración experimental para la realización de un esquema de QKD de alta dimensión basado en la codificación en dos bases mutuamente imparciales utilizando la coherencia temporal y el momento angular orbital de la luz.

Para la ejecución del sistema de comunicación basado en modulación de coherencia y momento angular orbital se requiere que Alice y Bob compartan una clave de transmisión $[\tau_k, \tau_q, l_a, l_b]$ formada por un par de retrasos de tiempo seleccionados de un subconjunto de M posibles retrasos de tiempo y un par de modos MAO seleccionados de un subconjunto de N posibles modos.

La mayor probabilidad de éxito para un atacante (Eve) es 32.42% con un promedio de 100 fotones para un ataque por interceptación del canal al sistema de comunicación con 10 posibles retrasos de tiempo y 10 posibles modos MAO para la clave de transmisión, siendo menor al 98.88% de probabilidad de éxito que se presenta en un sistema basado solo en la modulación de

coherencia bajo estas condiciones. Por lo tanto, se presenta un método para mejorar el nivel de seguridad de un sistema de comunicación, a partir de la cantidad de fotones utilizados en el sistema.

A partir del análisis de ataques al sistema desde la perspectiva de Eve, se concluye que el sistema de comunicación propuesto debe ser operado mediante una fuente con un promedio de 78 fotones para un correcto funcionamiento y una baja amenaza a la seguridad (Eve presenta una probabilidad máxima de detectar la clave y por ende descifrar el estado enviado igual a 14.98%). Adicionalmente se observa que Eve presenta una mayor probabilidad de éxito en la medida en que la información es codificada en la base ξ.

En términos de la cantidad de información enviada desde Alice a Bob, se encuentra que, en comparación con el clásico protocolo BB84, en la técnica propuesta se tiene el doble de capacidad de información por fotón, lo que permite una mayor tasa de distribución de claves.

Para operar experimentalmente a nivel de conteo de fotones con la menor incidencia de ruido, se requiere de un espacio de trabajo suficientemente oscuro con el mayor control posible de fuentes de luz no deseadas (LED, filtración de luz por orificios de ventanas y puertas, etc.) y en horas de la noche.

Como resultado para futuros trabajos de investigación con los contadores de fotones del laboratorio se obtiene una propuesta de sistema electrónico funcional basado en Arduino y un lenguaje de programación como Python que permite la adquisición y medición de la tasa de conteo de cualquier módulo con salida TTL (Ver Apéndice A).

De acuerdo a las mediciones realizadas con los contadores de fotones se verifica que la detección de fotones sigue una distribución de Poisson, donde su principal característica corresponde a un valor de media y varianza iguales.

Como se observa en los resultados obtenidos para los contadores de fotones en operación y abiertos y cerrados, se encuentra que presentan una tasa de conteo ocasionada por pulsos que aparecen en ausencia de cualquier luz incidente en el fotodiodo de avalancha y por fuentes de luz no deseadas en el ambiente respectivamente, las cuales se caracterizan previamente para tener en cuenta en mediciones posteriores, ya que constituyen el ruido del sistema.

Los resultados obtenidos para el valor de tasa de conteo experimental del haz láser concuerda con el valor calculado teóricamente, ya que presenta una diferencia de 6,8%, que es ocasionada por el ruido electrónico y del medio ambiente. Adicionalmente mediante este resultado se comprueba la influencia del perfil de intensidad gaussiano del haz y el área de detección en la cantidad de fotones por segundo.

Los resultados obtenidos para la tasa de conteo máxima en los puertos de salida de un cubo divisor de haz 10BC17MB.1 de marca Newport evidencian las pérdidas ocasionadas por el proceso de reflexión y absorción en el elemento, dado que los haces resultantes son de 47% (17178 fotones/s]) y 35% (12936 [fotones/s]) en el puerto de salida horizontal y vertical respectivamente.

De acuerdo a las especificaciones técnicas del espejo λ/20 20Z40ER.1 de marca Newport presenta una reflectividad mínima mayor al 90% , lo cual concuerda con los resultados obtenidos experimentalmente, dado que la razón entre la tasa de conteo incidente en el espejo (12936 [fotones/s]) y la tasa de conteo de salida (12015 [fotones/s]) es de 92.88%.

A partir del montaje de un interferómetro de Mach-Zehnder con un ancho de franjas mínimo de 500 [µm] fue posible mediante una cámara CMOS y los contadores de fotones evidenciar el

desplazamiento de las franjas en una distancia igual a λ/2, es decir, pasar de una interferencia constructiva a una destructiva y viceversa en los puertos de salida.

Algunos trabajos futuros que pueden derivarse de esta investigación incluyen el análisis de la posible vulnerabilidad del sistema propuesto a un ataque que involucre alguna forma de amplificación de luz, aunque la clonación de fotones es un problema abierto y parece contradecir las leyes fundamentales de la física, así como la implementación del sistema de comunicación basado en la modulación de coherencia y el momento angular orbital con base en la configuración experimental propuesta considerando los dispositivos y tecnología actual, con el fin de verificar experimentalmente los principios descritos en este trabajo.

6 Producción académica

En la Tabla 10 se muestran los trabajos realizados como producto de este proyecto de investigación (2016-2018).

Tabla 10.
Divulgación de resultados realizados durante el periodo de la maestría 2016-2018.

Título	Autores	Evento	Año
Estudio de la difracción en campo lejano de vórtices ópticos por un borde recto	López, P. Reyes Z. Guzmán A. Torres, Y.	Jornadas científicas de la escuela de Física Bucaramanga, Colombia	2016
Straight edge diffraction of OAM waves	López, P. Reyes Z. Guzmán A. Torres, Y.	3rd International Conference on applications of Optics and Photonics Faro, Portugal	2017

Diffracted optical vortices by an angular aperture. Proc. SPIE 10347 https://doi.org/10.1117/12.2274017	López, P. Reyes Z. Guzmán A. Mendoza, J. Torres, Y.	SPIE Optics + Photonics San Diego, California, Estados Unidos	2017
Generación de distribución de llave cuántica de alta dimensión mediante modulación de coherencia a nivel de conteo de fotones	López, P. Rhodes, W. Torres, Y.	Congreso Nacional de Física Cartagena, Colombia	2017
Difracción de vórtices ópticos por una abertura angular	Reyes Z. López, P. Guzmán A. Mendoza, J. Torres, Y.	Congreso Nacional de Física Cartagena, Colombia	2017
Generación de modos angulares para codificación espacial de información	López, P. Mendoza, J. Reyes Z. Torres, Y.	XV Encuentro Nacional de Óptica, VI Conferencia Andina y del Caribe en Óptica y sus aplicaciones - XV ENO & VI CANCOA Bucaramanga, Colombia	2017
Difracción angular de haces con momento angular orbital	Reyes Z. López, P. Guzmán A. Mendoza, J. Torres, Y.	XV ENO & VI CANCOA Bucaramanga, Colombia	2017
Modulación de solo fase en una matriz de cristal líquido LCOS	Mendoza, J. López, P. Reyes Z. Torres, Y.	XV ENO & VI CANCOA Bucaramanga, Colombia	2017
Diffracted optical vortices by an angular aperture	López, P. Reyes Z. Guzmán A. Mendoza, J. Torres, Y.	I Encuentro de Investigación Facultad de Ingenierías Fisicomecánicas, RESEARCH DAY FIMEC Bucaramanga, Colombia	2017
High-dimensional quantum key distribution by coherence modulation and orbital angular momentum at the photon-counting level.Proc. SPIE 10674 https://doi.org/10.1117/12.2307757	López, P. Torres, Y. Rhodes, W.	SPIE Photonics Europe Strasbourg, Francia	2018

High dimensional quantum key distribution Based on coherence modulation and orbital angular momentum. OSA Technical Digest https://doi.org/10.1364/FIO.2018.JW3A.74	López, P. Torres, Y. Rhodes, W.	Frontiers in Optics & Laser Science Conference (FIO/LS) Washington DC, Estados Unidos	2018
High dimensional quantum key distribution Based on coherence modulation and orbital angular momentum	López, P. Torres, Y. Rhodes, W.	RESEARCH DAY U18 Bucaramanga, Colombia	2018

Referencias Bibliográficas

Ali, S. (2016). Time-polarization coding in quantum cryptography. Optical and Quantum Electronics, 48(558), 1–10. https://doi.org/10.1007/s11082-016-0832-3

Allen, L., Beijersbergen, M. W., Speeruw, R. J. C., & Woerdman, J. P. (1992). Orbital angular momentum of light and transformation of Laguerre-Gaussian laser modes. Physical Review A. https://doi.org/10.1103/PhysRevA.45.8185

Andrews, D. L., & Babiker, M. (2013). The angular momentum of light. Cambridge University Press.

Bacco, D., Christensen, J. B., Castaneda, M. A. U., Ding, Y., Forchhammer, S., Rottwitt, K., & Oxenløwe, L. K. (2016). Two-dimensional distributed-phase-reference protocol for quantum key distribution. Scientific Reports, 6(36756), 1–7. https://doi.org/10.1038/srep36756

Bechmann-Pasquinucci, H., & Tittel, W. (2000). Quantum cryptography using laser alphabets. Physical Review A, 61(6), 062308. https://doi.org/10.1103/PhysRevA.61.062308

Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179).

Boughanmi, A. (2017). Secure Communication by Coherence modulation at the photon counting level., PhD Thesis, Florida Atlantic University.

Bourennane, M., Karlsson, A., & Björk, G. (2001). Quantum key distribution using multilevel

encoding. Physical Review A, 64(1), 012306. https://doi.org/10.1103/PhysRevA.64.012306

Bozinovic, N., Yue, Y., Ren, Y., Tur, M., Kristensen, P., Huang, H.,Ramachandran, S. (2013). Terabit-Scale Orbital Angular Momentum Mode Division Multiplexing in Fibers. Science, 340(6140), 1545–1548. https://doi.org/10.1126/science.1237861

Buttler, W., Lamoreaux, S. K., & Torgerson, J. R. (2012). Practical four-dimensional quantum key distribution without entanglement. Quantum Information and Computation, 12(1–2), 1–8.

Cahill, K. (2013). Monte Carlo methods. In Physical Mathematics (pp. 563–577). New York: Cambridge University Press.

Chunnilall, C. J., Degiovanni, I. Pietro, Kück, S., Müller, I., & Sinclair, A. G. (2014). Metrology of single-photon sources and detectors: a review. Optical Engineering, 53(8), 081910. https://doi.org/10.1117/1.OE.53.8.081910

CVI Melles Griot. (2009). Gaussian Beam Optics. Technical Guide, 2(1), 1–14. https://doi.org/10.1017/CBO9781139167994.020

Djordjevic, I. B. (2013). Multidimensional QKD based on combined orbital and spin angular momenta of photon. IEEE Photonics Journal, 5(6), 7600112. https://doi.org/10.1109/JPHOT.2013.2292301

Djordjevic, I. B., & Arabaci, M. (2010). LDPC-coded orbital angular momentum (OAM) modulation for free-space optical communication. Optics Express, 18(24), 24722–8. https://doi.org/10.1364/OE.18.024722

Douglas C., M., & George C., R. (2003). Tests of hypotheses for a single sample. In Applied statistics and probability for engineers (3rd ed.). John Wiley & Sons,Inc. https://doi.org/10.1007/BF00948843

Edmund Optics. (2012). Understanding Neutral Density Filters. Retrieved from https://www.edmundoptics.com/resources/application-notes/optics/understanding-neutral-density-filters/

Etcheverry, S., Cañas, G., Gómez, E. S., Nogueira, W. A. T., Saavedra, C., Xavier, G. B., & Lima, G. (2013). Quantum key distribution session with 16-dimensional photonic states. Scientific Reports, 3(2316), 1–5. https://doi.org/10.1038/srep02316

Fox, M. (2006). Photon statistics. In Quantum Optics: An introduction (pp. 75–101). New York: Oxford University Press.

Furdek, M., Skorin-Kapov, N., Zsigmond, S., & Wosinska, L. (2014). Vulnerabilities and security issues in optical networks. International Conference on Transparent Optical Networks, (July). https://doi.org/10.1109/ICTON.2014.6876451

Gibson, G., Courtial, J., Padgett, M., Vasnetsov, M., Pas'ko, V., Barnett, S., & Franke-Arnold, S. (2004). Free-space information transfer using light beams carrying orbital angular momentum. Optics Express, 12(22), 5448–5456. https://doi.org/10.1364/OPEX.12.005448

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum Cryptography. Review of Modern Physics, 74(January), 145–195. https://doi.org/10.1103/RevModPhys.74.145

Goedgebuer, J., Porte, H., & Mollier, P. (1993). Coherence modulation and correlation of stochastic light fields. Journal de Physique III, 3(7), 1413–1433. https://doi.org/10.1051/jp3:1993209

Goodwin, E. P., & Wyant, J. C. (2000). Field Guide to Interferometric Optical Testing. SPIE—The International Society for Optical Engineering.

Gutiérrez Martinez, C., Porte, H., & Goedgebuer, J. (1995). Microwave integrated optics LiNbO3 coherence modulator for high-speed optical communications. Microwave and

Optical Technology Letters, 10(1), 66–70.

Harrison, R. L. (2010). Introduction to Monte Carlo Simulation. In AIP (Vol. 1204, pp. 17–21). https://doi.org/10.1063/1.3295638.Introduction

Hodges, M., & Grabher, S. (2014). Single-photon avalanche diodes. Sensors and Metrology, 64–67.

Inoue, K., Waks, E., & Yamamoto, Y. (2002). Differential phase shift quantum key distribution. Physical Review Letters, 89(3), 379021–379023. https://doi.org/10.1103/PhysRevLett.89.037902

Inoue, K., Waks, E., & Yamamoto, Y. (2003). Differential-phase-shift quantum key distribution using coherent light. Physical Review A, 68(2), 022317. https://doi.org/10.1103/PhysRevA.68.022317

Kogelnik, H., & Li, T. (1966). Laser Beams and Resonators. Applied Optics, 5(10), 1550–1567. https://doi.org/10.1109/PROC.1966.5119

Lapeyre, B. (2007). Introduction to Monte-Carlo Methods. Halmstad, Sweden.

Lo, H.-K., Curty, M., & Tamaki, K. (2014). Secure Quantum Key Distribution. Nature Photonics, 8(August), 595–604. https://doi.org/10.1038/nphoton.2014.149

Luda, M. A., Larotonda, M. A., Paz, J. P., & Schmiegelow, C. T. (2014). Manipulating transverse modes of photons for quantum cryptography. Physical Review A - Atomic, Molecular, and Optical Physics, 89(4), 042325. https://doi.org/10.1103/PhysRevA.89.042325

Metropolis, N. (1987). The beginning of the Monte Carlo method. Los Alamos Science, 15, 125–130. https://doi.org/10.1128/JCM.05092-11

Metropolis, N., & Ulam, S. (1949). The Monte Carlo Method. Journal of American Statistical

Association, 44(247), 335–341. Retrieved from http://www.jstor.org/stable/2280232%5Cr

Mirhosseini, M., Magaña-Loaiza, O. S., O'Sullivan, M. N., Rodenburg, B., Malik, M., Lavery, M. P. J., Boyd, R. W. (2015). High-dimensional quantum cryptography with twisted light. New Journal of Physics, 17(033033), 1–12. https://doi.org/10.1088/1367-2630/17/3/033033

NIST/SEMATECH. (2012). Chi-Square Goodness-of-Fit Test. Retrieved from https://www.itl.nist.gov/div898/handbook/eda/section3/eda35f.htm.

Padgett, M. (2014). Light ' s Twist. Proceedings of the Royal Society A, 470(20140633), 10. https://doi.org/10.1098/rspa.2014.0633

Padgett, M., Courtial, J., & Allen, L. (2004). Light's Orbital Angular Momentum. Physics Today, 57(5), 35. https://doi.org/10.1063/1.1768672

Pedrotti, F. L., & Pedrotti, L. S. (1993). Coherence. In Introduction to Optics (2nd ed., pp. 247–265). Prentice-Hall Internacional Inc.

Phoenix, S. J. D., & Townsend, P. D. (1995). Quantum cryptography: How to beat the code breakers using quantum mechanics. Contemporary Physics, 36(3), 165–195. https://doi.org/10.1080/00107519508222150

Raymer, M. G. (2017). Quantum physics: what everyone needs to know. New York, NY: Oxford University Press.

Rejeb, R., Leeson, M. S., & Green, R. J. (2006). Fault and attack management in all-optical networks. IEEE Communications Magazine, 44(11), 79–85. https://doi.org/10.1109/MCOM.2006.248169

Rhodes, W. T., Boughanmi, A., & Torres Moreno, Y. (2016). High-security communication by coherence modulation at the photon-counting level. Applied Optics, 55(15), 3952–3957. https://doi.org/10.1364/AO.55.003952

Salamon, A., Levy-yurista, G., Tseytlin, M., Cho, P. S., Shpantzer, I., & Spring, S. (2003). Secure optical communications utilizing PSK modulation, polarization multiplexing and coherent digital homodyne detection with wavelength and polarization agility. IEEE Military Communications Conference, 1, 274–282.

Saleh, A. A. M., & Simmons, J. M. (2012). All-optical networking- evolution, benefits, challenges, and future vision. Proceedings of the IEEE, 100(5), 1105–1117. https://doi.org/10.1109/JPROC.2011.2182589

Schneier, B. (1996). Applied cryptography: Protocols, Algorithms and Source code in C (2nd ed.). John Wiley & Sons,Inc.

Schulze, C., Dudley, A., Brüning, R., Duparré, M., & Forbes, A. (2014). Measurement of the orbital angular momentum density of Bessel beams by projection into a Laguerre-Gaussian basis. Applied Optics, 53(26), 5924–33. https://doi.org/10.1364/AO.53.005924

Sergienko, A. V. (2006). Quantum Communications and Cryptography. Boca Raton, FL: CRC Press. Retrieved from https://www.crcpress.com/Quantum-Communications-and-Cryptography/Sergienko/p/book/9780849336843

Shannon, C. (1949). Communication theory of secrecy system. Bell System Technical Journal, 28(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134. https://doi.org/10.1109/SFCS.1994.365700

Sit, A., Bouchard, F., Fickler, R., Gagnon-Bischoff, J., Larocque, H., Heshami, K., Karimi, E. (2017). High-dimensional intracity quantum cryptography with structured photons. Optica, 4(9), 1006–1010. https://doi.org/10.1364/OPTICA.4.001006

Slussarenko, S., Karimi, E., Piccirillo, B., Marrucci, L., & Santamato, E. (2011). Efficient generation and control of different-order orbital angular momentum states for communication links. Journal of the Optical Society of America A, 28(1), 61–65. https://doi.org/10.1364/JOSAA.28.000061

Stipčević, M., Wang, D., & Ursin, R. (2013). Characterization of a commercially available large area, high detection efficiency single-photon avalanche diode. Journal of Lightwave Technology, 31(23), 3591–3596. https://doi.org/10.1109/JLT.2013.2286422

Sun, X., & Djordjevic, I. B. (2016). Physical-layer security in orbital angular momentum multiplexing free-space optical communications. IEEE Photonics Journal, 8(1), 1–10. https://doi.org/10.1109/JPHOT.2016.2519279

Thomas, M. C., & Joy, A. T. (2006). Elements of information theory (2nd ed.). John Wiley & Sons. https://doi.org/10.1007/978-94-010-9292-0

Vallone, G., D'Ambrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F., & Villoresi, P. (2014). Free-space quantum key distribution by rotation-invariant twisted photons. Physical Review Letters, 113(6), 060503. https://doi.org/10.1103/PhysRevLett.113.060503

Wacogne, B., Elflein, W., Pieralli, C., Mollier, P., Porte, H., & Jackson, D. A. (1998). Secrecy improvement in confidential coherence modulation by means of a new keying structure. Optics Communications, 154, 350–358.

Wacogne, B., & Jackson, D. A. (1996a). Enhanced security in a coherence modulation system using optical path difference corruption. IEEE Photonics Technology Letters, 8(7), 947–949. https://doi.org/10.1109/68.502280

Wacogne, B., & Jackson, D. D. (1996b). Security Vulnerability in Coherence Modulation

Communication Systems. IEEE Photonics Technology Letters, 8(3), 470–472.

Wacogne, B., Jackson, M. D., Fisher, N. E., Podoleanu, A., & Jackson, D. A. (1996). Double security level in a telecommunication system based on phase coding and false data transmission. Journal of Lightwave Technology, 14(5), 665–670. https://doi.org/10.1109/50.495144

Wang, J. (2016). Advances in communications using optical vortices. Photonics Research, 4(5), 14–28. https://doi.org/10.1364/PRJ.4.000B14

Wang, J., Yang, J.-Y., Fazal, I. M., Ahmed, N., Yan, Y., Huang, H., … Willner, A. E. (2012). Terabit free-space data transmission employing orbital angular momentum multiplexing. Nature Photonics, 6(7), 488–496. https://doi.org/10.1038/nphoton.2012.138

Yao, A. M., & Padgett, M. J. (2011). Orbital angular momentum: origins, behavior and applications. Advances in Optics and Photonics, 3(2), 161–204. https://doi.org/10.1364/AOP.3.000161

Zetie, K. P., Adams, S. F., & Tocknell, R. M. (2000). How does a Mach-Zehnder interferometer work? Physics Education, 35(1), 46–48. https://doi.org/10.1088/0031-9120/35/1/308

Apéndices

Apéndice A. Sistema electrónico para los contadores de fotones

Los contadores de fotones individuales COUNT 1000-S del fabricante Laser Components son un módulo que se compone de un fotodiodo de avalancha (APD por sus siglas en inglés) de silicio que permite la detección de fotones individuales (Ver Figura 1).

Figura 1. *Contador de fotones individuales COUNT 1000-S.*

El módulo presenta una entrada de alimentación y una salida TTL, que se conectan a la fuente de alimentación dual SPAD DSN 102 del fabricante PicoQuant que se muestra en la Figura 2, el cual es un dispositivo que funciona como fuente de alimentación de los contadores de fotones y a su vez permite controlar y monitorear el funcionamiento de los mismos, mostrando la tasa de conteo del módulo seleccionado. Además presenta un circuito de protección automático que apaga el voltaje de suministro a los módulos cuando se alcanzan niveles de exposición críticos a la luz.

Figura 2. *Fuente de alimentación dual SPAD DSN 102.*

Para la adquisición y medición de los datos, inicialmente se conecta cada una de las salidas TTL del DSN 102 correspondiente a cada contador de fotones, a un circuito amplificador como el que se muestra en la Figura 3, obteniendo señales TTL de 5 [V] de amplitud, las cuales se conectan al pin 5 y pin 47 de una placa de Arduino Uno y Mega respectivamente. Cada placa posee un microcontrolador programable sobre el cual se carga el código fuente que se presenta en la Figura 4, el cual permite realizar el conteo de flancos de la señal TTL durante un intervalo de tiempo de 1[s], lo cual concuerda con la tasa de conteo presentada en el DSN 102.

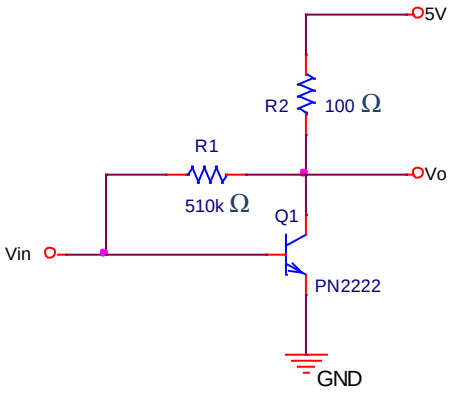

Figura 3. *Circuito amplificador para la señal TTL del contador de fotones.*

Figura 4. *Código de la plataforma Arduino para implementación de un contador de pulsos.*

Finalmente mediante el código de Python que se muestra en la Figura 5, se realiza la lectura y adquisición de la tasa de conteo desde el puerto serial COM4 y COM5 correspondiente a cada una de las placas de Arduino, los cuales posteriormente se almacenan en dos archivos de texto, donde la cantidad de datos en cada uno de estos se define en la condición de la sentencia while.

C:\Users\USUARIO\paulis\ReadSerial_2.py - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

ReadSerial_2.py

```
import winsound
frequency = 2500  # Set Frequency To 2500 Hertz
duration = 2000  # Set Duration To 1000 ms == 1 second
winsound.Beep(frequency, 1000)

arduino= serial.Serial('COM4',57600)
arduino2= serial.Serial('COM5',57600)
f=open('20181029DestapadoH0490_M_D5.txt','w')
f2=open('20181029DestapadoH0491_M_D5.txt','w')
muestra=0


while muestra<125:
    f.write(arduino.readline().decode('utf-8'))
    f2.write(arduino2.readline().decode('utf-8'))
    muestra=muestra+1
    time.sleep(1)
f.close()
f2.close()
arduino.close()
arduino2.close()
print("Fin")
winsound.Beep(frequency, duration)
```

Line 10, Column 37 Tab Size: 4 Python

Figura 5. *Código de Python para la adquisición de tasas de conteo de los contadores de fotones.*