UNIVERSIDAD CATÓLICA DEL NORTE

FACULTAD DE CIENCIAS

Departamento de Física

Criptografía cuántica con pulsos de múltiples fotones

Tesis para optar al grado de Magíster en Ciencias con mención Física

Mario Ernesto Brayan Miranda Rojas

Profesor Guía: Dr. Douglas Mundarain
Dra. María Loreto Ladrón de Guevara González

Antofagasta, Chile

2017

...a mis padres!

Agradecimientos

Agradezco el financiamiento otorgado por el programa de Magíster del Departamento de Física y la Dirección General de Postgrado de la Universidad Católica del Norte.

Resumen

La criptografía es un método de ocultamiento de información basado en la codificación y decodificación de mensajes enviados entre dos paticipantes, los cuales mediante diversas técnicas buscan asegurar la confidencialidad de la información transmitida para protegerse del ataque de posibles terceros ajenos a la comunicación. Clásicamente se ha buscado modelar sistemas criptográficos de acuerdo a los contextos históricos en los cuales se han desarrollado, hasta llegar al día de hoy en que incluso la física cuántica es utilizada en el desarrollo de sistemas de codificación cada vez mas complejos. Un ejemplo de los avances logrados en la Teoría Cuántica de la Información es el Protocolo BB84, el cual mediante las polarizaciones de pulsos monofotónicos enviados de un punto a otro, tiene como objetivo lograr una segura distribución de claves secretas, garantizando la detección de posibles intrusos que pudieran robar la información. En base a esto nosotros buscamos plantear un protocolo análogo al recien mencionado, implementando pulsos de múltiples fotones a fin de buscar en la práctica, una nueva alternativa para desarrollar una transmisión de información a una mayor distancia de la que nos permite la utilización de pulsos monofotónicos. Para esto consideramos los efectos de ruido propios del canal cuántico de comunicación, y los efectos de un beam splitter implementado por un intruso que busque desviar parte de la información que se desea transmitir.

Abstract

Cryptography is a method of hiding information based on the codification and decoding of messages between two participants, which through various techniques seeks to ensure the confidentiality of the information transmitted to protect it against the attack of third parties outside the communication. Classically it has been tried to model cryptographic systems according to the historical contexts in which they have been developed, until the present day in which even the quantum physics is used in the development of increasingly complex coding systems. An example of the advances achieved in the quantum theory of information is the BB84 Protocol, which through the polarizations of monophotonic pulses sent from one point to another, aims to achieve a secure distribution of secret keys, ensuring the detection of possible intruders that could steal The information. Based on this we seek to propose a protocol analogous to the aforementioned, implementing pulses of multiple photons in order to search in practice, a new alternative to develop the transmission of information at a greater distance than allows us the single-photon pulses. For this we consider the noise effects of the communication channel, and the effects of a beam splitter implemented by an intruder that seeks to divert some of the information that is wanted to be transmitted.

Índice general

Índice de figuras

Introducción

A lo largo de nuestra historia y en diferentes civilizaciones, el ser humano ha tenido la necesidad de comunicarse de alguna u otra forma con sus pares, intentanto intercambiar información útil que ayude cumplir algún propósito. Las formas de llevar a cabo la comunicación han sido variadas, y han evolucionado con el paso del tiempo desde simples técnicas como señales de humo, hasta los ya cotidianos procesos de mensajería instantánea que utilizamos hoy en día, aprovechando los diversos avances que la ciencia ha logrado en materia de tecnologías. Sin embargo, debemos considerar que si bien el envío de información de un punto a otro hoy puede parecer un proceso rápido y poco complejo, hay ciertos aspectos que deben tenerse en cuenta y que resultan fundamentales para lograr que la comunicación sea exitosa.

Uno de los aspectos mas importantes que se busca garantizar en cualquier proceso de intercambio de información, es mantener la integridad del mensaje que se esté intentando transmitir, es decir, se debe siempre procurar que el receptor replique de la mejor manera posible la información que el emisor quiere comunicarle. Por ejemplo, si utilizamos como canal de comunicación una linea telefónica y notamos que existe interferencia, o algún posible ruido que no permite una buena recepción de los mensajes, podríamos malintepretar la información que se nos pretende entregar, por lo que estaríamos ante una situación en la cual la integridad del mensaje comunicado se vería alterada, teniendo como resultado una comuni-

cación defectuosa. Otro punto relevante que en ocasiones se busca mantener, es la confidencialidad del mensaje que se pretende enviar. Para tales casos se implementan variadas formas de comunicación buscando que sólo el emisor y receptor puedan conocer la información que se está mandando, tratando siempre de evitar que un posible tercero pueda observar, interceptar o robar la información. A fin de mantener dicha confidencialidad se han implementado a lo largo de los años diferentes sistemas buscando evitar que la información enviada de un punto a otro sea malutilizada por intrusos o personas ajenas, siendo por ejemplo, La Máquina Enigma o La Escítala Espartana, dos de los sistemas de ocultamiento de información mas reconocidos históricamente. En nuestros días el caracter confidencial de la información juega un rol de vital importancia, sobre todo en procesos de transferencias de datos a través de ordenadores, principalmente en la utilización de claves secretas a través de internet donde siempre la seguridad de nuestra información personal se ve amenazada, por lo cual se hace necesario implementar fórmulas que ayuden a mantener el caracter confidencial de los datos que entregamos.

El proceso en sí, de ocultar la información ya sea cifrándola o codificándola recibe el nombre de criptografía, y tiene como principal objetivo lograr que únicamente emisor y receptor conozcan la forma de codificar y decodificar respectivamente dicha información. Clásicamente la criptografía se basa en la utilización de técnicas que le permitan a un determinado emisor encriptar una cierta información mediante un método previamente acordado con el receptor del mensaje, de manera tal que este último sea capaz de decodificar los datos recibidos y así reconstruir el mensaje original que se le está intentando entregar. Los ejemplos de criptografía clásica son variados, y van desde simples sistemas artesanales, hasta complejas maquinas uilizadas en el siglo XX, sin embargo con el correr de los años tales sitemas se han vuelto vulnerables ya que de alguna u otra manera se ha descubierto la forma de ocultar y revelar la información. En base a esto y buscando

nuevas alternativas al problema de la confidencilidad de la información, en la última parte del siglo XX se comienzan a utilizar las herramientas, hasta ese momento conocidas de la mecánica cuántica, a fin de lograr plantear algún modelo capaz de garantizar una transferencia segura de datos entre emisor y receptor. Surge así en 1984 un modelo criptográfico llamado Protocolo BB84, que proponía la utilización de pulsos monofotónicos en cuyas polarizaciones se guardaría la información que se deseaba comunicar, ofreciendo la posibilidad de detectar intrusos que pretendieran violar la confidencilidad de la información. A partir de entonces se ha utilizado la mecánica cuántica para establecer modelos de criptografía útiles y que vayan de la mano con los avances de la tecnología, abriendo así una nueva área investigativa que busca ser un aporte para el desarrollo de las actuales y futuras comunicaciones.

Nosotros proponemos un modelo criptográfico centrándonos en mantener la confidencialidad de claves secretas al momento de su transmisión a través de un canal cuántico, considerenado la presencia de un posible intruso que intente captar la información sin ser detectado. Para tal modelo utilizamos pulsos de múltiples fotones, considerando las ventajas que éstos ofrecen en la práctica en comparación a los pulsos monofotónicos. Además nos basamos en las características del Protocolo BB84 para plantear un modelo análogo que permita realizar una transmisión de fotones a una mayor distancia de la que nos permitiría la utilización de pulsos monofotónicos.

Capítulo 1

Conceptos previos

1.1. Criptografía

La criptografía ha estado presente en diversos momentos de la historia de la humanidad debido a la necesidad del hombre de ocultar información en diferentes procesos de comunicación. Su nombre se debe a la finalidad que ésta persigue, que es lograr ocultar (del griego, *criptos*) una cierta información o escritura (del griego, *grafos*) a posibles terceros [1], y ha sido utilizada como una herramienta de comunicación que ha ayudado a mantener la confidencialidad de mensajes que un emisor intente comunicar a determinados receptores. De esta manera se intenta cumplir con el objetivo de que la información no sea interceptada por intrusos, ocultando el contenido que puede llevar algún determinado mensaje. Es en este aspecto donde radica su diferencia con otra técnica de ocultamiento de datos: la esteganofragía. Ésta última busca trasmitir un mensaje sin que algún intruso sepa de su existencia, por lo tanto la seguridad del mensaje se garantiza y no se hace necesario implementar algún método para codificarlo. La criptografía en cambio tiene como objetivo mantener la confidencialidad del mensaje, implementado para ello algún sistema en el que sólo el emisor y receptor sean capaces de codificar y decodificar respectivamente la información, incluso sabiendo que un posible intru-

so conoce la existencia del mensaje.

Si bien la principal finalidad de la criptografía es mantener en lo posible la confidencialidad de la información, también se busca entregar seguridad en relación a otros aspectos que podrían ser puestos en duda en la transmisión de un mensaje. Tal es el caso de la autenticación, que en un mensaje nos ayuda a asegurarnos de que el emisor es realmente quien dice ser, evitando de esta manera la suplantación. Además, como en todo proceso de comunicación, la idea principal es mantener la integridad de mensaje para que así el receptor obtenga la información tal y como fue emitida por el emisor. Por último, la criptografía nos da la seguridad del no repudio, es decir, si un emisor envía un mensaje, éste no puede negar haber realizado dicha acción.

La utilización de la criptografía no es reciente, ya que ha sido implementada desde hace muchos años en diferentes momentos de la historia, donde las técnicas de cifrado de información fueron variadas y efectivas para ese entonces. Si bien el avance de las tecnologías ha permitido una evolución en los procesos de comunicación de un punto a otro, se debe tener en cuenta que no siempre el hombre contó con las herramientas que hoy nos brinda la computación y/o la informática. Al comienzo las comunicaciones se basaban en simples alteraciones textuales que podían ser descrifradas por un receptor gracias al conocimiento que éste tenía del método de codificación utilizado por el emisor. Luego los métodos fueron variando hasta utilizar la computación en procesos criptográficos basados en sistemas binarios desarrollados en ordenadores clásicos. Hoy en día se trabajan las ideas de utilizar las herramientas de la mecánica cúantica para desarrollar modelos criptográficos mas confiables y que otorguen una seguridad óptima en algun proceso de comunicación.

1.1.1. Criptografía Clásica

Los medios para llevar a cabo una comunicación pueden ser variados, sin embargo deben garantizar la seguridad del mensaje que se pretende transmitir. Ya hace muchos años diferentes civilizaciones buscaban llevar a cabo sistemas de comunicación que fueran confiables, a fin de evitar que receptores indeseados interceptaran el mensaje [2]. La Escítala por ejemplo, fue un método utilizado por los espartanos en campañas militares con el cual buscaban salvaguardar la información, siendo ésta enviada a través de un mensajero encargado de llevarla desde un lugar a otro. El método implementaba una franja de cuero o papiro donde era escrito el mensaje, además de dos varas, las cuales estaban una en poder del emisor y la otra en poder del receptor, teniendo como única condición que ambas debían tener el mismo diámetro. La idea era que el emisor enrollara la franja de cuero completamente a lo largo de una de las varas y luego escribiera el mensaje en forma vertical, es decir longitudinalmente desde la parte superior de la vara hacia la inferior, para que de esta manera al desenrollar la franja de cuero el mensaje se volviera ilegible. Luego el emisario llevaba el mensaje en la franja de cuero al receptor, quien sabiendo el diámetro de la vara utilizada por el emisior la enrollaba en otra de similares características, logrando leer verticalmente la información. La ventaja de este método radica en el hecho de que en caso de ser interceptado el emisario que llevaba el mensaje, la información no podría haber sido descifrada, ya que dicho proceso requería conocer el grosor de la vara utilizada al momento de ocultar la información.

Otro método simple y común que se ha utilizado por años en la codificación de mensajes es el Código César, el cual recibe su nombre gracias al emperador Julio César, quien lo utilizaba para transmitir información durante campañas militares, de tal modo que el contenido real del mensaje no fuera descifrado por posibles

Figura 1.1: Escítala Espartana.

intrusos. Este método consiste en un cifrado de desplazamiento, es decir en una sustitución de cada una de las letras del mensaje original por otra que se encuentre un cierto número de espacios mas adelante en el alfabeto utilizado. El Cifrado de César no es el primer método de sustitución del que se tenga registro, sin embargo es el mas reconocido y se basa en un desplazamiento de tres letras en el alfabeto, de modo que si en el mensaje original se tenía la letra A, en el mensaje cifrado aparecería la letra D, luego la letra B tendría que ser sustituida por la letra E, la C por la F, y así sucesivamente hasta lograr escribir un determinado mensaje. Si bien este método fue bastante utilizado, no se caracteriza por ser del todo seguro, ya que la forma de decodificar la información y obtener el mensaje original es bastante simple, siempre y cuando se sepa la cantidad de espacios en que se han desplazado cada una de las letras del mensaje codificado por el emisor.

a)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

b) *Mensaje original* / *Mensaje cifrado*

CHILE / *FKLOH*

Figura 1.2: Código César: a) Alfabeto original y alfabeto cifrado. b) Ejemplo del cifrado de un mensaje.

Otro contexto histórico donde estuvo presente la criptografía fue durante la primera y segunda guerra mundial a mediados del siglo XX. La forma de cifrar y descifrar mensajes fue llevada a cabo mayormente con una máquina electromecánica de cifrado rotativo llamada Enigma, la cual fue utilizada por las fuerzas alemanas para desarrollar sus diferentes procesos de comunicación debido a las características que ofrecía y que supuestamente garantizaban la seguridad de la información. El funcionamiento de la máquina se lograba gracias a las componentes eléctricas y mecánicas que esta poseía, y a un teclado que permitía escribir el mensaje como si se tratara de una máquina de escribir común y corriente, donde cada una de las letras correspondía a un interrumptor que enviaba una corriente a un sistema de engranajes mecánicos para finalmente iluminar una de las apolletas de un panel de luces, asociadas también cada una de ellas a una letra. En su parte mecánica la máquina contaba con un sistema de rotores, donde cada rotor correspondía a un disco plano con 26 contactos en cada una de sus caras, que representaban las letras del alfabeto. Los rotores avanzaban un espacio cada vez que se introducía una letra y estaban cableados internamente para transmitir la señal eléctrica que se recibía desde el teclado. La idea era que el cableado interno no uniera las letras de una cara con las mismas letras de la cara opuesta, sino que por ejemplo, la letra 1 de la primera cara estuviera conectada a la 15 de la otra cara, la 2 a la 21, las 3 a la 9, etc, y de esa forma la información se transmitía de rotor en rotor, sabiendo que todos ellos tenian cableados diferentes. Por lo tanto en la salida del último rotor se obtendría una letra distinta a la que se tecleó y esa señal llegaría finalmente a un reflector, el cual mandaría la señal de vuelta a través de la máquina pasando de la misma forma por los diferentes rotores, teniendo como punto final al panel de luces donde se iluminaría la correpondiente letra cifrada. Esto significaba que para codificar la información se debían reemplazar las letras del mensaje original, que se ingresaban a la máquina, por las letras que se iban iluminando en el panel de luces. Luego el hecho de que la Máquina Enigma tuviera

un reflector permitía envíar la señal de vuelta en sentido opuesto a través de ella, lo que hacía posible además de crifrar el mensaje, poder descifrarlo. Obviamente para lograr aquello era necesario que la configuración inicial de la máquina con la que se decodificaría la información fuera la misma que la configuración inicial de la máquina utilizada por el emisor al momento de codificar el mensaje, es decir que el cableado interno de ambas debía ser idéntico, de tal modo de poder ahora en sentido inverso reconstruir el mensaje original.

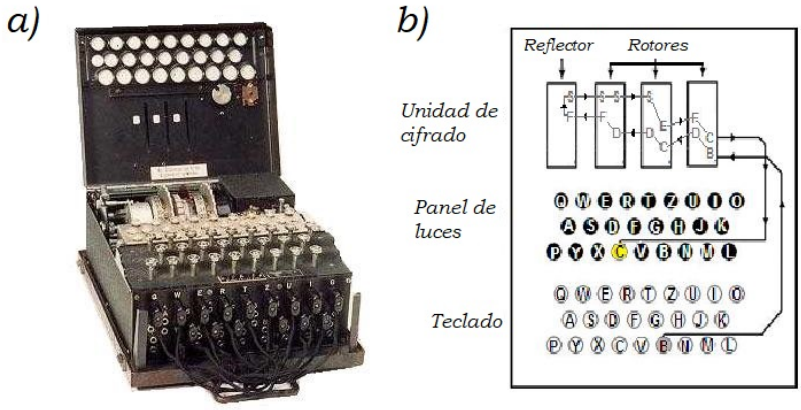

Figura 1.3: Máquina Enigma: a) Imagen referencial. b) Representación del circuito de la señal eléctrica a través de la máquina.

En la década del setenta, comenzó a desarrollarse un nuevo método de criptografía basado en un código criptográfico de clave pública, con el cual se pretendía salvaguardar la información que un determinado emisor transmitía a otros destinatarios. Este tipo de método utiliza dos claves para el envío de mensajes, una pública que puede ser entregada a cualquier persona, y otra privada, perteneciendo ambas a un mismo usuario. De esta forma un determinado emisor podría utilizar la clave pública de un receptor para codificar el mensaje, de modo que sólo éste último sea capaz de decodificarlo mediante la utilización de su clave privada, lo que garantizará la seguridad de la transmisión, ya que sólo el receptor conoce su

propia clave privada. Por otro lado, el emisor del mensaje puede codificar utilizando su propia clave privada de modo que cualquier receptor pueda ahora utilizar la clave pública del propio emisor para descifrarlo, con lo cual se logra corroborar la autentificación del emisor [3]. Un ejemplo de este tipo de modelo criptográfico es el Código RSA [4], el cual fue desarrollado en 1977, convirtiéndose en una útil herramienta para cifrar información y para validar idenificaciones mediante firmas digitales. El funcionamiento de este código se basa en la utilización de números para representar la información que se quiera transmitir, y en la factorización de números enteros, y su seguridad se garantiza gracias al problema de la factorización de numeros demasiado grandes en números primos de considerable extensión, lo cual convierte una encriptación realizada con el código RSA en un problema indescifrable incluso para los ordenadores que se utilizan hoy en día. Sin embargo, dicha seguridad fue puesta en riesgo por el profesor de matemáticas estadounidense Peter Shor, cuando en la década del noventa dio a conocer un algoritmo en el cual planteaba teóricamente la posibilidad de fractorizar números de cualquier extensíon, facilitando asi la obtención de los números primos utilizados en la codificación de la información [5]. Dicho algoritmo plantea que el problema de la factorización puede solucionarse implementando un ordenador cuántico capaz de desarrollar dicha función en un tiempo razonablemente menor a lo conocido hasta hoy. Esta idea se mantiene aún en un plano teórico ya que pese a los avances de la computación cuántica se estima que la creación de un ordenador de estas características no será posible al menos en un futuro cercano.

1.1.2. Criptografía Cuántica

Pese a la utilidad que en su momento representaron los modelos criptográficos descritos anteriormente, con el paso del tiempo éstos fueron perdiendo su eficiencia en cuanto a su segurirdad, ya que a través de diferentes criptoanálisis quedaron

al descubierto las maneras de encriptar y desencriptar la información en cada uno de ellos, lo que a su vez motivó el desarrollo de nuevos sistemas de transmisión de información seguros y confiables.

Además de los ya descritos, uno de los sistemas criptográficos mas famosos fue el Cifrado de Vernam, algoritmo creado por Gilbert Vernam en 1917 [6], el cual fue también implementado durante la segunda guerra mundial. Su modo de aplicarlo era muy sencillo, sólo se debía combinar el mensaje original con una clave aleatoria cuya extensión fuera igual a la extensión del mensaje. De esta forma si el emisor y receptor acordaban una cierta clave, éstos podrían codificar y decodificar respectivamente el mensaje, teniendo en cuenta que una vez recibido, la clave en cuestión no podía ser utilizada para transmitir un nuevo mensaje de diferente extensión. Un ejemplo del Cifrado de Vernam podría mostrarse de la siguiente forma, considerando que cada letra del alfabeto queda en correspondencia con un número, lo cual nos permite sumar las letras del mensaje original con las letras que conforman la clave secreta aleatoria:

Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numeración	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Mensaje	L	A		M	E	C	A	N	I	C	A		C	U	A	N	T	I	C	A							
Numeración	12	1		13	5	3	1	14	9	3	1		3	22	1	14	21	9	3	1							
Clave aleatoria	D	G		T	R	S	H	J	Z	P	O		T	F	B	H	U	S	R	V							
Numeración	4	7		21	19	20	8	10	27	17	16		21	6	2	8	22	20	19	23							
Codificación	O	H		G	W	V	I	W	I	S	P		W	A	C	U	O	B	U	W							
Numeración	16	8		7	24	23	9	24	9	20	17		24	1	3	22	16	2	22	24							

Figura 1.4: Ejemplo del Cifrado de Vernam

La obtención de los caracteres del mensaje codificado se logra teniendo en cuenta que la suma entre la clave aleatoria y el mensaje original debe ser una suma módulo 27, es decir, cuando se sobrepasa ese valor se debe volver al número

inicial. Finalmente, una vez que el mensaje codificado llegue al receptor éste deberá hacer el proceso inverso, restando ahora la clave aleatoria para reconstruír así el mensaje original enviado por el emisor. Este método fue estudiado por Claude Shannon, quien demosotró con su trabajo "Teoría de las comunicaciones secretas" [7] que dadas sus características este cifrado resultaba perfectamente seguro, ya que no había forma alguna de analizarlo criptográficamente. Sin embargo como ya se ha dicho, el problema de la utilización de este método radica en sólo poder utilizar la clave aleatoria una única vez, por lo que en caso de querer enviar un nuevo mensaje el emisor y receptor deberían comunicarse entre sí una nueva clave secreta a través de un canal seguro, de tal forma que ésta no sea descubierta por algún posible espía. Pero el hecho de contar con un canal seguro resulta imposible, ya que de contar con uno éste sería utilizado para enviar el propio mensaje antes que una clave de codificación, lo que nos lleva a concluir que este método resulta ideal en cuanto a la seguridad que nos ofrece, aunque no nos permite realizar una confiable distribución de clave secreta para enviar nuevos mensajes. En este punto es donde aparece la mecánica cuántica como una herramienta útil para solucionar este problema, y lograr así una distribución segura de claves secretas pese a la posible presencia de un intruso.

1.1.3. Protocolo BB84

En 1984 Charles Benett y Gilles Brassard llegaron a proponer un modelo de comunicación que ofrece la posibilidad de lograr una distribución confiable de claves de seguridad, su nombre, Protocolo BB84 [8]. Su principal finalidad se centraba en transmitir una clave binaria de seguridad entre un emisor y un receptor, denominados de aquí en adelante, Alice y Bob respectivamente, quienes haciendo uso tanto de un canal cuántico de comunicación, como de un canal clásico pudieran compartir los correspondientes bits, ceros o unos, a fin de lograr formar una clave

conocida únicamente por ambos. La manera de transmitir dicha información desde Alice hasta Bob se realiza mediante el envío de pulsos monofotónicos, de tal modo que el cero o uno que se está intentando compartir se codifica en la polarización del fotón que constituye dicho pulso, previo acuerdo de la convención bit/polarización entre Alice y Bob, la cual consideramos de la siguiente forma.

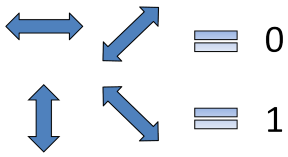

Figura 1.5: Protocolo BB84: Convención de polarizaciones.

- El bit 0 corresponde a polarización horizontal y/o polarización oblicua a 45^o.
- El bit 1 corresponde a polarización vertical y/o polarización oblicua a -45^o.

Con la convención de polarizaciones ya acordada, Alice polarizará en forma aleatoria el fotón que enviará, ya sea en la base (0,90) o (-45,45), para que posteriormente Bob eligа, también en forma aleatoria, la base con la cual medirá la polarización del fotón que reciba. Si la base que utilizaron ambos coincide, significará que Bob podrá medir exactamente lo que Alice intentó enviarle, de lo contrario sus resultados no coincidirán y deberán ser descartados. Por ejemplo, si Alice utiliza una polarización vertical para transmitir el bit uno, significa que Bob debería utilizar la base (0,90) para medir correctamente la polarización del fotón, ya que usando la base (-45,45) tendría la misma probabilidad de medir polarizacion oblicua a -45^o y a 45^o, lo que significa que podría obtener con igual probabilidad un cero o un uno.

En un escenario ideal de comunicación se puede pensar que en el proceso participan únicamente Alice y Bob, descartando la presencia de intrusos que intercepten

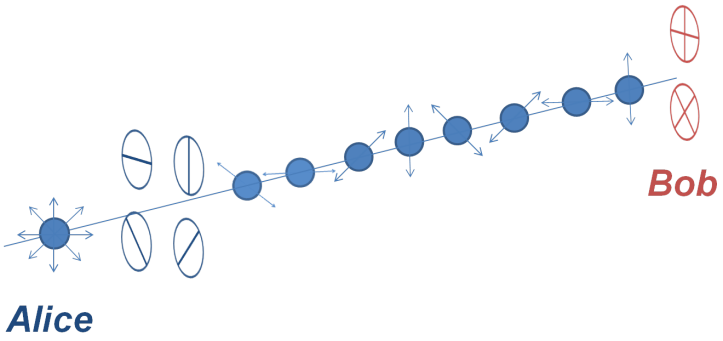

Figura 1.6: Protocolo BB84: Transmisión de bits mediante polarizaciones aleatorias.

los fotones. En tal caso, como Alice y Bob están codificando y decodificando la información utilizando bases aleatorias, se estima que al comparar las bases utilizadas sus elecciones coincidirán en la mitad de los casos, los cuales deberían ser utilizados para generar la clave. Sin embargo, si hablamos de criptografía debemos simpre plantear un modelo de comunicación capaz de garantizar la seguridad del mensaje en presencia o no de un intruso que intente robarnos información. Comencemos entonces desarrollando el protocolo considerando inicialmente que las bases utilizadas no son aleatorias, y trabajando únicamente con la base horizontal/vertical, suponiendo además que un tercero, Eva, intenta captar la información codificada en la polarización de cada fotón con la intención de descifrar la clave de seguridad que se está intentando comunicar.

En este esquema, el hecho de trabajar con una base determinada implica la imposibilidad de detectar un posible intruso, ya que si Alice codifica por ejemplo, en la base (0,90) y tanto Eva como Bob utilizan esa misma base, éste último podrá medir las mismas polarizaciones que envió Alice, sin percatarse que Eva midió previamente las mismas polarizaciones. Tal situación se ejemplifica en la siguiente figura y tabla, donde se muestra que la base usada por Eva no altera la polarización

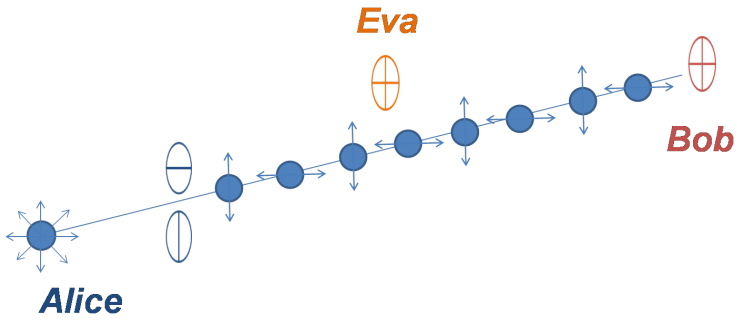

Figura 1.7: Protocolo BB84: Eva intenta captar la información enviada por Alice, quien polariza en la base horizontal/vertical.

enviada por Alice.

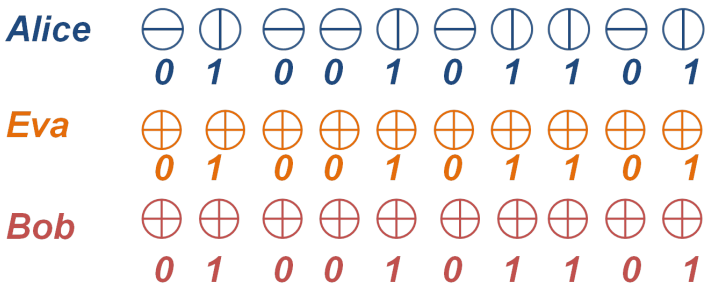

Figura 1.8: Protocolo BB84: Eva y Bob miden en la misma base de codificación de Alice, por lo que no es posible detectar la presencia de Eva.

Para permitir la detección de un intruso en la distribución de claves secretas, en el protocolo BB84 se plantea realizar un esquema similar al anterior pero variando de forma aleatoria las bases de polarización que utiliza Alice para codificar los bits que componen la clave. Esto implica que tanto Eva como Bob deberán también escoger de forma aleatoria las bases que utilizarán para medir la polarización del fotón.

Aqui los casos 2, 3, 6 y 8 son descartados inmediatamente debido a que la

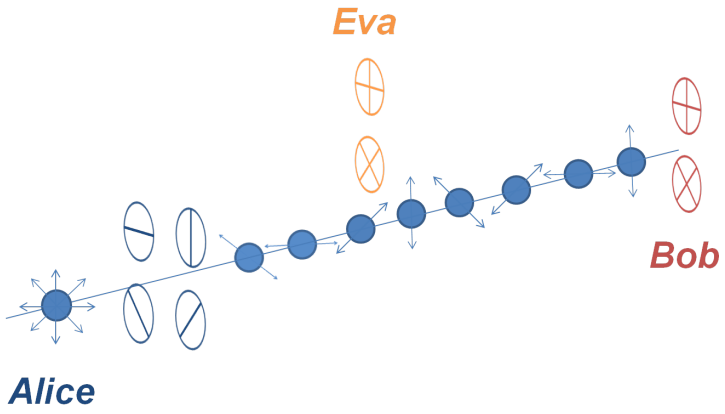

Figura 1.9: Esquema del Protocolo BB84.

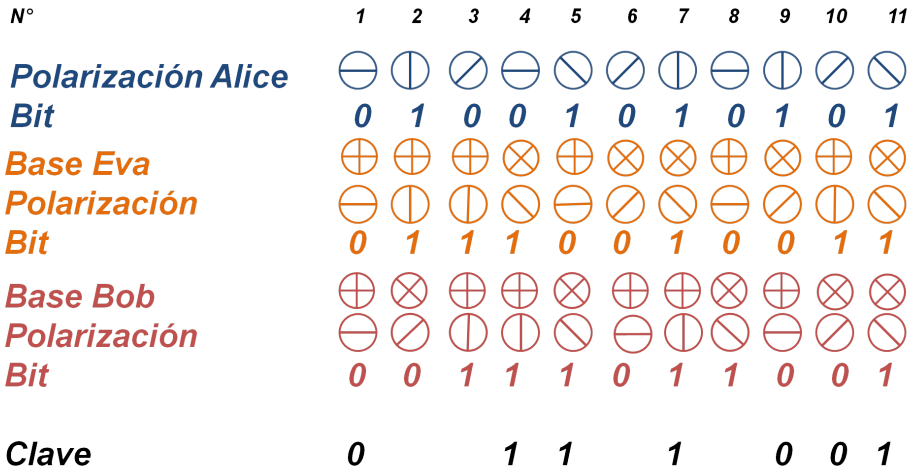

Figura 1.10: Protocolo BB84: Distribución de clave.

base utilizada por Bob no coincide con la base utilizada por Alice. Luego podemos ver que en los casos 1 y 11 la base usada por Alice coincide con la de Bob y además con la de Eva, por lo cual ésta última seguiría sin ser detectada ya que su medición no alteró las polarizaciones iniciales. La forma de descubrir su presencia es comparar una secuencia de la clave obtenida y verificar que esta vez coincidan los valores medidos, ya que pese a coincidir las bases de Alice y Bob, es posible que los resultados obtenidos hayan sido alterados por la medición previa de Eva.

Tal situación se observa en los casos 4, 5, 7, 9 y 10 donde la base utilizada por Eva difiere de las usada por Alice y Bob, lo cual genera que la polarización que recibe Bob esté condicionada por la medición previa de Eva, la que en algunos casos tendrá como consecuencia el volteo del valor del bit recibido por Bob, como se ve en los casos 4 y 9. En otros casos en cambio, los bits mantendrán su valor original aún cuando Eva haya intervenido en el proceso. Finalmente cuando se compara una parte de la clave y se verifica que hay diferencias en ciertos valores de los bits no descartados de Alice y Bob, se logra detectar la presencia del intruso y se aborta el proceso de comunicación, ya que no reune las características necesarias para desarrollar una transmisión segura de información.

1.2. Cuantización del campo electromagnético

Como se mostró en la sección anterior, el protocolo BB84 se basa en la utilización de pulsos monofotónicos para llevar a cabo un proceso de comunicación entre Alice y Bob, con la finalidad de establecer una clave secreta entre ambas partes impidiendo en lo posible que ésta sea descifrada por Eva. En nuestro trabajo, a diferencia del protocolo recién descrito, se pretenden implementar pulsos de multiples fotones, por lo que debemos hallar las herramientas que nos permitan representar el proceso. Para esto analizaremos las características cuánticas de la naturaleza de la luz mediante la cuantización del campo electromagnético. Comenzaremos con el tratamiento clásico del campo electromagnético centrándonos primeramente en las ecuaciones de Maxwell en el espacio libre:

$$\nabla \cdot \mathbf{B} = 0, \tag{1.1a}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}, \tag{1.1b}$$

$$\nabla \cdot \mathbf{D} = 0, \tag{1.1c}$$

$$\nabla \times \mathbf{H} = \frac{\partial \mathbf{D}}{\partial t}, \tag{1.1d}$$

donde $\mathbf{B} = \mu_0\mathbf{H}$ y $\mathbf{D} = \epsilon_0\mathbf{E}$, con μ_0 y ϵ_0 siendo respectivamente la permeabilidad magnética y a la permitividad eléctrica del vacío, las cuales cumplen con la relación $\mu_0\epsilon_0 = c^{-2}$ [9]. Además dado que las ecuaciones de Maxwell son invariantes ante transformaciones de gauge, se trabaja con uno que resulte conveniente en el tratamiento de problemas de óptica cuántica, como es el caso del gauge de Coulomb, donde los campos $\mathbf{E}$ y $\mathbf{B}$ se obtienen a partir del vector potencial $\mathbf{A}(\mathbf{r}, t)$ de la forma

$$\mathbf{B} = \nabla \times \mathbf{A} \tag{1.2a}$$

$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t} \tag{1.2b}$$

con la condición de gauge $\nabla\cdot \mathbf{A} = 0$, lo cual nos permite, reemplazando las expresiones de $\mathbf{B}$ y $\mathbf{E}$ en la ecuación (1.1d), y teniendo en cuenta la relación $\nabla \times (\nabla \times \mathbf{A}) = \nabla(\nabla\cdot \mathbf{A}) - \nabla^2\mathbf{A}$, llegar a

$$\nabla^2\mathbf{A} = \frac{1}{c^2}\frac{\partial^2\mathbf{A}}{\partial t^2}. \tag{1.3}$$

Para facilitar el desarrollo de esta expresión se considera un campo restringido a un cierto volumen finito del espacio, lo cual nos permite desarrollar la solución de $\mathbf{A}$ en una serie de Fourier

$$\mathbf{A}(\mathbf{r}, t) = \sum_k c_k\mathbf{u}_k(\mathbf{r})e^{-i\omega_k t} + \sum_k c_k^*\mathbf{u}_k^*(\mathbf{r})e^{i\omega_k t} \tag{1.4}$$

que reemplazándola en la expresión (1.3) da como resultado una ecuación de Helmholtz para el conjunto de funciones vectoriales $\mathbf{u}_k(\mathbf{r})$ correspondiente a

$$\left(\nabla^2 + \frac{\omega_k^2}{c^2}\right)\mathbf{u}_k(\mathbf{r}) = 0, \tag{1.5}$$

donde las funciones $\mathbf{u}_k(\mathbf{r})$ por ser obtenidas a partir de $\mathbf{A}$ también deben cumplir con la condición $\nabla\cdot \mathbf{u}_k(\mathbf{r}) = 0$. Además forman un conjunto ortonormal completo,

$$\int_V \mathbf{u}_k^*(\mathbf{r})\mathbf{u}_{k'}(\mathbf{r})dV = \delta_{kk'}. \tag{1.6}$$

La solución para la ecuación (1.5) va a depender del volumen considerado, ya que éste definirá las condiciones de borde. Por ejemplo, si consideramos como volumen un cubo de lado L, podremos definir condiciones de borde periódicas, las cuales corresponden a ondas viajeras. Para tal volumen las funciones modo de ondas planas apropiadas pueden ser escritas como

$$\mathbf{u}_k(\mathbf{r}) = L^{-\frac{3}{2}}\hat{\mathbf{e}}^{(\lambda)}e^{i\mathbf{kr}} \tag{1.7}$$

donde $\hat{\mathbf{e}}^{(\lambda)}$ corresponde a un vector unitario de polarización perpendicular a $\mathbf{k}$, con $\lambda = 1, 2$. Es decir, que existen dos posibles polarizaciones. Por otro lado, el índice k describe varias variables discretas y caracteriza un modo en particular, mientras que $\mathbf{k}$ corresponde al vector de propagación, cuyas componentes están dadas por

$$k_x = \frac{2\pi n_x}{L}, \qquad k_y = \frac{2\pi n_y}{L}, \qquad k_z = \frac{2\pi n_z}{L}, \tag{1.8}$$

con $n_x, n_y, n_z = 0, \pm1, \pm2, ...$

El vector $\mathbf{A}(\mathbf{r}, t)$ puede ser escrito ahora como

$$\mathbf{A}(\mathbf{r}, t) = \sum_k \sqrt{\frac{\hbar}{2\omega_k\epsilon_0}}\left[a_k\mathbf{u}_k(\mathbf{r})e^{-i\omega_k t} + a_k^*\mathbf{u}_k^*(\mathbf{r})e^{i\omega_k t}\right], \tag{1.9}$$

donde a_k son constantes adimensionales que representan la amplitud compleja del modo k correspondiente. Luego el campo eléctrico estará dado por

$$\mathbf{E}(\mathbf{r}, t) = i\sum_k \sqrt{\frac{\hbar\omega_k}{2\epsilon_0}}\left[a_k\mathbf{u}_k(\mathbf{r})e^{-i\omega_k t} - a_k^*\mathbf{u}_k^*(\mathbf{r})e^{i\omega_k t}\right]. \tag{1.10}$$

Clásicamente estas amplitudes de Fourier corresponden a números complejos, y por lo tanto para cuantizar el campo se deben elegir estas amplitudes como operadores, considerando a_k como $\hat{a}_k$, y a_k^* como $\hat{a}_k^\dagger$. Luego los estados de luz son los vectores en el espacio de Hilbert en el que actúan estos operadores, y el campo $\mathbf{E}(\mathbf{r}, t)$ viene dado entonces por

$$\mathbf{E}(\mathbf{r}, t) = i\sum_k \sqrt{\frac{\hbar\omega_k}{2\epsilon_0}}\left[\hat{a}_k\mathbf{u}_k(\mathbf{r})e^{-i\omega_k t} - \hat{a}_k^\dagger\mathbf{u}_k^*(\mathbf{r})e^{i\omega_k t}\right]. \tag{1.11}$$

Dado que los fotones tienen espín 1, las realaciones de conmutación adecuadas entre los operadores $\hat{a}_k$ y $\hat{a}_k^\dagger$ deben ser las relaciones de conmutación bosónicas.

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0 \tag{1.12a}$$

$$[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'} \tag{1.12b}$$

El comportamiento dinámico de las amplitudes del campo eléctrico puede entonces ser descrito por un conjunto de osciladores armónicos independientes, los cuales obedecen las relaciones de conmutación (1.12a) y (1.12b). El estado cuántico de cada uno de los modos puede ser representado por un vector estado $|\Psi\rangle_k$ del espacio de Hilbert correspondiente, y por ende el estado del campo total puede ser obtenido como un producto tensorial entre los estados de cada uno de los modos independientes.

Finalmente, el Hamiltoniano del campo electromagnético estará dado por

$$H = \frac{1}{2}\int_V \left(\epsilon_0 \mathbf{E}^2 + \mu_0 \mathbf{H}^2\right) dV, \tag{1.13}$$

donde ya es conocida la expresión que define $\mathbf{E}$, y analogamente podemos obtener $\mathbf{H}$. Luego reemplazando ambos campos en (1.13) y teniendo en cuenta la condicion (1.6) junto con $\nabla\cdot\, \mathbf{u}_k(\mathbf{r}) = 0$, se obtiene que

$$H = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2}\right), \tag{1.14}$$

cuyos autovalores vienen dados por

$$E_k = \hbar\omega_k \left(n_k + \frac{1}{2}\right) \tag{1.15}$$

para cada modo k. Por lo tanto, teniendo ya definida la cuantización del campo electromágnetico, nos centraremos ahora en las formas de representarlo mediante estados cuánticos.

1.3. Estados cuánticos

Una vez cuantizado el campo electromagnético definiremos los estados con los cuales lo representaremos. Primero estudiamos los estados número o estados de Fock, en base a los cuales obtendremos la definición de estados coherentes, con los que representaremos los pulsos de multiples fotones. Veremos también que estos últimos corresponden a un caso especial de una familia mas general de estados llamados estados comprimidos.

1.3.1. Estados número o estados de Fock

Como se mostró en la subsección anterior, el Hamiltoniano correspondiente a la cuatización del campo electromagnético tiene los autovalores $\hbar\omega_k(n_k + \frac{1}{2})$, donde n_k corresponde a un número entero que representa el número de fotones del k-ésimo modo, cuyos valores pueden ir desde cero a infinito. Identificamos entonces al operador $\hat{a}_k^\dagger \hat{a}_k$ como el operador número de fotones $\hat{N}_k$, ya que sus autovalores corresponden precisamente a n_k, y sus autoestados son escritos como $|n_k\rangle$, los cuales son conocidos como estados número o estados de Fock

$$\hat{N}_k|n_k\rangle = \hat{a}_k^\dagger \hat{a}_k|n_k\rangle = n_k|n_k\rangle. \tag{1.16}$$

Estos estados forman un conjunto ortogonal y completo, por lo tanto cumplen con las relaciones

$$\langle n_k|m_k\rangle = \delta_{nm} \tag{1.17}$$

y

$$\sum_{n_k=0}^{\infty} |n_k\rangle\langle n_k| = 1. \tag{1.18}$$

La forma en que actúan tanto $\hat{a}^\dagger$ como $\hat{a}$ sobre los estados $|n\rangle$ va estar dada por

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle, \tag{1.19a}$$

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \tag{1.19b}$$

de modo que para obtener una representación de los estados número se define como estado fundamental, o estado del vacío a $|0\rangle$, que cumple con

$$\hat{a}|0\rangle = 0, \tag{1.20}$$

y cuya energía corresponde a $\frac{1}{2}\sum_k \hbar\omega_k$. Luego, para obtener los vectores $|n_k\rangle$ que definan estados mayormente excitados, bastará con aplicar el operador de creación $\hat{a}^\dagger$ tantas veces como sea necesario, de tal forma que

$$|n_k\rangle = \frac{\left(\hat{a}_k^\dagger\right)^{n_k}}{(n_k!)^{\frac{1}{2}}}|0\rangle, \tag{1.21}$$

donde $n_k = 0, 1, 2, ...$

1.3.2. Estados coherentes

La expresión (1.21) corresponde a la definición de los estados número, y otorga una forma útil de representar fotones de alta energía, como por ejemplo los rayos γ donde el número de fotones es pequeño. Por el contrario, cuando se trata de problemas en los cuales está involucrado un número mayor de fotones, estos estados no son la mejor opción, aunque si pueden ser utilizados para definir una base de nuevos estados que describan problemas en los cuales el numero de fotones sea grande. Tales estados son los estados coherentes $|\alpha\rangle$, los cuales tienen un número indefinido de fotones, por lo cual nos serán útiles para representar pulsos se múltiples fotones.

Recordemos que al cuantizar el campo electromagnético se obtuvo que este puede ser descrito como un conjunto de osciladores armónicos independientes, donde el número de fotones involucrados se obtiene a partir del operador número $\hat{N} = \hat{a}_k^\dagger \hat{a}_k$, donde $\hat{a}_k$ corresponde al operador de anhiquilación y $\hat{a}_k^\dagger$ al operador de creación, los cuales puenden ser representados respectivamente como un número complejo y su adjunto conjugado, tal que [9]

$$\hat{a} = \frac{1}{\sqrt{2}}\left(\hat{X}_1 + i\hat{Y}_1\right), \tag{1.22a}$$

$$\hat{a}^\dagger = \frac{1}{\sqrt{2}}\left(\hat{X}_1 - i\hat{Y}_1\right), \tag{1.22b}$$

donde los operadores hermíticos $\hat{X}_1$ y $\hat{Y}_1$ se denominan operadores cuadratura, los cuales podemos despejar para hallar la relación de incertidumbre entre ambos.

$$\hat{X}_1 = \frac{1}{\sqrt{2}}\left(\hat{a} + \hat{a}^\dagger\right) \tag{1.23a}$$

$$\hat{Y}_1 = \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right). \tag{1.23b}$$

La relación de conmutación entre ambas cuadraturas será por lo tanto

$$[\hat{X}_1, \hat{Y}_1] = i, \tag{1.24}$$

y las varianzas de cada una

$$V(\hat{X}_1) = (\Delta\hat{X}_1)^2 = \langle\hat{X}_1^2\rangle - \langle\hat{X}_1\rangle^2 \tag{1.25a}$$

$$V(\hat{Y}_1) = (\Delta\hat{Y}_1)^2 = \langle\hat{Y}_1^2\rangle - \langle\hat{Y}_1\rangle^2 \tag{1.25b}$$

por lo tanto el correspondiente principio de incertidumbre es

$$\Delta\hat{X}_1\Delta\hat{Y}_1 \geq \frac{1}{2}. \tag{1.26}$$

Para el caso de los estados coherentes se cuple que $\Delta\hat{X}_1 = \Delta\hat{Y}_1 = \frac{1}{\sqrt{2}}$, por lo que representan una familia de estados de mínima incerteza, y se pueden considerar como un caso particular dentro de la familia de estados que satisfacen la desigualdad (1.26). Los estados coherentes $|\alpha\rangle$ se definen como los autoestados del operador de anhiquilación del oscilador armónico, tal que:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{1.27}$$

donde el autovalor α es un número complejo. El estado coherente $|\alpha\rangle$ se puede generar a partir del vacío mediante la aplicación del operador desplazamiento $\hat{D}(\alpha)$ sobre el estado $|0\rangle$, de modo que

$$\hat{D}(\alpha)|0\rangle = |\alpha\rangle, \tag{1.28}$$

donde

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \tag{1.29}$$

con α siendo un valor complejo arbitrario. Dada la forma que tiene la expresión (1.29), ésta puede ser desarrollada teniendo en cuenta el teorema de operadores

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}\ e^{\hat{B}}\ e^{-\frac{[\hat{A},\hat{B}]}{2}} \tag{1.30}$$

que se cumple cuando $\hat{A}$ y $\hat{B}$ satisfacen la relación $[\hat{A},[\hat{A},\hat{B}]] = [\hat{B},[\hat{A},\hat{B}]] = 0$, por lo cual la nueva forma de $\hat{D}(\alpha)$ será

$$\hat{D}(\alpha) = e^{-\frac{|\alpha|^2}{2}}\ e^{\alpha\hat{a}^\dagger}\ e^{-\alpha^*\hat{a}}, \tag{1.31}$$

que además cumple con las propiedades

$$\hat{D}^\dagger(\alpha) = \hat{D}^{-1}(\alpha) = \hat{D}(-\alpha), \tag{1.32a}$$

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha, \tag{1.32b}$$

$$\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*, \tag{1.32c}$$

las cuales cuales pueden ser utilizadas para demostrar la igualdad (1.27), considerando la expresión

$$\hat{D}^\dagger(\alpha)\hat{a}|\alpha\rangle = \hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha)|0\rangle = (\hat{a}+\alpha)|0\rangle = \hat{a}|0\rangle + \alpha|0\rangle = \alpha|0\rangle, \tag{1.33}$$

que al ser multiplicada en ambos lados por $\hat{D}(\alpha)$ permite demostrar la ecuación de autovalores $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$.

Descritas las propiedades del operador que permite generar los estados coherentes, analizamos la forma de representar matemáticamente estos últimos. Para ello buscamos la forma que tiene $|\alpha\rangle$ como superposición de los estados número $\{|n\rangle\}$, tal que

$$|\alpha\rangle = \sum_{n=0}^{\infty} |n\rangle\langle n|\alpha\rangle = \sum_{n=0}^{\infty}\langle n|\alpha\rangle|n\rangle. \tag{1.34}$$

Luego para obtener el valor de $\langle n|\alpha\rangle$ multiplicamos por $\langle n|$ a ambos lados la expresión (1.27):

$$\langle n|\hat{a}|\alpha\rangle = \sqrt{n+1}\langle n+1|\alpha\rangle = \alpha\langle n|\alpha\rangle, \tag{1.35}$$

de modo que

$$\langle n+1|\alpha\rangle = \frac{\alpha}{\sqrt{n+1}}\langle n|\alpha\rangle. \tag{1.36}$$

Por lo tanto, dada la definición (1.21) podemos obtener las expresiones correspondientes para $\langle n|\alpha\rangle$ y $\langle n+1|\alpha\rangle$ que satisfacen (1.36)

$$\langle n|\alpha\rangle = \langle 0|\frac{\hat{a}^n}{\sqrt{n!}}|\alpha\rangle = \frac{\alpha^n}{\sqrt{n!}}\langle 0|\alpha\rangle \tag{1.37a}$$

$$\langle n+1|\alpha\rangle = \langle 0|\frac{\hat{a}^{(n+1)}}{\sqrt{(n+1)!}}|\alpha\rangle = \frac{\alpha^{(n+1)}}{\sqrt{(n+1)!}}\langle 0|\alpha\rangle. \tag{1.37b}$$

Esto nos permite reemplazar (1.37a) en (1.34):

$$|\alpha\rangle = \sum_{n=0}^{\infty}|n\rangle\langle n|\alpha\rangle = \sum_{n=0}^{\infty}\langle n|\alpha\rangle|n\rangle = \langle 0|\alpha\rangle\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{1.38}$$

por lo que sólo restaría definir $\langle 0|\alpha\rangle$, para lo cual debemos considerar que el estado $|\alpha\rangle$ debe estar normalizado tal que $|\langle\alpha|\alpha\rangle|^2 = 1$.

$$|\langle\alpha|\alpha\rangle|^2 = |\langle 0|\alpha\rangle|^2\sum_{n=0}^{\infty}\frac{|\alpha|^{2n}}{n!} = |\langle 0|\alpha\rangle|^2 e^{|\alpha|^2} = 1, \tag{1.39}$$

luego

$$\langle 0|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}}\ , \tag{1.40}$$

por lo que el estado coherente queda finalmente definido como

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}}\ \sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{1.41}$$

con la distribución de probabilidad de fotones dada por

$$P_n = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}e^{-|\alpha|^2}}{n!}, \tag{1.42}$$

que corresponde a una distribución de Poisson, donde $|\alpha|^2$ es el número medio de fotones, es decir

$$\bar{n} = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = |\alpha|^2. \tag{1.43}$$

1.3.3. Estados comprimidos

Los estados coherentes corresponden a estados cuyas cuadraturas son iguales, y cumplen con la relación $\Delta\hat{X}_1 = \Delta\hat{Y}_1 = \frac{1}{\sqrt{2}}$, por lo que representan estados de mínima incerteza, y son un caso especial dentro de una clase más general de estados que cumplen con la relación (1.26). El resto de los estados que junto a los estados coherentes satisfacen el principio de incertidumbre, pueden presentar mayor incertidumbre en una de sus cuadraturas, lo que a fin de cumplir con (1.26), conlleva una incerteza menor en la otra. Estos son los llamados estados comprimidos y se definen como

$$|\alpha, \epsilon\rangle = D(\alpha)S(\epsilon)|0\rangle, \tag{1.44}$$

donde $S(\epsilon)$ corresponde al operador squeeze o de compresión dado por

$$S(\epsilon) = e^{\frac{1}{2}(\epsilon^* \hat{a}^2 - \epsilon \hat{a}^{\dagger 2})} \tag{1.45}$$

con ϵ siendo un parámetro complejo tal que $\epsilon = re^{i\theta}$.

Capítulo 2

Formalismo teórico

A fin de lograr un modelo de detección de intrusos en un proceso de comunicación entre Alice y Bob, estudiaremos los efectos producidos por un beam splitter y por un canal cuántico de comunicación sobre un pulso láser de múltiples fotones enviado por Alice. Como es de esperarse, en dicho proceso la cantidad de fotones recibidos por Bob no será la misma que la enviada por Alice, es decir que cierta parte de la información enviada se perderá a lo largo del camino recorrido por la luz. En principio Alice y Bob podrían considerar esta diferencia en la cantidad de partículas enviadas y recibidas como pérdidas producidas por el canal cúantico de comunicación, lo cual sucede de forma natural y no involucra a terceras personas. Por otro lado, si bien las pérdidas pueden originarse por la acción del canal, debemos tener en cuenta que éstas también podrían ser consecuencia de la presencia de un intruso, quien mediante la implementación de un beam splitter puede interceptar el pulso enviado y desviar parte de la luz con la intención de captar la información que se pretende comunicar. Esto nos dice entonces que al momento de analizar la información recibida, no será posible detectar la presencia de un posible intruso, ya que no se tendrá la certeza de la causa de las pérdidas.

Nosotros estudiamos la posibilidad de diferenciar las pérdidas producidas por

un canal cuántico de comunicación de las pérdidas originas por un beam splitter, lo cual permitiría detectar la presencia de un tercero. Para tal propósito analizamos las disribuciones de probabilidad del estado final en poder de Bob una vez que éste recibe la información proveniente de Alice, la que se envía a través de pulsos de múltiples fotones representados mediante estados coherentes. Además añadimos un fotón extra al estado enviado por Alice a fin de analizar los cambios en las distribuciones de probabilidad que éste podría generar.

2.1. Estado coherente

Para analizar los efectos producidos por el beam splitter y por el canal cuántico de comunicación, consideramos el pulso inicial enviado por Alice como un estado coherente $|\alpha\rangle$ el cual a medida que se transmite es modificado en base a las características del canal o del beam splitter. Por lo tanto considerando (1.41) y (1.42) podemos analizar la distribución de probabilidad del estado coherente una vez que sea transmitido y recibido por Bob.

2.2. Estado coherente con fotón añadido

El segundo estado que analizamos corresponde a un estado coherente con un fotón extra, a fin de estudiar posibles alteraciones en las distribuciones de probabilidad del estado recibido por Bob luego de las acciones del canal y del beam splitter. El fotón añadido lo obtenemos teóricamente aplicando simplemente el operador $\hat{a}^\dagger$ sobre el estado coherente $|\alpha\rangle$ [12] quedando el estado resultante definido por

$$|\alpha,1\rangle = \frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}} = \frac{\hat{a}^\dagger}{\sqrt{1+|\alpha|^2}} e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle = \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{1+|\alpha|^2}} \sum_{n=0}^{\infty} \frac{\alpha^n\sqrt{(n+1)!}}{n!}|n+1\rangle. \tag{2.1}$$

En la práctica en cambio, el proceso se torna mas complejo, y se hace necesario implementar un PDC (parametric down-converter) [13] mediante el cual se logre añadir un único fotón a un pulso de multiples fotones. Dichas operaciones de añadir (o sustraer) un fotón a (o de) un determinado pulso, fueron consideradas como un proceso netamente teórico hasta el año 2004, cuando experimentalmente se logró extraer un fotón de un pulso mediante la utilización de un beam splitter de baja reflectividad [14].

2.3. Representación del beam splitter

La representación cuántica del beam splitter requiere recordar su descripción gráfica considerando e identificando los operadores de aniquilación asociados a cada puerto de entrada y salida del dispositivo [15], los cuales nos ayudarán a analizar los efectos que éste tenga sobre los pulsos de fotones que estudiaremos.

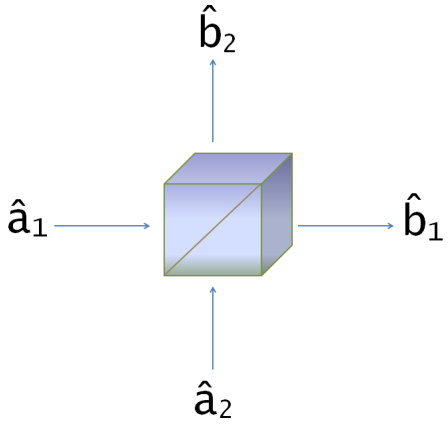

Figura 2.1: Geometría del beam splitter: Puertos de entrada operadores $\hat{a}_1$ y $\hat{a}_2$. Puertos de salida operadores $\hat{b}_1$ y $\hat{b}_2$.

La información que Alice quiera enviar se ubicará en el puerto del operador $\hat{a}_1$ y la información que reciba Bob ocupará el puerto del operador $\hat{b}_1$. Por su parte Eva recibirá la información que logre desviar en el puerto del operador $\hat{b}_2$ y en

el puerto del operador $\hat{a}_2$ habrá sólo vacío. Luego para obtener la distribución de probabilidad del estado en poder de Bob debemos representar el beam splitter mediante un operador cuántico que actúe sobre el estado inicial $|\alpha\rangle$ enviado por Alice. Definimos entonces como punto de partida el porcentaje de transmisión y reflexión del dispositivo, dados por τ y ρ respectivamente,

$$\tau \equiv \cos^2(\theta) \tag{2.2a}$$

$$\rho \equiv \sin^2(\theta), \tag{2.2b}$$

donde $0 \leq \theta \leq \frac{\pi}{2}$, corresponde al parámetro angular que determina las magnitudes que caracterizan al beam splitter. Por otro lado, los cambios de fase que puede generar el beam splitter sobre el campo de entrada son representados por ϕ_τ, y ϕ_ρ para los campos transmitidos y reflejados respectivamente. Según esto el dispositivo en cuestión puede ser representado mediante un operador cuántico definido por [16] [17] [18]:

$$\hat{\mathbf{B}}(\Phi, \Theta, \Psi) = e^{-i\Phi\hat{L}_3}\ e^{-i\Theta\hat{L}_2}\ e^{-i\Psi\hat{L}_3}\ , \tag{2.3}$$

donde los parámetros Φ, Ψ y Θ se relacionan con θ, ϕ_τ, y ϕ_ρ de acuerdo a

$$\theta = \frac{\Theta}{2}, \quad \phi_\tau = \frac{1}{2}(\Psi + \Phi), \quad \phi_\rho = \frac{1}{2}(\Psi - \Phi). \tag{2.4}$$

Como alternativa a lo descrito hasta aqui, se puede considerar la acción del beam splitter sobre algun estado de entrada, como los efectos opuestos del operador beam splitter sobre el mismo estado, tal que

$$|\psi_{out}\rangle = \hat{B}^\dagger|\psi_{in}\rangle \tag{2.5}$$

y

$$\hat{\rho}_{out} = \hat{B}^\dagger\hat{\rho}_{in}\hat{B}. \tag{2.6}$$

Por lo tanto, para obtener los estados resultantes de la acción del beam splitter se necesita $\hat{\mathbf{B}}^\dagger$;

$$\hat{\mathbf{B}}^\dagger(\Phi, \Theta, \Psi) = e^{i\Psi\hat{L}_3}\ e^{i\Theta\hat{L}_2}\ e^{i\Phi\hat{L}_3}, \tag{2.7}$$

donde los momentos angulares $\hat{L}_1, \hat{L}_2$ y $\hat{L}_3$ corresponden a

$$\hat{L}_1 = \frac{1}{2}(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1) \tag{2.8a}$$

$$\hat{L}_2 = \frac{1}{2i}(\hat{a}_1^\dagger \hat{a}_2 - \hat{a}_2^\dagger \hat{a}_1) \tag{2.8b}$$

$$\hat{L}_3 = \frac{1}{2}(\hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2). \tag{2.8c}$$

Ademas se definen $\hat{L}_+$ y $\hat{L}_-$ como

$$\hat{L}_+ = \hat{L}_1 + i\hat{L}_2 = \hat{a}_1^\dagger \hat{a}_2 \tag{2.9a}$$

$$\hat{L}_- = \hat{L}_1 - i\hat{L}_2 = \hat{a}_2^\dagger \hat{a}_1, \tag{2.9b}$$

con lo cual se tiene que

$$\hat{\mathbf{B}}^\dagger(\Phi, \Theta, \Psi) = e^{i\Psi \hat{L}_3}\ e^{\frac{\Theta}{2}(\hat{L}_+ - \hat{L}_-)}\ e^{i\Phi \hat{L}_3} = \hat{U}_3 \hat{U}_2 \hat{U}_1, \tag{2.10}$$

tal que $\hat{U}_3 = e^{i\Psi \hat{L}_3}$, $\hat{U}_2 = e^{\frac{\Theta}{2}(\hat{L}_+ - \hat{L}_-)}$ y $\hat{U}_1 = e^{i\Phi \hat{L}_3}$.

Como los operadores $\hat{U}_1$ y $\hat{U}_3$ están asociadas a $\hat{L}_3$ podemos aplicarlos directamente dado que se sabe la forma en que operan. Mientras que para conocer la forma en que opera $\hat{U}_2$, debemos reescribirlo como [19]

$$\hat{U}_2(\Theta) = e^{\frac{\Theta}{2}(\hat{L}_+ - \hat{L}_-)}\ = e^{\lambda_1(\Theta)\hat{L}_-}\ e^{\lambda_0(\Theta)\hat{L}_3}\ e^{\lambda_2(\Theta)\hat{L}_+}\ , \tag{2.11}$$

y encontrar el valor de los términos λ_0, λ_1 y λ_2 tomando la derivada con respecto a θ de la igualdad (2.11), de modo que

$$\begin{aligned}
\frac{d\hat{U}_2}{d\Theta} &= \frac{1}{2}(\hat{L}_+ - \hat{L}_-)\hat{U}_2(\Theta) \\
&= \lambda_1{}'(\Theta)\hat{L}_- e^{\lambda_1(\Theta)\hat{L}_-}\ e^{\lambda_0(\Theta)\hat{L}_3}\ e^{\lambda_2(\Theta)\hat{L}_+} \\
&+ \lambda_0{}'(\Theta) e^{\lambda_1(\Theta)\hat{L}_-}\ \hat{L}_3 e^{\lambda_0(\Theta)\hat{L}_3}\ e^{\lambda_2(\Theta)\hat{L}_+} \\
&+ \lambda_2{}'(\Theta) e^{\lambda_1(\Theta)\hat{L}_-}\ e^{\lambda_0(\Theta)\hat{L}_3}\ \hat{L}_+ e^{\lambda_2(\Theta)\hat{L}_+} \\
&= \lambda_1{}'(\Theta)\hat{L}_-\hat{U}_2(\Theta) + \lambda_0{}'(\Theta) e^{\lambda_1(\Theta)\hat{L}_-}\hat{L}_3 e^{-\lambda_1(\Theta)\hat{L}_-}\hat{U}_2(\Theta) \\
&+ \lambda_2{}'(\Theta) e^{\lambda_1(\Theta)\hat{L}_-} e^{\lambda_0(\Theta)\hat{L}_3}\ \hat{L}_+ e^{-\lambda_0(\Theta)\hat{L}_3}\ e^{-\lambda_1(\Theta)\hat{L}_-}\hat{U}_2(\Theta),
\end{aligned} \tag{2.12}$$

por lo tanto

$$\frac{1}{2}(\hat{L}_+ - \hat{L}_-) = \lambda_1{}'(\Theta)\hat{L}_- + \lambda_0{}'(\Theta)e^{\lambda_1(\Theta)\hat{L}_-}\hat{L}_3 e^{-\lambda_1(\Theta)\hat{L}_-} + \lambda_2{}'(\Theta)e^{\lambda_1(\Theta)\hat{L}_-}e^{\lambda_0(\Theta)\hat{L}_3}\ \hat{L}_+ e^{-\lambda_0(\Theta)\hat{L}_3}\ e^{-\lambda_1(\Theta)\hat{L}_-}. \tag{2.13}$$

Recordemos que [20] [21]

$$e^A\ Be^{-A} = B + [A,B] + \frac{1}{2!}[A,[A,B]] + ..., \tag{2.14}$$

y que $\hat{L}_+$, $\hat{L}_-$ y $\hat{L}_3$ cumplen con

$$[\hat{L}_-, \hat{L}_+] = -2\hat{L}_3, \tag{2.15a}$$

$$[\hat{L}_3, \hat{L}_\pm] = \pm\hat{L}_\pm, \tag{2.15b}$$

formando el algebra del grupo SU(2) [22].

Aplicando (2.14), (2.15a) y (2.15b) al segundo y tercer sumando del lado derecho de la ecuación (2.13) se tiene que

$$\begin{aligned} e^{\lambda_1(\Theta)\hat{L}_-}\hat{L}_3 e^{-\lambda_1(\Theta)\hat{L}_-} &= \hat{L}_3 + \lambda_1(\Theta)[\hat{L}_-, \hat{L}_3] + \frac{1}{2!}[\lambda_1(\Theta)\hat{L}_-, [\lambda_1(\Theta)\hat{L}_-, \hat{L}_3]] + ... \\ &= \hat{L}_3 + \lambda_1(\Theta)\hat{L}_- + \frac{1}{2!}[\lambda_1(\Theta)\hat{L}_-, \lambda_1(\Theta)\hat{L}_-] \\ &= \hat{L}_3 + \lambda_1(\Theta)\hat{L}_- \end{aligned} \tag{2.16}$$

$$\begin{aligned} e^{\lambda_0(\Theta)\hat{L}_3}\hat{L}_+ e^{-\lambda_0(\Theta)\hat{L}_3} &= \hat{L}_+ + \lambda_0(\Theta)[\hat{L}_3, \hat{L}_+] + \frac{1}{2!}[\lambda_0(\Theta)\hat{L}_3, [\lambda_0(\Theta)\hat{L}_3, \hat{L}_+]] + ... \\ &= \hat{L}_+ + \lambda_0(\Theta)\hat{L}_+ + \frac{1}{2!}[\lambda_0(\Theta)\hat{L}_3, \lambda_0(\Theta)\hat{L}_+] + ... \\ &= \hat{L}_+ + \lambda_0(\Theta)\hat{L}_+ + \frac{\lambda_0^2}{2}\hat{L}_+ + ... \\ &= \sum_{n=o}^{\infty} \frac{\lambda_0^n}{n!}\hat{L}_+ \\ &= e^{\lambda_0}\ \hat{L}_+. \end{aligned} \tag{2.17}$$

Por lo que

$$\begin{aligned}\frac{1}{2}(\hat{L}_+ - \hat{L}_-) &= \lambda_1{}'(\Theta)\hat{L}_- + \lambda_0{}'(\Theta)(\hat{L}_3 + \lambda_1(\Theta)\hat{L}_-) + \lambda_2{}'(\Theta)e^{\lambda_1(\Theta)\hat{L}_-}e^{\lambda_0}\ \hat{L}_+e^{-\lambda_1(\Theta)\hat{L}_-} \\ &= \lambda_1{}'(\Theta)\hat{L}_- + \lambda_0{}'(\Theta)(\hat{L}_3 + \lambda_1(\Theta)\hat{L}_-) + \lambda_2{}'(\Theta)e^{\lambda_0}\ e^{\lambda_1(\Theta)\hat{L}_-}\hat{L}_+e^{-\lambda_1(\Theta)\hat{L}_-},\end{aligned} \tag{2.18}$$

donde el tercer sumando de la derecha aún se puede resolver aplicando la expresión (2.14), tal que

$$\begin{aligned}e^{\lambda_1(\Theta)\hat{L}_-}\hat{L}_+e^{-\lambda_1(\Theta)\hat{L}_-} &= \hat{L}_+ + \lambda_1(\Theta)[\hat{L}_-, \hat{L}_+] + \frac{1}{2!}[\lambda_1(\Theta)\hat{L}_-, [\lambda_1(\Theta)\hat{L}_-, \hat{L}_+]] + ... \\ &= \hat{L}_+ - \lambda_1(\Theta)2\hat{L}_3 + \lambda_1^2(\Theta)[\hat{L}_-, \hat{L}_3] + ... \\ &= \hat{L}_+ - 2\lambda_1(\Theta)\hat{L}_3 - \lambda_1^2(\Theta)\hat{L}_-,\end{aligned} \tag{2.19}$$

entonces

$$\begin{aligned}\frac{1}{2}(\hat{L}_+ - \hat{L}_-) &= \lambda_1{}'(\Theta)\hat{L}_- + \lambda_0{}'(\Theta)(\hat{L}_3 + \lambda_1(\Theta)\hat{L}_-) + \lambda_2{}'(\Theta)e^{\lambda_0(\Theta)}\ (\hat{L}_+ - 2\lambda_1(\Theta)\hat{L}_3 - \lambda_1^2(\Theta)\hat{L}_-) \\ &= \lambda_2^{'}(\Theta)e^{\lambda_0(\Theta)}\ \hat{L}_+ + (\lambda_0^{'} - 2\lambda_1(\Theta)\lambda_2^{'}(\Theta)e^{\lambda_0(\Theta)}\ )\hat{L}_3 \\ &+ (\lambda_1^{'}(\Theta) + \lambda_1(\Theta)\lambda_0^{'}(\Theta) - \lambda_1^2(\Theta)\lambda_2^{'}e^{\lambda_0(\Theta)}\ )\hat{L}_-,\end{aligned} \tag{2.20}$$

y comparando ambos lados de la ecuación se tiene que

$$\lambda_2^{'}(\Theta)e^{\lambda_0(\Theta)} = \frac{1}{2} \tag{2.21}$$

$$\lambda_1^{'}(\Theta) + \lambda_1(\Theta)\lambda_0^{'}(\Theta) - \lambda_1^2(\Theta)\lambda_2^{'}(\Theta)e^{\lambda_0(\Theta)} = -\frac{1}{2} \tag{2.22}$$

$$\lambda_0^{'}(\Theta) - 2\lambda_1(\Theta)\lambda_2^{'}e^{\lambda_0(\Theta)}\ = 0. \tag{2.23}$$

De la ecuación (2.21) se obtiene que

$$\lambda_2^{'}(\Theta) = \frac{1}{2}e^{-\lambda_0(\Theta)}, \tag{2.24}$$

lo que al ser reemplazado en (2.23) da

$$\lambda_0^{'}(\Theta) = \lambda_1(\Theta). \tag{2.25}$$

A su vez, reemplazando (2.24) y (2.25) en la ecuación (2.22), se obtiene la ecuación diferenclal

$$\lambda_1^{'}(\Theta) + \lambda_1^2(\Theta) - \lambda_1^2(\Theta)\frac{1}{2}e^{-\lambda_0}\ e^{\lambda_0}\ = \lambda_1^{'}(\Theta) + \frac{1}{2}\lambda_1^2(\Theta) = -\frac{1}{2}, \tag{2.26}$$

que reordenada corresponde a

$$\frac{d\lambda_1(\Theta)}{1+\lambda_1^2(\Theta)} = -\frac{1}{2}d\Theta, \tag{2.27}$$

cuya solución se obtiene considerando que

$$\int \frac{1}{a^2+x^2}dx = \frac{1}{a}\arctan\left(\frac{x}{a}\right). \tag{2.28}$$

Por lo tanto, de (2.27) se obtiene que

$$\longrightarrow \lambda_1(\Theta) = \tan\left(-\frac{\Theta}{2}\right). \tag{2.29}$$

Luego podemos reemplazar λ_1 en (2.25), donde

$$\lambda_0^{'}(\Theta) = \tan\left(-\frac{\Theta}{2}\right), \tag{2.30}$$

de modo que

$$\lambda_0(\Theta) = \int_0^{\Theta} \tan\left(-\frac{\Theta}{2}\right)d\Theta. \tag{2.31}$$

$$\longrightarrow \lambda_0(\Theta) = -2\ln\left(\sec\left(\frac{-\Theta}{2}\right)\right). \tag{2.32}$$

Este resultado lo reemplazamos en la ecuación (2.24),

$$\lambda_2^{'} = \frac{1}{2}e^{2\ln\left(\sec\left(-\frac{\Theta}{2}\right)\right)}, \tag{2.33}$$

donde

$$\lambda_2(\Theta) = \frac{1}{2}\int \sec^2\left(-\frac{\Theta}{2}\right)d\Theta \tag{2.34}$$

$$\longrightarrow \lambda_2(\Theta) = -\tan\left(-\frac{\Theta}{2}\right). \tag{2.35}$$

Con estos resultados se representa $\hat{U}_2$ como

$$\begin{aligned}\hat{U}_2(\Theta) = e^{\frac{\Theta}{2}(\hat{L}_+ - \hat{L}_-)} &= e^{\lambda_1(\Theta)\hat{L}_-}\ e^{\lambda_0(\Theta)\hat{L}_3}\ e^{\lambda_2(\Theta)\hat{L}_+} \\ &= e^{\tan\left(-\frac{\Theta}{2}\right)\hat{L}_-}\ e^{-2\ln\left(\sec\left(\frac{-\Theta}{2}\right)\right)\hat{L}_3}\ e^{-\tan\left(-\frac{\Theta}{2}\right)\hat{L}_+}\ ,\end{aligned} \tag{2.36}$$

por lo tanto la representación final de $\hat{\mathbf{B}}^\dagger$ tendrá la forma

$$\hat{\mathbf{B}}^\dagger(\Phi,\Theta,\Psi) = e^{i\Psi\hat{L}_3}\ e^{\tan\left(-\frac{\Theta}{2}\right)\hat{L}_-}\ e^{-2\ln\left(\sec\left(\frac{-\Theta}{2}\right)\right)\hat{L}_3}\ e^{-\tan\left(-\frac{\Theta}{2}\right)\hat{L}_+}\ e^{i\Phi\hat{L}_3}. \tag{2.37}$$

2.4. Representación del canal cuántico

Al momento de enviar la información mediante un pulso debemos considerar que el canal utilizado para transmitirlo no es ideal y que puede producir pérdidas de parte de la información, por lo que Bob no recibirá la misma cantidad de fotones que Alice envió. De esta manera el ruido propio de dicho canal será un constante problema en la comunicación, aunque no impedirá el intercambio de información siempre y cuando la cantidad de pérdidas no sea significativa. Bajo estas condiciones debemos considerar entonces que el estado enviado por Alice interactúa con el entorno en el cual está siendo transmitido, de tal forma que el estado final que se obtiene una vez transmitida la información dependerá de las características del canal utilizado y del tiempo que le lleve al pulso ir desde Alice a Bob, por lo que debemos considerar la interacción entre el canal y el estado enviado, para luego analizar la evolución temporal de ésta como un sistema abierto.

Los sistemas cuánticos abiertos han sido mayormente estudiados en el campo de la óptica cuántica, teniendo como proncipal objetivo el hecho de describir la evolución temporal de dichos sistemas mediante la implementación de una acuación diferencial que describa el comportamiento no unitario que implica la interacción con el entorno. Tal objetivo se logra mediante la ecuación maestra [23], que puede

ser escrita de manera mas general en la forma de Lindblad [24]

$$\frac{d\hat{\rho}}{dt} = -\frac{i}{\hbar}[\hat{H}, \hat{\rho}] + \sum_j \left[2\hat{L}_j \hat{\rho} \hat{L}_j^\dagger - \{\hat{L}_j^\dagger \hat{L}_j, \hat{\rho}\}\right], \tag{2.38}$$

donde $\hat{H}$ es un Hamiltoniano efectivo sobre el sistema en cuestión. Por otro lado, los $\hat{L}_j$ son los operadores de Lindblad que representan el acoplamiento del sistema con su entorno, los que en nuestro caso corresponden al estado enviado por Alice y al canal cuántico de comunicación respectivamente. El término de la forma $\{x, y\}$ dentro de la sumatiora denota un anticomutador entre x e y, tal que $\{x, y\} = xy + yx$.

En general se asume que el sistema y el entorno se vinculan como un estado producto, por lo que para determinar los $\hat{L}_j$ se comienza con un modelo Hamiltoniano sistema-entorno. Como ejemplo de la ecuacón de Lindblad podemos considerar un átomo de dos niveles acoplado al vacío, presentando emisión espontánea. La evolución temporal del átomo es descrita mediante el Hamiltoniano $\hat{H} = -\hbar\omega\hat{\sigma}_z/2$, donde $\hbar\omega$ es la diferencia de energía entre los niveles del átomo. De esta manera la emisión espontánea de un fotón dará cuenta que el átomo excitado en el nivel $|1\rangle$ decae a su estado fundamental $|0\rangle$. Esta emisión es representada por el operador de Lindblad $\sqrt{\mathcal{K}}\sigma_-$, donde $\hat{\sigma}_- \equiv |0\rangle\langle 1|$ representa el decaimiento en el nivel de energía del átomo, y $\mathcal{K}$ corresponde a la tasa de emisión de fotones. De este modo la ecuación maestra que describirá este proceso tendrá la forma

$$\frac{d\hat{\rho}}{dt} = -\frac{i}{\hbar}\left[\hat{H}, \hat{\rho}\right] + \mathcal{K}\left[2\hat{\sigma}_-\hat{\rho}\hat{\sigma}_+ - \hat{\sigma}_+\hat{\sigma}_-\hat{\rho} - \hat{\rho}\hat{\sigma}_+\hat{\sigma}_-\right], \tag{2.39}$$

donde $\hat{\sigma}_+ \equiv \hat{\sigma}_-^\dagger$ es el operador de aumento de energía del átomo para pasar del estado $|0\rangle$ al estado $|1\rangle$. La solución a esta ecuación diferencial se logra haciendo el cambio de variable

$$\hat{\tilde{\rho}}(t) \equiv e^{i\hat{H}t}\hat{\rho}(t)e^{-i\hat{H}t}, \tag{2.40}$$

de tal forma que

$$\frac{d\hat{\tilde{\rho}}}{dt} = \mathcal{K}\left[2\hat{\tilde{\sigma}}_-\hat{\tilde{\rho}}\hat{\tilde{\sigma}}_+ - \hat{\tilde{\sigma}}_+\hat{\tilde{\sigma}}_-\hat{\tilde{\rho}} - \hat{\tilde{\rho}}\hat{\tilde{\sigma}}_+\hat{\tilde{\sigma}}_-\right], \tag{2.41}$$

donde

$$\hat{\tilde{\sigma}}_- \equiv e^{i\hat{H}t}\hat{\sigma}_- e^{-i\hat{H}t} \equiv e^{-i\omega t}\hat{\sigma}_- \tag{2.42a}$$

$$\hat{\tilde{\sigma}}_+ \equiv e^{i\hat{H}t}\hat{\sigma}_+ e^{-i\hat{H}t} \equiv e^{i\omega t}\hat{\sigma}_+. \tag{2.42b}$$

Por lo tanto la ecuación que resulta finalmente como descripción de la evolución temporal del operador densidad corresponde a

$$\frac{d\hat{\tilde{\rho}}}{dt} = \mathcal{K}\left[2\hat{\sigma}_-\hat{\tilde{\rho}}\hat{\sigma}_+ - \hat{\sigma}_+\hat{\sigma}_-\hat{\tilde{\rho}} - \hat{\tilde{\rho}}\hat{\sigma}_+\hat{\sigma}_-\right]. \tag{2.43}$$

Dicha evolución define la interacción del sistema físico con el entorno, tal que si la representamos como el producto entre los espacios que corresponden al sistema y al ambiente, obtendremos la evolución del conjunto como consecuencia de la acción de una operación unitaria $\hat{U}$, quedando el operador densidad del sistema definido como

$$\hat{\rho}(t) = \mathcal{E}(\hat{\rho}(t_0)) = Tr_E(\hat{U}(\hat{\rho}\otimes\hat{\rho}_E)\hat{U}^\dagger) = \sum_n \langle e_n|\hat{U}(\hat{\rho}\otimes\hat{\rho}_E)\hat{U}^\dagger|e_n\rangle = \sum_n \hat{E}_n(t)\hat{\rho}\hat{E}_n^\dagger(t), \tag{2.44}$$

donde $\hat{\rho}$ corresponde al operador densidad del sistema, que interactúa con el entorno representado por $\hat{\rho}_E$ en la base $\{|e_n\rangle\}$ y los $\hat{E}_n$ son los operadores de Kraus, que satisfacen la condición $\sum_n \hat{E}_n^\dagger\hat{E}_n = \mathcal{I}$ y son temporalmente dependientes [25].

En el contexto de nuestro trabajo el sistema afectado por el entorno corresponde al pulso enviado por Alice, el cual se verá afectado por la acción del canal cuántico utilizado y cuya matriz densidad $\hat{\rho}_P$ evolucionará temporalmente de acuerdo a

$$\frac{d\hat{\rho}_P(t)}{dt} = \mathcal{K}\left(2\hat{a}\hat{\rho}_P(t)\hat{a}^\dagger - \hat{a}^\dagger\hat{a}\hat{\rho}_P(t) - \hat{\rho}_P(t)\hat{a}^\dagger\hat{a}\right), \tag{2.45}$$

teniendo como solución la expresión

$$\hat{\rho}_P(t) = \sum_{n=0}^{\infty}\frac{\mathcal{T}^n}{n!}e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\hat{a}^n\hat{\rho}_P(t_0)\hat{a}^{\dagger n}e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}, \tag{2.46}$$

con $\mathcal{T} = 1 - |e^{-\mathcal{K}t}|^2$, donde además consideramos que el canál cuántico actúa básicamente como un baño a temperatura $T = 0$ [26]. Luego, de acuerdo a (2.44) podemos reescribir $\hat{\rho}_P(t)$ como

$$\hat{\rho}_P(t) = \sum_{n=0}^{\infty} \hat{M}_n \hat{\rho}_P(t_0) \hat{M}_n^\dagger, \tag{2.47}$$

identificando el operador de Kraus para la amplitud de amortiguación del canal cuántico de comunicación como

$$\hat{M}_n = \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}} \hat{a}^n, \tag{2.48}$$

cumpliendo con la condición $\sum_{n=0}^{\infty} \hat{M}_n^\dagger \hat{M}_n = 1$, y siendo una operación cuántica que preserva la traza, tal que $Tr\hat{\rho}(t) = Tr \sum_{n=0}^{\infty} \hat{M}_n^\dagger \hat{\rho}(t_0) \hat{M}_n = Tr\hat{\rho}(t_0) = 1$.

Capítulo 3

Modelo

Teniendo en cuenta la forma que toma el operador $\hat{\mathbf{B}}$, veremos como se ve afectado un estado coherente debido a la acción de un beam splitter. Además podemos saber los efectos que tendrá el canal cuántico sobre un estado coherente teniendo en cuenta la ecuación de pérdidas.

3.1. Acción de un beam splitter

3.1.1. Estado coherente

Ahora que se conoce la forma del operador $\hat{\mathbf{B}}^{\dagger}$ podemos aplicarlo al estado $|\psi_{in}\rangle$ que se obtiene como resultado del producto entre el estado $|\alpha\rangle$ en el puerto

de entrada de Alice, y el estado $|0\rangle$ en el puerto de entrada de Eva.

$$\begin{aligned}
|\psi_{out}\rangle &= \hat{\mathbf{B}}^{\dagger}|\psi_{in}\rangle = \hat{\mathbf{B}}^{\dagger}\left(|\alpha\rangle \otimes |0\rangle\right) \\
&= e^{i\Psi\hat{L}_3}\; e^{\tan\left(-\frac{\Theta}{2}\right)\hat{L}_-}\; e^{-2\ln\left(\sec\left(\frac{-\Theta}{2}\right)\right)\hat{L}_3}\; e^{-\tan\left(-\frac{\Theta}{2}\right)\hat{L}_+}\; e^{i\Phi\hat{L}_3}\left(|\alpha\rangle \otimes |0\rangle\right) \\
&= |\alpha' e^{\frac{i\Psi}{2}}\rangle \otimes |\beta e^{-\frac{i\Psi}{2}}\rangle \\
&= |\alpha\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\; e^{\frac{i\Psi}{2}}\rangle \otimes |-\alpha\sin\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}e^{-\frac{i\Psi}{2}}\rangle \\
&= |\alpha\cos(\theta)e^{\frac{i}{2}(\Phi+\Psi)}\rangle \otimes |-\alpha\sin(\theta)e^{\frac{i}{2}(\Phi-\Psi)}\rangle \\
&= |\alpha\cos(\theta)e^{i\phi_\tau}\rangle \otimes |-\alpha\sin(\theta)e^{-i\phi_\rho}\rangle \\
&= |\alpha''\rangle \otimes |\beta'\rangle,
\end{aligned} \tag{3.1}$$

donde $|\alpha''\rangle$ representa el estado en poder de Bob y $|\beta'\rangle$ el estado en poder de Eva una vez completado el proceso de envío de cada pulso, siendo sus distribuciones de probabilidad respectivamente

$$P_{out}^{Bob} = |\langle n|\alpha''\rangle|^2 = \frac{e^{-|\alpha''|^2}|\alpha''|^{2n}}{n!} \tag{3.2}$$

y

$$P_{out}^{Eva} = |\langle n|\beta'\rangle|^2 = \frac{e^{-|\beta'|^2}|\beta'|^{2n}}{n!}. \tag{3.3}$$

3.1.2. Estado coherente con fotón añadido

Ahora veremos como el operador $\hat{\mathbf{B}}^{\dagger}$ actua sobre un estado coherente con un fotón añadido. Dicho estado se representa como

$$|\alpha, 1\rangle = \frac{\hat{a}^{\dagger}|\alpha\rangle}{\sqrt{1+|\alpha|^2}} = \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{1+|\alpha|^2}}\sum_{n=0}^{\infty}\frac{\alpha^n\sqrt{(n+1)!}}{n!}|n+1\rangle, \tag{3.4}$$

por lo que el estado de entrada para el beam splitter tendrá la forma

$$|\psi_{in}\rangle = |\alpha, 1\rangle \otimes |0\rangle = \frac{\hat{a}^{\dagger}|\alpha\rangle}{\sqrt{1+|\alpha|^2}} \otimes |0\rangle. \tag{3.5}$$

El estado de salida se puede obtener entonces de forma análoga a lo hecho con el estado coherente en la subsección anterior, de modo que:

$$
\begin{aligned}
|\psi_{out}\rangle = \hat{\mathbf{B}}^{\dagger}|\psi_{in}\rangle &= \hat{\mathbf{B}}^{\dagger}\left(\frac{\hat{a}^{\dagger}|\alpha\rangle}{\sqrt{1+|\alpha|^2}}\otimes|0\rangle\right) \\
&= e^{i\Psi\hat{L}_3}\ e^{\tan\left(-\frac{\Theta}{2}\right)\hat{L}_-}\ e^{-2\ln\left(\sec\left(\frac{-\Theta}{2}\right)\right)\hat{L}_3}\ e^{-\tan\left(-\frac{\Theta}{2}\right)\hat{L}_+}\ e^{i\Phi\hat{L}_3}\left(\frac{\hat{a}^{\dagger}|\alpha\rangle}{\sqrt{1+|\alpha|^2}}\otimes|0\rangle\right) \\
&= \frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(e^{\frac{i\Psi}{2}}\ \cos\left(\frac{\Theta}{2}\right)\hat{a}_1^{\dagger}|\alpha' e^{\frac{i\Psi}{2}}\ \rangle\otimes|\beta e^{-\frac{i\Psi}{2}}\ \rangle - e^{-\frac{i\Psi}{2}}\ \sin\left(\frac{\Theta}{2}\right)|\alpha' e^{\frac{i\Psi}{2}}\ \rangle\otimes\hat{a}_2^{\dagger}|\beta e^{-\frac{i\Psi}{2}}\ \rangle\right) \\
&= \frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{i\phi_\tau}\ \cos\left(\theta\right)\hat{a}_1^{\dagger}|\alpha''\rangle\otimes|\beta'\rangle - e^{-i\phi_\rho}\ \sin\left(\theta\right)|\alpha''\rangle\otimes\hat{a}_2^{\dagger}|\beta'\rangle\right).
\end{aligned}
\tag{3.6}
$$

Dicho estado cumple con la condición de normalización $\langle\psi_{out}|\psi_{out}\rangle = 1$, y su operador densidad viene dado por

$$
\begin{aligned}
\rho_{out} &= |\psi_{out}\rangle\langle\psi_{out}| \\
&= \frac{1}{1+|\alpha|^2}\left(e^{i\phi_\tau}\ \cos\left(\theta\right)\hat{a}_1^{\dagger}|\alpha''\rangle\otimes|\beta'\rangle - e^{-i\phi_\rho}\ \sin\left(\theta\right)|\alpha''\rangle\otimes\hat{a}_2^{\dagger}|\beta'\rangle\right) \\
&\left(e^{-i\phi_\tau}\ \cos\left(\theta\right)\langle\alpha''|\hat{a}_1\otimes\langle\beta'| - e^{i\phi_\rho}\ \sin\left(\theta\right)\langle\alpha''|\otimes\langle\beta'|\hat{a}_2\right) \\
&= \frac{1}{1+|\alpha|^2}\Bigg(\cos^2\left(\theta\right)\hat{a}_1^{\dagger}|\alpha''\rangle\langle\alpha''|\hat{a}_1|\beta'\rangle\langle\beta'| - e^{i(\phi_\tau+\phi_\rho)}\cos\left(\theta\right)\sin\left(\theta\right)\hat{a}_1^{\dagger}|\alpha''\rangle\langle\alpha''|\beta'\rangle\langle\beta'|\hat{a}_2 \\
&- e^{-i(\phi_\tau+\phi_\rho)}\cos\left(\theta\right)\sin\left(\theta\right)|\alpha''\rangle\langle\alpha''|\hat{a}_1\hat{a}_2^{\dagger}|\beta'\rangle\langle\beta'| + \sin^2\left(\theta\right)|\alpha''\rangle\langle\alpha''|\hat{a}_2^{\dagger}|\beta'\rangle\langle\beta'|\hat{a}_2\Bigg),
\end{aligned}
\tag{3.7}
$$

mediante el cual podemos obtener ρ_{out}^{Bob}, tomando la traza parcial sobre el estado de Eva, tal que

$$\begin{aligned}\rho_{out}^{Bob} &= Tr_{Eva}(\rho_{out}) = Tr_{Eva}(|\psi_{out}\rangle\langle\psi_{out}|) \\ &= \frac{1}{1+|\alpha|^2}\Bigg(\cos^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1 + \alpha e^{i\phi_\tau}\cos(\theta)\sin^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''| \\ &+ \alpha^* e^{-i\phi_\tau}\cos(\theta)\sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_1 + \sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|(1+|\alpha|^2\sin^2(\theta))\Bigg),\end{aligned} \tag{3.8}$$

donde consideramos $\phi_\tau = 0$, lo que significa que el estado de Bob no presenta ningun cambio de fase con respecto al estado enviado por Alice. Además ρ_{out}^{Bob} cumple con $Tr\{\rho_{out}^{Bob}\} = 1$. Luego la probabilidad de Bob de obtener n fotones será:

$$\begin{aligned}P_n &= \langle n|\rho_{out}^{Bob}|n\rangle \\ &= \frac{e^{-|\alpha''|^2}}{1+|\alpha|^2}\Bigg(\cos^2(\theta)\,n\sum_{n=1}^{\infty}\frac{\alpha''^{2(n-1)}}{(n-1)!} \\ &+ 2\alpha\cos(\theta)\sin^2(\theta)\sqrt{n}\sum_{n=1}^{\infty}\frac{\alpha''^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\alpha''^{n}}{\sqrt{n!}} \\ &+ (\sin^2 + |\alpha|^2\sin^4(\theta))\sum_{n=0}^{\infty}\frac{\alpha''^{2n}}{n!}\Bigg),\end{aligned} \tag{3.9}$$

cumpliendo con la condición $\sum_{n=0} P_n = 1$.

$$\begin{aligned}\sum_{n=0} P_n &= \frac{e^{-|\alpha''|^2}}{1+|\alpha|^2}\Bigg(\Big(\sin^2 + |\alpha|^2\sin^4(\theta)\Big) + \sum_{n=1}^{\infty}\Bigg[\cos^2(\theta)\,n\frac{\alpha''^{2(n-1)}}{(n-1)!} \\ &+ 2\alpha\cos(\theta)\sin^2(\theta)\,\frac{\alpha''^{(2n-1)}}{(n-1)!} + (\sin^2 + |\alpha|^2\sin^4(\theta))\frac{\alpha''^{2n}}{n!}\Bigg]\Bigg) \\ &= 1.\end{aligned} \tag{3.10}$$

De la misma manera podemos obtener la matriz densidad de Eva ρ_{out}^{Eva}

$$\begin{aligned}\rho_{out}^{Eva} &= Tr_{Bob}(\rho_{out}) = Tr_{Bob}(|\psi_{out}\rangle\langle\psi_{out}|) \\ &= \frac{1}{1+|\alpha|^2}\Bigg(\cos^2(\theta)(1+|\alpha|^2\cos^2(\theta))|\beta'\rangle\langle\beta'| - \alpha^* e^{i\phi_\rho}\cos^2(\theta)\sin(\theta)\,|\beta'\rangle\langle\beta'|\hat{a}_2 \\ &- \alpha e^{-i\phi_\rho}\cos^2(\theta)\sin(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2\Bigg).\end{aligned} \tag{3.11}$$

donde consideramos $\phi_\rho = 0$, lo que significa que el estado de Eva no presenta ningun cambio de fase con respecto al estado enviado por Alice. Además ρ_{out}^{Eva} cumple con $Tr\{\rho_{out}^{Eva}\} = 1$. Luego la probabilidad de Eva de obtener n fotones será:

$$\begin{aligned} P_n &= \langle n|\rho_{out}^{Eva}|n\rangle \\ &= \frac{e^{-|\beta'|^2}}{(1+|\alpha|^2)}\Bigg(\left(\cos^2(\theta) + |\alpha|^2\cos^4(\theta)\right)\sum_{n=0}^{\infty}\frac{\beta'^{2n}}{n!} \\ &- 2\alpha\cos^2(\theta)\sin(\theta)\sqrt{n}\sum_{n=1}^{\infty}\frac{\beta'^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\beta'^{n}}{\sqrt{n!}} \\ &+ \sin^2(\theta)\sum_{n=1}^{\infty}\frac{\beta'^{2(n-1)}}{(n-1)!}\Bigg), \end{aligned} \tag{3.12}$$

lo cual cumple con la condición $\sum_{n=0} P_n = 1$.

$$\begin{aligned} \sum_{n=0} P_n &= \frac{e^{-|\beta'|^2}}{(1+|\alpha|^2)}\Bigg(\left(\cos^2(\theta) + |\alpha|^2\cos^4(\theta)\right) + \sum_{n=1}^{\infty}\Bigg[(\cos^2 + |\alpha|^2\cos^4(\theta))\frac{\beta'^{2n}}{n!} \\ &- 2\alpha\cos^2(\theta)\sin(\theta)\frac{\beta'^{(2n-1)}}{(n-1)!} + \sin^2(\theta)n\frac{\beta'^{2(n-1)}}{(n-1)!}\Bigg]\Bigg) \\ &= 1. \end{aligned} \tag{3.13}$$

3.2. Acción de un canal cuántico de comunicación

Para estudiar los efectos del canal cuántico de comunicación utilizamos las ecuaciones de amplitud de amortiguamiento descritas en el capítulo dos, mediante las cuales podemos obener la distribución de probabilidad del estado recibido por Bob, lo que nos permite calcular las pérdidas de fotones a medida que el pulso recorre el canal de transmisión. Para esto consideramos que la matriz densidad del estado inicial enviado por Alice evolucionará de acuerdo a

$$\frac{d\rho}{dt} = \mathcal{K}(2\hat{a}\rho\hat{a}^\dagger - \hat{a}^\dagger\hat{a}\rho - \rho\hat{a}^\dagger\hat{a}), \tag{3.14}$$

cuya solución está dada por

$$\rho(t) = \sum_{n=0}^{\infty} M_n \rho(0) M_n^{\dagger}, \tag{3.15}$$

donde $M_n = \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^{\dagger}\hat{a}}\ \hat{a}^n$ corresponde al operador de Krauss.

3.2.1. Estado coherente

En este caso el estado inicial será $|\alpha\rangle$, por lo que se tendrá que $\rho(0) = |\alpha\rangle\langle\alpha|$. Luego el operador $\hat{M}_n$ actuará sobre el estado coherente de la siguiente manera

$$\begin{aligned}
\hat{M}_n|\alpha\rangle &= \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^{\dagger}\hat{a}}\ \hat{a}^n|\alpha\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^{\dagger}\hat{a}}\ \alpha^n|\alpha\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \alpha^n e^{-\mathcal{K}t\hat{a}^{\dagger}\hat{a}}\ |\alpha\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \alpha^n e^{-\mathcal{K}t\hat{a}^{\dagger}\hat{a}}\ e^{-\frac{|\alpha|^2}{2}}\ \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \alpha^n e^{-\frac{|\alpha|^2}{2}}\ \sum_{n=0}^{\infty} \frac{\alpha^n e^{-\mathcal{K}t\hat{a}^{\dagger}\hat{a}}}{\sqrt{n!}}|n\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \alpha^n e^{-\frac{|\alpha|^2}{2}}\ \sum_{n=0}^{\infty} \frac{(\alpha e^{-\mathcal{K}t})^n}{\sqrt{n!}}|n\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \alpha^n e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha e^{-\mathcal{K}t}\rangle,
\end{aligned} \tag{3.16}$$

por lo tanto

$$\begin{aligned}
\rho(t) = \sum_{n=0}^{\infty} \hat{M}_n|\alpha\rangle\langle\alpha|\hat{M}_n^{\dagger} &= \sum_{n=0}^{\infty} \frac{\mathcal{T}^n}{n!}|\alpha|^{2n} e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| \\
&= \sum_{n=0}^{\infty} \frac{(\mathcal{T}|\alpha|^2)^n}{n!} e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| \\
&= e^{\mathcal{T}|\alpha|^2} e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| \\
&= |\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|,
\end{aligned} \tag{3.17}$$

con $\mathcal{T} = 1 - |e^{-\mathcal{K}t}|^2$. Luego la distribución de probabilidad de dicho estado corresponderá a

$$P_{out} = |\langle n|\alpha e^{-\mathcal{K}t}\rangle|^2 = \frac{e^{-|\alpha e^{-\mathcal{K}t}|^2}|\alpha e^{-\mathcal{K}t}|^{2n}}{n!}. \tag{3.18}$$

3.2.2. Estado coherente con fotón añadido

Si el estado inicial corresponde a un estado coherente con un foton añadido, éste será de la forma

$$|\alpha, 1\rangle = \frac{\hat{a}^\dagger}{\sqrt{1+|\alpha|^2}}|\alpha\rangle = \frac{1}{\sqrt{1+|\alpha|^2}}|\psi'(0)\rangle. \tag{3.19}$$

Para ver como actúa el operador de Krauss consideramos solo $|\psi'(0)\rangle = \hat{a}^\dagger|\alpha\rangle$ de tal modo que

$$M_n|\psi'(0)\rangle = \sqrt{\frac{\mathcal{T}^n}{n!}}e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \hat{a}^n\hat{a}^\dagger|\alpha\rangle, \tag{3.20}$$

donde

$$\begin{aligned}
\hat{a}^n\hat{a}^\dagger &= \hat{a}^{n-1}\hat{a}\hat{a}^\dagger \\
&= \hat{a}^{n-1}(1+\hat{a}^\dagger\hat{a}) \\
&= \hat{a}^{n-1} + \hat{a}^{n-2}\hat{a}\hat{a}^\dagger\hat{a} \\
&= \hat{a}^{n-1} + \hat{a}^{n-2}(1+\hat{a}^\dagger\hat{a})\hat{a} \\
&= 2\hat{a}^{n-1} + \hat{a}^{n-2}\hat{a}^\dagger\hat{a}^2 \\
&= 2\hat{a}^{n-1} + \hat{a}^{n-3}(1+\hat{a}^\dagger\hat{a})\hat{a}^2 \\
&= 3\hat{a}^{n-1} + \hat{a}^{n-3}\hat{a}^\dagger\hat{a}^3 \\
&= ... \\
&= n\hat{a}^{n-1} + \hat{a}^\dagger\hat{a}^n,
\end{aligned} \tag{3.21}$$

por lo tanto

$$\begin{aligned}
M_n|\psi'(0)\rangle &= \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ (n\hat{a}^{n-1} + \hat{a}^\dagger\hat{a}^n)|\alpha\rangle \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \left(n\hat{a}^{n-1}|\alpha\rangle + \hat{a}^\dagger\hat{a}^n|\alpha\rangle\right) \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \left(n\alpha^{n-1}|\alpha\rangle + \hat{a}^\dagger\alpha^n|\alpha\rangle\right) \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \left(n\alpha^{n-1}e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ |\alpha\rangle + \alpha^n e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \hat{a}^\dagger e^{\mathcal{K}t\hat{a}^\dagger\hat{a}}\ e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ |\alpha\rangle\right) \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} \left(n\alpha^{n-1}e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha e^{-\mathcal{K}t}\rangle + \alpha^n e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \hat{a}^\dagger e^{\mathcal{K}t\hat{a}^\dagger\hat{a}}\ e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha e^{-\mathcal{K}t}\rangle\right).
\end{aligned} \tag{3.22}$$

La expresión $e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \hat{a}^\dagger e^{\mathcal{K}t\hat{a}^\dagger\hat{a}}$ se puede desarrollar teniendo en cuenta que $e^A\ Be^{-A} = B + [A,B] + \frac{1}{2!}[A,[A,B]] + ...$, tal que

$$e^{-\mathcal{K}t\hat{a}^\dagger\hat{a}}\ \hat{a}^\dagger e^{\mathcal{K}t\hat{a}^\dagger\hat{a}}\ = \hat{a}^\dagger - \mathcal{K}t[\hat{a}^\dagger\hat{a}, \hat{a}^\dagger] + ... = e^{-\mathcal{K}t}\ \hat{a}^\dagger, \tag{3.23}$$

con esto

$$\begin{aligned}
M_n|\psi'(0)\rangle &= \sqrt{\frac{\mathcal{T}^n}{n!}} \left(n\alpha^{n-1}e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha e^{-\mathcal{K}t}\rangle + \alpha^n e^{-\mathcal{K}t}\ \hat{a}^\dagger e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha e^{-\mathcal{K}t}\rangle\right). \\
&= \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ \alpha^{n-1}\left(n|\alpha e^{-\mathcal{K}t}\rangle + \alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\right),
\end{aligned} \tag{3.24}$$

y por lo tanto

$$M_n|\alpha,1\rangle = \frac{1}{\sqrt{1+|\alpha|^2}} \sqrt{\frac{\mathcal{T}^n}{n!}} e^{-\frac{|\alpha|^2}{2}(1-|e^{-\mathcal{K}t}|^2)}\ \alpha^{n-1}\left(n|\alpha e^{-\mathcal{K}t}\rangle + \alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\right). \tag{3.25}$$

Finalmente la matriz densidad del estado que tendrá Bob una vez que reciba el pulso corresponderá a

$$\begin{aligned}\rho(t) &= \sum_{n=0}^{\infty} M_n|\alpha,1\rangle\langle\alpha,1|M_n^\dagger \\ &= \frac{1}{1+|\alpha|^2}\Big[\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \mathcal{T}\alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \mathcal{T}e^{-\mathcal{K}t}\ \alpha^*|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a} \\ &+ e^{-2\mathcal{K}t}\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\Big],\end{aligned} \tag{3.26}$$

cumpliendo con $Tr\{\rho(t)\} = 1$. Luego, para obtener la distribución de probabilidad de $\hat{\rho}(t)$, calculamos $Pn = \langle n|\rho(t)|n\rangle$

$$\begin{aligned}Pn &= \langle n|\rho(t)|n\rangle \\ &= \frac{e^{-|\alpha e^{-\mathcal{K}t}|^2}}{1+|\alpha|^2}\Big[\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2n}}{n!} \\ &+ 2\alpha\mathcal{T}e^{-\mathcal{K}t}\ \sqrt{n}\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n-1}}{\sqrt{(n-1)!}}\ \sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n}}{\sqrt{n!}} \\ &+ e^{-2\mathcal{K}t}n\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2(n-1)}}{(n-1)!}\ \Big],\end{aligned} \tag{3.27}$$

lo cual cumple con la condición $\sum_{n=0} P_n = 1$

$$\begin{aligned}\sum_{n=0} P_n &= \frac{e^{-|\alpha e^{-\mathcal{K}t}|^2}}{1+|\alpha|^2}\Bigg(\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right) + \sum_{n=1}\Big[\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2n}}{n!} \\ &+ 2\alpha\mathcal{T}e^{-\mathcal{K}t}\ \frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2n-1}}{(n-1)!}\ + e^{-2\mathcal{K}t}n\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2(n-1)}}{(n-1)!}\ \Big]\Bigg) \\ &= 1.\end{aligned} \tag{3.28}$$

Capítulo 4

Resultados

En base a los cálculos vistos en la sección anterior podemos analizar los efectos producidos tanto por el beam splitter como por el canal cuántico de comunicación sobre los dos estados estudiados.

4.1. Efectos sobre un estado coherente

Para el caso de transmitir la información mediante un estado coherente $|\alpha\rangle$ podemos ver que los resultados estarán dados de la siguiente forma.

4.1.1. Beam splitter

En este caso consideramos que Alice envía un estado coherente $|\alpha\rangle$, el cual ocupa uno de los puertos de entrada del beam splitter, mientras que en el otro puerto se encuentra el estado $|0\rangle$, que representa la presencia de Eva queriendo captar la información que se pretende transmitir a Bob. De este modo el estado de entrada al beam splitter corresponderá a

$$|\psi_{in}\rangle = |\alpha\rangle \otimes |0\rangle, \tag{4.1}$$

a partir del cual se obtiene que el estado final luego de la accioón del Beam Splitter es

$$|\psi_{out}\rangle = |\alpha\cos(\theta)e^{i\phi_\tau}\rangle \otimes |-\alpha\sin(\theta)e^{-i\phi_\rho}\rangle = |\alpha''\rangle \otimes |\beta'\rangle, \tag{4.2}$$

lo cual indica que el estado final que recibe Bob está dado por $|\psi_{Bob}\rangle = |\alpha\cos(\theta)e^{i\phi_\tau}\rangle$, mientras que la información que obtiene Eva está representada por el estado $|\psi_{Eva}\rangle = |-\alpha\sin(\theta)e^{-i\phi_\rho}\rangle$. Donde los términos $e^{i\phi_\tau}$ y $e^{-i\phi_\rho}$ representan cambios de fases de los correspondientes estados de salida con respecto al estado de entrada enviado por Alice. Por su parte el parámetro θ determina el porcentaje de transmisión y reflexión del Beam Splitter, lo cual es controlado por Eva. Por otro lado, las distribuciones de probabilidad de los estados en poder de Eva y Bob pueden ser obtenidas de acuerdo a

$$\begin{aligned} P_{nm}^{Out} &= |\langle n, m|\psi_{out}\rangle|^2 \\ &= e^{-|\alpha|^2}\frac{|\alpha\cos(\theta)|^{2n}}{n!}\frac{|\alpha\sin(\theta)|^{2m}}{m!}, \end{aligned} \tag{4.3}$$

que representa la probabilidad de que Bob y Eva obtengan n y m partículas respectivamente. Luego al sumar sobre las partículas de Eva podemos obtener la distribución de probabilidades de Bob, de manera que

$$\begin{aligned} P_{out}^{Bob} &= \sum_{m=0}^{\infty} P_n(\alpha'')P_m(\beta') \\ &= \frac{e^{-|\alpha\cos(\theta)|^2}\ |\alpha\cos(\theta)|^{2n}}{n!}. \end{aligned} \tag{4.4}$$

Análogamente para Eva

$$\begin{aligned} P_{out}^{Eva} &= \sum_{n=0}^{\infty} P_n(\alpha'')P_m(\beta') \\ &= \frac{e^{-|\alpha\sin(\theta)|^2}\ |\alpha\sin(\theta)|^{2m}}{m!}. \end{aligned} \tag{4.5}$$

Al graficar ambas distribuciones de probabilidad se observa la relación existente entre el ángulo θ del beam splitter y el número de fotones captados tanto por Bob como por Eva. A medida que θ crece es mas probable que Eva obtenga un mayor número de partículas, lo que significa un menor número de partículas captadas por Bob.

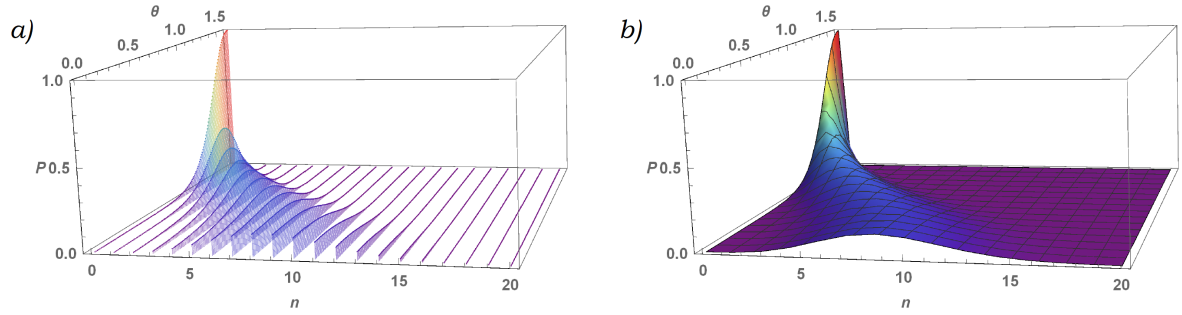

Figura 4.1: Beam splitter: a) Probabilidad P_{out}^{Bob} en función de θ y n discreto. b) Visualización de la probabilidad P_{out}^{Bob}.

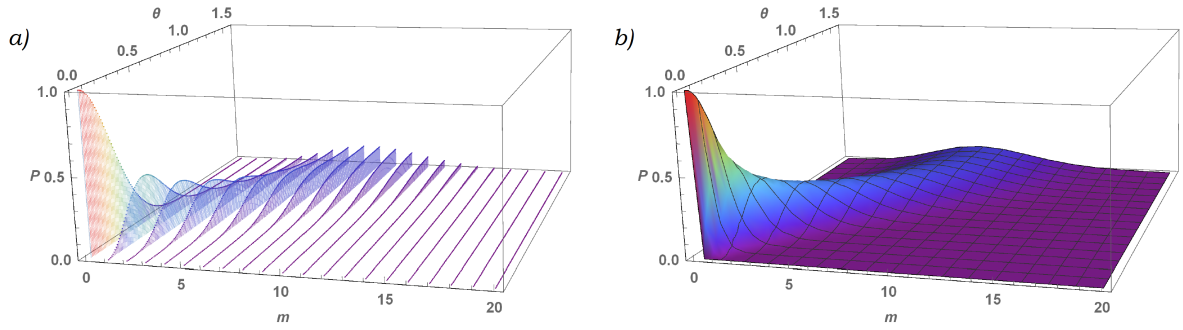

Figura 4.2: Beam splitter: a) Probabilidad P_{out}^{Eva} en función de θ y m discreto. b) Visualización de la probabilidad P_{out}^{Eva}.

4.1.2. Canal cuántico de comunicación

De los efectos producidos por un canal cuántico de comunicación sobre el estado inicial $|\alpha\rangle$ podemos observar que el estado resultante en poder de Bob viene dado por

$$|\psi_{out}\rangle = |\alpha e^{-\mathcal{K}t}\rangle, \tag{4.6}$$

teniendo en cuenta que se consideró $\mathcal{T} = 1 - |e^{-\mathcal{K}t}|^2$ a fin de cumplir con la condición de normalización de la traza de la matriz densidad del estado $|\psi_{out}\rangle$. El valor de $\mathcal{T}$ queda definido por un lado, por el parámetro $\mathcal{K}$ que va a caracterizar el canal cuántico en base a las pérdidas que este puede generar, y por otro lado

por la variable t que corresponde al tiempo que le toma a la información recorrer dicho canal. Luego la distribución de probabilidades para este estado corresponde a

$$P_{out} = \frac{e^{-|\alpha e^{-\mathcal{K}t}|^2} \left|\alpha e^{-\mathcal{K}t}\right|^{2n}}{n!}. \tag{4.7}$$

4.1.3. Comparación de estados

Los estados resultantes obtenidos en ambos casos son estados coherentes, lo cual sugiere que el estado $|\alpha \cos(\theta)\rangle$ y el estado $|\alpha e^{-\mathcal{K}t}\rangle$ poseen similares características. Esto significa que para un estado coherente $|\alpha\rangle$ enviado por Alice, el canal cuántico de comunicación produce un efecto similar al producido por un beam splitter. Mas aún, en la literatura se plantea que para estos estados un canal cuántico de comunicación puede ser modelado como un beam splitter caracterizado por un cierto ángulo θ, por lo cual los efectos de ambos, beam splitter y canal cuántico, sobre un estado coherente $|\alpha\rangle$ serían los mismos. Considerando esto podemos decir que

$$\cos(\theta) = e^{-\mathcal{K}t}, \tag{4.8}$$

con lo cual se define $Q = \mathcal{K}t = -\ln(\cos(\theta))$, teniendo en cuenta que $\theta \in [0, \frac{\pi}{2})$ dado el dominio de la función $\ln(x)$. Todo esto nos permite obtener una distribución de probabilidad igual para el caso de que el estado inicial se vea afectado por un beam splitter o por el canal cuántico de comunicación.

Podemos entonces fijar el ángulo θ en un determinado valor de modo de dejar caracterizado el canal cuántico y conocer la distribución de probabilidades final luego de las pérdidas provocadas por éste. En este caso fijamos el ángulo en $\theta = \frac{\pi}{4}$, y calculamos la distribución de probabilidad del estado en poder de Bob, con lo que se obtienen iguales graficas de las probabilidades finales del beam splitter y el canal cuántico.

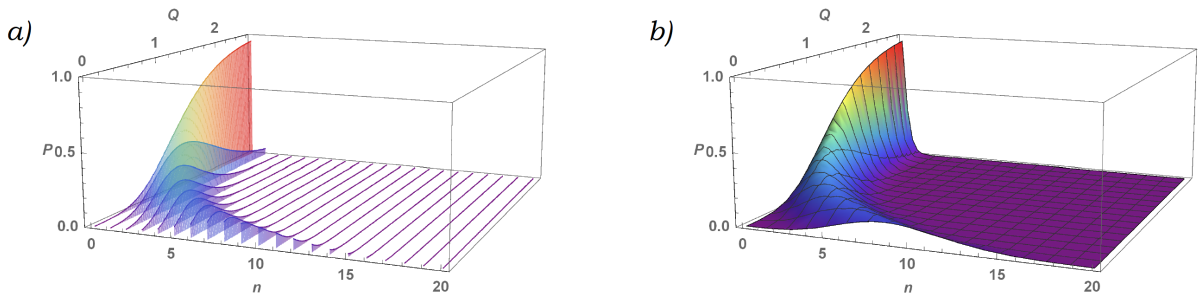

Figura 4.3: Canal cuántico: a) Probabilidad P_{out} en función de θ y n discreto. b) Visualización de la probabilidad P_{out}.

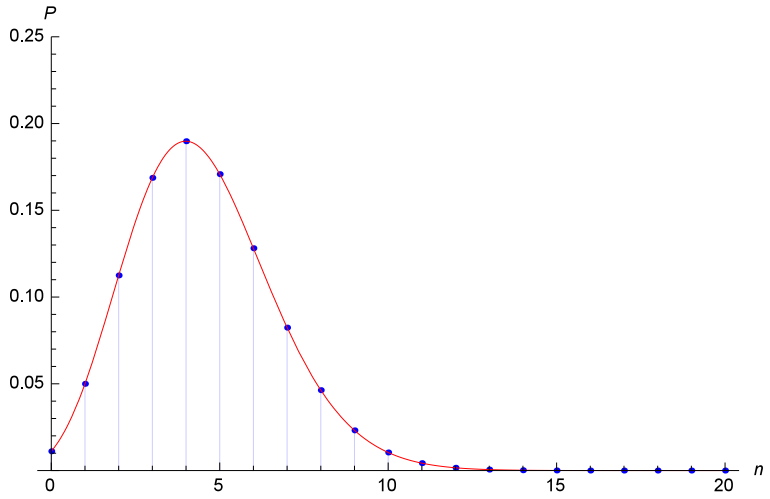

Figura 4.4: Distribuciones de probabilidad del estado en poder de Bob bajo la acción del Beam Splitter (Azul) y bajo la acción del canal cuántico (Rojo). En ambas se deben considerar únicamente valores discretos de n.

4.2. Efectos sobre un estado coherente con un fotón añadido

Ya vimos que el canal cuántico puede modelarse como un beam splitter con un cierto ángulo θ, lo que nos permitió caracterizarlo y conocer la distribución de probabilidades que tiene asociada. Con esto, en el caso de que Alice envíe ahora

un estado coherente con un fotón añadido a través del mismo canal, podemos estimar cuántas pérdidas éste va a producir. De igual manera, podemos analizar las pérdidas que provocaría un beam splitter sobre este estado con fotón añadido a fin de compararlas con las pérdidas generadas por el canal..

4.2.1. Beam splitter

Para este caso, como ya se ha mencionado, Alice envía el estado $|\alpha, 1\rangle$, lo cual genera que el estado de entrada al beam splitter sea

$$|\psi_{in}\rangle = |\alpha, 1\rangle \otimes |0\rangle, \tag{4.9}$$

del cual se obtiene como salida el estado

$$|\psi_{out}\rangle = \frac{1}{\sqrt{1+|\alpha|^2}} \left(e^{i\phi_\tau} \ \cos(\theta)\, \hat{a}_1^\dagger |\alpha''\rangle \otimes |\beta'\rangle - e^{-i\phi_\rho} \ \sin(\theta)\, |\alpha''\rangle \otimes \hat{a}_2^\dagger |\beta'\rangle \right), \tag{4.10}$$

que cumple con la condición de normalización $\langle\psi_{out}|\psi_{out}\rangle = 1$, mostrando además que el fotón añadido inicialmente puede quedar en poder de Bob o de Eva.

Para analizar la distribución de probabilidad del estado que recibe Bob tomaremos la traza parcial en Eva de la matriz densidad $\hat{\rho}_{out} = |\psi_{out}\rangle\langle\psi_{out}|$, de tal forma que $\hat{\rho}_{out}^{Bob} = Tr_{Eva}(|\psi_{out}\rangle\langle\psi_{out}|)$.

$$\begin{aligned}\hat{\rho}_{out}^{Bob} = \frac{1}{1+|\alpha|^2} \Bigg(& \cos^2(\theta)\, \hat{a}_1^\dagger |\alpha''\rangle\langle\alpha''|\hat{a}_1 + \alpha e^{i\phi_\tau} \cos(\theta) \sin^2(\theta)\, \hat{a}_1^\dagger |\alpha''\rangle\langle\alpha''| \\ & + \alpha^* e^{-i\phi_\tau} \cos(\theta) \sin^2(\theta)\, |\alpha''\rangle\langle\alpha''|\hat{a}_1 + \sin^2(\theta)\, |\alpha''\rangle\langle\alpha''|(1+|\alpha|^2 \sin^2(\theta)) \Bigg).\end{aligned} \tag{4.11}$$

Donde consideramos $\phi_\tau = 0$ en favor de Eva. Además ρ_{out}^{Bob} cumple con $Tr\{\rho_{out}^{Bob}\} = 1$, por lo que podemos calcular la probabilidad de Bob de obtener n fotones, la

cual estará dada por:

$$\begin{aligned} P_n &= \langle n|\rho_{out}^{Bob}|n\rangle \\ &= \frac{e^{-|\alpha''|^2}}{(1+|\alpha|^2)}\Bigg(\cos^2(\theta)\, n \sum_{n=1}^{\infty}\frac{\alpha''^{2(n-1)}}{(n-1)!} \\ &+ 2\alpha\cos(\theta)\sin^2(\theta)\sqrt{n}\sum_{n=1}^{\infty}\frac{\alpha''^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\alpha''^{n}}{\sqrt{n!}} \\ &+ (\sin^2 + |\alpha|^2\sin^4(\theta))\sum_{n=0}^{\infty}\frac{\alpha''^{2n}}{n!}\Bigg), \end{aligned} \tag{4.12}$$

de modo que $\sum_{n=0}^{\infty} P_n = 1$.

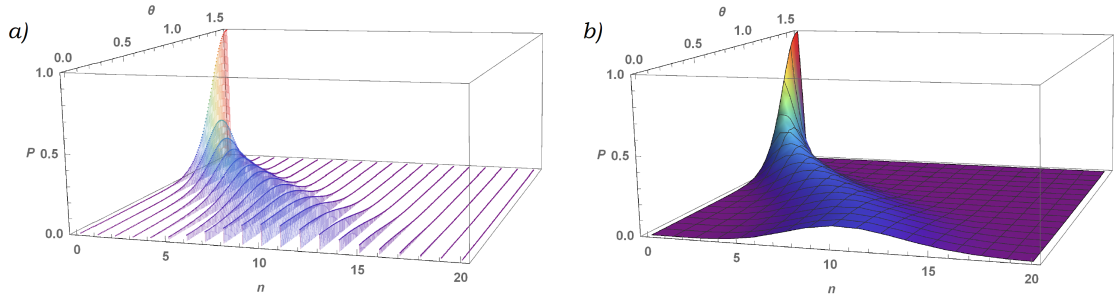

Figura 4.5: Beam splitter: a) Probabilidad P_{out}^{Bob} en función de θ y n discreto. b) Visualización de la probabilidad P_{out}^{Bob}.

De igual manera la matriz densidad de Eva puede ser obtenida tomando la traza parcial en Bob de $\hat{\rho}_{out}$, es decir, $\hat{\rho}_{out}^{Eva} = Tr_{Bob}(|\psi_{out}\rangle\langle\psi_{out}|)$.

$$\begin{aligned} \rho_{out}^{Eva} = \frac{1}{(1+|\alpha|^2)}\Big(&\cos^2(\theta)(1+|\alpha|^2\cos^2(\theta))|\beta'\rangle\langle\beta'| - \alpha^* e^{i\phi_\rho}\cos^2(\theta)\sin(\theta)\,|\beta'\rangle\langle\beta'|\hat{a}_2 \\ &- \alpha e^{-i\phi_\rho}\cos^2(\theta)\sin(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2\Big), \end{aligned} \tag{4.13}$$

con $\phi_\rho = 0$. Por otro lado también se cumple que $Tr\{\rho_{out}^{Eva}\} = 1$, por lo que la

distribución de probabilidades de Eva corresponde a:

$$\begin{aligned} P_m &= \langle m|\rho_{out}^{Eva}|m\rangle \\ &= \frac{e^{-|\beta'|^2}}{(1+|\alpha|^2)}\Bigg((\cos^2(\theta)+|\alpha|^2\cos^4(\theta))\sum_{n=0}^{\infty}\frac{\beta'^{2m}}{m!} \\ &- 2\alpha\cos^2(\theta)\sin(\theta)\sqrt{m}\sum_{n=1}^{\infty}\frac{\beta'^{(m-1)}}{\sqrt{(m-1)!}}\sum_{n=0}^{\infty}\frac{\beta'^{m}}{\sqrt{m!}} \\ &+ \sin^2(\theta)\sum_{n=1}^{\infty}\frac{\beta'^{2(m-1)}}{(m-1)!}\Bigg), \end{aligned} \tag{4.14}$$

con $\sum_{m=0}^{\infty} P_m = 1$.

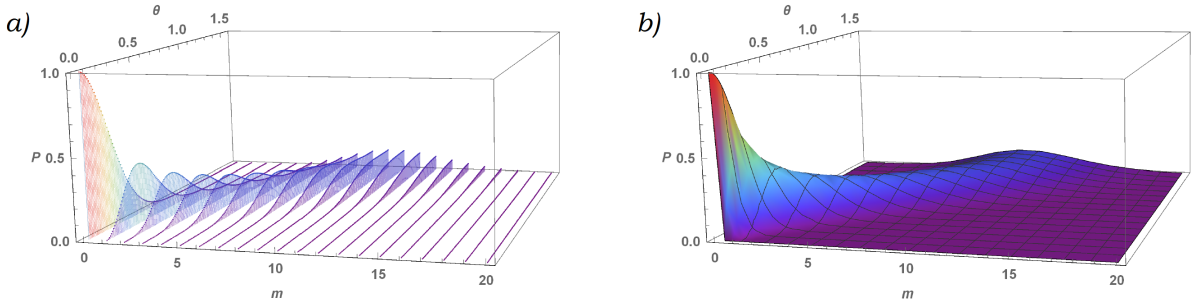

Figura 4.6: Beam splitter: a) Probabilidad P_{out}^{Eva} en función de θ y m discreto. b) Visualización de la probabilidad P_{out}^{Eva}.

El comportamiento de las distribuciones de probabilidad es bastante similiar al obtenido para el caso de un estado coherente $|\alpha\rangle$, pero con un leve desplazamiento hacia la derecha, lo que se debe al fotón extra que se ha añadido.

4.2.2. Canal cuántico de comunicación

En este caso en el que Alice envía un estado $|\alpha, 1\rangle$ el canal cuántico actúa sobre éste generando un estado mezcla, a diferencia del caso del estado coherente $|\alpha\rangle$ donde se obtuvo un estado puro. La matriz densidad resultante ahora viene dada

por

$$\hat{\rho}(t) = \sum_{n=0}^{\infty} M_n|\alpha,1\rangle\langle\alpha,1|M_n^{\dagger}$$
$$= \frac{1}{1+|\alpha|^2}\Big(\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \mathcal{T}\alpha e^{-\mathcal{K}t}\ \hat{a}^{\dagger}|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \mathcal{T}e^{-\mathcal{K}t}\ \alpha^*|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}$$
$$+ e^{-2\mathcal{K}t}\hat{a}^{\dagger}|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\Big), \tag{4.15}$$

con $Tr\{\hat{\rho}(t)\} = 1$. Luego la distribución de probabilidad asociada al efecto del canal cuántico sobre el estado $|\alpha,1\rangle$ es

$$P_n = \frac{e^{-|\alpha e^{-\mathcal{K}t}|^2}}{1+|\alpha|^2}\Big(\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2n}}{n!}$$
$$+ 2\alpha\mathcal{T}e^{-\mathcal{K}t}\ \sqrt{n}\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n-1}}{\sqrt{(n-1)!}}\ \sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n}}{\sqrt{n!}} \tag{4.16}$$
$$+ e^{-2\mathcal{K}t}n\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2(n-1)}}{(n-1)!}\ \Big),$$

cumpliendo con $\sum_{n=0}^{\infty} P_n = 1$.

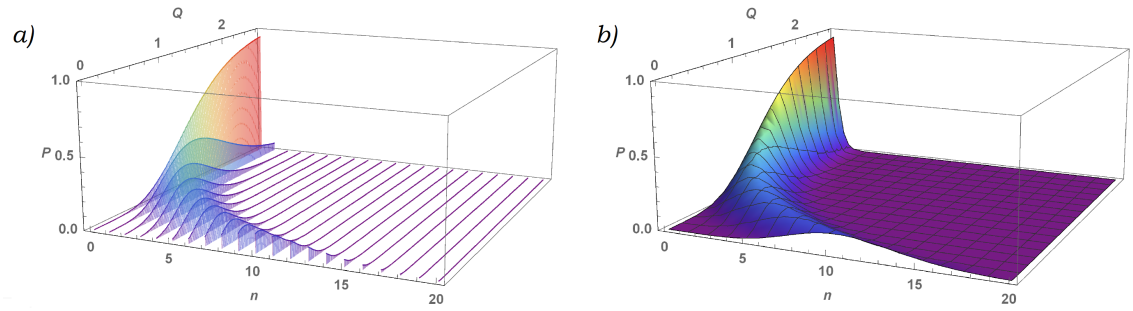

Figura 4.7: Canal cuántico: a) Probabilidad P_{out} en función de θ y n discreto. b) Visualización de la probabilidad P_{out}.

4.2.3. Comparación de estados

Conociendo ambas distribuciones de probabilidad de los estados finales en poder de Bob, podemos realizar la misma comparación que hicimos en el caso del estado coherente, donde fijamos el parámetro $\theta = 45°$ a fin de caracterizar el canal de comunicación como un beam splitter para luego comparar las distribuciones y ver si es posible diferenciar los efectos de ambos. Debemos recordar además que $\mathcal{K}t = -\ln(\cos(\theta))$, y por lo tanto $\mathcal{T} = 1 - |e^{-\mathcal{K}t}|^2 = \sin^2(\theta)$, lo cual da como resultado que las matrices densidad $\hat{\rho}(t)$ y $\hat{\rho}_{out}^{Bob}$ (cuando Alice envía $|\alpha, 1\rangle$) asociadas al canal y al beam splitter respectivamente, sean totalmente equivalentes. Lo anterior queda demostrado al graficar ambas distribuciones de probabilidad con $\theta = \frac{\pi}{4}$.

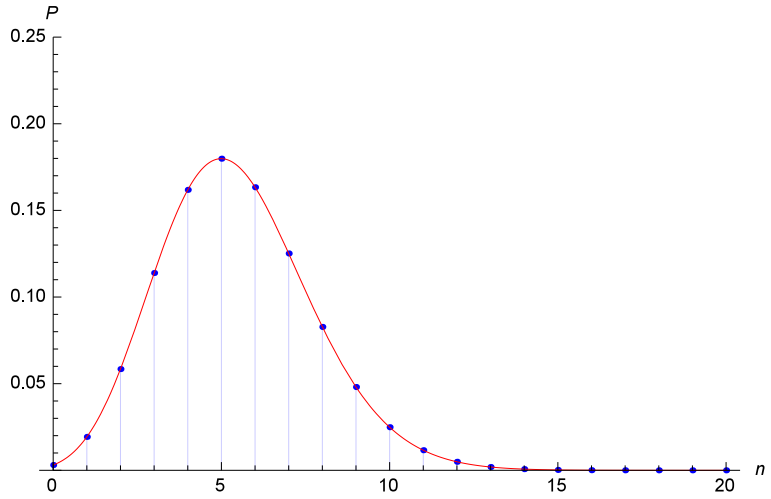

Figura 4.8: Distribuciones de probabilidad del estado en poder de Bob bajo la acción del Beam Splitter (Azul) y bajo la acción del canal cuántico (Rojo). En ambas se deben considerar únicamente valores discretos de n.

Por lo tanto, al igual que en el caso de enviar un estado coherente $|\alpha\rangle$, vemos que para un estado coherente con un fotón añadido la distribución de probabilidad para los efectos de un beam splitter es equivalente a la que obtiene por efectos del canal cuántico de comunicación, lo que hace imposible diferenciarlos en base a la

estadística de fotones.

4.3. Modelo criptográfico

Si bien el hecho de añadir un fotón extra a un estado coherente no permite diferenciar los efectos del beam splitter de los efectos del canal cuántico para detectar la presencia de un intruso, podemos implementar un modelo criptográfico basándonos en los estados finales obtenidos por Bob cuando Alice envía un estado $|\alpha\rangle$ o un estado $|\alpha, 1\rangle$, apoyándonos además en las propiedades del operador desplazamiento $\hat{D}(\alpha)$.

Comencemos considerando los estados $|\psi_{out}\rangle$ obtenidos para $|\psi_{in}\rangle = |\alpha\rangle \otimes |0\rangle$,

$$|\psi_{out}\rangle = |\alpha''\rangle \otimes |\beta'\rangle, \tag{4.17}$$

y para $|\psi_{in}\rangle = |\alpha^{+}\rangle \otimes |0\rangle$,

$$|\psi_{out}\rangle = \frac{1}{\sqrt{1+|\alpha|^2}}\Big(\cos(\theta)\,\hat{a}_1^{\dagger}|\alpha''\rangle \otimes |\beta'\rangle - \sin(\theta)\,|\alpha''\rangle \otimes \hat{a}_2^{\dagger}|\beta'\rangle\Big), \tag{4.18}$$

a los cuales podemos aplicar el operador $\hat{D}^{\dagger}(\alpha'')$ considerando que $\hat{D}(\alpha'')|0\rangle = |\alpha''\rangle$, lo cual significa que dicha operación está siendo aplicada por Bob sobre el pulso que ha recibido una vez que el beam splitter o el canal de comunicación han actuado sobre el pulso inicial enviado por Alice. Al realizar esta operación sobre (4.17) se tiene que

$$\hat{D}^{\dagger}(\alpha'')|\psi_{out}\rangle = \hat{D}^{\dagger}(\alpha'')\left(|\alpha''\rangle \otimes |\beta'\rangle\right) = |0\rangle \otimes |\beta'\rangle, \tag{4.19}$$

lo que significa que al aplicar $\hat{D}^{\dagger}$ Bob detectaría cero fotones, mientras que el estado de Eva no sufriría modificaciones. Por otro lado, si utilizamos (4.18) el resultado

será

$$\hat{D}^\dagger(\alpha'')|\psi_{out}\rangle = \hat{D}^\dagger(\alpha'')\left(\frac{1}{\sqrt{1+|\alpha|^2}}\Big(\cos(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\otimes|\beta'\rangle - \sin(\theta)\,|\alpha''\rangle\otimes\hat{a}_2^\dagger|\beta'\rangle\Big)\right)$$
$$= \frac{1}{\sqrt{1+|\alpha|^2}}\left(\cos(\theta)|1\rangle\otimes|\beta'\rangle + |0\rangle\otimes\left(\alpha^*\cos^2(\theta)|\beta'\rangle - \sin(\theta)\hat{a}_2^\dagger|\beta'\rangle\right)\right), \tag{4.20}$$

lo que muestra que en este caso Bob podría detectar un fotón, o por el contrario, no detectar ninguno. En base a esto podemos analizar cuales son las probabilidades de que Bob y Eva detecten uno o cero fotones aplicando o no el operador $\hat{D}^\dagger$. Además consideramos que Eva usa el beam splitter con una inclinación pequeña, lo que le permite tener un menor riesgo de ser detectada.

- 1. Alice envía el estado $|\alpha\rangle$.

  En este caso el estado final es $|\psi_{out}\rangle = |\alpha\cos(\theta)e^{i\phi_\tau}\rangle\otimes|-\alpha\sin(\theta)e^{-i\phi_\rho}\rangle$, por lo que sin aplicar el operador $\hat{D}^\dagger$ la probabilidad de que Bob obtenga cero fotones corresponde a

  $$P_{n=0} = e^{-|\alpha|^2\cos^2(\theta)}, \tag{4.21}$$

  mientras que la probabilidad de que obtenga uno o mas fotones es

  $$P_{n\geq 1} = 1 - P_{n=0} = 1 - e^{-|\alpha|^2\cos^2(\theta)}. \tag{4.22}$$

  De igual manera para Eva, la probabilidad de obtener cero fotones es

  $$P_{n=0} = e^{-|\alpha|^2\sin^2(\theta)}, \tag{4.23}$$

  y su probabilidad de captar uno o mas fotones es

  $$P_{n\geq 1} = 1 - P_{n=0} = 1 - e^{-|\alpha|^2\sin^2(\theta)}. \tag{4.24}$$

- 2. Alice envía el estado $|\alpha\rangle$ y Bob aplica el operador $\hat{D}^\dagger$.

  Para el estado $\hat{D}^\dagger(\alpha'')|\psi_{out}\rangle$ resulta evidente, segun (4.19), que Bob siempre detectará cero fotones.

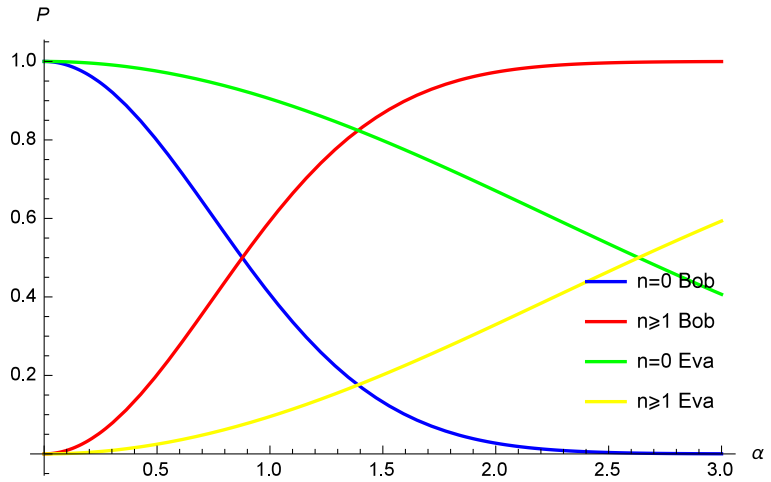

Figura 4.9: Probabilidades de Bob y Eva (sin aplicar $\hat{D}^{\dagger}$) de obtener cero o mas fotones cuando Alice envía un estado coherente $|\alpha\rangle$.

- 3. Alice envía el estado $|\alpha, 1\rangle$.
  En este caso $|\psi_{out}\rangle = \frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{i\phi_\tau}\ \cos(\theta)\hat{a}_1^{\dagger}|\alpha''\rangle \otimes |\beta'\rangle - e^{-i\phi_\rho}\ \sin(\theta)|\alpha''\rangle \otimes \hat{a}_2^{\dagger}|\beta'\rangle\right)$, por lo que la probabilidad de que Bob obtenga cero fotones es

$$P_{n=0} = \frac{e^{-|\alpha''|^2}}{1+|\alpha|^2}\left(\sin^2(\theta) + |\alpha|^2 \sin^4(\theta)\right), \tag{4.25}$$

  lo que implica que su probabilidad de obtener uno o mas fotones será

$$P_{n\geq 1} = 1 - \frac{e^{-|\alpha''|^2}}{1+|\alpha|^2}\left(\sin^2(\theta) + |\alpha|^2 \sin^4(\theta)\right). \tag{4.26}$$

  Por otro lado, para el caso de Eva, la probabilidad de obtener cero fotones corresponde a

$$P_{n=0} = \frac{e^{-|\beta'|^2}}{1+|\alpha|^2}\left(\cos^2(\theta) + |\alpha|^2 \cos^4(\theta)\right), \tag{4.27}$$

  y su probabilidad de obtener uno o mas fotones es

$$P_{n\geq 1} = 1 - \frac{e^{-|\beta'|^2}}{1+|\alpha|^2}\left(\cos^2(\theta) + |\alpha|^2 \cos^4(\theta)\right). \tag{4.28}$$

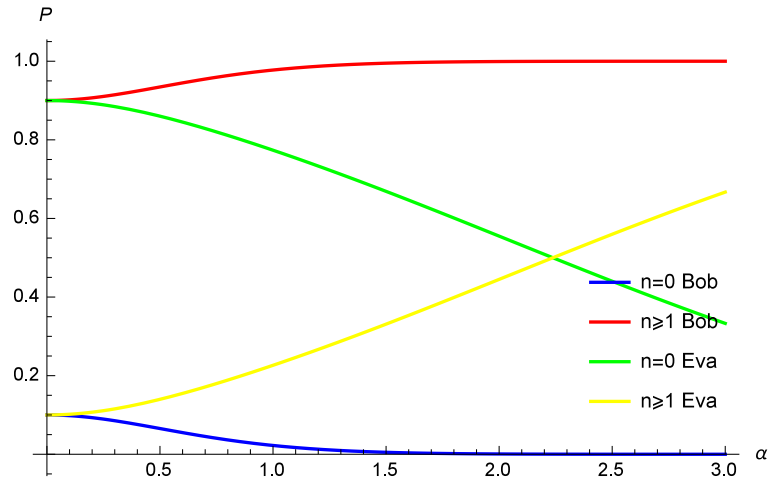

Figura 4.10: Probabilidades de Bob y Eva (sin aplicar $\hat{D}^\dagger$) de obtener cero o un fotón cuando Alice envía un estado coherente $|\alpha, 1\rangle$.

- 4. Alice envía el estado $|\alpha, 1\rangle$ y Bob aplica $\hat{D}^\dagger$.

  Como sabemos el resultado de dicha operación viene dado por

  $$D^\dagger(\alpha'')|\psi^+_{out}\rangle = \frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{i\phi_\tau}\ \cos(\theta)|1\rangle\otimes|\beta'\rangle + |0\rangle\otimes(\alpha^*\cos^2(\theta)|\beta'\rangle - e^{-i\phi_\rho}\ \sin(\theta)\hat{a}_2^\dagger|\beta'\rangle)\right), \tag{4.29}$$

  luego la probabilidad de que Bob obtenga un fotón corresponde a

  $$P_{n=1} = \frac{\cos^2(\theta)}{1+|\alpha|^2}, \tag{4.30}$$

  y la probabilidad de que obtenga cero fotones será

  $$P_{n=0} = 1 - \frac{\cos^2(\theta)}{1+|\alpha|^2}. \tag{4.31}$$

  Por otro lado las probabilidades de Eva se mantienen ya que no ha aplicado aún ninguna operación sobre su estado.

- 5. Alice envía el estado $|\alpha, 1\rangle$ y tanto Bob como Eva aplican $\hat{D}^\dagger$.

  En este caso el estado resultante es

  $$D^\dagger(\beta')D^\dagger(\alpha'')|\psi^+_{out}\rangle = \frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{i\phi_\tau}\ \cos(\theta)|1\rangle\otimes|0\rangle + \alpha|0\rangle\otimes|0\rangle - e^{i\phi_\tau}\ \sin(\theta)|0\rangle\otimes|1\rangle\right), \tag{4.32}$$

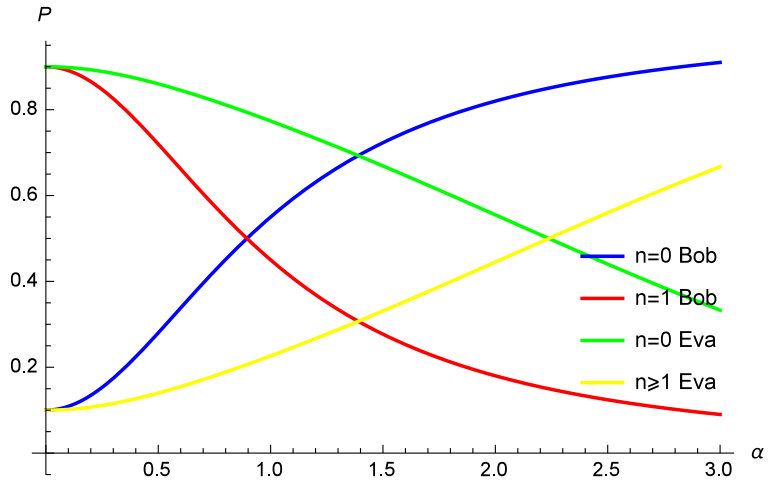

Figura 4.11: Probabilidades de Bob y Eva de obtener cero o un fotón cuando Alice envía un estado coherente $|\alpha, 1\rangle$ y Bob aplica el operador $\hat{D}^{\dagger}(\alpha'')$.

donde la probabilidad de que Bob obtenga un fotón sigue siendo

$$P_{n=1} = \frac{\cos^2(\theta)}{1+|\alpha|^2}, \tag{4.33}$$

y su probabilidad de obtener cero fotones es

$$P_{n=0} = 1 - \frac{\cos^2(\theta)}{1+|\alpha|^2}. \tag{4.34}$$

La probabilidad de que Eva obtenga un fotón corresponde a

$$P_{n=1} = \frac{\sin^2(\theta)}{1+|\alpha|^2}, \tag{4.35}$$

y la probabilidad de que obtenga cero fotones será:

$$P_{n=0} = 1 - \frac{\sin^2(\theta)}{1+|\alpha|^2}. \tag{4.36}$$

El análisis de los gráficos da cuenta de que las probabilidades de Bob son favorables en cuanto a la detección de fotones en comparación a las probabilidades de Eva, ya sea aplicando o no el operador $\hat{D}^{\dagger}$. Esto nos sugiere plantear un modelo criptográfico basado en la detección de fotones por parte de Bob cuando aplica

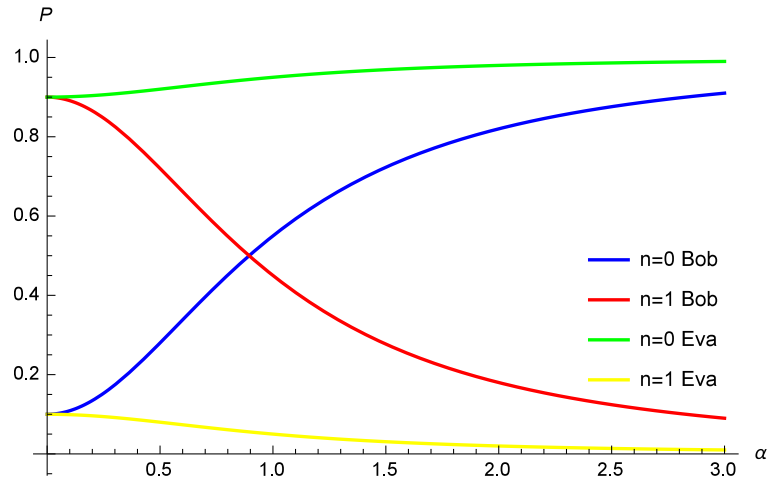

Figura 4.12: Probabilidades de Bob y Eva de obtener cero o un fotón cuando Alice envía un estado coherente $|\alpha, 1\rangle$ y Bob aplica el operador $\hat{D}^{\dagger}(\alpha'')$, mientras Eva aplica $\hat{D}^{\dagger}(\beta')$.

el operador desplazamiento, en el cual el fotón extra que hemos añadido al estado coherente pueda ser usado como portador de la información que queramos comunicar.

4.3.1. Criptografía con estados $|\alpha\rangle$ y estados $|\alpha, 1\rangle$

Con lo descrito anteriormente podemos plantear un modelo criptográfico en el cual Alice codifique los bits 0 y 1 mediante el envio aleatorio de estados $|\alpha\rangle$ y estados $|\alpha, 1\rangle$, de manera tal que cuando envíe un estado $|\alpha\rangle$ estará intentando transmitir el bit 0, y cuando envíe el estado $|\alpha, 1\rangle$ intentará comunicar el bit 1. Luego aplicando $\hat{D}^{\dagger}$ Bob podrá medir también aleatoriamente $|0\rangle$ y $|1\rangle$, para posteriormente transmitir sus resultados a Alice, y analizar los casos que deberán ser descartados y los casos que serán utilizados para generar la clave binaria secreta.

A continuación se presenta el modelo criptográfico desde el punto en el que Alice envía la información hasta el punto final de la obtención de la clave de seguridad.

- 1. Alice envía la información a Bob:

  Recordemos que el principal objetivo es lograr una confiable distribución de clave secreta, la cual se genera mediante un código binario de ceros y unos que deben ser transmitidos de alguna forma. En este caso Alice intentará comunicar los bits de la clave utilizando el estado $|\alpha\rangle$ para transmitir un cero y el estado $|\alpha, 1\rangle$ para transmitir un uno, enviándolos aleatoriamente de manera tal que Bob obtenga ceros y unos también de forma aleatoria.

- 2. Bob recibe la información y aplica el operador $\hat{D}^{\dagger}$:

  Una vez que Bob reciba el pulso enviado por Alice aplicará el operador $\hat{D}^{\dagger}$, de manera tal que cuando el estado transmitido sea $|\alpha\rangle$ él detectará cero fotones, y cuando el estado sea $|\alpha, 1\rangle$ tendrá una probabilidad de captar cero o un fotón, lo cual no garantiza que cuando Alice pretenda comunicar el bit 1 Bob capte lo mismo. Por tal razón los resultados obtenidos por Bob deberán ser comunicados a Alice a fin de descartar los casos en que las mediciones no coincidan con la información enviada.

- 3. Bob reenvía la información a Alice:

  Luego de que Bob aplique el operador $\hat{D}^{\dagger}$ y obtenga los resutados de esta acción, deberá comunicarlos a Alice, para eso utiliza también estados $|\alpha\rangle$ y estados $|\alpha, 1\rangle$. De esta forma, cuando mida cero fotones enviará a Alice un estado $|\alpha\rangle$ y cuando logre captar un fotón le enviará un estado $|\alpha, 1\rangle$.

- 4. Alice recibe la información de Bob y aplica el operador $\hat{D}^{\dagger}(\alpha'')$:

  Cuando Alice reciba la información que le envía Bob, también aplicará el operador $\hat{D}^{\dagger}$, de modo de captar uno o cero fotones. De esta forma ella determinará finalmente cuales son los caso que deberán descartar y cuales deberán considerar para generar la clave secreta.

- 5. Alice comunica a Bob que resultados descartar:

Dentro del protocolo de comunicación entre Alice y Bob, exiten cuatro posibilidades de acuerdo a los resultados de las mediciones que ambos realicen. Éstas son descritas a continuación:

- 5a. Cuando Alice pretenda comunicar un cero y envíe el estado $|\alpha\rangle$, con certeza sabrá que la medición de Bob será cero, y que él le reenviará un estado $|\alpha\rangle$, y por lo tanto ella también medirá un cero. Tal caso no será descartado y se utilizará para generar la clave secreta.

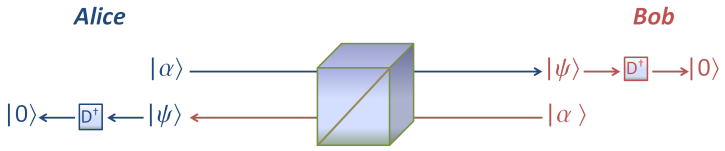

Figura 4.13: 5a. Protocolo: Alice comunica el bit 0 enviando un estado $|\alpha\rangle$.

- 5b. Si Alice pretende comunicar un uno, ella enviará el estado $|\alpha, 1\rangle$, por lo cual aplicando $\hat{D}^\dagger$ Bob podría medir cero o uno. En caso de que Bob mida un cero, enviará de vuelta un estado $|\alpha\rangle$, lo que implica que la medición de Alice será cero. Esto significa que la información que recibió de Bob no coincide con la que ella le envió, por lo cual dicho caso deberá ser descartado.

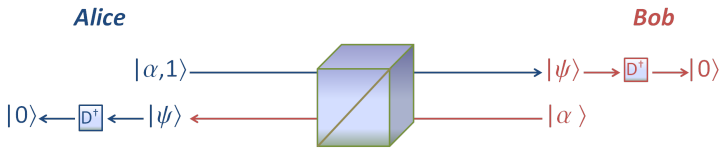

Figura 4.14: 5b. Protocolo: Alice comunica el bit 1 enviando un estado $|\alpha, 1\rangle$ y Bob obtiene el bit 0.

- 5c. De igual forma, si Alice envía el estado $|\alpha, 1\rangle$ pretendiendo comunicar el bit 1, y Bob logra captar un fotón, éste enviará de vuelta un estado $|\alpha, 1\rangle$, abriendo la posibilidad de que Alice aplicando $\hat{D}^\dagger$ capte uno o

cero fotones. Si Alice mide cero fotones, deberá también descartar dicho caso, ya que no tendrá ninguna certeza acerca de la medición de Bob.

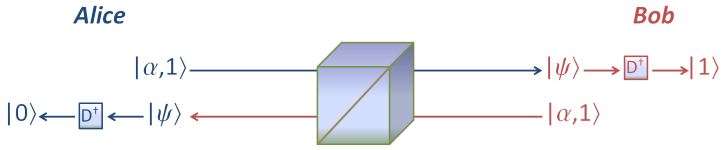

Figura 4.15: 5c. Protocolo: Alice comunica el bit 1 enviando un estado $|\alpha, 1\rangle$ y Bob mide un fotón. Luego Bob reenvía un estado $|\alpha, 1\rangle$ y Alice no logra captar fotones.

- 5d. Si ahora Alice envía el estado $|\alpha, 1\rangle$ y capta un fotón luego de aplicar $\hat{D}^\dagger$ sobre el pulso que reciba de Bob, será porque éste último le envió también un estado $|\alpha, 1\rangle$, lo que significará que logró captar un fotón en su medición. Con esto Alice sabrá que Bob recibió correctamente la información que ella le envió y por lo tanto tal caso será considerado para generar la clave secreta.

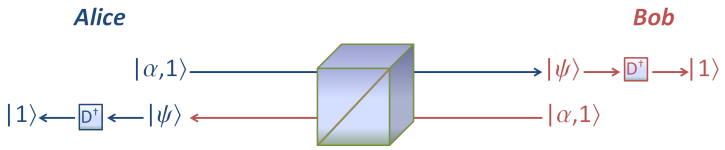

Figura 4.16: 5d. Protocolo: Alice comunica el bit 1 enviando un estado $|\alpha, 1\rangle$ y obtiene de vuelta el bit 1.

A continuación se muestran a modo de ejemplo, ocho pulsos que Alice envía a Bob utilizando aleatoriamente los estados $|\alpha\rangle$ y $|\alpha, 1\rangle$. En la primera columna *Bit* se tiene la información que Alice pretende enviar, las columnas *Alice* y *Bob* muestran los estados que ambos transmitirán, mientras que en las columnas *Bob* $D^\dagger$ y *Alice* $D^\dagger$ se muestran los resultados de sus mediciones luego de aplicar el operador $\hat{D}^\dagger$. La segunda columa *Bit* corresponde a la información que recibe

Alice cuando Bob le envía los pulsos de regreso, con la cual puede decidir que casos considerar para generar la clave secreta.

n^o	Bit	Alice	Bob $D^\dagger$	Bob	Alice $D^\dagger$	Bit	Clave
1	0	$\|\alpha\rangle$	0	$\|\alpha\rangle$	0	0	✓
2	1	$\|\alpha, 1\rangle$	1	$\|\alpha, 1\rangle$	1	1	✓
3	0	$\|\alpha\rangle$	0	$\|\alpha\rangle$	0	0	✓
4	1	$\|\alpha, 1\rangle$	0	$\|\alpha\rangle$	0	0	
5	1	$\|\alpha, 1\rangle$	1	$\|\alpha, 1\rangle$	1	1	✓
6	0	$\|\alpha\rangle$	0	$\|\alpha\rangle$	0	0	✓
7	1	$\|\alpha, 1\rangle$	1	$\|\alpha, 1\rangle$	1	1	✓
8	1	$\|\alpha, 1\rangle$	1	$\|\alpha, 1\rangle$	0	0	

(4.37)

De lo anterior se desprende que la clave secreta con la que se quedarían ambos luego de comprobar los casos favorables y descartar el resto será 010101. Nótese que sólo hemos considerado las acciones que pueden realizar Alice y Bob, por lo cual hasta el momento el protocolo no garantiza seguridad alguna ya que desconocemos las posibilidades que tiene Eva de intervenir en el proceso.

4.3.2. Posibilidades de Eva

Si los ceros y unos que componen la clave son comunicados según el estado que envía Alice, significa que a Eva le bastaría saber los casos en que se envía un estado $|\alpha\rangle$ o un estado $|\alpha, 1\rangle$ y luego espiar a Alice y Bob para saber los casos que no serán descartados en la formulación de la clave. Analicemos entonces las posibilidades que tiene Eva de captar dicha información durante el proceso de comunicación.

En primer lugar la unica manera que tiene Eva de saber que tipo de estados se están enviando es mediante la aplicación del operador $\hat{D}^\dagger$ sobre el conjunto de

fotones que ella logre desviar, a fin de poder medir también uno o cero fotones, lo que le permitiría saber si el estado enviado lleva o no un fotón añadido. Para tal análisis tomemos en cuenta las posibilidades de mediciones de Alice y Bob explicadas en el ítem 5. del protocolo.

- 5a. Alice envía un estado $|\alpha\rangle$

  En este caso con certeza sabemos que Bob y Eva recibirán respectivamente los estado coherentes $|\alpha''\rangle$ y $|\beta'\rangle$ y por lo tanto ambos medirán cero fotones cuando apliquen el operador $\hat{D}^\dagger$.

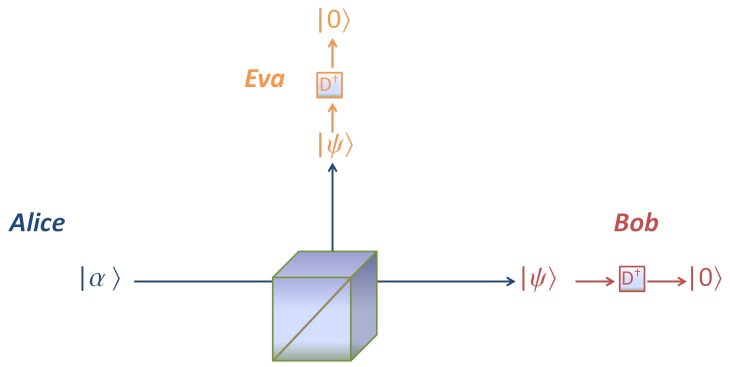

Figura 4.17: 5a. Protocolo: Alice comunica el bit 0 enviando el estado $|\alpha\rangle$, el cual es interceptado por Eva.

- 5b. Alice envía un estado $|\alpha, 1\rangle$

  En este caso las posibilidades aumentan ya que al igual que Bob, Eva podría medir cero o un fotón cuando aplique el operador $\hat{D}^\dagger$. Si mide cero no tendrá la certeza si Alice envió $|\alpha, 1\rangle$ o $|\alpha\rangle$, y si mide uno sabrá que Alice envió el estado $|\alpha, 1\rangle$ y que, de acuerdo a lo mostrado en la ecuación (4.32), Bob medirá cero y tal caso será descartado.

Según lo descrito hasta ahora, Eva no ha ganado información valiosa sobre los tipos de estados enviados, por lo que la opción que le queda para conocer la

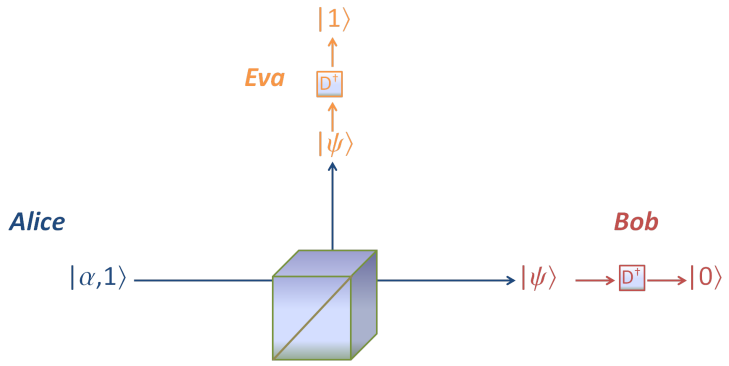

Figura 4.18: 5b. Protocolo: Alice comunica el bit 1 enviando el estado $|\alpha, 1\rangle$, el cual es interceptado por Eva, quien logra captar un fotón luego de aplicar $\hat{D}^\dagger$, lo que significa que tal caso será descartado por Alice y Bob.

medición de Bob y por ende ganar información sobre el estado enviado por Alice, es interceptar el pulso que Bob envía de vuelta. Veamos entonces los casos posibles:

- 5a. Alice envía un estado $|\alpha\rangle$

  En este caso Bob medirá cero fotones y por lo tanto enviará de vuelta un estado $|\alpha\rangle$, por lo tanto Alice y Eva obtendrán también un cero como resultado de su medición. Con esto Eva aún desconoce si su resultado se debe a que Bob reenvió un estado $|\alpha\rangle$ o un estado $|\alpha, 1\rangle$.

- 5b. Alice envía un estado $|\alpha, 1\rangle$

  Como ya sabemos, si en este caso Eva logra medir un fotón sabrá de inmediato que dicho pulso será descartado, por lo tanto nos centramos en el caso en que ella mida cero fotones, situación que de acuerdo a (4.32) ofrece dos posibilidades:

  - Eva mide cero fotones y Bob mide cero fotones.

    En este caso, como Bob enviará de vuelta un estado $|\alpha\rangle$, Eva aplicará $\hat{D}^\dagger$ y nuevamente medirá cero, por lo cual mantendrá la misma incerteza sobre el estado que realmente está enviando Bob, al igual que en el caso

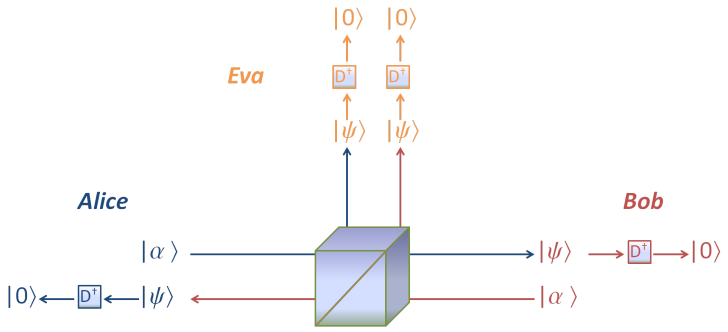

Figura 4.19: 5a. Protocolo: Alice envía el estado $|\alpha\rangle$, por lor que Bob captará cero fotones. Por su parte, Eva intercepta el pulso enviado por Alice y luego el enviado por Bob, mediendo cero fotones en las dos ocasiones.

en que Alice envía un estado $|\alpha\rangle$ (caso 5a.).

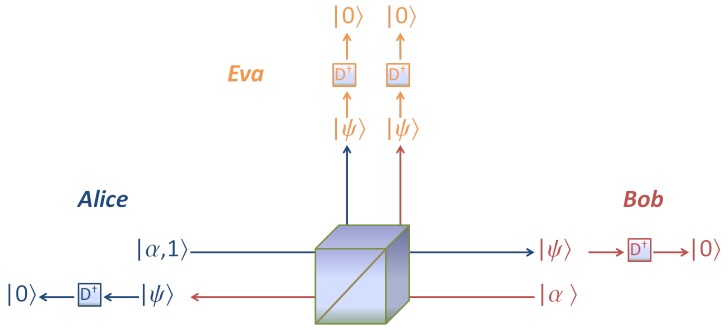

Figura 4.20: 5b. Protocolo: Alice comunica el bit 1 enviando el estado $|\alpha, 1\rangle$. En este caso ni Eva ni Bob logran captar un fotón, lo que implica que este caso será descartado cuando Alice reciba el pulso de Bob. Por su parte Eva no sabrá que tipo de estado se envió.

- Eva mide cero fotones y Bob mide un fotón
  Cuando Bob mida un fotón enviará de vuelta un estado $|\alpha, 1\rangle$, por lo cual Eva y Alice podrían medir cada una cero o uno. Es claro que cuando Eva mida uno, Alice con certeza medirá cero, por lo cual Eva sabrá que dicho caso será descartado. Por otro lado, si Eva mide cero, de nuevo

no sabrá que tipo de estado envió de vuelta Bob.

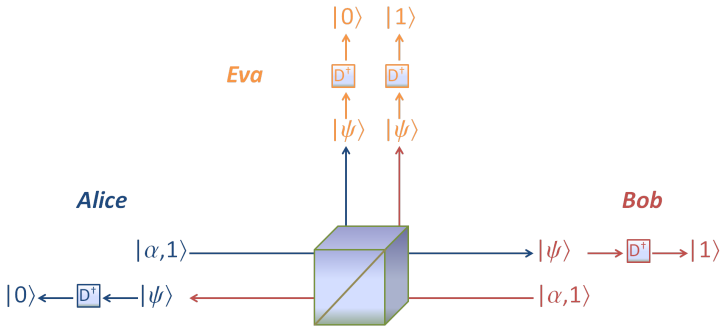

Figura 4.21: 5b. Protocolo: Alice comunica el bit 1 enviando el estado $|\alpha, 1\rangle$. En este caso Bob logra captar un fotón, por lo que enviará de vuelta un estado $|\alpha, 1\rangle$. Eva capta un fotón cuando intercepta el pulso que devuelve Bob, lo que implica que el pulso será descartado.

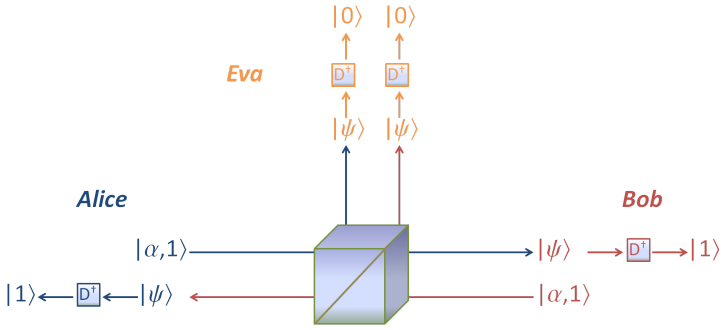

Figura 4.22: Alice comunica el bit 1 enviando el estado $|\alpha, 1\rangle$. En este caso Bob logra captar un fotón, por lo que enviará de vuelta un estado $|\alpha, 1\rangle$. Alice capta un fotón cuando recibe el pulso que devuelve Bob, por lo que dicho pulso será utilizado para crear la clave. Por su parte, Eva mide cero fotones y desconoce el tipo de estado que se envió.

De todo lo recién mostrado podemos concluír que el caso que no le favorece a Eva es cuando Alice envía $|\alpha, 1\rangle$, Bob logra medir un fotón, devuelve el mismo tipo de estado y Alice también mide un fotón, lo cual no ocurrirá con mucha frecuencia

ya que cuando se envía este tipo de estados es mas probable que a la hora de la medición se capten cero fotones. Por lo tanto en general, enviando estados $|\alpha\rangle$ y estados $|\alpha, 1\rangle$ la probabilidad de obtener ceros cuando se aplique $\hat{D}^\dagger$ será mucho mayor que la probabilidad de obtener un uno, por lo cual Eva podría asumir que la mayoria de los bits que se pretenden comunicar son ceros y se equivocará en muy pocos casos, lo cual pondría en riesgo la seguridad del protocolo. Podemos por lo tanto intentar sacar un mayor provecho al caso recién mencionado, que es el que menos favorece a Eva, y por ende el mas conveniente para Alice y Bob. La forma de hacerlo será codificando la información en dicho pulso a través de la polarización del fotón que ambos logren captar cuando aplican el operador $\hat{D}^\dagger$, lo que sugiere un acoplamiento del protocolo que aquí hemos descrito con el protocolo BB84.

4.3.3. Implementación del protocolo BB84

Para acoplar el protocolo BB84 a nuestro protocolo, consideraremos el caso en el cual Alice tiene la certeza de que Bob logró captar el fotón añadido, de tal forma que en la polarización de dicho fotón vaya codificada la información que nos permita generar la clave secreta, de forma análoga a lo ya visto en el protocolo BB84.

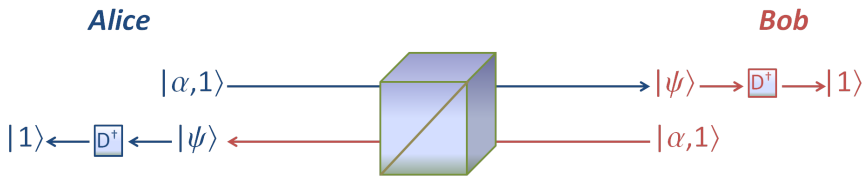

Figura 4.23: Alice envía el estado $|\alpha, 1\rangle$. Luego Bob aplica $\hat{D}^\dagger$ y capta un fotón. Producto de su medición Bob envía de vuelta un estado $|\alpha, 1\rangle$. Finalmente Alice aplica $\hat{D}^\dagger$ y capta también un fotón.

Para complementar ambos protocolos lo primero es acordar la convención de polarizaciones y bits que utilizarán Alice y Bob, mediante la cual podrán codificar

y decodificar la información transmitida, en este caso utilizaremos la misma del protocolo BB84 explicado en el capítulo 1. Posteriormente Alice polarizará aleatoriamente los pulsos de los estados $|\alpha\rangle$ y $|\alpha, 1\rangle$, los cuales también enviará de forma aleatoria. De esta forma, cuando Bob logre captar un fotón sabrá el bit que éste representa, ya que previo a aplicar $D^\dagger$ habrá elegido una base para medir la polarización del pulso y dependiendo de su resultado determinar si la información recibida representa un cero o un uno. Posteriormente Alice y Bob deberán comparar las bases que ambos utilizaron para descartar los casos en que sus elecciones no coincidan. En este escenario la única posibilidad de Eva es medir la polarización de todos los pulsos que intercepte, ya que ella no tiene forma de saber cuando se logró concretar la situación mostrada en la figura 4.23, por lo que deberá medir en todos los casos y esperar a que Alice y Bob se informen los casos no descartados que utilizarán para generar la clave secreta. Mas aún, Eva ni siquera tiene forma de saber si Alice envió el estado $|\alpha\rangle$ o el estado $|\alpha, 1\rangle$, por lo que Alice y Bob podrían engañarla comparando las bases de polarización utilizadas en todos los pulsos transmitidos, incluso cuando Alice envíe el estado $|\alpha\rangle$. Con esto Eva podrá creer que la situación de la figura 4.23 se concretó y que existe la posibilidad de que el bit comunicado sea tanto cero como uno, siendo que Bob en dicho caso, pese utilizar una base para medir polarización captará cero fotones, y el bit comunicado por Alice siempre será cero. Con esto, podemos ejemplificar el protocolo de la siguiente forma, teniendo presente que cuando se envíe un estado $|\alpha\rangle$ sólo se podrá comunicar el bit cero, mientras que cuando se envíe el estado $|\alpha, 1\rangle$ será posible transmitir el bit cero o el bit uno, dependiendo de la polarización que lleve el fotón añadido.

La siguiente tabla muestra una serie de pulsos en los cuales se han enviado aleatoriamente estados $|\alpha\rangle$ y $|\alpha, 1\rangle$, lo cuales a su vez fueron polarizados en bases aleatorias. La primera y segunda columna *Bit* muestran respectivamente la infor-

mación transmitida por Alice y la informacion captada por Bob. Por otro lado la primera y segunda columna *Base* dan cuenta de las bases utilizadas por Alice y Bob respectivamente a la hora de codificar y decodificar. Finalmente las columnas *Alice* y *Bob* representan los tipos de estados que ambos transmiten y las columnas $Bob\hat{D}^{\dagger}$ y $Alice\hat{D}^{\dagger}$ los resultados que cada uno obtiene luego de aplicar el operador $\hat{D}^{\dagger}$.

n^o	Bit	Base	Alice	Bob $D^\dagger$	Base	Bob	Alice $D^\dagger$	Bit	Clave
1	0	$\times$	$\|\alpha,1\rangle$	1	$\times$	$\|\alpha,1\rangle$	1	0	✓
2	1	$+$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	1	1	✓
3	0	$\times$	$\|\alpha\rangle$	0	$(\times)$	$\|\alpha\rangle$	0	0	✓
4	1	$+$	$\|\alpha,1\rangle$	0	$(+)$	$\|\alpha\rangle$	0	0	
5	1	$\times$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	1	1	
6	0	$+$	$\|\alpha\rangle$	0	$(+)$	$\|\alpha\rangle$	0	0	✓
7	1	$\times$	$\|\alpha,1\rangle$	1	$\times$	$\|\alpha,1\rangle$	1	1	✓
8	1	$+$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	0	0	
9	0	$\times$	$\|\alpha\rangle$	0	$(\times)$	$\|\alpha\rangle$	0	0	✓
10	1	$+$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	1	1	✓
11	0	$\times$	$\|\alpha\rangle$	0	$(\times)$	$\|\alpha\rangle$	0	0	✓
12	1	$+$	$\|\alpha,1\rangle$	0	$(+)$	$\|\alpha\rangle$	0	0	
13	0	$+$	$\|\alpha,1\rangle$	1	$\times$	$\|\alpha,1\rangle$	1	1	
14	0	$+$	$\|\alpha\rangle$	0	$(+)$	$\|\alpha\rangle$	0	0	✓
15	1	$\times$	$\|\alpha,1\rangle$	1	$\times$	$\|\alpha,1\rangle$	1	1	✓
16	1	$+$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	0	0	
17	0	$\times$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	1	1	
18	0	$\times$	$\|\alpha\rangle$	0	$(\times)$	$\|\alpha\rangle$	0	0	✓
19	0	$+$	$\|\alpha,1\rangle$	1	$+$	$\|\alpha,1\rangle$	1	0	✓
20	1	$+$	$\|\alpha,1\rangle$	1	$\times$	$\|\alpha,1\rangle$	1	1	

(4.38)

Los casos en que la base de Bob se muestra entre paréntesis indican que en realidad él no captó fotones, sin embargo igualmente comparan dicha base para dificultar el trabajo de Eva al querer descifrar la clave secreta. En caso contrario, si Alice y Bob comparan sólo las bases de los casos en que ambos midieron un

fotón, Eva sabrá que debe descartar todo el resto de los pulsos. Veamos entonces algunos de los pulsos mostrados en (4.38) a fin de analizar las causas que llevan a Alice a descartar ciertos casos y otros no.

- Pulsos 3, 6, 9, 11, ,14, 18.

  En estos casos Bob siempre medirá cero fotones aunque previamente igual utilizará una base para medir polarización, por lo tanto el bit que se pretende enviar va implícito en el tipo de estado transmitido y no en la polarización del pulso. Con su medición Bob puede suponer que Alice le intentó comunicar un cero enviándole el estado $|\alpha\rangle$ (que efectivamente es lo que está sucediendo), o por el contrario suponer que Alice le envió el estado $|\alpha, 1\rangle$ y que debido a la medición que él obtuvo dicho pulso será descartado, información que no tendrá hasta que Alice le diga con que pulsos quedarse. Por otro lado, como Eva no tiene forma de saber que tipo de estado está enviando Alice, su mejor opción será medir de todas maneras la polarización del pulso, confiando en que Alice está codificando los bits en la polarización. Finalmente cuando Bob le comunique a Alice la supuesta base que utilizó para medir, Eva no tendrá forma de saber si realmente utilizarán la polarización o no. Esto implica que en caso de que Alice decida no descartar dicho pulso, existirá la posibilidad de que Eva mida polarización y obtenga el bit uno, cuando en realidad el bit enviado fue siempre cero.

- Pulsos 1, 2, 7, 10, 15, 19.

  En estos casos Alice ha enviado un estado $|\alpha, 1\rangle$, codificando ceros y unos a través de polarizaciones en la base (0,90) en los casos 2 ,10 y 19, y polarizaciónes en la base (-45,45) para los casos 1, 7 y 15. El primer criterio que debe considerar Alice un vez que reciba el pulso que le devuelve Bob es verificar si éste logró captar el fotón añadido, lo cual en este caso, ha sucedido con éxito. Una vez que Alice compruebe dicha situación deberá esperar que Bob

mediante un canal clásico le indique la base que utilizó para medir la polarización del fotón que captó en cada caso. Si Alice verifica, como en estos casos, que las bases coincidieron, entonces tales pulsos serán utilizados para generar la clave secreta.

- Pulso 4, 8, 12, 16.
  En estos pulsos Alice no lográ captar de vuelta el fotón añadido que envió a Bob, por lo que dichos casos serán descartados una vez que se comparen las supuestas bases utilizadas para medir las polarizaciones, ya que recordemos que Bob mecionará una cierta base haya o no captado el fotón.

- Pulso 5, 13, 17, 20. En estos casos Alice intentó enviar ceros y unos codificados en diferentes bases de polarización del fotón añadido, comprobando con su medición que Bob captó un fotón. Sin embargo cuando Bob le comunica las bases que utilizó, Alice nota que éstas no coinciden con las que ella uso al comienzo, por lo cual debe descartar los pulsos en cuestión.

Por lo tanto de los pulsos que son útiles para generar la clave, Alice y Bob utilizarán con certeza los que hayan implicado un fotón añadido, quedando a criterio de Alice el utilizar o no los pulsos en que no se añadió el fotón. De esta forma si Alice decide considerar todos los pulsos seleccionados de la tabla, la clave de seguridad será 010010100100. De esta forma se cumpliría el objetivo de lograr una distribución de clave secreta de forma segura, permitiéndole a un determinado receptor utilizarla para decodificar una cierta información cifrada inicialmente por el emisor.

Capítulo 5

Conclusiones

El desarrollo de este trabajo tuvo como objetivo modelar un sistema criptográfico mediante el cual, en primera instancia, se lograra la detección de posibles espías en un proceso de comunicación de caracter confidencial entre un emisor y un receptor, buscando garantizar en cualquier caso la seguridad de la información transmitida. En base a esto se buscó diferenciar los efectos propios de un canal cuántico de comunicación de los efectos de un beam splitter, el cual suponemos es implementado por un intruso a fin de desviar parte de la información transmitida a través del canal con pulsos de múltiples fotones. Para tal propósito analizamos las distribuciones de probabilidad de los estados en poder del receptor de la información, de lo cual concluímos que a través de éstas no es posible diferenciar las acciones del beam splitter y el canal cuántico cuando se considera $\phi_\tau = 0$, dado que los efectos de ambos son idénticos, ya sea en el caso de transmitir estados coherentes $|\alpha\rangle$ o estados coherentes con fotón añadido $|\alpha, 1\rangle$. Sin embargo, notamos que al enviar un estado $|\alpha\rangle$ la estadística de fotones del estado en poder de Bob no depende de ϕ_τ, mientras que para el estado $|\alpha, 1\rangle$ la estadística de fotones si depende de esta fase, lo cual significa que en caso de que Eva utilice un beam splitter caracterizado por $\phi_\tau \neq 0$, Bob podría detectarla analizando la distribución de probabilidad del estado recibido.

Por otro lado, basándonos en los resultados obtenidos al analizar las distribuciones de probabilidad de los estados recibidos por Bob, planteamos un modelo criptográfico mediante el cual se logre garantizar la confidencilidad de la información que se quiere transmitir. Para esto hacemos uso de las propiedades del operador desplazamiento $\hat{D}$, las cuales nos permiten establecer un intercambio de información entre Alice Y Bob a fin de discernir si el pulso transmitido en cada caso corresponde a un estado $|\alpha\rangle$ o a un estado $|\alpha, 1\rangle$, los cuales en principio fueron considerados para representar los bits 0 y 1 respectivamente, para mediante ellos lograr compartir una clave de seguridad binaria.

Este método sin embargo no reune las condiciones necesarias para garantizar en un cien por ciento la seguridad de la transmisión de la información, por lo cual proponemos acoplarlo al Protocolo BB84, utilizando las polarizaciones de los pulsos enviados como un vehículo para comunicar los bits que componen la clave que se quiere transmitir. De este modo proponemos un sistema de criptografía cuántica en el cual el intercambio de información queda sujeto a dos criterios; por una parte el tipo de estado enviado, y por otra, el tipo de polarización de cada uno de los pulsos. De esta forma si se envía el estado $|\alpha\rangle$ significará que se está intentando comunicar directamente el bit 0, y si se envía el estado $|\alpha, 1\rangle$ se deberá analizar la polarización para determinar si el bit comunicado corresponde a 0 ó 1. En tal situación las posibilidades de Eva se reducen, ya que según lo mostrado, no tiene forma alguna de saber el tipo de estados que están compartiendo Alice y Bob, lo que significa que no podrá saber si la información está siendo codificada en el tipo de estado o en la polarización del mismo.

Capítulo 6

Apéndice

- Acción del beam splitter sobre el estado coherente $|\alpha\rangle$

El estado $|\psi_{out}\rangle$ lo obtenemos aplicando uno a uno los operadores que conforman el operdar $\hat{B}^\dagger$, comenzando por $e^{i\Phi\hat{L}_3}\,(|\alpha\rangle \otimes |0\rangle)$.

$$
\begin{aligned}
\longrightarrow e^{i\Phi\hat{L}_3}\,(|\alpha\rangle \otimes |0\rangle) &= e^{\frac{i\Phi}{2}\hat{a}_1^\dagger\hat{a}_1}\ |\alpha\rangle \otimes e^{-\frac{i\Phi}{2}\hat{a}_2^\dagger\hat{a}_2}\ |0\rangle \\
&= e^{\frac{i\Phi}{2}\hat{a}_1^\dagger\hat{a}_1}\ e^{-\frac{|\alpha|^2}{2}}\ \sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \otimes |0\rangle \\
&= e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}e^{\frac{i\Phi}{2}n}|n\rangle \otimes |0\rangle \\
&= e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n}{\sqrt{n!}}|n\rangle \otimes |0\rangle \\
&= e^{-\frac{|\alpha|^2}{2}}\ e^{\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ \sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n}{\sqrt{n!}}|n\rangle \otimes |0\rangle \\
&= e^{-\frac{|\alpha|^2}{2}(1-|e^{i\Phi}|)}\ |\alpha e^{\frac{i\Phi}{2}}\rangle \otimes |0\rangle \\
&= |\alpha e^{\frac{i\Phi}{2}}\rangle \otimes |0\rangle
\end{aligned}
\tag{6.1}
$$

$$
\begin{aligned}
\longrightarrow e^{-\tan(-\frac{\Theta}{2})\hat{L}_+}\left(|\alpha e^{\frac{i\Phi}{2}}\rangle \otimes |0\rangle\right) &= e^{\tan(\frac{\Theta}{2})\hat{a}_1^\dagger\hat{a}_2}\left(|\alpha e^{\frac{i\Phi}{2}}\rangle \otimes |0\rangle\right) \\
&= |\alpha e^{\frac{i\Phi}{2}}\rangle \otimes |0\rangle
\end{aligned}
\tag{6.2}
$$

$$
\begin{aligned}
\longrightarrow e^{-2\ln(\sec(-\frac{\Theta}{2}))\hat{L}_3}\left(|\alpha e^{\frac{i\Phi}{2}}\rangle\otimes|0\rangle\right) &= e^{-2\ln(\sec(\frac{\Theta}{2}))\frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1-\hat{a}_2^\dagger\hat{a}_2)}\left(|\alpha e^{\frac{i\Phi}{2}}\rangle\otimes|0\rangle\right)\\
&= e^{-\ln(\sec\left(\frac{\Theta}{2}\right))\hat{a}_1^\dagger\hat{a}_1}|\alpha e^{\frac{i\Phi}{2}}\rangle\otimes e^{\ln(\sec\left(\frac{\Theta}{2}\right))\hat{a}_2^\dagger\hat{a}_2}|0\rangle\\
&= e^{\ln(\cos\left(\frac{\Theta}{2}\right))n}e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ \sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n}{\sqrt{n!}}|n\rangle\otimes|0\rangle\\
&= e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ \sum_{n=0}^{\infty}\frac{(e^{\ln(\cos\left(\frac{\Theta}{2}\right))}\ \alpha e^{\frac{i\Phi}{2}})^n}{\sqrt{n!}}|n\rangle\otimes|0\rangle\\
&= e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ \sum_{n=0}^{\infty}\frac{(\cos\left(\frac{\Theta}{2}\right)\alpha e^{\frac{i\Phi}{2}})^n}{\sqrt{n!}}|n\rangle\otimes|0\rangle\\
&= e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ e^{\frac{|\alpha'|^2}{2}}\ e^{\frac{-|\alpha'|^2}{2}}\ \sum_{n=0}^{\infty}\frac{\alpha'^n}{\sqrt{n!}}|n\rangle\otimes|0\rangle\\
&= e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}(1-|\cos\left(\frac{\Theta}{2}\right)|^2)}\ |\alpha'\rangle\otimes|0\rangle\\
&= e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}|\alpha'\rangle\otimes|0\rangle,\quad con\quad \alpha'=\cos\left(\frac{\Theta}{2}\right)\alpha e^{\frac{i\Phi}{2}}
\end{aligned}
\tag{6.3}
$$

$$
\begin{aligned}
\longrightarrow e^{-\tan(\frac{\Theta}{2})\hat{L}_-}\left(e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}|\alpha'\rangle\otimes|0\rangle\right) &= e^{-\tan(\frac{\Theta}{2})\hat{a}_2^\dagger\hat{a}_1}\left(e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}|\alpha'\rangle\otimes|0\rangle\right)\\
&= e^{-\tan(\frac{\Theta}{2})\alpha'\hat{a}_2^\dagger}\left(e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}|\alpha'\rangle\otimes|0\rangle\right)\\
&= e^{-\sin(\frac{\Theta}{2})\alpha e^{\frac{i\Phi}{2}}\hat{a}_2^\dagger}\left(e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}\ |\alpha'\rangle\otimes|0\rangle\right)\\
&= e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}\ |\alpha'\rangle\otimes e^{|-\sin(\frac{\Theta}{2})\alpha e^{\frac{i\Phi}{2}}|^2}D(\beta)|0\rangle\\
&= |\alpha'\rangle\otimes|\beta\rangle,
\end{aligned}
\tag{6.4}
$$

con $\beta=\tan\left(-\frac{\Theta}{2}\right)\alpha'=-\sin\left(\frac{\Theta}{2}\right)\alpha e^{\frac{i\Phi}{2}}$.

$$
\begin{aligned}
\longrightarrow e^{i\Psi\hat{L}_3}(|\alpha'\rangle\otimes|\beta\rangle) &= e^{i\Psi\frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1-\hat{a}_2^\dagger\hat{a}_2)}(|\alpha'\rangle\otimes|\beta\rangle)\\
&= e^{\frac{1}{2}i\Psi\hat{a}_1^\dagger\hat{a}_1}|\alpha'\rangle\otimes e^{-\frac{1}{2}i\Psi\hat{a}_2^\dagger\hat{a}_2}|\beta\rangle\\
&= e^{\frac{1}{2}i\Psi\hat{a}_1^\dagger\hat{a}_1}e^{-\frac{|\alpha'|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha'^n}{\sqrt{n!}}|n\rangle\otimes e^{-\frac{1}{2}i\Psi\hat{a}_2^\dagger\hat{a}_2}e^{-\frac{|\beta|}{2}^2}\sum_{n=0}^{\infty}\frac{\beta^n}{\sqrt{n!}}|n\rangle\\
&= e^{\frac{1}{2}i\Psi n}e^{-\frac{|\alpha'|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha'^n}{\sqrt{n!}}|n\rangle\otimes e^{-\frac{1}{2}i\Psi n}e^{-\frac{|\beta|}{2}^2}\sum_{n=0}^{\infty}\frac{\beta^n}{\sqrt{n!}}|n\rangle\\
&= e^{-\frac{|\alpha'|^2}{2}}e^{\frac{|\alpha' e^{\frac{i\Psi}{2}}|^2}{2}}e^{-\frac{|\alpha' e^{\frac{i\Psi}{2}}|^2}{2}}\sum_{n=0}^{\infty}\frac{(\alpha' e^{\frac{i\Psi}{2}})^n}{\sqrt{n!}}|n\rangle\otimes e^{-\frac{|\beta|^2}{2}}e^{\frac{|\beta e^{-\frac{i\Psi}{2}}|^2}{2}}e^{-\frac{|\beta e^{-\frac{i\Psi}{2}}|^2}{2}}\sum_{n=0}^{\infty}\frac{(\beta e^{-\frac{i\Psi}{2}})^n}{\sqrt{n!}}|\\
&= e^{-\frac{|\alpha'|^2}{2}(1-|e^{\frac{i\Psi}{2}}|^2)}|\alpha' e^{\frac{i\Psi}{2}}\rangle\otimes e^{-\frac{|\beta|^2}{2}(1-|e^{-\frac{i\Psi}{2}}|^2)}|\beta e^{-\frac{i\Psi}{2}}\rangle\\
&= |\alpha''\rangle\otimes|\beta'\rangle.
\end{aligned}
\tag{6.5}
$$

- Acción del beam splitter sobre el estado coherente con fotón anñadido.

  Al aplicar uno a uno los operadores de $\hat{B}^\dagger$ se obtiene:

$$
\begin{aligned}
\longrightarrow e^{i\Phi\hat{L}_3}\left(\frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}}\otimes|0\rangle\right) &= e^{i\Phi\frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1-\hat{a}_2^\dagger\hat{a}_2)}\left(\frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}}\otimes|0\rangle\right)\\
&= e^{\frac{i\Phi}{2}\hat{a}_1^\dagger\hat{a}_1}\frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}}\otimes e^{-\frac{i\Phi}{2}\hat{a}_2^\dagger\hat{a}_2}|0\rangle\\
&= e^{\frac{i\Phi}{2}\hat{a}_1^\dagger\hat{a}_1}\frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{1+|\alpha|^2}}\sum_{n=0}^{\infty}\frac{\alpha^n\sqrt{(n+1)!}}{n!}|n+1\rangle\otimes|0\rangle\\
&= \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{1+|\alpha|^2}}\sum_{n=0}^{\infty}\frac{\alpha^n\sqrt{(n+1)!}}{n!}e^{\frac{i\Phi}{2}\hat{a}_1^\dagger\hat{a}_1}|n+1\rangle\otimes|0\rangle\\
&= \frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{1+|\alpha|^2}}\sum_{n=0}^{\infty}\frac{\alpha^n\sqrt{(n+1)!}}{n!}e^{\frac{i\Phi}{2}(n+1)}|n+1\rangle\otimes|0\rangle\\
&= e^{\frac{i\Phi}{2}}\frac{e^{-\frac{|\alpha|^2}{2}}}{\sqrt{1+|\alpha|^2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n\sqrt{(n+1)!}}{n!}|n+1\rangle\otimes|0\rangle\\
&= e^{\frac{i\Phi}{2}}e^{-\frac{|\alpha|^2}{2}}e^{\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\frac{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}{\sqrt{1+|\alpha|^2}}\frac{e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}}{\sqrt{1+|\alpha e^{\frac{i\phi}{2}}|^2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n\sqrt{(n+1)!}}{n!}|n+1\rangle\otimes|0\rangle\\
&= e^{\frac{i\Phi}{2}}\frac{e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}}{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n\sqrt{(n+1)!}}{n!}|n+1\rangle\otimes|0\rangle\\
&= e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\phi}{2}},1\rangle\otimes|0\rangle
\end{aligned}
\tag{6.6}
$$

$$
\begin{aligned}
\longrightarrow e^{-\tan(-\frac{\Theta}{2})\hat{L}_+}\left(e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle\right) &= e^{\tan(\frac{\Theta}{2})\hat{a}_1^\dagger\hat{a}_2}\left(e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle\right)\\
&= e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle
\end{aligned}
\tag{6.7}
$$

$$
\begin{aligned}
\longrightarrow & e^{-2\ln(\sec(-\frac{\Theta}{2}))\hat{L}_3}\left(e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle\right) = e^{-2\ln(\sec(\frac{\Theta}{2}))\frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1-\hat{a}_2^\dagger\hat{a}_2)}\left(e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle\right) \\
&= e^{-\ln(\sec(\frac{\Theta}{2}))\hat{a}_1^\dagger\hat{a}_1}e^{\frac{i\Phi}{2}}|\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes e^{\ln(\sec(\frac{\Theta}{2}))\hat{a}_2^\dagger\hat{a}_2}|0\rangle \\
&= e^{\ln(\cos(\frac{\Theta}{2}))\hat{a}_1^\dagger\hat{a}_1}\left(e^{\frac{i\Phi}{2}}\frac{e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}}{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n\sqrt{(n+1)!}}{n!}|n+1\rangle\right)\otimes|0\rangle \\
&= e^{\ln(\cos(\frac{\Theta}{2}))(n+1)}\left(e^{\frac{i\Phi}{2}}\frac{e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}}{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}})^n\sqrt{(n+1)!}}{n!}|n+1\rangle\right)\otimes|0\rangle \\
&= e^{\ln(\cos(\frac{\Theta}{2}))}\left(e^{\frac{i\Phi}{2}}\frac{e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}}{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}\sum_{n=0}^{\infty}\frac{(\alpha e^{\frac{i\Phi}{2}}\cos\left(\frac{\Theta}{2}\right))^n\sqrt{(n+1)!}}{n!}|n+1\rangle\right)\otimes|0\rangle \\
&= \cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}}\ e^{\frac{|\alpha e^{\frac{i\Phi}{2}}\cos(\frac{\Theta}{2})|^2}{2}}\ \frac{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}\cos\left(\frac{\Theta}{2}\right)|^2}}{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}|\cos\left(\frac{\Theta}{2}\right)\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle \\
&= \cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha e^{\frac{i\Phi}{2}}|^2}{2}(1-|\cos(\frac{\Theta}{2})|^2)}\ \frac{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}\cos\left(\frac{\Theta}{2}\right)|^2}}{\sqrt{1+|\alpha e^{\frac{i\Phi}{2}}|^2}}|\cos\left(\frac{\Theta}{2}\right)\alpha e^{\frac{i\Phi}{2}},1\rangle\otimes|0\rangle \\
&= \cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2(\frac{\Theta}{2})}\ \frac{\sqrt{1+|\alpha\cos\left(\frac{\Theta}{2}\right)|^2}}{\sqrt{1+|\alpha|^2}}|\alpha',1\rangle\otimes|0\rangle
\end{aligned}
\tag{6.8}
$$

$$
\begin{aligned}
\longrightarrow & e^{-\tan\left(\frac{\Theta}{2}\right)\hat{L}_-}\left(\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}\ \frac{\sqrt{1+|\alpha\cos\left(\frac{\Theta}{2}\right)|^2}}{\sqrt{1+|\alpha|^2}}|\alpha',1\rangle\otimes|0\rangle\right)\\
&= e^{-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\hat{a}_1}\left(\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}\ \frac{\hat{a}_1^\dagger}{\sqrt{1+|\alpha|^2}}|\alpha'\rangle\otimes|0\rangle\right)\\
&= \frac{\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}}{\sqrt{1+|\alpha|^2}}\left(e^{-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\hat{a}_1}\ \hat{a}_1^\dagger\quad e^{\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\hat{a}_1}\ e^{-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes|0\rangle\right)\\
&= \frac{\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}}{\sqrt{1+|\alpha|^2}}\left(\hat{a}_1^\dagger-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\right)e^{-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes|0\rangle\\
&= \frac{\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}}{\sqrt{1+|\alpha|^2}}\left(\hat{a}_1^\dagger-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\right)|\alpha'\rangle\otimes e^{-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\alpha'}\ |0\rangle\\
&= \frac{\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}}{\sqrt{1+|\alpha|^2}}\left(\hat{a}_1^\dagger-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\right)|\alpha'\rangle\otimes e^{\frac{|-\tan\left(\frac{\Theta}{2}\right)\alpha'|^2}{2}}\ |-\alpha'\tan\left(\frac{\Theta}{2}\right)\rangle\\
&= \frac{\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ e^{-\frac{|\alpha|^2}{2}\sin^2\left(\frac{\Theta}{2}\right)}}{\sqrt{1+|\alpha|^2}}\left(\hat{a}_1^\dagger-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\right)|\alpha'\rangle\otimes e^{\frac{|-\sin\left(\frac{\Theta}{2}\right)\alpha|^2}{2}}\ |-\alpha\sin\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}\ \rangle\\
&= \frac{\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\hat{a}_1^\dagger-\tan\left(\frac{\Theta}{2}\right)\hat{a}_2^\dagger\right)|\alpha'\rangle\otimes|\beta\rangle\\
&= \frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger|\alpha'\rangle\otimes|\beta\rangle-\sin\left(\frac{\Theta}{2}\right)|\alpha'\rangle\otimes\hat{a}_2^\dagger|\beta\rangle\right)
\end{aligned}
\tag{6.9}
$$

$$
\begin{aligned}
&\longrightarrow e^{i\Psi\hat{L}_3}\left(\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger|\alpha'\rangle\otimes|\beta\rangle-\sin\left(\frac{\Theta}{2}\right)|\alpha'\rangle\otimes\hat{a}_2^\dagger|\beta\rangle\right)\right)\\
&=e^{i\Psi\frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1-\hat{a}_2^\dagger\hat{a}_2)}\left(\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger|\alpha'\rangle\otimes|\beta\rangle-\sin\left(\frac{\Theta}{2}\right)|\alpha'\rangle\otimes\hat{a}_2^\dagger|\beta\rangle\right)\right)\\
&=\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ \hat{a}_1^\dagger|\alpha'\rangle\otimes e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ |\beta\rangle-\sin\left(\frac{\Theta}{2}\right)e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ \hat{a}_2^\dagger|\beta\rangle\right)\\
&=\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ \hat{a}_1^\dagger e^{-\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ |\beta\rangle\right)\\
&-\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\sin\left(\frac{\Theta}{2}\right)e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ \hat{a}_2^\dagger e^{\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ |\beta\rangle\right)\\
&=\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger e^{\frac{i\Psi}{2}}\ e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ |\beta\rangle\right)\\
&-\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\sin\left(\frac{\Theta}{2}\right)e^{\frac{i\Psi}{2}\hat{a}_1^\dagger\hat{a}_1}\ |\alpha'\rangle\otimes\hat{a}_2^\dagger e^{-\frac{i\Psi}{2}}\ e^{-\frac{i\Psi}{2}\hat{a}_2^\dagger\hat{a}_2}\ |\beta\rangle\right)\\
&=\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger e^{\frac{i\Psi}{2}}\ e^{\frac{i\Psi}{2}n}\ |\alpha'\rangle\otimes e^{-\frac{i\Psi}{2}n}\ |\beta\rangle\right)\\
&-\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(\sin\left(\frac{\Theta}{2}\right)e^{\frac{i\Psi}{2}n}\ |\alpha'\rangle\otimes\hat{a}_2^\dagger e^{-\frac{i\Psi}{2}}\ e^{-\frac{i\Psi}{2}n}\ |\beta\rangle\right)\\
&=\frac{e^{\frac{i\Phi}{2}}}{\sqrt{1+|\alpha|^2}}\left(e^{\frac{i\Psi}{2}}\ \cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger|\alpha' e^{\frac{i\Psi}{2}}\ \rangle\otimes|\beta e^{-\frac{i\Psi}{2}}\ \rangle-e^{-\frac{i\Psi}{2}}\ \sin\left(\frac{\Theta}{2}\right)|\alpha' e^{\frac{i\Psi}{2}}\ \rangle\otimes\hat{a}_2^\dagger|\beta e^{-\frac{i\Psi}{2}}\ \rangle\right)\\
&=\frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{\frac{i}{2}(\Phi+\Psi)}\ \cos\left(\frac{\Theta}{2}\right)\hat{a}_1^\dagger|\alpha\cos\left(\frac{\Theta}{2}\right)e^{\frac{i}{2}(\Phi+\Psi)}\ \rangle\otimes|-\alpha\sin\left(\frac{\Theta}{2}\right)e^{\frac{i}{2}(\Phi-\Psi)}\ \rangle\right)\\
&-\frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{\frac{i}{2}(\Phi-\Psi)}\ \sin\left(\frac{\Theta}{2}\right)|\alpha\cos\left(\frac{\Theta}{2}\right)e^{\frac{i}{2}(\Phi+\Psi)}\ \rangle\otimes\hat{a}_2^\dagger|-\alpha\sin\left(\frac{\Theta}{2}\right)e^{\frac{i}{2}(\Phi-\Psi)}\ \rangle\right)\\
&=\frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{i\phi_\tau}\ \cos\left(\theta\right)\hat{a}_1^\dagger|\alpha\cos\left(\theta\right)e^{i\phi_\tau}\ \rangle\otimes|-\alpha\sin\left(\theta\right)e^{-i\phi_\rho}\ \rangle\right)\\
&-\frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{-i\phi_\rho}\ \sin\left(\theta\right)|\alpha\cos\left(\theta\right)e^{i\phi_\tau}\ \rangle\otimes\hat{a}_2^\dagger|-\alpha\sin\left(\theta\right)e^{-i\phi_\rho}\ \rangle\right)\\
&=\frac{1}{\sqrt{1+|\alpha|^2}}\left(e^{i\phi_\tau}\ \cos\left(\theta\right)\hat{a}_1^\dagger|\alpha''\rangle\otimes|\beta'\rangle-e^{-i\phi_\rho}\ \sin\left(\theta\right)|\alpha''\rangle\otimes\hat{a}_2^\dagger|\beta'\rangle\right)
\end{aligned}
\tag{6.10}
$$

- Condición de normalización para el estado resultante de la acción del beam splitter sobre el estado $|\alpha, 1\rangle \otimes |0\rangle$.

$$
\begin{aligned}
\longrightarrow \langle\psi_{out}|\psi_{out}\rangle &= \frac{1}{1+|\alpha|^2}\left(e^{-i\phi_\tau}\ \cos(\theta)\,\langle\alpha''|\hat{a}_1 \otimes \langle\beta'| - e^{i\phi_\rho}\ \sin(\theta)\,\langle\alpha''| \otimes \langle\beta'|\hat{a}_2\right) \\
&\left(e^{i\phi_\tau}\ \cos(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle \otimes |\beta'\rangle - e^{-i\phi_\rho}\ \sin(\theta)\,|\alpha''\rangle \otimes \hat{a}_2^\dagger|\beta'\rangle\right) \\
&= \frac{1}{1+|\alpha|^2}(\cos^2(\theta)\,\langle\alpha''|\hat{a}_1\hat{a}_1^\dagger|\alpha''\rangle\langle\beta'|\beta'\rangle - e^{-i(\phi_\tau+\phi_\rho)}\ \cos(\theta)\sin(\theta)\,\langle\alpha''|\hat{a}_1|\alpha''\rangle\langle\beta'|\hat{a}_2^\dagger \\
&- e^{i(\phi_\rho+\phi_\tau)}\ \cos(\theta)\sin(\theta)\,\langle\alpha''|\hat{a}_1^\dagger|\alpha''\rangle\langle\beta'|\hat{a}_2|\beta'\rangle + \sin^2(\theta)\,\langle\alpha''|\alpha''\rangle\langle\beta'|\hat{a}_2\hat{a}_2^\dagger|\beta'\rangle) \\
&= \frac{1}{1+|\alpha|^2}(\cos^2(\theta)\,(1+|\alpha''|^2) - e^{-i(\phi_\tau+\phi_\rho)}\ \cos(\theta)\sin(\theta)\,\alpha''\beta'^* \\
&- e^{i(\phi_\rho+\phi_\tau)}\ \cos(\theta)\sin(\theta)\,\alpha''^*\beta' + \sin^2(\theta)\,(1+|\beta'|^2)) \\
&= \frac{1}{1+|\alpha|^2}(\cos^2(\theta)\,(1+|\alpha''|^2) + e^{-i(\phi_\tau+\phi_\rho)}\ |\alpha|^2\cos^2(\theta)\sin^2(\theta)\,e^{i(\phi_\tau+\phi_\rho)} \\
&+ e^{i(\phi_\rho+\phi_\tau)}\ |\alpha|^2\cos^2(\theta)\sin^2(\theta)\,e^{-i(\phi_\rho+\phi_\tau)}\ + \sin^2(\theta)\,(1+|\beta'|^2)) \\
&= \frac{1}{1+|\alpha|^2}(1+|\alpha|^2\cos^4(\theta) + 2|\alpha|^2\cos^2(\theta)\sin^2(\theta)\sin^2(\theta) + |\alpha|^2\sin^4(\theta)) \\
&= \frac{1}{1+|\alpha|^2}(1+|\alpha|^2(\cos^2(\theta)+\sin^2(\theta))^2) \\
&= \frac{1}{1+|\alpha|^2}(1+|\alpha|^2) \\
&= 1.
\end{aligned}
\tag{6.11}
$$

- Operador densidad de Bob luego de la acción del beam splitter sobre el estado

$|\alpha, 1\rangle$.

$$\rho_{out}^{Bob} = Tr_{Eva}(\rho_{out}) = Tr_{Eva}(|\psi_{out}\rangle\langle\psi_{out}|)$$
$$= Tr_{Eva}(\frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1|\beta'\rangle\langle\beta'| - e^{i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''||\beta'\rangle\langle\beta'|\hat{a}_2$$
$$- e^{-i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_1\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2))$$
$$= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1 Tr(|\beta'\rangle\langle\beta'|) - e^{i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|Tr(|\beta'\rangle\langle\beta'|\hat{a}_2)$$
$$- e^{-i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_1 Tr(\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|) + \sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|Tr(\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2))$$
$$= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1 - e^{i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\beta'$$
$$- e^{-i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_1\beta'^* + \sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|(1+|\beta'|^2))$$
$$= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1 + \alpha e^{i\phi_\tau}\cos(\theta)\sin^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|$$
$$+ \alpha^* e^{-i\phi_\tau}\cos(\theta)\sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_1 + \sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|(1+|\alpha|^2\sin^2(\theta))), \tag{6.12}$$

- Desarrollo $Tr\{\rho_{out}^{Bob}\} = 1$.

$$
\begin{aligned}
Tr\{\rho_{out}^{Bob}\} &= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\, Tr\{\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1\} + \alpha e^{i\phi_\tau}\cos(\theta)\sin^2(\theta)\, Tr\{\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\} \\
&+ \alpha^* e^{-i\phi_\tau}\cos(\theta)\sin^2(\theta)\, Tr\{|\alpha''\rangle\langle\alpha''|\hat{a}_1\} + \sin^2(\theta)\, Tr\{|\alpha''\rangle\langle\alpha''|\}(1+|\alpha|^2\sin^2(\theta))) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,(1+|\alpha''|^2) + \alpha e^{i\phi_\tau}\cos(\theta)\sin^2(\theta)\,\alpha''^* \\
&+ \alpha^* e^{-i\phi_\tau}\cos(\theta)\sin^2(\theta)\,\alpha'' + \sin^2(\theta)\,(1+|\alpha|^2\sin^2(\theta))) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,(1+|\alpha''|^2) + |\alpha|^2\cos^2(\theta)\sin^2(\theta) \\
&+ |\alpha|^2\cos^2(\theta)\sin^2(\theta) + \sin^2(\theta)\,(1+|\alpha|^2\sin^2(\theta))) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2\cos^4(\theta) + 2|\alpha|^2\cos^2(\theta)\sin^2(\theta) + |\alpha|^2\sin^4(\theta))) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2[\cos^4(\theta) + 2\cos^2(\theta)\sin^2(\theta) + \sin^4(\theta)]) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2(\cos^2(\theta)+\sin^2(\theta))^2) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2) \\
&= 1
\end{aligned}
\tag{6.13}
$$

- Probabilidad de Bob de obtener n fotones:

$$
\begin{aligned}
P_n &= \langle n|\rho_{out}^{Bob}|n\rangle \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,\langle n|\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1|n\rangle + \alpha\cos(\theta)\sin^2(\theta)\,\langle n|\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|n\rangle \\
&+ \alpha^*\cos(\theta)\sin^2(\theta)\,\langle n|\alpha''\rangle\langle\alpha''|\hat{a}_1|n\rangle + (\sin^2(\theta)+|\alpha|^2\sin^4(\theta))\langle n|\alpha''\rangle\langle\alpha''|n\rangle) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,|\langle n|\hat{a}_1^\dagger|\alpha''\rangle|^2 + \alpha\cos(\theta)\sin^2(\theta)\,\langle n|\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|n\rangle \\
&+ \alpha^*\cos(\theta)\sin^2(\theta)\,\langle n|\alpha''\rangle\langle\alpha''|\hat{a}_1|n\rangle + (\sin^2+|\alpha|^2\sin^4(\theta))|\langle n|\alpha''\rangle|^2) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\left|\sqrt{n}e^{-\frac{|\alpha''|^2}{2}}\sum_{n=1}^{\infty}\frac{\alpha''^{(n-1)}}{\sqrt{(n-1)!}}\right|^2 \\
&+ \alpha\cos(\theta)\sin^2(\theta)\,e^{-|\alpha''|^2}\sqrt{n}\sum_{n=1}^{\infty}\frac{\alpha''^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\alpha''^{n}}{\sqrt{n!}} \\
&+ \alpha^*\cos(\theta)\sin^2(\theta)\,e^{-|\alpha''|^2}\sqrt{n}\sum_{n=0}^{\infty}\frac{\alpha''^{n}}{\sqrt{n!}}\sum_{n=1}^{\infty}\frac{\alpha''^{(n-1)}}{\sqrt{(n-1)!}} \\
&+ (\sin^2+|\alpha|^2\sin^4(\theta))\left|e^{-\frac{|\alpha''|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha''^{n}}{\sqrt{n!}}\right|^2) \\
&= \frac{e^{-|\alpha''|^2}}{(1+|\alpha|^2)}(\cos^2(\theta)\,n\sum_{n=1}^{\infty}\frac{\alpha''^{2(n-1)}}{(n-1)!} \\
&+ 2\alpha\cos(\theta)\sin^2(\theta)\sqrt{n}\sum_{n=1}^{\infty}\frac{\alpha''^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\alpha''^{n}}{\sqrt{n!}} \\
&+ (\sin^2+|\alpha|^2\sin^4(\theta))\sum_{n=0}^{\infty}\frac{\alpha''^{2n}}{n!})
\end{aligned}
\tag{6.14}
$$

- Obtención de la matriz densidad de Eva ρ_{out}^{Eva}

$$
\begin{aligned}
&\rho_{out}^{Eva} = Tr_{Bob}(\rho_{out}) = Tr_{Bob}(|\psi_{out}\rangle\langle\psi_{out}|) \\
&= Tr_{Bob}(\frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1|\beta'\rangle\langle\beta'| - e^{i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\beta'\rangle\langle\beta'|\hat{a}_2 \\
&- e^{-i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_1\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,|\alpha''\rangle\langle\alpha''|\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2)) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,Tr(\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|\hat{a}_1)|\beta'\rangle\langle\beta'| - e^{i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,Tr(\hat{a}_1^\dagger|\alpha''\rangle\langle\alpha''|)|\beta'\rangle\langle\beta'|\hat{a}_2 \\
&- e^{-i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,Tr(|\alpha''\rangle\langle\alpha''|\hat{a}_1)\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,Tr(|\alpha''\rangle\langle\alpha''|)\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)(1+|\alpha''|^2)|\beta'\rangle\langle\beta'| - e^{i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,\alpha''^*|\beta'\rangle\langle\beta'|\hat{a}_2 \\
&- e^{-i(\phi_\tau+\phi_\rho)}\cos(\theta)\sin(\theta)\,\alpha''\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)(1+|\alpha|^2\cos^2(\theta))|\beta'\rangle\langle\beta'| - \alpha^* e^{i\phi_\rho}\cos^2(\theta)\sin(\theta)\,|\beta'\rangle\langle\beta'|\hat{a}_2 \\
&- \alpha e^{-i\phi_\rho}\cos^2(\theta)\sin(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'| + \sin^2(\theta)\,\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2).
\end{aligned}
\tag{6.15}
$$

- Desarrollo $Tr\{\rho_{out}^{Eva}\} = 1$.

$$
\begin{aligned}
Tr\{\rho_{out}^{Eva}\} &= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)(1+|\alpha|^2\cos^2(\theta))Tr\{|\beta'\rangle\langle\beta'|\} - \alpha^* e^{i\phi_\rho}\cos^2(\theta)\sin(\theta)\,Tr\{|\beta'\rangle\langle\beta'|\hat{a}_2 \\
&- \alpha e^{-i\phi_\rho}\cos^2(\theta)\sin(\theta)\,\{\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\} + \sin^2(\theta)\,Tr\{\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2\}) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,(1+|\alpha|^2\cos^2(\theta)) - \alpha^* e^{i\phi_\rho}\cos^2(\theta)\sin(\theta)\,\beta' \\
&- \alpha e^{-i\phi_\rho}\cos^2(\theta)\sin(\theta)\,\beta'^* + \sin^2(\theta)\,(1+|\beta'|^2)) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta) + |\alpha|^2\cos^4(\theta) + \alpha^*\cos^2(\theta)\sin^2(\theta)\,\alpha \\
&+ \alpha\cos^2(\theta)\sin^2(\theta)\,\alpha^* + \sin^2(\theta) + |\alpha|^2\sin^4(\theta))) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2\cos^4(\theta) + 2|\alpha|^2\cos^2(\theta)\sin^2(\theta) + |\alpha|^2\sin^4(\theta))) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2[\cos^4(\theta) + 2\cos^2(\theta)\sin^2(\theta) + \sin^4(\theta)]) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2(\cos^2(\theta) + \sin^2(\theta))^2) \\
&= \frac{1}{(1+|\alpha|^2)}(1+|\alpha|^2) \\
&= 1
\end{aligned}
\tag{6.16}
$$

- Probabilidad de Eva de obtener n fotones.

$$
\begin{aligned}
P_n &= \langle n|\rho_{out}^{Eva}|n\rangle \\
&= \frac{1}{(1+|\alpha|^2)}((\cos^2(\theta)+|\alpha|^2\cos^4(\theta))\langle n|\beta'\rangle\langle\beta'|n\rangle - \alpha^*\cos^2(\theta)\sin(\theta)\,\langle n|\beta'\rangle\langle\beta'|\hat{a}_2|n\rangle \\
&- \alpha\cos^2(\theta)\sin(\theta)\,\langle n|\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|n\rangle + \sin^2(\theta)\,\langle n|\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|\hat{a}_2|n\rangle) \\
&= \frac{1}{(1+|\alpha|^2)}(\cos^2(\theta)\,|\langle n|\beta'\rangle|^2 - \alpha^*\cos^2(\theta)\sin(\theta)\,\langle n|\beta'\rangle\langle\beta'|\hat{a}_2|n\rangle \\
&- \alpha\cos^2(\theta)\sin(\theta)\,\langle n|\hat{a}_2^\dagger|\beta'\rangle\langle\beta'|n\rangle + \sin^2(\theta)|\langle n|\hat{a}_2^\dagger|\beta'\rangle|^2) \\
&= \frac{1}{(1+|\alpha|^2)}((\cos^2(\theta)+|\alpha|^2\cos^4(\theta))\left|e^{-\frac{|\beta'|^2}{2}}\sum_{n=0}^{\infty}\frac{\beta'^n}{\sqrt{n!}}\right|^2 \\
&- \alpha^*\cos^2(\theta)\sin(\theta)\,e^{-|\beta'|^2}\sqrt{n}\sum_{n=1}^{\infty}\frac{\beta'^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\beta'^n}{\sqrt{n!}} \\
&- \alpha\cos^2(\theta)\sin(\theta)\,e^{-|\beta'|^2}\sqrt{n}\sum_{n=0}^{\infty}\frac{\beta'^n}{\sqrt{n!}}\sum_{n=1}^{\infty}\frac{\beta'^{(n-1)}}{\sqrt{(n-1)!}} \\
&+ \sin^2(\theta)\left|\sqrt{n}e^{-\frac{|\beta'|^2}{2}}\sum_{n=1}^{\infty}\frac{\beta'^{(n-1)}}{\sqrt{(n-1)!}}\right|^2) \\
&= \frac{e^{-|\beta'|^2}}{(1+|\alpha|^2)}((\cos^2(\theta)+|\alpha|^2\cos^4(\theta))\sum_{n=0}^{\infty}\frac{\beta'^{2n}}{n!} \\
&- 2\alpha\cos^2(\theta)\sin(\theta)\sqrt{n}\sum_{n=1}^{\infty}\frac{\beta'^{(n-1)}}{\sqrt{(n-1)!}}\sum_{n=0}^{\infty}\frac{\beta'^n}{\sqrt{n!}} \\
&+ \sin^2(\theta)\sum_{n=1}^{\infty}\frac{\beta'^{2(n-1)}}{(n-1)!})
\end{aligned}
\tag{6.17}
$$

- Matriz densidad final luego de la acción del canal cuántico de comunicación.

$$\rho(t) = \sum_{n=0}^{\infty} M_n|\alpha,1\rangle\langle\alpha,1|M_n^\dagger = \frac{1}{1+|\alpha|^2}\sum_{n=0}^{\infty}\frac{\mathcal{T}^n}{n!}e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha|^{2(n-1)} \quad [\quad n^2|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|$$
$$+\ \alpha e^{-\mathcal{K}t}\ n\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \alpha^* e^{-\mathcal{K}t}\ n|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a} + |\alpha|^2 e^{-2\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a} \quad]$$
$$= \frac{1}{1+|\alpha|^2}e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha|^{-2}\{\left(\sum_{n=0}^{\infty}\frac{\mathcal{T}^n}{n!}|\alpha|^{2n}n^2\right)|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|$$
$$+\left(\sum_{n=0}^{\infty}\frac{\mathcal{T}^n}{n!}|\alpha|^{2n}n\right)\alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|$$
$$+\left(\sum_{n=0}^{\infty}\frac{\mathcal{T}^n}{n!}|\alpha|^{2n}n\right)e^{-\mathcal{K}t}\ \alpha^*|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a} + \left(\sum_{n=0}^{\infty}\frac{\mathcal{T}^n}{n!}|\alpha|^{2n}\right)|\alpha|^2 e^{-2\mathcal{K}t}\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\}$$
$$= \frac{1}{1+|\alpha|^2}e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha|^{-2}\{\mathcal{T}|\alpha|^2\left(e^{\mathcal{T}|\alpha|^2}\ +\mathcal{T}|\alpha|^2 e^{\mathcal{T}|\alpha|^2}\ \right)|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|$$
$$+\left(\mathcal{T}|\alpha|^2 e^{\mathcal{T}|\alpha|^2}\ \right)\alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \left(\mathcal{T}|\alpha|^2 e^{\mathcal{T}|\alpha|^2}\ \right)e^{-\mathcal{K}t}\ \alpha^*|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}$$
$$+\left(e^{\mathcal{T}|\alpha|^2}\ \right)|\alpha|^2 e^{-2\mathcal{K}t}\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\}$$
$$= \frac{1}{1+|\alpha|^2}e^{-|\alpha|^2(1-|e^{-\mathcal{K}t}|^2)}\ |\alpha|^{-2}e^{\mathcal{T}|\alpha|^2}\{\mathcal{T}|\alpha|^2\left(1+\mathcal{T}|\alpha|^2\right)|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|$$
$$+\left(\mathcal{T}|\alpha|^2\right)\alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \left(\mathcal{T}|\alpha|^2\right)e^{-\mathcal{K}t}\ \alpha^*|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}$$
$$+|\alpha|^2 e^{-2\mathcal{K}t}\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\}$$
$$= \frac{1}{1+|\alpha|^2}\Bigg[\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \mathcal{T}\alpha e^{-\mathcal{K}t}\ \hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}| + \mathcal{T}e^{-\mathcal{K}t}\ \alpha^*|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}}$$
$$+\ e^{-2\mathcal{K}t}\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\Bigg]. \tag{6.18}$$

- Desarrollo $Tr\{\rho(t)\} = 1$.

$$
\begin{aligned}
Tr\{\rho(t)\} &= \frac{1}{1+|\alpha|^2}\{\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right) Tr\{|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\} + \mathcal{T}\alpha e^{-\mathcal{K}t}\ Tr\{\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\} \\
&\quad + \mathcal{T}\alpha^* e^{-\mathcal{K}t}\ Tr\{|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\} + e^{-2\mathcal{K}t} Tr\{\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}\}\} \\
&= \frac{1}{1+|\alpha|^2}\{\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right) + \mathcal{T}\alpha e^{-\mathcal{K}t}\ \alpha^* e^{-\mathcal{K}t} + \mathcal{T}\alpha^* e^{-\mathcal{K}t}\ \alpha e^{-\mathcal{K}t} + e^{-2\mathcal{K}t}(1+|\alpha|^2 e^{-2\mathcal{K}t})\} \\
&= \frac{1}{1+|\alpha|^2}\{\mathcal{T} + e^{-2\mathcal{K}t} + |\alpha|^2(\mathcal{T}^2 + 2\mathcal{T}e^{-2\mathcal{K}t}\ + e^{-4\mathcal{K}t})\} \\
&= \frac{1}{1+|\alpha|^2}\{\mathcal{T} + e^{-2\mathcal{K}t} + |\alpha|^2(\mathcal{T} + e^{-2\mathcal{K}t})^2\} \\
&= \frac{1}{1+|\alpha|^2}\{1 - |e^{-\mathcal{K}t}|^2 + e^{-2\mathcal{K}t} + |\alpha|^2(1 - |e^{-\mathcal{K}t}|^2 + e^{-2\mathcal{K}t})^2\} \\
&= \frac{1}{1+|\alpha|^2}\{1+|\alpha|^2\} \\
&= 1
\end{aligned}
\tag{6.19}
$$

- Distribución de probabilidad de $\rho(t)$.

$$
\begin{aligned}
Pn &= \langle n|\rho(t)|n\rangle \\
&= \frac{1}{1+|\alpha|^2}\{\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)\langle n|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|n\rangle + \mathcal{T}\alpha e^{-\mathcal{K}t}\ \langle n|\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|n\rangle \\
&+ \mathcal{T}e^{-\mathcal{K}t}\ \alpha^*\langle n|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}|n\rangle + e^{-2\mathcal{K}t}\langle n|\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}|n\rangle\} \\
&= \frac{1}{1+|\alpha|^2}\{\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)|\langle n|\alpha e^{-\mathcal{K}t}\rangle|^2 + \alpha\mathcal{T}e^{-\mathcal{K}t}\ \langle n|\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|n\rangle \\
&+ \alpha^*\mathcal{T}e^{-\mathcal{K}t}\ \langle n|\alpha e^{-\mathcal{K}t}\rangle\langle\alpha e^{-\mathcal{K}t}|\hat{a}|n\rangle + e^{-2\mathcal{K}t}|\langle n|\hat{a}^\dagger|\alpha e^{-\mathcal{K}t}\rangle|^2\} \\
&= \frac{1}{1+|\alpha|^2}\{\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)\left|e^{\frac{-|\alpha e^{-\mathcal{K}t}|^2}{2}}\sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^n}{\sqrt{n!}}\right|^2 \\
&+ \alpha\mathcal{T}e^{-\mathcal{K}t}\ \sqrt{n}e^{-|\alpha e^{-\mathcal{K}t}|^2}\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n-1}}{\sqrt{(n-1)!}}\ \sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^n}{\sqrt{n!}} \\
&+ \alpha^*\mathcal{T}e^{-\mathcal{K}t}\ \sqrt{n}e^{-|\alpha e^{-\mathcal{K}t}|^2}\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n-1}}{\sqrt{(n-1)!}}\ \sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^n}{\sqrt{n!}} \\
&+ e^{-2\mathcal{K}t}\left|e^{\frac{-|\alpha e^{-\mathcal{K}t}|^2}{2}}\sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^n}{\sqrt{n!}}\right|^2\} \\
&= \frac{e^{-|\alpha e^{-\mathcal{K}t}|^2}}{1+|\alpha|^2}\Bigg[\mathcal{T}\left(1+\mathcal{T}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2n}}{n!} \\
&+ 2\alpha\mathcal{T}e^{-\mathcal{K}t}\ \sqrt{n}\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{n-1}}{\sqrt{(n-1)!}}\ \sum_{n=0}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^n}{\sqrt{n!}} \\
&+ e^{-2\mathcal{K}t}n\sum_{n=1}^{\infty}\frac{\left(\alpha e^{-\mathcal{K}t}\right)^{2(n-1)}}{(n-1)!}\ \Bigg]
\end{aligned}
\tag{6.20}
$$

Bibliografía

[1] P. Caballero. *Introducción a la Criptografía*. Ed. Ra-Ma. Madrid 2002.

[2] S. Fernández. *La Criptografía Clásica*. Revista SIGMA N^o 24. Abril 2004.

[3] J. Nechvatal, *Public Key Cryptography*, in Contemporary Cryptography, The Science of Information Integrity, G. Simmons ed., IEEE Press. 1991.

[4] R. L. Rivest, A. Shamir, L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM. Vol. **21**, p. 120-126 (1978).

[5] P. W. Shor. *Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM J. Sci. Statist. Comput. 26 (1997) 1484 quant-ph/9508027.

[6] G. S. Vernam. *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*, J. Amer. Inst. Elec. Eng. 45, 109-115, 1926.

[7] C. E. Shannon, *Communication theory of secrecy systems*, Bell Syst. Tech. J., vol. 28, pp. 656-715, 1949.

[8] C. H. Bennett, G. Brassard. *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175-179, 1984.

[9] D. F. Walls, G. J. Milburn, *Quantum Optics*, Springer-verlag, 1995.

[10] M. Fox, *Quantum Optics: An Introduction*. Oxford University Press, Oxford. 2007.

[11] M. O. Scully, M. S. Zubairy, *Quantum Optics*. Cambridge University Press, Cambridge. 1997.

[12] S. Sivakumar, *Photon-added coherent states as nonlinear coherent states*. J. Phys. A **32**, 3441, 1999.

[13] M. Kim, M. Bellini, *The quantum mechanics of photon addition and subtraction*. SPIE Newsroom DOI:10.1117/2.1200811.1369. December 2008.

[14] J. Wenger, R. Tualle-Brouri, P. Grangier, *Non-Gaussian statistics from individual pulses of squeezed light*, Phys. Rev. Lett. 92, No. 15, pp. 153601. 2004.

[15] M. E. V. Ruiz, A. S. Ramirez, *Sobre algunos modelos de implementación para la computación cuántica*, Escuela de Ciencias y Humanidades, Universidad EAFIT.

[16] R. A. Campos, B. E. A. Saleh, M. C. Teich. *Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statistics*. Phys. Rev. A **40**, 1371 (1989).

[17] P. Jordan, Z. Phys. **94**, 531 (1935).

[18] J. Schwinger, U.S. Atomic Energy Commission Resport. No. NYO-3071 (U.S. GPO, Washington, D.C., 1952); reprinted in *Quantum Theory of Angular Momentum*, edited by L. C. Biedenharn and H. van Dam (Academic, New York, 1965).

[19] D. Rodney Truax. *Baker-Campbell-Hausdorff relations and unitarity of SU(2) and SU(1,1) squeeze operators*. Phys. Rev. D **31**, 1988 (1985).

[20] W. Miller, Jr., *Symmetry Groups and Their Applications*, (Academic, New York, 1972), Chap. 5.

[21] J. G. F. Belinfante and B. Kolman, *A Survey of Lie Groups and Lie Algebras with Applications and Computational Methods*, (SIAM, Philadelphia, 1972).

[22] A. O. Barut, in *Lectures in Theoretical Physics*, proceedings of the Institute for Theorical Physics, Boulder, 1966, edited by W. E. Britten, A. O. Barut, and M. Guenin (Gordon and Breach, New York, 1967), Vol. **IXA**, p. 125.

[23] A. Nazir *Lecture notes on open quantum systems* http://www3.imperial.ac.uk/people/a.nazir. 2013.

[24] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University. 2000.

[25] S. Omkar, R. Srikanth, S. Banerjee, *Dissipative and non-dissipative single-qubit channels: dynamics and geometry*. Quant. Info. Proc. **12**, 3725. 2013.

[26] H.-y. Fan, L-y. Hu, Optics Communications **282**, 932-935. 2009.