UVa FacultaddeCiencias

TRABAJO DE FIN DE GRADO

Grado en FÍSICA

Protocolos de seguridad con estados cuánticos de la luz

Autor: Mª Elisabet Pelazas Rivero

Tutores: Juan Carlos García Escartín
Luis Miguel Nieto Calzada

22 de julio de 2021

Índice general

Índice de figuras

Resumen

Los protocolos de Criptografía Cuántica utilizan las leyes de la Física para garantizar la seguridad en la comunicación, lo cual marca la diferencia con respecto a los protocolos clásicos, que recurren a problemas matemáticos cuya solución es muy difícil computar. Uno de los problemas centrales es la autenticación de los usuarios que tratan de establecer una comunicación por un canal que es inseguro, pudiendo haber tanto espías escuchando como impostores suplantando la identidad de los usuarios legítimos.

En este trabajo, presentamos una solución basada en aplicar la Óptica Cuántica para identificar a un usuario que conoce una determinada contraseña y que comparte con otro. Concretamente, proponemos un protocolo de comprobación de contraseñas consistente en generar a partir de la contraseña compartida, otra compuesta por una cadena de estados ópticos coherentes que se deberá comparar para confirmar la identidad del usuario en cuestión. Obtendremos cotas de la información que un atacante puede obtener de esta contraseña a partir de las limitaciones de la medida cuántica. Además, es importante destacar que haremos uso solamente de dispositivos y tecnología disponibles en la actualidad, incluyendo finalmente un tratamiento realista.

Abstract

Quantum Cryptography protocols use the laws of Physics to guarantee communication security instead of complex mathematical problems as the classical ones do. A central problem is to authenticate the identity of the users who want to communicate with each other by means of an insecure channel.

In this work, we present an application of Quantum Optics to the identification of a user who knows a certain password which is shared with another one. Specifically, the protocol uses optical coherent states to preserve the privacy of the password, even in the presence of an eavesdropper or impostors. The limitations of quantum measurement will give bounds on the information attackers can learn about the password. Furthermore, it is important to highlight that we will only use devices and technology which are currently available, including finally a realistic treatment.

Palabras clave: Criptografía Cuántica, comprobación de contraseñas, cota de Holevo, divisor de haz, entropía de von Neumann, estados coherentes, fotón, medida de discriminación sin

ambigüedad, protocolos de seguridad cuántica, Teoría de la Información Cuántica, Teorema de no clonación.

Introducción

La seguridad en las comunicaciones ha supuesto a lo largo de la historia un desafío. Los sistemas criptográficos actuales basan su seguridad en problemas matemáticos de difícil resolución, como la factorización, pero se ha demostrado su fragilidad cuando se emplean algoritmos cuánticos, como el de Shor [66]. La posibilidad de superar el rendimiento clásico sacando provecho de las leyes de la Física ha llevado a que actualmente se realice una activa investigación en el área de la Computación Cuántica y, en consecuencia, de la Criptografía Cuántica, contexto en que se enmarca el desarrollo del trabajo.

De hecho, para comenzar este trabajo querríamos hacer mención al panorama actual de la Computación y la Criptografía Cuántica, áreas de activa investigación que han despertado el interés tanto de profesionales como del público en general. De hecho, puesto que la Criptografía actual sería vulnerable al algoritmo de Shor, muchas entidades han comenzado ya a organizarse con el fin de reforzar sus sistemas criptográficos ante ataques cuánticos y, más a largo plazo, en caso de que se extendieran los ordenadores cuánticos, estar preparados para implementar sistemas de Criptografía Cuántica para reducir posibles riesgos. En particular, el NIST (National Institute of Standards and Technology, EEUU) publicó en 2016 un informe [54] sobre la computación en la era post-cuántica solicitando propuestas de algoritmos resistentes a ataques cuánticos para evaluarlos y estandarizar uno o varios de ellos. Actualmente están analizándose las candidaturas y esperan publicar los resultados entre 2022 y 2024.

Sin embargo, debemos ser conscientes de las limitaciones de este campo emergente [4]. Respecto a la Computación Cuántica, los ordenadores hasta ahora se ha probado que son excepcionalmente rápidos para tareas específicas, como resolver ciertos problemas matemáticos pero, en otra variedad de problemas como partidas de ajedrez, programar los vuelos de una aerolínea... hay expertos que piensan que no superarán a los clásicos.

Aparte de estas limitaciones intrínsecas, existen las que plantean los numerosos obstáculos técnicos que hay en la construcción de estos dispositivos. Por ejemplo, principalmente, la decoherencia cuántica, que hace referencia al ínfimo tiempo de supervivencia de los estados cuánticos. Además, muchas computadoras como las construidas por Google e IBM (las principales compañías que participan en esta carrera) necesitan helio-3, un derivado de la investigación nuclear y los cables superconductores requeridos se fabrican solamente en una empresa en todo el mundo ubicada en Japón. Asimismo, el control de sistemas de múltiples qubits requiere la generación y la coordinación de numerosas señales eléctricas con una resolución enormemente precisa. Por último, existen también otros inconveniente relativos al tamaño de los procesadores o las bajas temperaturas necesarias.

De hecho, aún no se ha resuelto el problema de qué hardware utilizar, pero se han definido una serie de condiciones que deben cumplir [25]. No obstante, la investigación continua. Google

asegura haber conseguido la *supremacía cuántica* [7], término acuñado para hacer referencia a la realización de una tarea en un ordenador cuántico utilizando exponencialmente menos recursos que en un ordenador clásico, a pesar de que IBM lo pone en duda [56]. Otro hecho destacable es que el primer ordenador cuántico para uso comercial fue presentado por IBM en 2019 [59], de 20 qubits, cantidad que se sigue mejorando.

A pesar de las limitaciones existentes para llevar a cabo actualmente una implementación práctica que supere a la clásica, lo cual ni siquiera se sabe con seguridad si es posible, es importante seguir avanzando en las investigaciones para resolver esta duda por los posibles descubrimientos colaterales que ello implique, tanto en el campo de la Física Cuántica como en el de de la Computación Clásica.

A continuación vamos a exponer el problema y el objetivo esencial que se abordan en este Trabajo Fin de Grado, con el fin de preparar al lector para abordar el resto de contenidos del manuscrito. En concreto, nos planteamos comprobar que dos usuarios (llamémoslos Alice y Bob) que comparten una contraseña p, de s bits y previamente establecida, son legítimos, pues supondremos que la comunicación es completamente insegura de forma que no se dispone ni de un canal público autenticado, ni de un canal privado inseguro, y se conocen todas las máquinas que se utilizan para la implementación, así como el conjunto de N estados coherentes simétricos de igual amplitud al que recurriremos:

$$|\psi_{key}\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_M\rangle\,, \quad |\alpha_j\rangle = |\alpha_j| e^{i\phi_j}, \quad \phi_j = \frac{2\pi j}{N}, \quad j = 0, \ldots, N-1.$$

Como ejemplo más intuitivo para entender el problema y la solución que se plantean en el trabajo podemos suponer que $|\psi_{key}\rangle$ protege una *tarjeta de crédito* y p es la contraseña que se establece físicamente cuando se solicita en el banco. Por tanto, hay que establecer una forma de demostrar que, al utilizarla para pagar, el usuario es legítimo. Por su parte, el espía podría llevar a cabo las siguientes operaciones análogas a los ataques que estudiamos y resolvemos:

- Con una tarjeta falsa conseguir sacar dinero. O incluso lograrlo sin ninguna tarjeta, que sería equivalente a utilizar el estado vacío como $|\psi_{key}\rangle$, lo cual demostraremos que se trata del mejor ataque de este tipo.
- Mediante un cajero falso leer la información de la tarjeta para utilizarla en un cajero de verdad después.
- Colocar una antena cercana al cajero y obtener información para conseguir falsificar la tarjeta.

La solución propuesta se basa en garantizar la seguridad del protocolo gracias a las leyes de la Física, en concreto, de la Mecánica Cuántica. Esta es la principal diferencia con respecto a la Criptografía Clásica, donde la seguridad se basa en problemas matemáticos cuya solución es computacionalmente muy difícil de resolver.

En concreto, inspirándonos en la ideas propuestas en [29] y [6], nuestra solución pretende generalizarlas para utilizar una cadena $|\psi\rangle_{key}$ compuesta por M de esos estados coherentes, cuyas fases se elegirán aleatoriamente a partir del *hash* de la concatenación de p y una cadena de t bits aleatoria r_i, $H(p\|r_i)$, lo cual se trata de una función matemática que introduce aleatoriedad. Esta contraseña será la que se deberá comprobar con el fin de asegurar la identidad de ambos extremos, para lo cual detallaremos un *test de comparación* de estados coherentes mediante un *divisor de haz*. También es importante destacar que se emplearán dispositivos y tecnología

disponibles en la actualidad, por lo que el protocolo será realizable experimentalmente. De manera resumida, se puede observar en qué consiste este proceso en el diagrama que se muestra en la Figura 1.

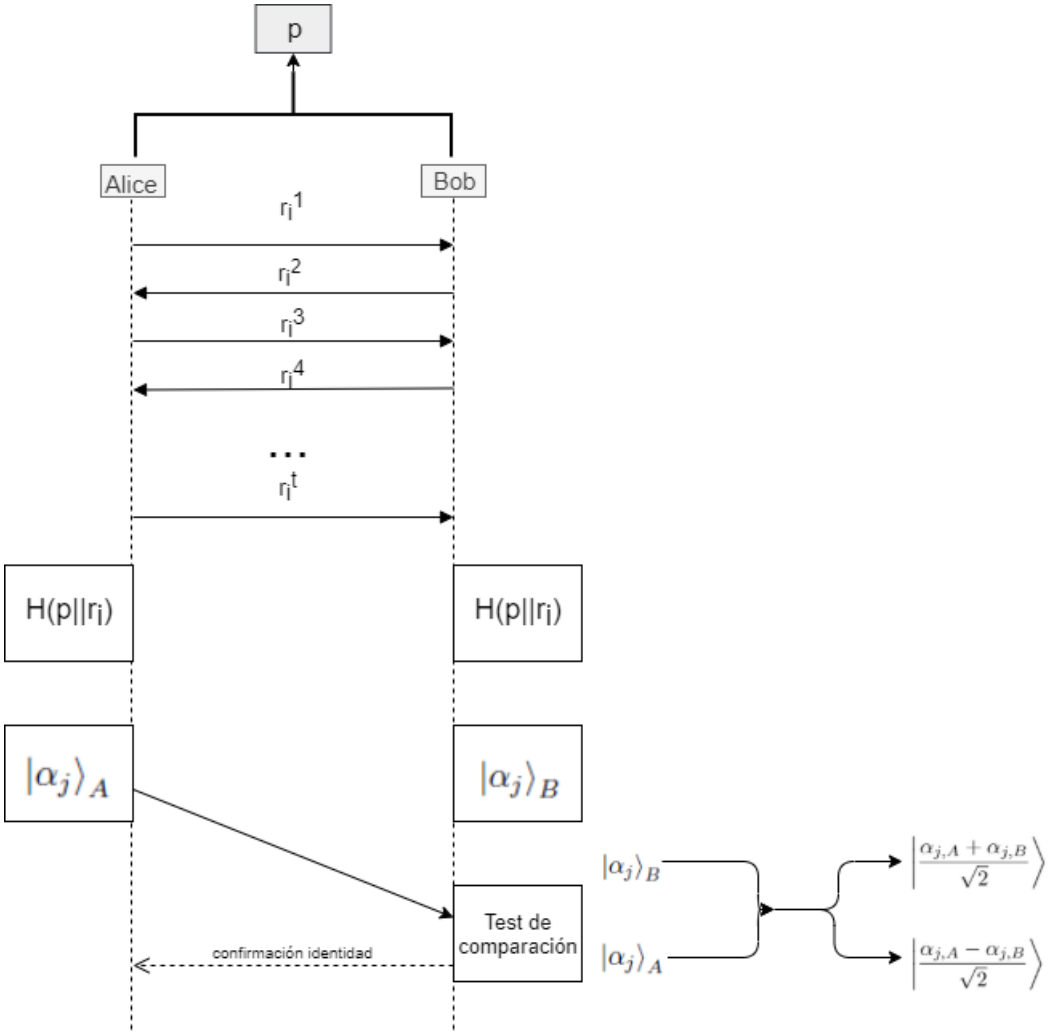


Figura 1: Diagrama del protocolo de comprobación de contraseñas con estados coherentes propuesto: caso en que Alice demuestra su identidad a Bob.

Notemos que deberemos repetir este procedimiento para los M estados que componen la cadena $|\psi_{key}\rangle$ y atribuiremos cualquier fallo que implique no superar el test a la presencia de un espía.

A este respecto, mostraremos los tipos de ataque que pueden tener lugar, buscando evitar tanto la falsificación de estados como la recuperación de la contraseña basándonos en resultados que expondremos a lo largo del manuscrito. Para ello, es importante notar que los estados coherentes se pueden comparar fácilmente con técnicas sencillas de óptica, como los divisores de haz y los *fotodetectores*, tal y como se muestra en [6] y tratamos de mostrar en el diagrama de la Figura 1. Asegurar este proceso de comparación no resulta trivial, pues dos estados que no sean ortogonales entre sí no se pueden distinguir sin ambigüedad, por lo que añadiremos su justificación mediante el *límite IDP* [24, 36, 58]. De hecho, los estados coherentes poseen la propiedad de no ser ortogonales entre sí y se ha generalizado este resultado probando cotas [20]

que garantizan que la operación puede llevarse a cabo de manera adecuada.

Además, para garantizar en lo posible la confidencialidad utilizaremos ciertos resultados de Teoría de la Información Cuántica. Concretamente, el hecho de cuantificar la información accesible es un tema central y se lleva a cabo mediante la *entropía de von Neumann* [22] y la *cota de Holevo* [34], entre otras que expondremos. Asimismo, es fundamental el *Teorema de no clonación*, que imposibilita que se puedan realizar copias exactas de estados cuánticos.

Por último, mostraremos algunos resultados gráficos relativos a ciertos casos prácticos, para encontrar una elección óptima de todos los parámetros que intervienen que garantice la seguridad incluso en el caso real en que haya ruido y pérdidas en el canal y en las detecciones.

En definitiva, con el fin de abordar la consecución del objetivo señalado, la organización del trabajo es la siguiente:

- En primer lugar, para situar el contexto en que se desarrollan los contenidos del manuscrito, mostraremos en esta introducción los antecedentes históricos de la Criptografía Cuántica.
- A continuación, dando por sabidos los postulados de la Mecánica Cuántica y la notación de Dirac, comenzaremos en el Capítulo 1 repasando las propiedades del sistema cuántico más simple, pero de vital importancia en el desarrollo de la teoría, pues aparecerá constantemente: el *oscilador armónico cuántico*. Se sentarán así las bases de la cuantificación del campo electromagnético que resulta fundamental a la hora de establecer la teoría de la Óptica Cuántica y, en particular, los *estados cuánticos de la luz*.
- Apoyándonos en lo anterior, se desarrollan en el Capítulo 2 los resultados concretos en que se fundamenta la realización del protocolo de seguridad con estados cuánticos de la luz. En particular, trataremos con detalle los *estados coherentes*, la interpretación mecánico-cuántica de los *divisores de haz* y aspectos relacionados con la *medida cuántica*. Además, se introducirán los aspectos más relevantes de la Teoría de la Información Cuántica.
- En relación a esto último, se detallarán en el Capítulo 3 las bases de la Criptografía Cuántica para haber establecido completamente el contexto ideal en que proponer el protocolo de seguridad con estados coherentes. Además, expondremos las ideas principales de algunos ejemplos de protocolos ya existentes, relativos a la *Distribución Cuántica de Claves* (el BB84) y a *comprobación de contraseñas* ([29] y el escenario "llave-candado" [6]).
- Finalmente, en el Capítulo 4 se habrán sentado las bases teóricas y entendido la motivación de la solución que propondremos mediante nuestro particular protocolo de seguridad con estados coherentes. Se tratará de inspirarse en el escenario "llave-candado" propuesto en [6] para comprobar una contraseña de estados coherentes que generaremos aleatoriamente utilizando las ideas de [29], profundizando y ampliando conceptos anteriormente vistos para concluir que es factible y seguro.

Antecedentes históricos

La *Óptica Cuántica* es la rama de la Física que estudia la luz concebida como un sistema cuántico, para lo cual se requiere la Teoría Cuántica de Campos. Esto supone un desafío porque la teoría cuántica de campos se desarrolló con otro fin distinto: estudiar la Física de Partículas. No obstante, comenzando con el trabajo de Roy Glauber en los años 60 y continuando hasta el

presente, el desarollo teórico y experimental de la Óptica Cuántica ha avanzado hasta completar con éxito dicho desafío de adaptar la teoría de la cuantización del campo a la óptica y es, a día de hoy, una de las áreas más activas de investigación en Física.

Esta teoría cuántica de la luz resulta necesaria para solventar varios de los problemas que han surgido desde comienzos del siglo XX con la teoría clásica, como son la explicación de la radiación del cuerpo negro, el efecto fotoeléctrico o el efecto Compton. Asimismo, está muy ligada a la *Teoría de la Información Cuántica* y existe un gran interés en producir estados cuánticos de la luz que permitan crear protocolos de tranmisión de información y de seguridad utilizando estados cuánticos de la luz, objetivo del presente trabajo.

La naturaleza de la luz ha resultado enigmática desde la antigüedad. El intento de explicar la dualidad onda-partícula impulsó el desarrollo de la Física durante el siglo XX y el nacimiento de la Mecánica Cuántica. Al hilo de estos acontecimientos, la teoría cuántica de campos fue desarrollada entre 1920 y 1950 por Dirac, Fock, Pauli, Schwinger, Tomonaga y Feynmann, entre otros. Establecieron que el campo electromagnético se puede descomponer en distintos modos y la dinámica de cada uno de ellos en el vacío es equivalente a la del oscilador armónico cuántico.

Se sentaron así las bases del desarrollo de la Óptica Cuántica, llevado a cabo en torno a los años 60 por Glauber, Sudarshan, Klauber y Mandel [33, 38, 48]. En concreto, Glauber mediante su teoría de la coherencia óptica [33], logró reconciliar en 1963 la contradicción existente entre la concepción de las interferencias como ondas electromagnéticas (Maxwell) y el hecho de que la fotodetección implique la aniquilación de fotones individuales para liberar fotoelectrones de un determinado material (efecto fotoeléctrico). Su contribución consistió en asociar a los estados coherentes, originalmente descritos por Schrödinger en 1926 como un paquete de ondas gaussiano para explicar la evolución del oscilador armónico, el concepto de *coherencia* en Óptica Cuántica, que también estudiaremos más adelante.

Puesto que el campo electromagnético en el vacío se puede considerar como la superposición de muchos modos clásicos, cada uno de ellos gobernados por una ecuación de un oscilador armónico, los estados coherentes se convirtieron en la herramienta para conectar la teoría clásica con la Óptica Cuántica. Es más, se considera que encarnan esta transición porque, además de ser estados de mínima incertidumbre, son autovalores del operador de aniquilación y dicho autovalor (escrito en forma compleja) cumple las ecuaciones de Maxwell. Por tanto, ambas teorías predicen idénticos efectos para estos estados, por lo que se consideran los más clásicos, de ahí que nos interesen especialmente estos en concreto para lograr el objetivo propuesto en este manuscrito. A esto se suma el hecho de que se generan fácilmente utilizando un láser.

La "clasicidad" de los estados coherentes pone de manifiesto un aspecto destacable de la teoría de la luz: el alto grado de acuerdo que existe entre las predicciones clásicas y la teoría cuántica, a pesar de las diferencias fundamentales entre ambas. Por tanto, veremos cómo la teoría cuántica proporciona diferentes descripciones conceptuales de los experimentos, pero, en definitiva, la cuantización del campo electromagnético necesaria para construirla apenas tiene impacto en los fenómenos observables.

En cuanto al creciente avance de la Óptica Cuántica, resulta importante centrar nuestra atención en que está íntimamente relacionado con la Teoría de la Información Cuántica, que está atrayendo un enorme interés en vista a su naturaleza y a sus potenciales aplicaciones revolucionarias en computación y en la seguridad de las comunicaciones. La información se representa, se

almacena, se procesa, se transmite y es leída por sistemas físicos: "la información es física" [40], tal y como resumió Landauer, quien comenzó a preguntarse si las leyes físicas imponían algunas limitaciones al proceso de cómputo al inicio de la década de los 60.

La conexión entre la Óptica Cuántica y la Teoría de la Información Cuántica no es casualidad. La activa investigación en la primera ha permitido un tremendo progreso de las fuentes de radiación coherente y la detección de señales, ahora es posible llevar a cabo experimentos que involucren solamente uno o pocos átomos y fotones al mismo tiempo. Así, se proporciona una forma conveniente de realizar experimentos con los que poder sentar las bases de la implementación práctica de un sistema de procesamiento de la información o de comunicaciones.

Los nuevos conceptos fundamentales en Teoría de la Información Cuántica que han aparecido en los últimos años, gracias a la labor investigadora de Feynmann, Benioff, Deutsch, Jozsa, Bennett, Ekert, Landauer y otros, han motivado el desarrollo de la *Computación Cuántica*. Se basa en que, en lugar de utilizar bits clásicos que solamente pueden reperesentar los valores 0 y 1, la unidad básica es el sistema cuántico de dos niveles conocido como *qubit*, que puede existir en superposición coherente de ambos valores lógicos. Todas las operaciones computacionales se implementan mediante transformaciones unitarias, que actúan simultáneamente sobre todos los estados de una superposición. Asimismo, a partir de dichas transformaciones se construyen puertas lógicas, que deberán ser reversibles.

La utilización de estas superposiciones de sistemas mecánico-cuánticos y la posibilidad de que exista entrelazamiento, proporciona un aumento exponencial de la velocidad de computación en numerosos problemas que no se pueden resolver eficientemente mediante ordenadores clásicos. En 1994, Shor [66] descubrió el algoritmo cuántico que lleva su nombre y que proporciona solución eficiente a un importante problema práctico: la factorización. Como consecuencia, después se han llevado a cabo posibles realizaciones prácticas de computadoras cuánticas [7, 59].

La Teoría de la Información Cuántica está, por tanto, íntimamente relacionada con la Computación Cuántica pero también, como cabe esperar, con las comunicaciones cuánticas y, en consecuencia, con la forma de garantizar que estas sean seguras: la *Criptografía Cuántica*. Se plantea de esta forma el contexto en que se desarrolla el presente trabajo que tiene por objetivo exponer un protocolo de que, basado en la Óptica Cuántica, ofrezca garantías de seguridad. En particular, se fundamentará en las buenas propiedades de los estados coherentes.

La Criptografía tiene una larga historia y está presente ya en las primeras civilizaciones, que buscaban desarrollar técnicas para enviar mensajes durante las campañas militares. No obstante, su estudio como ciencia ha comenzado en los últimos cien años.

En la Antigüedad se utilizaban mensajes cifrados, cuyo problema es que pueden ser fácilmente detectados analizando la frecuencia de aparición de las letras. Esto se trató de mejorar hasta que surgieron los sistemas de criptografía de clave pública cuyo pilar fundamental es la existencia de dos claves, una pública (para cifrar el mensaje) y otra privada (para descifrarlo), la cual solo debe tener el receptor, de forma que se logra la confidencialidad.

Actualmente, el algoritmo de este tipo más usado fue desarrollado en 1979 y es conocido como RSA (Rivest, Shamir y Adleman) [60]. Se basa en utilizar para el encriptado del mensaje una función que es fácil de computar por cualquiera (la multiplicación) pero enormemente difícil de invertir sin poseer la clave privada (la factorización de números enteros). A día de hoy

es seguro, pero el algoritmo cuántico de Shor [66] es capaz de romperlo con facilidad, lo cual supondría un problema si se lograra disponer en el futuro de computadoras cuánticas.

Con respecto a la autenticación de los usuarios, habitualmente se recurre a la utilización de la función *"hash"*, que detallaremos, para encriptar la contraseña que comparten los usuarios. Además, para mayor seguridad se añaden bits aleatorios, conocidos como *sal criptográfica*, a dicha contraseña porque a veces se establece como demasiado trivial (12345, la fecha de cumpleaños...).

Por su parte, la Criptografía Cuántica basa su seguridad en las leyes de la Mecánica Cuántica, en lugar de en problemas de difícil resolución. Es más segura que la clásica porque se basa en que cualquier medida que un espía pueda realizar en el canal de comunicación altera el estado cuántico que encripta el mensaje, tal y como predice *el principio de incertidumbre*. Además, el *Teorema de no clonación* imposibilita el hecho de realizar copias exactas de los estados cuánticos. Por tanto, tiene el potencial de poder resolver algunos problemas clásicos de Criptografía: el intercambio de la clave, lo que se conoce como *Distribución Cuántica de Claves (QKD)* [32], y la autenticación de los usuarios con *protocolos de comprobación de contraseñas*.

Las primeras ideas sobe QKD surgieron en 1970, pero hasta 1984 no se publicó el primer protocolo: el BB84 (Bennet y Brassard) [13] basado en la polarización de los fotones, que permite establecer diferentes bases. Un atacante que mida en una base diferente no podrá extraer información. Respecto a los protocolos de comprobación de contraseñas, tomamos como ejemplo [29], que será en el que nos inspiremos. Su seguridad se basa en las leyes de la Mecánica Cuántica, que también se usan para la generación de bits aleatorios que serían los análogos a la sal criptográfica, aunque en el caso cuántico, las nuevas limitaciones que aparecen hacen que aumente la seguridad.

No obstante, estos protocolos utilizan fotones individuales y la generación y detección de estos es una tarea complicada, lo cual ha motivado que se haya tratado de generalizar estas ideas a otros estados cuánticos de la luz, en particular, los estados coherentes por las razones anteriormente mencionadas.

Capítulo 1

Resultados previos. Óptica Cuántica

La teoría clásica del electromagnetismo da cuenta de un amplio rango de fenómenos que concuerdan con los obtenidos a partir de una teoría cuántica, pero existen otros que no es capaz de describir. De hecho, el concepto de *cuantización* es cierto que ya se incluye en la deducción de la ley de Planck pero, en este caso, los campos $\mathbf{E}$ y $\mathbf{B}$ son tratados como variables clásicas, mientras que los átomos se deben estudiar desde el punto de vista de la Mecánica Cuántica. Por tanto, se requiere una teoría más consistente, con los campos representados por $\hat{\mathbf{E}}$ y $\hat{\mathbf{B}}$, expresiones de los operadores que representan los observables del campo electromagnético.

En este capítulo, analizaremos en líneas generales el procedimiento mediante el cual se aplican las leyes de la Mecánica Cuántica al campo electromagnético y veremos cómo se obtienen dichas expresiones, usando principalmente como referencia [46] (*Capítulo 4* y *Capítulo 5*). En este desarrollo, en esencia, se debe pasar de considerar a los vectores de campo clásicos como tal, a considerarlos operadores cuánticos. Esta transición no es posible hacerla directamente y en ella es de gran importancia el formalismo del *oscilador armónico cuántico*.

En cuanto a las aplicaciones de esta teoría cuántica, destacamos las que tiene en el estudio de la Óptica Cuántica, el área fundamental del presente trabajo. Esto justifica la necesidad de exponer estos resultados teóricos previos, en particular, para poder explicar después los *estados coherentes* de la luz utilizados en el protocolo seguridad propuesto.

Por tanto, para abordarlo, la organización del capítulo es la siguiente:

- Formulación cuántica del oscilador armónico, de la cual deriva todo lo demás.
- Formalización de la *cuantización del campo electromagnético*, que pasa a considerarse la superposición de modos clásicos gobernados por una ecuación de un oscilador armónico clásico.
- Finalmente, se expone la introducción a la Óptica Cuántica de un solo modo, lo que permite simplificar el operador campo eléctrico anteriormente deducido y definir el *grado cuántico de coherencia óptica*, característico de los *estados de un solo modo* (estados de Fock, estados coherentes y estados comprimidos) que describiremos.

1.1. Oscilador armónico cuántico

La clave para llevar a cabo la transición a la teoría cuántica es escribir la clásica de forma que la dependencia de las variables del campo con el oscilador armónico sea apropiada. En esta

sección vamos a mostrar algunos resultados importantes que serán necesarios posteriormente. La justificación de todos ellos se puede consultar en [46] (págs. 133-149).

El hamiltoniano para un oscilador armónico cuántico en una dimensión es:

$$\hat{\mathcal{H}} = \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega^2\hat{q}^2, \tag{1.1.1}$$

donde $\hat{q}$ y $\hat{p}$ son los operadores posición y momento respectivamente, que cumplen la relación de conmutación

$$[\hat{q}, \hat{p}] = i\hbar. \tag{1.1.2}$$

Es conveniente reemplazar $\hat{q}$ y $\hat{p}$ por operadores adimensionales definidos como

$$\hat{a} = (2m\hbar\omega)^{-1/2}(m\omega\hat{q} + i\hat{p}), \tag{1.1.3}$$

y

$$\hat{a}^\dagger = (2m\hbar\omega)^{-1/2}(m\omega\hat{q} - i\hat{p}), \tag{1.1.4}$$

o, de manera inversa:

$$\hat{q} = (\hbar/2m\omega)^{1/2}\left(\hat{a}^\dagger + \hat{a}\right) \tag{1.1.5}$$

$$\hat{p} = i(m\hbar\omega/2)^{1/2}\left(\hat{a}^\dagger - \hat{a}\right). \tag{1.1.6}$$

Los operadores $\hat{a}$ y $\hat{a}^\dagger$ se denominan, respectivamente, operadores *destrucción* (o *aniquilación*) y *creación* del oscilador armónico. Son extremadamente útiles en los cálculos, aunque no sean observables, y tienen propiedades simples como las que se enumeran a continuación.

Sea $|n\rangle$ un estado propio del hamiltoniano $\hat{\mathcal{H}}$ con autovalor E_n (energía correspondiente al nivel n), se tiene que:

$$\left[\hat{a}, \hat{a}^\dagger\right] = \hat{a}\hat{a}^\dagger - \hat{a}^\dagger\hat{a} = 1, \tag{1.1.7}$$

mientras que, su suma, da lugar a una expresión alternativa del hamiltoniano como:

$$\hat{\mathcal{H}} = \frac{1}{2}\hbar\omega\left(\hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}\right) = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right). \tag{1.1.8}$$

Además, los operadores destrucción y creación actúan sobre $|n\rangle$, respectivamente, tal y como se muestra a continuación:

$$\hat{a}\,|n\rangle = n^{1/2}\,|n-1\rangle\,, \quad n = 0, 1, 2, \ldots \tag{1.1.9}$$

$$\hat{a}^\dagger|n\rangle = (n+1)^{1/2}\,|n+1\rangle\,, \quad n = 0, 1, 2, \ldots \tag{1.1.10}$$

Si escribimos las transiciones en una matriz, muchos de sus elementos van a ser nulos, lo que facilita los cálculos:

$$\langle n-1|\hat{a}|n\rangle = n^{1/2} \quad \text{y} \quad \left\langle n+1\left|\hat{a}^\dagger\right|n\right\rangle = (n+1)^{1/2}. \tag{1.1.11}$$

Además, se define el *operador número* $\hat{n}$ como:

$$\hat{n} = \hat{a}^\dagger\hat{a}, \tag{1.1.12}$$

que cumple que:

$$\hat{n}|n\rangle = n|n\rangle. \tag{1.1.13}$$

También, se deduce de (1.1.8) que

$$E_n = \left(n + \frac{1}{2}\right)\hbar\omega, \quad n = 0, 1, 2, \ldots \tag{1.1.14}$$

A veces conviene más utilizar con expresiones adimensionales de los operadores posición y momento. Con este propósito se definen los *operadores de cuadratura* como

$$\hat{X} = (m\omega/2\hbar)^{1/2}\hat{q} = \frac{1}{2}\left(\hat{a}^\dagger + \hat{a}\right), \tag{1.1.15}$$

y

$$\hat{Y} = (2m\hbar\omega)^{-1/2}\hat{p} = \frac{1}{2}i\left(\hat{a}^\dagger - \hat{a}\right), \tag{1.1.16}$$

o, de manera inversa:

$$\hat{a} = \hat{X} + i\hat{Y} \tag{1.1.17}$$

y

$$\hat{a}^\dagger = \hat{X} - i\hat{Y}. \tag{1.1.18}$$

Con lo cual, el hamiltoniano (1.1.8) se puede expresar como

$$\hat{\mathcal{H}} = \hbar\omega\left(\hat{X}^2 + \hat{Y}^2\right), \tag{1.1.19}$$

donde se cumple la relación de conmutación

$$[\hat{X}, \hat{Y}] = i/2. \tag{1.1.20}$$

A partir de aquí, se deduce una expresión del *principio de incertidumbre de Heisenberg* adimensional:

$$(\Delta X)^2(\Delta Y)^2 \geq 1/16. \tag{1.1.21}$$

La demostración de este último resultado se puede consultar en [17].

En los cálculos posteriores, se utilizarán los operadores $\hat{a}$ y $\hat{a}^\dagger$ o el par $\hat{X}$ y $\hat{Y}$ según convenga.

1.2. Cuantización del campo electromagnético

El objetivo de esta sección es ver, en líneas generales a partir del desarrollo de [46] (*Capítulo 4*), cómo se formaliza la cuantización del campo electromagnético a partir de los resultados expuestos sobre el oscilador armónico cuántico, así como dar las expresiones de los operadores campo eléctrico y campo magnético $\hat{\mathbf{E}}$ y $\hat{\mathbf{B}}$, ya que nos serán necesarias con posterioridad en el estudio de los *estados coherentes*.

En primer lugar, se considera una región cúbica del espacio de lado L, sin límites reales, conocida como *cavidad de cuantización*. Esta suposición tiene la ventaja de que se puede considerar que el campo electromagnético se puede excitar solo en modos discretos y, por tanto, los resultados se simplifican. Este concepto, aunque con límites, ya se utilizó en la teoría clásica para deducir la cuantización que induce la ley de Planck. No obstante, ahora en lugar de soluciones de onda estacionarias, se utilizan ondas no estacionarias y sujetas a condiciones frontera periódicas. Además, se parte del potencial vector, en lugar de partir del campo eléctrico.

Cada modo del campo de radiación en la cavidad de cuantización se denota por $\mathbf{k}\lambda$, donde $\mathbf{k}$ es el vector de onda y $\lambda = 1, 2$ indica las dos direcciones posibles de polarización transversal. Por tanto, el campo electromagnético se cuantifica asociando a cada uno de los modos, un oscilador armónico cuántico.

Las componentes del vector de onda $\mathbf{k}$ son, tal y como se deduce de [46] (págs. 4-6):

$$k_x = 2\pi v_x/L, \quad k_y = 2\pi v_y/L, \quad k_z = 2\pi v_z/L, \quad v_x, v_y, v_z = 0, \pm 1, \pm 2, \pm 3 \ldots, \tag{1.2.1}$$

y $e_{\mathbf{k},\lambda}$ son los vectores de polarización, unitarios, perpendiculares entre sí y perpendiculares al vector de onda $\mathbf{k}$.

Así, las relaciones para los operadores de destrucción y creación mostradas en (1.1.9) y (1.1.10) se escriben como

$$\hat{a}_{\mathbf{k}\lambda} |n_{\mathbf{k}\lambda}\rangle = n_{\mathbf{k}\lambda}^{1/2} |n_{\mathbf{k},\lambda} - 1\rangle \tag{1.2.2}$$

y

$$\hat{a}_{\mathbf{k}\lambda}^{\dagger} |n_{\mathbf{k}\lambda}\rangle = (n_{\mathbf{k}\lambda} + 1)^{1/2} |n_{\mathbf{k}\lambda} + 1\rangle . \tag{1.2.3}$$

La interpretación física de estas expresiones es que, estos operadores, destruyen y crean un fotón de energía $\hbar\omega_k$ en el modo $\mathbf{k}\lambda$. Además, $n_{\mathbf{k}\lambda}$ denota el número de fotones excitados en la cavidad en el modo $\mathbf{k}\lambda$ son los estados propios del operador número

$$\hat{n}_{\mathbf{k}\lambda} = \hat{a}_{\mathbf{k}\lambda}^{\dagger} \hat{a}_{\mathbf{k}\lambda}, \tag{1.2.4}$$

con la relación de autovalores

$$\hat{n}_{\mathbf{k}\lambda} |n_{\mathbf{k}\lambda}\rangle = \hat{a}_{\mathbf{k}}^{\dagger} \hat{a}_{\mathbf{k}\lambda} |n_{\mathbf{k}\lambda}\rangle = n_{\mathbf{k}\lambda} |n_{\mathbf{k}\lambda}\rangle \quad n_{\mathbf{k}\lambda} = 0, 1, 2, \ldots, \tag{1.2.5}$$

expresiones similares a (1.1.12) y (1.1.13).

Por su parte, la relación de conmutación análoga a (1.1.7) es:

$$\left[\hat{a}_{\mathbf{k}\lambda}, \hat{a}_{\mathbf{k}'\lambda'}^{\dagger}\right] = \delta_{\mathbf{k},\mathbf{k}'}\delta_{\lambda,\lambda'}. \tag{1.2.6}$$

Con todo, el estado del campo se escribe como producto de los estados de los modos individuales:

$$|n_{\mathbf{k}_1 1}, n_{\mathbf{k}_1 2}, n_{\mathbf{k}_2 1}, n_{\mathbf{k}_2 2}, \ldots\rangle = |n_{\mathbf{k}_1 1}\rangle |n_{\mathbf{k}_1 2}\rangle |n_{\mathbf{k}_2 1}\rangle |n_{\mathbf{k}_2 2}\rangle \ldots = |\{n_{\mathbf{k}\lambda}\}\rangle , \tag{1.2.7}$$

donde $\{n_{\mathbf{k}\lambda}\}$ denota el conjunto completo de números que especifican los niveles de excitación de todos los osciladores armónicos asociados con los modos de la cavidad.

De forma similar a (1.1.8), el hamiltoniano se obtiene sumando las contribuciones de todos estos osciladores armónicos:

$$\hat{\mathcal{H}}_{\mathrm{R}} = \sum_{\mathbf{k}} \sum_{\lambda} \hat{\mathcal{H}}_{\mathbf{k}\lambda}, \tag{1.2.8}$$

donde

$$\hat{\mathcal{H}}_{\mathbf{k}\lambda} = \frac{1}{2}\hbar\omega_k \left(\hat{a}_{\mathbf{k}\lambda}\hat{a}_{\mathbf{k}\lambda}^{\dagger} + \hat{a}_{\mathbf{k}}^{\dagger}\hat{a}_{\mathbf{k}\lambda}\right). \tag{1.2.9}$$

Estamos ya en condiciones de deducir las expresiones de los operadores cuánticos asociados a los campos eléctrico y magnético $\hat{\mathbf{E}}$ y $\hat{\mathbf{B}}$, pero antes, definamos el ángulo de fase para las funciones de onda de cada modo tal y como sigue:

$$\chi_{\mathbf{k}}(\mathbf{r}, t) = \omega_k t - \mathbf{k} \cdot \mathbf{r} - \frac{\pi}{2}. \tag{1.2.10}$$

Por tanto, tal y como se demuestra en [46] (págs. 141 y 142):

$$\hat{\mathbf{E}}(\mathbf{r},t) = \hat{\mathbf{E}}^{+}(\mathbf{r},t) + \hat{\mathbf{E}}^{-}(\mathbf{r},t), \tag{1.2.11}$$

donde

$$\hat{\mathbf{E}}^{+}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda} \mathrm{e}_{\mathbf{k}\lambda} \left(\hbar\omega_k / 2\varepsilon_0 V\right)^{1/2} \hat{a}_{\mathbf{k}\lambda} \exp\left[-i\chi_{\mathbf{k}}(\mathbf{r},t)\right], \tag{1.2.12}$$

y

$$\hat{\mathbf{E}}^{-}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda} e_{\mathbf{k}\lambda} \left(\hbar\omega_k / 2\varepsilon_0 V\right)^{1/2} \hat{a}^{\dagger}_{\mathbf{k}\lambda} \exp\left[i\chi_{\mathbf{k}}(\mathbf{r},t)\right], \quad V = L^3, \tag{1.2.13}$$

donde ε_0 es la permitividad del vacío. $\hat{\mathbf{E}}^{+}$ y $\hat{\mathbf{E}}^{-}$ se denominan las *partes de frecuencia positiva y negativa del campo eléctrico*, respectivamente.

Igualmente:

$$\hat{\mathbf{B}}(\mathbf{r},t) = \hat{\mathbf{B}}^{+}(\mathbf{r},t) + \hat{\mathbf{B}}^{-}(\mathbf{r},t), \tag{1.2.14}$$

donde

$$\hat{\mathbf{B}}^{+}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda} \mathbf{k} \times \mathbf{e}_{\mathbf{k}\lambda} \left(\hbar / 2\varepsilon_0 \omega_k V\right)^{1/2} \hat{a}_{\mathbf{k}\lambda} \exp\left[-i\chi_{\mathbf{k}}(\mathbf{r},t)\right], \tag{1.2.15}$$

y

$$\hat{\mathbf{B}}^{-}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda} \mathbf{k} \times \mathbf{e}_{\mathbf{k}\lambda} \left(\hbar / 2\varepsilon_0 \omega_k V\right)^{1/2} \hat{a}^{\dagger}_{\mathbf{k}\lambda} \exp\left[i\chi_{\mathbf{k}}(\mathbf{r},t)\right], \quad V = L^3. \tag{1.2.16}$$

Tanto $\hat{\mathbf{E}}$ como $\hat{\mathbf{B}}$ son hermíticos, por lo que representan los observables del campo electromagnético en la cavidad.

Finalmente, utilizando los operadores de cuadratura definidos en (1.1.15) y (1.1.16), se puede generalizar la relación de conmutación (1.1.20) a

$$\left[\hat{X}_{\mathbf{k}\lambda}, \hat{Y}_{\mathbf{k}'\lambda'}\right] = (i/2)\delta_{\mathbf{k},\mathbf{k}'}\delta_{\lambda,\lambda'}, \tag{1.2.17}$$

así como dar una expresión alternativa de (1.2.11) que nos será de utilidad:

$$\hat{\mathbf{E}}_{\mathrm{T}}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda} e_{\mathbf{k}\lambda} \left(2\hbar\omega_k / \varepsilon_0 V\right)^{1/2} \left\{ \hat{X}_{\mathbf{k}\lambda} \cos\left[\chi_{\mathbf{k}}(\mathbf{r},t)\right] + \hat{Y}_{\mathbf{k}\lambda} \sin\left[\chi_{\mathbf{k}}(\mathbf{r},t)\right] \right\}. \tag{1.2.18}$$

Vemos que los operadores $\hat{X}_{\mathbf{k}\lambda}$ y $\hat{Y}_{\mathbf{k}\lambda}$ están asociados con las cuadraturas del seno y el coseno del ángulo de fase correspondiente, tal y como es de esperar por su nomenclatura.

1.3. Óptica cuántica de un solo modo

En general, los haces de luz se consideran como un solo modo excitado del campo. En esta sección, adaptaremos la teoría expuesta anteriormente a dicho caso, además de explicar el concepto de *coherencia óptica*, tanto desde el punto de vista clásico como desde el cuántico introducido por Glauber.

Se dispone de tres bases diferentes para representar los estados cuánticos de un solo modo de la radiación electromagnética: los *estados numéricos o de Fock* $|n\rangle$, los *estados coherentes* $|\alpha\rangle$ y los *estados comprimidos*, que consisten en introducir más parámetros y dejaremos fuera de nuestro estudio. Cabe destacar que solo los estados coherentes podrían ser descritos mediante la

teoría de Maxwell. En función del problema de Óptica Cuántica al que nos estemos enfrentando, podemos hacer uso de cualquiera de las tres bases; en nuestro caso, vamos a emplear la de los estados coherentes, desarrollada en la siguiente sección.

Además, cabe destacar que la "clasicidad", referida al posible estudio mediante las ecuaciones de Maxwell de los estados, no es invariante bajo superposiciones lineales. Por ejemplo, veremos que los estados coherentes (los más parecidos a los estados clásicos) son superposición lineal de los estados no clásicos de Fock.

En lo que sigue emplearemos como referencias, principalmente, [46] (*Capítulo 5*) y [61].

1.3.1. Simplificación del operador de campo eléctrico

Veamos, en primer lugar, los operadores que describen el campo de un solo modo. En este caso, se supone que la dirección de propagación es el eje z y omitimos los subíndices que indican el modo $\mathbf{k}\lambda$ seleccionado, ya que solamente se trabaja con ese concreto. Se pueden simplificar (1.2.11)-(1.2.13) a:

$$\hat{E}(\chi) = \hat{E}^{+}(\chi) + \hat{E}^{-}(\chi) = (\hbar\omega/2\varepsilon_0 V)^{1/2} \left\{ \hat{a}\mathrm{e}^{-\mathrm{i}\chi} + \hat{a}^{\dagger}\mathrm{e}^{\mathrm{i}\chi} \right\}. \tag{1.3.1}$$

La dependencia en z y t se engloba en el término del ángulo de fase χ cuya expresión (1.2.10) se simplifica tal que así:

$$\chi = \omega t - kz - \frac{\pi}{2}, \tag{1.3.2}$$

donde $k = \omega/c$ en el vacío. No obstante, conviene simplificar aún más (1.3.1). Con el convenio de que el campo eléctrico se mide en unidades de $2\left(\hbar\omega/2\varepsilon_0 V\right)^{1/2}$, se tiene que:

$$\hat{E}(\chi) = \hat{E}^{+}(x) + \hat{E}^{-}(\chi) = \frac{1}{2}\hat{a}\mathrm{e}^{-\mathrm{i}\chi} + \frac{1}{2}\hat{a}^{\dagger}\mathrm{e}^{\mathrm{i}\chi} = \hat{X}\cos\chi + \hat{Y}\sin\chi, \tag{1.3.3}$$

donde los operadores de cuadratura para el modo seleccionado $\mathbf{k}\lambda$ se definen como en (1.1.15) y (1.1.16).

A partir de las relaciones de conmutación (1.1.7) y (1.1.20) se tiene que:

$$\left[\hat{E}\left(\chi_1\right), \hat{E}\left(\chi_2\right)\right] = -\frac{i}{2}\sin\left(\chi_1 - \chi_2\right). \tag{1.3.4}$$

Se puede demostrar, tal y como se hace en [14], que se cumple la siguiente relación de incertidumbre:

$$\Delta E\left(\chi_1\right)\Delta E\left(\chi_2\right) \geq \frac{1}{4}\left|\sin\left(\chi_1 - \chi_2\right)\right|. \tag{1.3.5}$$

Es importante destacar que esta incertidumbre es independiente de la medida del ángulo de fase χ tanto para el vacío como para los estados de Fock o los estados coherentes de un solo modo. En estos casos, (1.3.5) se satisface con el máximo valor en el lado derecho:

$$\left(\Delta E\left(\chi\right)\right)^2 \geq \frac{1}{4}. \tag{1.3.6}$$

1.3.2. Grado cuántico de coherencia óptica

La coherencia óptica se refiere a la correlación entre las fluctuaciones en distintos puntos del espacio-tiempo para un determinado campo electromagnético. Estos fenómenos se describen en términos estadísticos por necesidad, e incluyen como el caso más simple el de las interferencias. Hasta la primera mitad del siglo pasado, la clasificación de la coherencia se basaba en la intensidad promedio de las superposiciones del campo, en función de la visibilidad de las franjas de interferencia: los campos que no producían franjas de interferencia se llamaban incoherentes y, por otro lado, el máximo orden de coherencia se asignaba a los que lo hacían con máxima visibilidad.

El experimento de Young introdujo estos conceptos y, posteriormente, el de Brown y Twiss (1955) abrió la puerta a la inclusión de la cuantización del campo. En ese momento, convivían dos fenómenos contradictorios: por un lado, la interferencia se concebía como algo propiamente natural de las ondas electromagnéticas (teoría de Maxwell) y, por otro, el efecto fotoeléctrico de Einstein implicaba la aniquilación de fotones individuales para liberar fotoelectrones de un determinado material.

Glauber, en 1963, reconcilió ambos fenómenos al considerar la coherencia óptica desde un punto de vista cuántico y definiendo el *grado cuántico de coherencia de primer y segundo orden*. En líneas generales, demostró que para que un estado cuántico sea coherente, debe ser un autovector del operador de aniquilación con un autovalor complejo (tal y como veremos en la siguiente sección). Es interesante destacar que este autovalor es una solución de las correspondientes ecuaciones de Maxwell. Pasemos, por tanto, a la descripción matemática de la coherencia desde el punto de vista cuántico.

La *señal coherente* $\mathcal{S}$ que transporta un haz de luz se define como el valor esperado del operador de campo eléctrico definido en (1.3.3):

$$\mathcal{S} = \langle E(\chi) \rangle. \tag{1.3.7}$$

Es claro a partir esto, de la definición del operador de campo y de los elementos de matriz de los operadores destrucción y creación (1.1.11), que las señales coherentes que no se desvanecen ocurren solamente para estados que son superposición de estados de Fock con valor de n que difieren en una unidad.

Además, la relación de incertidumbre (1.3.5) crea un *ruido* $\mathcal{N}$ que debe relacionarse con la coherencia y que se define como:

$$\mathcal{N} = (\Delta E(\chi))^2, \tag{1.3.8}$$

y la *relación señal a ruido* es:

$$\text{SNR} = \frac{\mathcal{S}^2}{\mathcal{N}} = \frac{\langle E(\chi) \rangle^2}{(\Delta E(\chi))^2}. \tag{1.3.9}$$

Por su parte, el *grado cuántico de coherencia de primer y segundo orden* se definen en [46] (sección 4.12, págs. 176-178). Nos centraremos en su simplificación para el caso que nos ocupa de haces de luz de un solo modo:

$$g^{(1)}(z_1, t_1; z_2, t_2) = g^{(1)}(\tau) = g^{(1)}(\chi_1; \chi_2) = \exp\{i(\chi_1 - \chi_2)\}, \tag{1.3.10}$$

y

$$g^{(2)}(\tau) = g^{(2)}(\chi_1; \chi_2) = \left\langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \right\rangle / \left\langle \hat{a}^\dagger \hat{a} \right\rangle^2, \tag{1.3.11}$$

donde $\tau = \chi_2 - \chi_1$. Nótese que la expresión (1.3.11) es independiente de la posición y el tiempo pero, al contrario que lo que ocurre con (1.3.10), depende de la naturaleza del haz de luz. De hecho, a partir de las propiedades de los operadores de destrucción y creación (1.1.7) y (1.1.12), el segundo orden de coherencia se puede expresar en función del número medio de fotones como:

$$g^{(2)}(\tau) = \frac{\langle \hat{n}(\hat{n}-1)\rangle}{\langle \hat{n}\rangle^2} = \frac{\langle \hat{n}^2\rangle - \langle \hat{n}\rangle}{\langle \hat{n}\rangle^2} = 1 + \frac{(\Delta n)^2 - \langle \hat{n}\rangle}{\langle \hat{n}\rangle^2}. \tag{1.3.12}$$

Puesto que $|g^{(1)}(\tau)| = 1$, deducimos que todos los haces de luz de un solo modo son coherentes de primer orden. Se dirá que son coherentes de segundo orden si también se cumple que $g^{(2)}(\tau) = 1$.

1.3.3. Estados cuánticos de un solo modo

Tras esta descripción teórica, estamos ya en condiciones de proceder al estudio de los estados coherentes de la luz $|\alpha\rangle$, objeto de este trabajo y para lo cual dedicaremos la próxima sección. No obstante, antes cabe mencionar que existen otros dos tipos de estados cuánticos de un solo modo: los *estados numéricos o de Fock* $|n\rangle$ y los *estados comprimidos*. Los tres, como se comentó anteriormente, forman tres bases; dejaremos fuera de nuestro estudio los últimos porque no nos son de utilidad para lograr el objetivo propuesto. Por tanto, pretendemos con esta sección dar solamente una descripción, en líneas generales, de los estados numéricos, pues serán necesarios para estudiar los estados coherentes posteriormente.

Los estados de Fock tienen un número de fotones bien definido, pero son difíciles de generar y estudiar experimentalmente. Sin embargo, son el punto de partida natural para el tratamiento de la luz de un solo modo y los necesitaremos para analizar los estados coherentes, ya que son superposiciones lineales de estos. Varias propiedades se han enunciado ya en la Sección 1.1. Enunciemos algunas más con el fin de poder después compararlas con las de los estados coherentes.

El grado cuántico de coherencia de segundo orden es:

$$g^{(2)}(\tau) = 1 - \frac{1}{n} \text{ para } n \geq 1. \tag{1.3.13}$$

En cuanto a la incertidumbre posición-momento, que se enunció en (1.1.21), tenemos en este caso que

$$(\Delta X)^2 = (\Delta Y)^2 = \frac{1}{2}\left(n + \frac{1}{2}\right). \tag{1.3.14}$$

Por tanto, solo el vacío $|0\rangle$ presenta mínima incertidumbre. Es más, mientras que la incertidumbre en el número de fotones es nula, la fase de estos estados es completamente aleatoria.

La señal coherente, por su parte, se desvanece, $\mathcal{S} = 0$ y el ruido vale $\mathcal{N} = \frac{1}{2}\left(n + \frac{1}{2}\right)$.

Respecto a su tratamiento clásico, los estados $|n \geq 1\rangle$ no son autovectores del operador aniquilación, por lo que no son clásicos en el sentido de no ser coherentes y no poder estudiarse mediante las ecuaciones de Maxwell.

Capítulo 2

Fundamento teórico. Estados coherentes y su discriminación

Estamos ya en condiciones de pasar a exponer la teoría en que se fundamentará el protocolo de seguridad cuántica propuesto en el presente trabajo. Puesto que para la comunicación se aprovechan las propiedades de los estados coherentes de la luz y, para compararlos, divisores de haz, explicaremos en detalle ambos conceptos.

Además, con el fin de aportar garantías de seguridad, se deben tener en cuenta cómo se realizan medidas bajo las leyes de la Mecánica Cuántica y cómo se puede discriminar sin ambigüedad entre varios estados. Asimismo, es importante conocer algunos resultados relativos a la Teoría de la Información Cuántica, como la *cota de Holevo* o la *entropía de Von Neumann*.

Todo ello permitirá establecer el contexto en que se desarrolla la Criptografía Cuántica y, en particular, nuestro escenario de comunicación.

Para lograrlo, la organización del capítulo es la siguiente:

- Descripción detallada de los *estados coherentes*, apoyándonos en los resultados previos. Se comprenderán así las buenas propiedades que poseen y que motivan su elección para el protocolo de seguridad con estados cuánticos de la luz que propondremos.

- Interpretación mecánico-cuántica de los *divisores de haz* como mecanismo para la comparación posterior de los estados coherentes que compongan la contraseña privada en el protocolo.

- Desarrollo teórico de aspectos relativos a la medida cuántica, como son algunos de los tipos que hay y el problema de *discriminación* entre estados cuánticos *sin ambigüedad*, cuya resolución se particularizará a estados coherentes.

- Por último, se introduce la Teoría de la Información Cuántica, íntimamente relacionada con la Óptica Cuántica y que deriva de la teoría anteriormente descrita. Se detallarán algunos aspectos fundamentales como el *qubit*, el *Teorema de no clonación*, la cuantificación de la *información almacenada y accesible* en los estados cuánticos, así como algunas tecnologías de *generación y detección de fotones*.

2.1. Estados coherentes de la luz

Tal y como se acaba de mencionar en el capítulo anterior, ni los estados de Fock ni los estados comprimidos pueden ser tratados mediante las ecuaciones de Maxwell, por lo que se consideran alejados en similitud a los estados clásicos. Esta es la principal diferencia con los estados coherentes (también conocidos como *estados de Glauber*) y en lo que radica su importancia, lo cual motiva esta sección aparte.

En definitiva, los estados coherentes de la luz gozan de especial utilidad porque se pueden tratar como si fueran clásicos, lo cual supone una gran simplificación tanto a nivel teórico como práctico. Además, son fáciles de generar experimentalmente, ya que se producen mediante un *láser*. Por tanto, serán los que utilicemos en nuestro particular protocolo de seguridad cuántico.

Expongamos a continuación de manera detallada algunos resultados relativos a sus propiedades, los cuales se entenderán fácilmente gracias a introducción teórica previa. Se utilizará, principalmente, como referencia [46] (*Capítulo 5*), además de [61].

Los estados coherentes son superposiciones lineales de estados de Fock y se definen como

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{(n!)^{1/2}}|n\rangle. \tag{2.1.1}$$

En esta expresión α es un número complejo, luego se puede expresar como: $\alpha = |\alpha|e^{i\theta}$, donde $|\alpha|$ y θ son la amplitud y la fase del estado $|\alpha\rangle$.

Es obvio que el estado $|\alpha\rangle$ está normalizado, ya que

$$\langle\alpha \mid \alpha\rangle = \exp\left(-|\alpha|^2\right)\sum_{n}\frac{{\alpha^*}^n\alpha^n}{n!} = 1. \tag{2.1.2}$$

Además, los estados coherentes no son ortogonales entre sí:

$$\langle\alpha \mid \beta\rangle = \exp\left(-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2\right)\sum_{n}\frac{{\alpha^*}^n\beta^n}{n!} = \exp\left(-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2 + \alpha^*\beta\right). \tag{2.1.3}$$

Con lo cual, el módulo del producto escalar de dos estados coherentes diferentes se puede escribir

$$|\langle\alpha \mid \beta\rangle|^2 = \exp\left(-|\alpha-\beta|^2\right). \tag{2.1.4}$$

Los $|\alpha\rangle$ forman un conjunto sobre-completo de estados para el oscilador armónico, y de ahí su falta de ortogonalidad. Sin embargo, respecto a esto podemos notar a partir de (2.1.4) que los estados se aproximan a la ortogonalidad si $|\alpha-\beta| \gg 1$.

Observemos ahora que estados coherentes $|\alpha\rangle$ son también autovectores del operador destrucción con autovalores α, en concordancia con la definición de coherencia introducida por Glauber:

$$\hat{a}|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n}\frac{\alpha^n}{(n!)^{1/2}}n^{1/2}|n-1\rangle = \alpha|\alpha\rangle. \tag{2.1.5}$$

En consecuencia, es evidente que el operador de creación satisface la relación:

$$\langle\alpha|\hat{a}^\dagger = \langle\alpha|\alpha^*. \tag{2.1.6}$$

Además, se puede demostrar (ver [46], sección 5.3, pág. 191) que se puede reescribir la definición (2.1.1) como

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_n \frac{\left(\alpha\hat{a}^\dagger\right)^n}{n!}|0\rangle = \exp\left(\alpha\hat{a}^\dagger - \frac{1}{2}|\alpha|^2\right)|0\rangle, \tag{2.1.7}$$

lo cual se suele expresar de manera más compacta:

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle, \tag{2.1.8}$$

donde $\hat{D}(\alpha)$ es el *operador desplazamiento* que se define como:

$$\hat{D}(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right). \tag{2.1.9}$$

Este operador satisface la condición de operador unitario, pues:

$$\hat{D}^\dagger(\alpha)\hat{D}(\alpha) = \hat{D}(\alpha)\hat{D}^\dagger(\alpha) = \mathbb{I}. \tag{2.1.10}$$

Gracias a las relaciones (2.1.5) y (2.1.6) se puede obtener fácilmente el valor esperado del operador $\hat{n}$ (1.1.12), que está relacionado con el módulo de la amplitud de los estados coherentes:

$$\langle\hat{n}\rangle = \langle\alpha|\hat{n}|\alpha\rangle = \left\langle \alpha \left| \hat{a}^\dagger\hat{a} \right| \alpha \right\rangle = |\alpha|^2. \tag{2.1.11}$$

Esto quiere decir que un estado coherente $|\alpha\rangle$ tiene un número promedio de fotones igual a $|\alpha|^2$.

Además, también se puede demostrar (ver en [46], sección 5.3, págs. 192-193) que la varianza en el número de fotones es

$$(\Delta n)^2 = |\alpha|^2 = \langle\hat{n}\rangle. \tag{2.1.12}$$

Por tanto, a partir de (2.1.11) y (2.1.12) se tiene que la incertidumbre en el número de fotones de un estado coherente es

$$\frac{\Delta n}{\langle\hat{n}\rangle} = \frac{1}{|\alpha|} = \frac{1}{\sqrt{\langle\hat{n}\rangle}}, \tag{2.1.13}$$

que es inversamente proporcional al valor de la amplitud del estado coherente $|\alpha|$.

Otro aspecto importante es que se puede calcular fácilmente la probabilidad de encontrar n fotones a partir de la definición (2.1.1), obteniéndose una distribución de Poisson:

$$P(n) = |\langle n \mid \alpha\rangle|^2 = \exp\left(-|\alpha|^2\right)\frac{|\alpha|^{2n}}{n!} = \mathrm{e}^{-\langle\hat{n}\rangle}\frac{\langle\hat{n}\rangle^n}{n!}. \tag{2.1.14}$$

Recordemos que la distribución de Poisson se aproxima a una gaussiana para valores suficientemente altos del número medio de fotones $\langle\hat{n}\rangle$.

En cuanto al grado cuántico de coherencia, los estados coherentes además de serlo de primer orden, también lo son de segundo orden: tal y como se deduce a partir de (1.3.12), $g^{(2)}(\tau) = 1$, lo cual explica que se denominen estados coherentes.

Por otro lado, los valores esperados de los operadores de cuadratura definidos en (1.1.15) y (1.1.16) se pueden calcular utilizando las propiedades (2.1.5) y (2.1.6)

$$\langle\alpha|\hat{X}|\alpha\rangle = \frac{1}{2}\left\langle \alpha \left| \hat{a}^\dagger + \hat{a} \right| \alpha \right\rangle = \frac{1}{2}\left(\alpha^* + \alpha\right) = \mathrm{Re}\,\alpha = |\alpha|\cos\theta, \tag{2.1.15}$$

y

$$\langle\alpha|\hat{Y}|\alpha\rangle = \mathrm{Im}\,\alpha = |\alpha|\sin\theta. \tag{2.1.16}$$

Además, un simple cálculo demuestra que

$$\hat{X}^2 = \frac{1}{4}\left(\hat{a}^\dagger\hat{a}^\dagger + 2\hat{a}^\dagger\hat{a} + \hat{a}\hat{a} + 1\right), \tag{2.1.17}$$

y

$$\hat{Y}^2 = \frac{1}{4}\left(-\hat{a}^\dagger\hat{a}^\dagger + 2\hat{a}^\dagger\hat{a} - \hat{a}\hat{a} + 1\right). \tag{2.1.18}$$

Con lo cual, se deduce que las varianzas de la cuadraturas cumplen

$$(\Delta X)^2 = (\Delta Y)^2 = \frac{1}{4}. \tag{2.1.19}$$

En consecuencia, en contraste con la relación análoga (1.3.14) que presentan los estados de Fock, tenemos que los estados coherentes presentan la mínima incertidumbre permitida por el principio de incertidumbre de Heisenberg (1.1.21) en las cuadraturas para cualquiera número medio de fotones $|\alpha|^2$.

Todo esto se puede observar claramente en la representación en el espacio de fases que se muestra en la Figura 2.1. El espacio de fases en Mecánica Cuántica no permite localizar con

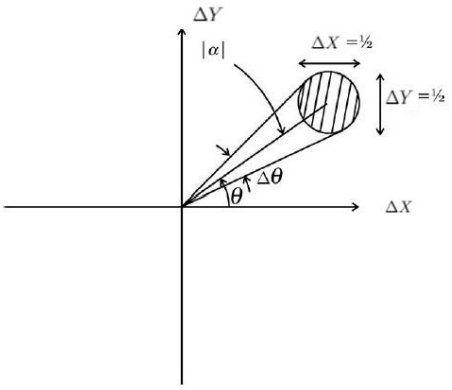


Figura 2.1: Representación en el espacio de fases de un estado coherente de amplitud $|\alpha|$ y fase θ. Fuente: [30] (*Capítulo 3*, pág. 57).

precisión el estado de un sistema determinado, tal y como sí que ocurre en la Mecánica Clásica, puesto que las cuadraturas definidas en (1.1.15) y (1.1.16) no conmutan, lo cual se vio en (1.1.20).

No obstante, se puede apreciar en la Figura 2.1 que los operadores de cuadratura de los estados coherentes presentan la misma incertidumbre que, además, es mínima. Esta incertidumbre se representa mediante un círculo. Nótese que dicho círculo es el mismo para todos los estados coherentes. Además, a medida que aumenta $|\alpha|$, decrece la incertidumbre en la fase $\Delta\theta$, tal y como se esperaría en el límite clásico. Por su parte, el vacío, que tiene amplitud nula, presenta la incertidumbre en la fase más alta posible, $\Delta\theta = 2\pi$, por lo que se representa mediante un círculo de radio 1/4 centrado en el origen.

Además, se deduce de la geometría del diagrama, que si se cumple que $|\alpha| \gg 1$:

$$\Delta\theta = \frac{1}{2|\alpha|} = \frac{1}{2\langle\hat{n}\rangle^{1/2}}. \tag{2.1.20}$$

Así, a partir de las expresiones (2.1.13) y (2.1.20) se tiene que

$$\Delta n \Delta\theta = \frac{1}{2}, \tag{2.1.21}$$

y se pone en evidencia que la incertidumbre en el número medio de fotones (2.1.13) y en la fase (2.1.20) varían como $1/|\alpha|$; es decir, cuanto mayor sea el número medio de fotones (o, equivalentemente, la amplitud), mejor definida estará la onda electromagnética asociada al estado coherente, tanto en amplitud como en fase.

Por otra parte, en cuanto a la señal coherente y al ruido, definidos en (1.3.7) y (1.3.8), respectivamente, se tiene que

$$S = \langle\alpha|\hat{E}(\chi)|\alpha\rangle = |\alpha|\cos(\chi - \theta), \tag{2.1.22}$$

y

$$\mathcal{N} = (\Delta E(\chi))^2 = \frac{1}{4}, \tag{2.1.23}$$

donde hemos usado (1.3.3) para $\hat{E}(\chi)$. El ruido es, por tanto, independiente de la fase y tiene el valor mínimo permitido por (1.3.6).

La relación señal a ruido vale según (1.3.9)

$$\mathrm{SNR} = 4|\alpha|^2\cos^2(\chi - \theta) = 4\langle n\rangle\cos^2(\chi - \theta), \tag{2.1.24}$$

cuyo valor máximo se alcanza para $\chi = \theta$.

En conclusión, los estados coherentes de la luz describen el máximo grado de coherencia y un comportamiento similar al clásico. Además, presentan mínima incertidumbre y se generan fácilmente mediante un láser.

2.2. Interpretación mecánico-cuántica de los divisores de haz

El divisor de haz es un componente muy importante en la mayoría de los experimentos sobre la naturaleza cuántica de la luz. Nos interesa saber cómo funciona desde el punto de vista de la Física Cuántica, ya que lo emplearemos en la comparación de estados coherentes para garantizar la seguridad en la comunicación. La principal ventaja es que, a pesar de que generalmente los divisores de haz se utilizan para producir entrelazamiento, cuando la entrada son estados coherentes a la salida se siguen teniendo estados coherentes, y la relación entre sus amplitudes concuerda con la clásica. Veámoslo, siguiendo el desarrollo de [30] (*Capítulo 6*).

En primer lugar, sabemos que un divisor de haz clásico produce que un campo clásico de amplitud $\mathcal{E}_1$ se divida en dos campos de amplitudes $\mathcal{E}_2$ y $\mathcal{E}_3$. Podríamos pensar que para considerarlo cuánticamente bastaría sustituir los valores de estas amplitudes por operadores de aniquilación. Sin embargo, se puede demostrar que esto no funciona (ver [30], págs. 137 y 138). Resolvamos este problema a continuación.

Existen dos direcciones de entrada a las cuales llamamos puertos, que se corresponden a modos ortogonales (separados en el espacio) y que denotamos con los subíndices 0 y 1; análogamente, existen dos direcciones de salida, que también denominamos puertos y denotamos con los subíndices 2 y 3. Uno de los puertos de entrada no se utiliza por lo que, estando su entrada vacía, clásicamente no tiene efecto en la salida. Sin embargo, desde el punto de vista cuántico, este puerto contiene un modo cuantizado del campo. Aunque este sea el vacío, las fluctuaciones en el vacío conllevan importantes efectos físicos. Entonces, el esquema del divisor de haz es tal y como se muestra en la Figura 2.2. En ella se representan todas las entradas del divisor de haz

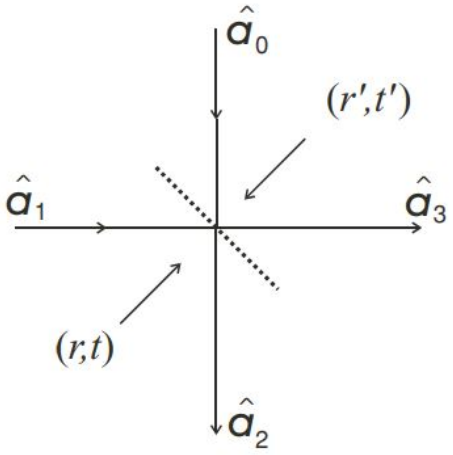


Figura 2.2: Interpretación mecánico-cuántica del divisor de haz. Fuente: [30] (*Cap. 6*, pág. 138).

cuando se tienen en cuenta las leyes de la Física Cuántica, siendo $\hat{a}_0$ el operador de destrucción de campo que representa la entrada vacante en la descripción clásica. Por su parte, $\hat{a}_1$ hace referencia al otro puerto de entrada y, tanto $\hat{a}_2$ como $\hat{a}_3$ a los dos de salida. Además, hay dos posibilidades de elección de los coeficientes de transmisión y reflexión, permitiendo la posibilidad de tener un divisor de haz asimétrico.

Por tanto, las transformaciones que el divisor de haz lleva a cabo para los operadores de campo son

$$\hat{a}_2 = r\hat{a}_1 + t'\hat{a}_0, \quad \hat{a}_3 = t\hat{a}_1 + r'\hat{a}_0, \tag{2.2.1}$$

o, en forma matricial

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} t' & r \\ r' & t \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}, \tag{2.2.2}$$

siendo la matriz de los coeficientes de de reflexión y transmisión ortogonal. Con lo cual, se trata de una transformación unitaria.

Los operadores de destrucción asociados a los campos de entrada y salida deben satisfacer las relaciones de conmutación canónicas:

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{ij}, \quad [\hat{a}_i, \hat{a}_j] = 0 = \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger\right] \quad (i,j = 0,1,2,3). \tag{2.2.3}$$

Por tanto, se debe cumplir que:

$$\left|r'\right| = |r|, \quad |t| = \left|t'\right|, \quad |r|^2 + |t|^2 = 1, \quad r^*t' + r't^* = 0, \quad \text{y} \quad r^*t + r't'^* = 0. \tag{2.2.4}$$

Es obvio que para que sea un divisor de haz 50 : 50 (es decir, que refleja y transmite en la misma proporción) debe ocurrir que

$$|r| = |t| = |r'| = |t'| = \frac{1}{\sqrt{2}}. \tag{2.2.5}$$

Veamos qué salida se obtiene cuando inciden dos estados coherentes $|\alpha\rangle$ y $|\beta\rangle$ en un divisor de haz. Para ello, utilizaremos la relación (2.1.8), la relación inversa conjugada de (2.2.2) y el hecho de que el divisor de haz (en inglés *beam splitter*) lleva a cabo la transformación $|0\rangle_0 |0\rangle_1 \xrightarrow{BS} |0\rangle_2 |0\rangle_3$:

$$\begin{aligned}
|\alpha\rangle_0 |\beta\rangle_1 &= \hat{D}_0(\alpha)\hat{D}_1(\beta) |0\rangle_0 |0\rangle_1 = \exp\Big\{\alpha\hat{a}_0^\dagger - \alpha^*\hat{a}_0\Big\} \exp\Big\{\beta\hat{b}_1^\dagger - \beta^*\hat{b}_1\Big\} |0\rangle_0 |0\rangle_1 \\
&\xrightarrow{BS} \exp\Big\{\alpha(t'\hat{a}_2^\dagger + r'\hat{b}_3^\dagger) - \alpha^*(t'^*\hat{a}_2 + r'^*\hat{b}_3)\Big\} \exp\Big\{\beta(r\hat{a}_2^\dagger + t\hat{b}_3^\dagger) - \beta^*(r^*\hat{a}_2 + t^*\hat{b}_3)\Big\} |0\rangle_2 |0\rangle_3 \\
&= \exp\Big\{(t'\alpha + \beta r)\hat{a}_2^\dagger - (t'^*\alpha^* + r^*\beta^*)\hat{a}_2\Big\} \exp\Big\{(\beta t + \alpha r')\hat{b}_3^\dagger - (\beta^* t^* + \alpha^* r'^*)\hat{b}_3\Big\} |0\rangle_2 |0\rangle_3 \\
&= |t'\alpha + r\beta\rangle_2 |t\beta + r'\alpha\rangle_3 .
\end{aligned} \tag{2.2.6}$$

Con lo cual, a la salida se obtienen estados coherentes cuyas amplitudes son las que se esperarían en Óptica Clásica y, además, no se produce entrelazamiento.

2.3. Teoría de la medida cuántica

Se expondrán a continuación algunos resultados relativos a la teoría cuántica de la medida, una operación fundamental a llevar a cabo en la comunicación cuántica. Nos apoyaremos en estos resultados para garantizar posteriormente la seguridad de nuestro protocolo de seguridad. Como referencia se utilizará principalmente [55] (*Capítulo 2*).

En particular, repasaremos el concepto de *medida cuántica*, así como algunos resultados relacionados, y veremos otros dos tipos de medida que se pueden deducir a partir de él: *medidas proyectivas o de von Neumann* y *medidas POVM*. Ambas resultarán imprescindibles posteriormente a la hora de estudiar las *medidas de discriminación sin ambigüedad* (Sección 2.4), así como la información accesible de un estado cuántico (Sección 2.5.3).

Trabajaremos en un espacio complejo de Hilbert $\mathcal{H}$ conocido como *espacio de estados* y que se asocia a cada sistema físico aislado. Como sabemos, el estado de este sistema se describe completamente mediante un vector $|\psi\rangle \in \mathcal{H}$. En estas condiciones, las *medidas cuánticas* se describen mediante una colección de operadores de medida $\{M_n\}_n$. El índice n hace referencia al posible resultado de la medida en el experimento. Si el estado del sistema cuántico es $|\psi\rangle$ inmediatamente antes de la medida, entonces la probabilidad de que ocurra el resultado n viene dada por

$$\mathcal{P}(n) = \left\langle \psi \left| M_n^\dagger M_n \right| \psi \right\rangle, \tag{2.3.1}$$

y el estado del sistema después de la medida es

$$\frac{M_n|\psi\rangle}{\sqrt{\mathcal{P}(n)}}. \tag{2.3.2}$$

Los operadores de medida satisfacen

$$\sum_n M_n^\dagger M_n = \mathbb{I}, \tag{2.3.3}$$

condición necesaria para que las probabilidades sumen 1. Como vemos a partir de (2.3.2), en Mecánica Cuántica el proceso de medida altera de forma incontrolada la evolución del sistema. Esto supone una gran diferencia con la Física Clásica y una de las bases en que se fundamente la Criptografía Cuántica.

Acabamos de definir la *medida cuántica en general*; un caso especial es el de las *medidas proyectivas o de von Neumann*, en las cuales las medidas son proyecciones ortogonales y verifican

$$M_n M_m = \delta_{nm} M_n. \tag{2.3.4}$$

En este caso, podemos definir un observable M como el operador hermítico

$$M = \sum_n n M_n. \tag{2.3.5}$$

El valor medio de la medida es

$$\sum_n np(n) = \sum_n n \left\langle \varphi \left| M_n^\dagger M_n \right| \varphi \right\rangle = \sum_n n \left\langle \varphi \left| M_n \right| \varphi \right\rangle = \langle \varphi | M | \varphi \rangle. \tag{2.3.6}$$

En cambio, si consideramos la descomposición espectral de este operador

$$M = \sum_n \lambda_n P_n, \tag{2.3.7}$$

donde cada P_n es el proyector en cada subespacio propio, se tiene que la probabilidad de obtener el resultado n es

$$\mathcal{P}(n) = \langle \psi | P_n | \psi \rangle . \tag{2.3.8}$$

El estado después de la medida será

$$\frac{P_n |\psi\rangle}{\sqrt{\mathcal{P}(n)}}. \tag{2.3.9}$$

Sin embargo, en algunos casos, no nos interesará el estado de la partícula tras la medida, sino solo las probabilidades de los diferentes resultados. Esto lleva a utilizar el formalismo conocido como *POVM (Positive Operator Valued Measurements)*. Supongamos que tenemos una colección de operadores de medida $\{M_n\}_n$. Se definen los *operadores positivos* como $E_n = M_n^\dagger M_n$. Tenemos que $\sum_n E_n = \mathbb{I}$ y que la probabilidad de obtener el resultado m es

$$p(m) = \langle \varphi | E_m | \varphi \rangle . \tag{2.3.10}$$

De manera inversa, siempre que tengamos una colección de operadores positivos $\{E_n\}_n$ tales que $\sum_n E_n = \mathbb{I}$, se puede definir la medida $\{M_n\}_n$ donde $M_n = \sqrt{E_n}$.

Además, es conveniente utilizar la *representación de Krauss* de las operaciones cuánticas puesto que una medida POVM no proporciona la información completa necesaria para describir el proceso de cambio que se produce al medir y, para solucionar esto, se descompone cada elemento POVM en un producto

$$E_n = A_n^\dagger A_n, \tag{2.3.11}$$

donde A_n son los *operadores de Krauss*, que son operadores lineales a los que se les asocia cada posible resultado de una medida y cumplen que

$$\sum_n A_n^\dagger A_n = \mathbb{I}. \tag{2.3.12}$$

2.4. Discriminación entre estados cuánticos sin ambigüedad

En esta sección, siguiendo principalmente [20], estudiaremos las *medidas de discriminación sin ambigüedad* y, finalmente, expondremos la fórmula de máxima probabilidad de discriminación sin ambigüedad (o *Unambiguous State Discrimination, USD)* entre N estados coherentes simétricos, que nos resultará de especial utilidad para aportar garantías en nuestro particular protocolo de seguridad. Para ello, utilizaremos los resultados que acabamos de exponer sobre la teoría de la medida cuántica.

Es posible manipular el estado de un sistema cuántico en formas más interesantes que las que puedan ofrecer las operaciones unitarias o las medidas generales, en particular las de von Neumann. Un tipo de operación de especial interés el que se conoce como *operación probabilística*. Se trata de una operación que, con una probabilidad menor que uno, transformará el estado del sistema en una manera que no se puede llevar a cabo por ningún proceso determinista. Aunque estas operaciones, en general, tienen una probabilidad de error no nula, se puede saber si la transformación se ha llevado a cabo o no.

Una clase importante de operaciones probabilísticas son aquellas que permiten discriminar sin ambigüedad entre estados no ortogonales, esto es, con una probabilidad de error nula. Cuando se lleva a cabo en un sistema cuántico preparado en uno de los estados no ortogonales $|\psi_j\rangle$, tal operación transformará, con una determinada probabilidad, el estado en otro perteneciente al conjunto ortonormal $|\phi_j\rangle$. Estos últimos pueden se pueden discriminar sin ambigüedad utilizando una medida de von Neumann. Aunque esta operación no se puede llevar a cabo con total seguridad, siempre podemos determinar si la transformación ha tenido lugar o no. Cuando el intento falla, obtenemos un resultado no concluyente.

Los pioneros en tratar de resolver el problema de la discriminación sin ambigüedad fueron Ivanovic [36], Dieks [24] y Peres [58]. Esto se centraron en resolverlo para dos estados no ortogonales, lo cual se demostró experimentalmente [35]. Posteriormente, la investigación se centró en resolver el problema para múltiples estados. En particular, Chefles demostró en [19] que la condición necesaria y suficiente para que un conjunto de estados $|\psi_j\rangle$ se pueda discriminar sin ambigüedad es que sean linealmente independientes. Además, él mismo junto con Barnett [20], determinaron la máxima probabilidad con que se pueden discriminar N estados simétricos, suponiendo que tienen las mismas probabilidades a priori. También, lo aplicaron a N estados coherentes simétricos, por lo que es especialmente de nuestro interés.

En primer lugar, justifiquemos por qué el problema se centra en discriminar estados que no son ortogonales. Veamos que, en caso contrario, se pueden discriminar sin ambigüedad: sean $|\phi_1\rangle$ y $|\phi_2\rangle$ estados cuánticos ortogonales. Si tomamos los operadores de medida $M_i = |\phi_i\rangle\langle\phi_i|$ $(i = 1, 2)$ y $M_0 = \mathbb{I} - \sum_i M_i$. Todos ellos suman, trivialmente, $\mathbb{I}$. Entonces, si $|\phi\rangle$ se prepara en el estado $|\phi_i\rangle$, se tiene que

$$\mathcal{P}(i) = \langle\phi| M_i |\phi\rangle = 1, \quad y \quad \mathcal{P}(j) = 0, \quad \forall j \neq i.$$

Por tanto, efectivamente, ambos estados estados se pueden discriminar sin ambigüedad.

En segundo lugar, veamos la máxima probabilidad de discriminación sin ambigüedad entre dos estados no ortogonales $|\psi_1\rangle$ y $|\psi_2\rangle$ (ambos con las mismas probabilidades a priori). Tal y como se demuestra en [24] y [58], vale

$$\mathcal{P}_D = 1 - |\langle\psi_1|\psi_2\rangle|\,, \tag{2.4.1}$$

lo cual se conoce como *límite de Ivanovic-Dieks-Peres (IDP).*

Consideremos ahora un conjunto de N estados cuánticos puros y linealmente independientes, $|\psi_j\rangle$, donde $j = 0, \ldots, N-1$ en el espacio de Hilbert $\mathcal{H}$, $N-$dimensional. Si los estados no son ortogonales, no existe ninguna operación cuántica que pueda discriminarlos de forma determinista. Suponiendo que los estados tienen probabilidades a priori η_j, se puede demostrar, tal y como se hace en [20] (pág.2) que la probabilidad de identificar correctamente el estado es

$$\mathcal{P}_D = \sum_j \eta_j \mathcal{P}_j = \sum_j \eta_j \left\langle \psi_j \left| A_j^\dagger A_j \right| \psi_j \right\rangle, \tag{2.4.2}$$

donde A_j es el operador de Krauss que corresponde a la detección del estado $|\psi_j\rangle$ y tiene la forma:

$$A_j = \frac{\mathcal{P}_j^{1/2}}{\left\langle \psi_j^\perp \mid \psi_j \right\rangle} |\phi_j\rangle \langle \psi_j^\perp|, \tag{2.4.3}$$

siendo $\mathcal{P}_j$ la probabilidad condicionada, dado un sistema en el estado $|\psi_j\rangle$, de que sea identificado; $|\phi_j\rangle$ forman una base ortonormal en $\mathcal{H}$; y $|\psi_j^\perp\rangle$ es el *estado recíproco*, definido como aquel en $\mathcal{H}$ que es ortogonal a todos los $|\psi_{j'}\rangle$ para $j \neq j'$. Además, se definen los operadores A_F como los que indican un error en el intento de discriminación. Por tanto, se cumple que

$$A_F^\dagger A_F + \sum_j A_j^\dagger A_j = \mathbb{I}. \tag{2.4.4}$$

Nótese que la expresión (2.4.2) se puede expresar como una operación POVM si definimos los operadores positivos hermíticos $E_{D_j} = A_j^\dagger A_j$ (con $E_D = \sum_j A_j^\dagger A_j$) y $E_F = A_F^\dagger A_F$.

2.4.1. Estados coherentes simétricos

Puesto que en el protocolo propuesto en el trabajo trabajaremos con una contraseña compuesta por estados coherentes simétricos, nos interesa aplicar estos resultados de discriminación a este caso concreto. Para ello, comenzaremos viendo los resultados generales aplicables a cualquier estado cuántico simétrico para después particularizarlos a dicho caso de estudio.

2.4.1.1. Estados simétricos

Consideremos un conjunto de estados $|\psi_j\rangle$ en $\mathcal{H}$ simétricos y linealmente independientes, es decir, tales que existe una transformación unitaria U en $\mathcal{H}$ de forma que:

$$\begin{aligned} |\psi_j\rangle &= U |\psi_{j-1}\rangle = U^j |\psi_0\rangle, \\ |\psi_0\rangle &= U |\psi_{N-1}\rangle, \\ U^N &= \mathbb{I}. \end{aligned} \tag{2.4.5}$$

El motivo de esta elección es que, en estas condiciones, se pueden obtener expresiones cerradas que podremos manejar. La transformación unitaria U se puede expresar como

$$U = \sum_{k=0}^{N-1} e^{i\phi_k} |\gamma_k\rangle \langle \gamma_k|, \tag{2.4.6}$$

donde $\langle \gamma_k | \gamma_{k'} \rangle = \delta_{kk'}$. Las fases deben ser

$$\phi_k = \frac{2\pi k}{N}, \quad k = 0, \ldots, N-1. \tag{2.4.7}$$

Con lo cual, los estados simétricos tienen la forma

$$|\psi_j\rangle = \sum_{k=0}^{N-1} c_k \exp\left\{ i\frac{2\pi jk}{N} \right\} |\gamma_k\rangle\,, \tag{2.4.8}$$

para cierto c_k tal que $\sum_k |c_k|^2 = 1$.

Utilizando los resultados anteriores, se demuestra en [20] (pág.4) que la *máxima probabilidad de discriminación entre estados simétricos linalmente independientes* está acotada superiormente por

$$\mathcal{P}_D \leq N \min |c_k|^2\,, \quad k = 0, \ldots, N-1, \tag{2.4.9}$$

donde

$$|c_k|^2 = \frac{1}{N^2} \sum_{j,j'} \exp\left\{ i\frac{-2\pi kr\,(j-j')}{N} \right\} \langle \psi_{j'} \mid \psi_j \rangle\,, \quad k = 0, \ldots, N-1. \tag{2.4.10}$$

La cota (2.4.9) es claramente menor que 1 salvo que todos los $|c_k|^2$ sean iguales a N^{-1}, en cuyo caso los $|\psi_j\rangle$ serían ortogonales.

2.4.1.2. Aplicación a estados coherentes simétricos

Estamos ya en condiciones de pasar a analizar el caso de estados simétricos coherentes. Se trata de aplicar la cota (2.4.9) a estados coherentes, que sabemos por (2.1.1) que tienen la forma

$$|\psi_j\rangle = |\alpha_j\rangle = \exp\left\{ -\frac{|\alpha|^2}{2} \right\} \sum_{n=0}^{\infty} \frac{\alpha_j^n}{\sqrt{n!}} |n\rangle, \tag{2.4.11}$$

donde $j = 0, \ldots, N-1$ y $\alpha_j = \alpha \exp\left\{ i\frac{2\pi j}{N} \right\}$. Por tanto, $|\alpha_j| = |\alpha|$ y las fases están equidistribuidas alrededor de un círculo a intervalos regulares de $2\pi/N$. Podemos apreciar mejor esto en el ejemplo concreto que se muestra a continuación en la Figura 2.3.

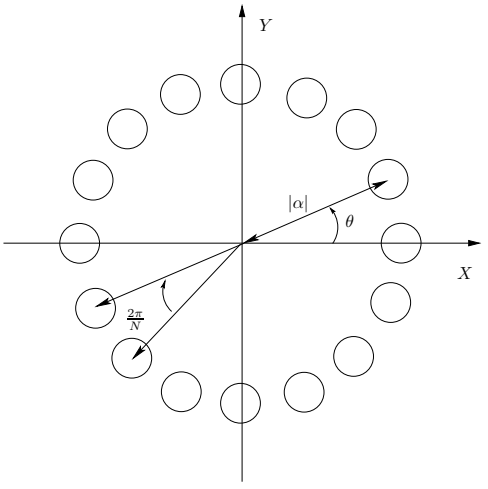


Figura 2.3: Diagrama de estados coherentes simétricos para $N = 16$ y fase inicial nula.

Denotemos por $P_{\mathcal{H}}$ el proyector sobre $\mathcal{H}$, el subespacio generado por $|\alpha_j\rangle$. La transformación unitaria que lleva cada estado en su sucesor es

$$U = P_{\mathcal{H}} \exp\left\{ i\frac{2\pi\hat{n}}{N} \right\} P_{\mathcal{H}}, \tag{2.4.12}$$

donde $\hat{n}$ es el operador número definido en (1.1.12). Como sabemos, las cantidades de interés para determinar el máximo valor de $\mathcal{P}_D$ son el módulo cuadrado de c_k. A partir de la expresión (2.4.10), se llega a que, en este caso

$$|c_k|^2 = \frac{1}{N}\sum_j \exp\left\{i\frac{-2\pi jk}{N}\right\}\exp\left\{|\alpha|^2\left(\exp\left\{i\frac{2\pi j}{N}\right\}-1\right)\right\}. \tag{2.4.13}$$

Así, la *probabilidad de máxima discriminación entre N estados simétricos coherentes* es

$$\mathcal{P}_D^{(N)} = N \min_{k=0,\ldots,N-1} |c_k|^2. \tag{2.4.14}$$

Sin embargo, la suma que aparece en (2.4.13) no se simplifica fácilmente y se debe llevar a cabo numéricamente. Además, también supone un problema encontrar el valor mínimo de los $|c_k|^2$ que nos permitirá determinar el valor de $\mathcal{P}_D^{(N)}$. Esto último es debido a que para un N cualquiera, ninguno de los $|c_k|^2$ permanece como el menor para todos los valores de $|\alpha|^2$, tal y como se puede observar en la Figura 2.4.

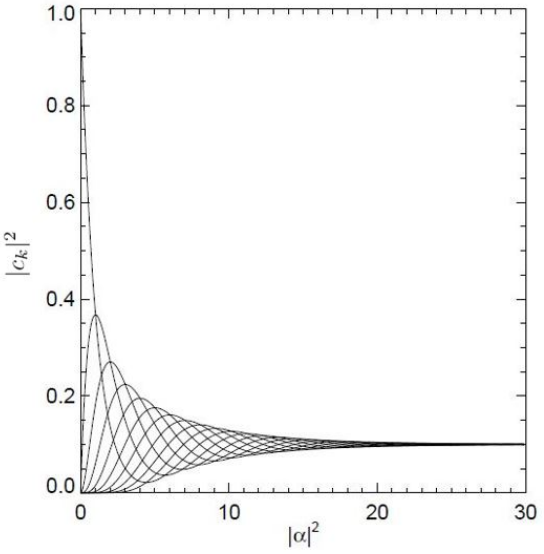


Figura 2.4: Dependencia de $|c_k|^2$ con $|\alpha|^2$ para 10 estados simétricos. Fuente: [20].

Para un N cualquiera, cada $|c_k|^2$ es menor que los otros para un cierto rango de $|\alpha|^2$. En $|\alpha|^2 = 0$, se tiene que $|c_0|^2 = 1$ y el resto de $|c_k|^2$, son nulos. Los resultados numéricos de [20] indican que, según aumenta $|\alpha|^2$, el menor de los $|c_k|^2$ es, sucesivamente, $|c_{N-1}|^2$,$|c_{N-2}|^2$,... y así hasta llegar a $|c_0|^2$, momento a partir del cual el ciclo se repite indefinidamente.

Es evidente a partir de la Figura 2.4 que el punto en el que el mínimo de estos coeficientes cambia tiene lugar cuando la derivada del último es cero. Esto es debido a que

$$\frac{d\left(|c_r|^2\right)}{d\left(|\alpha|^2\right)} = |c_{r-1}|^2 - |c_r|^2\,. \tag{2.4.15}$$

Se deduce, por tanto, que cuando la derivada de $|c_k|^2$ con respecto a $|\alpha|^2$ se anula, se tiene que $|c_k|^2 = |c_{k-1}|^2$. Este es el punto en el que funciones se cruzan y, por tanto, el menor de los coeficientes deja de ser $|c_k|^2$ y pasa a ser $|c_{k-1}|^2$.

Finalmente, importante destacar que ocurre lo siguiente:

$$|c_k|^2 \longrightarrow 1/N \quad \text{cuando} \quad |\alpha|^2 \longrightarrow \infty, \quad \forall k.$$

Asimismo,

$$\mathcal{P}_D^{(N)} \longrightarrow 1 \quad \text{cuando} \quad |\alpha|^2 \longrightarrow \infty, \quad \forall k, N.$$

Es decir, si las amplitudes de los estados coherentes son suficientemente grandes, el solapamiento se reduce y la probabilidad de máxima discriminación tiende a la unidad. Esto concuerda con lo que habíamos visto de que cuando la amplitud es muy grande, tienden a ser ortogonales y nos aproximamos a los resultados que teníamos para estados ortogonales ya comentados. Además, cabe mencionar que $\mathcal{P}_D$ es una función creciente con $|\alpha|^2$, aunque su derivada es discontinua cuando un nuevo $|c_k|^2$ se convierte en el más pequeño. Esto se observa gráficamente en la Figura 2.5.

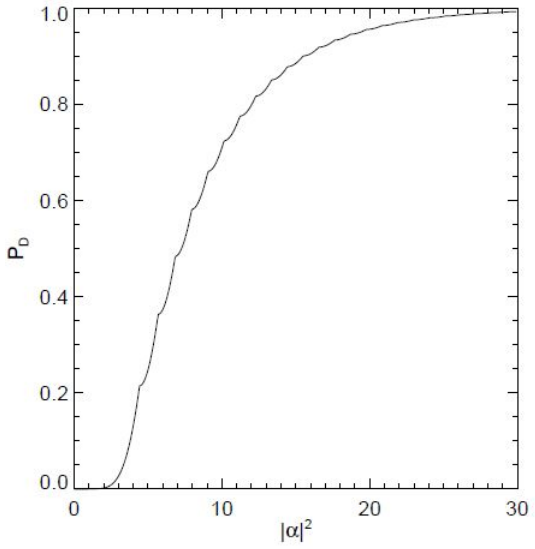


Figura 2.5: Probabilidad de máxima discriminación entre 10 estados simétricos coherentes como función de $|\alpha|^2$. Fuente: [20].

2.5. Teoría de la Información Cuántica

Veamos, a grandes rasgos, algunos aspectos básicos de la Teoría de la Información Cuántica que serán necesarios para plantear y entender el protocolo de seguridad propuesto en el presente trabajo. Utilizaremos como referencias [55] (*Capítulos 3, 7*), [74] (*Capítulos 1,2*) y [39] (*Capítulos 1, 2, 3*).

2.5.1. El qubit

En Teoría de la Información Cuántica el *qubit* juega el mismo papel que el *bit* en la clásica: es la unidad básica de información. Formalmente, es el sistema cuántico cuyo espacio vectorial asociado es un espacio de Hilbert de dimensión 2, que se suele considerar que es $\mathbb{C}^2$. Usaremos la notación $\{|0\rangle, |1\rangle\}$ para la base canónica de $\mathbb{C}^2$. Esta base se suele llamar *base computacional*.

Entonces, mientras que un bit clásico puede estar en el estado 0 o en el estado 1, un estado arbitrario para un qubit es el vector

$$|\phi\rangle = a\,|0\rangle + b\,|1\rangle\,, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

Si trabajamos en el espacio producto tensorial $\left(\mathbb{C}^2\right)^{\otimes q}$, tenemos que un estado cuántico $|\phi\rangle \in \left(\mathbb{C}^2\right)^{\otimes q}$ es un *estado producto* si se puede descomponer como producto de q estados de un solo qubit. En caso contrario, diremos que es un estado *entrelazado*.

Para uno o varios qubits las transformaciones que podemos hacer son transformaciones unitarias y lineales que vienen representadas por matrices unitarias, puesto que estas conservan el producto interno y, por tanto, la probabilidad y el módulo. Además, deben ser reversibles (por los postulados de la Mecánica Cuántica).

Es habitual escribir los circuitos en términos de puertas lógicas cuánticas, que son dichas transformaciones unitarias. Todas deben ser reversibles, lo cual supone la principal diferencia con la Computación Clásica. Las más interesantes son las entrelazantes, es decir, aquellas que transforman estados separables en entrelazados.

2.5.2. Teorema de no clonación

En Computación Clásica la copia de bits es trivial. La motivación de esta subsección, por su parte, es demostrar que no es posible clonar un qubit, o un estado cuántico cualquiera, lo cual aportará garantías de seguridad en nuestro protocolo en el sentido de que no es posible evadir la imposibilidad de realizar una medida exacta en un estado desconocido haciendo muchas copias exactas y midiendo estas; si fuera posible, en cambio, tener un número ilimitado de copias exactas, podríamos medir y reconstruir experimentalmente una copia exacta del estado cuántico original. Formalicémoslo.

Teorema 2.5.1. *(Teorema de no clonación): no es posible clonar perfectamente un estado cuántico desconocido utilizando transformaciones unitarias.*

Demostración: supongamos que tenemos una máquina de copias cuánticas con dos entradas: el dato de entrada es $|\psi\rangle$ y el estado en el que debemos copiarlo, $|\phi\rangle$. Por tanto, el estado inicial de la máquina es $|\psi\rangle \otimes |\phi\rangle$.

Alguna transformación unitaria debe actuar sobre el sistema para transformarlo en

$$U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle.$$

Supongamos que este procedimiento se aplica a dos estados puros en particular, $|\psi\rangle$ y $|\varphi\rangle$. Entonces, tendremos

$$\begin{cases} U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle, \\ U(|\varphi\rangle \otimes |\phi\rangle) = |\varphi\rangle \otimes |\varphi\rangle \end{cases}$$

Sin embargo, utilizando el hecho de que una transformación unitaria conserva el producto interno, se debe cumplir que

$$\langle\psi|\varphi\rangle\,\langle\phi|\phi\rangle = \langle\psi|\varphi\rangle\,\langle\psi|\varphi\rangle\,,$$
$$\langle\psi|\varphi\rangle = |\langle\psi|\varphi\rangle|^2,$$

de donde deducimos que $|\psi\rangle$ y $|\phi\rangle$ son, o bien el mismo estado, o bien ortogonales. En consecuencia, solo se pueden clonar estados cuánticos que sean ortogonales entre sí y, por tanto, clonar un estado desconocido, en general, es imposible. □

2.5.3. Información accesible

La información almacenada en cada estado no tiene por qué ser la que hay accesible, y esto es de vital importancia a la hora de garantizar la seguridad en la comunicación. En Teoría de la Información Clásica, la información de un sistema con $N = 2^n$ estados que podemos obtener es $n = \log_2 N$ bits. Veamos en esta sección cómo cuantificar y controlar esta cantidad de información cuántica a la que se puede acceder.

Supongamos que un observador que llamaremos Alice prepara un estado cuántico x a partir del conjunto $\mathcal{E} = \{(p_x)_x, (\rho_x)_x\}$, es decir un conjunto de estados cuánticos ρ_x que ocurren con una probabilidad p_x, donde ρ_x es la matriz de densidad que para un estado puro $|\psi_x\rangle$ se define como $\rho_x = |\psi_x\rangle \langle\psi_x|$. Bob conoce este conjunto pero no sabe qué estado en particular ha elegido Alice. El objetivo de otro observador, Bob, es adquirir tanta información como sea posible sobre x. La forma en que adquirirá información será llevando a cabo medidas POVM $\{E_y\}_y$, las cuales describimos en la Sección 2.3. Si Alice eligió x, Bob obtendrá en la medida y con probabilidad

$$p(y|x) = \mathrm{Tr}(E_y \rho_x), \tag{2.5.1}$$

donde Tr es la traza de los operadores correspondientes. Esta probabilidad condicionada determina la información que Bob consigue, de media, esto es, la *información mutua*. Esta última cantidad es información mutua media que se transmite entre dos variables aleatorias X e Y y se define como

$$I(X,Y) = \sum_{y\in Y} \sum_{x\in X} p_{XY}(x,y) \log \left(\frac{p_{XY}(x,y)}{p_X(x) p_Y(y)} \right), \tag{2.5.2}$$

de forma que, teniendo solo acceso a X o a Y, podemos cuantificar la información que tenemos sobre la variable aleatoria que no medimos.

Volviendo al caso que nos ocupa, puesto que Bob puede realizar cualquier medida, lo interesante es que escoja la mejor opción. Se define la *información accesible* del conjunto $\mathcal{E} = \{(p_x)_x, (\rho_x)_x\}$ como

$$I_{acc}(\mathcal{E}) = \max_{\{E_y\}_y} I(X,Y). \tag{2.5.3}$$

Puesto que tenemos un conjunto de estados cuánticos ρ_x que ocurren con una probabilidad p_x, entonces el estado completo del sistema está caracterizado por el operador densidad que se define a partir de las matrices de densidad ρ_x de todos los estados posibles y su probabilidad p_x.

$$\rho = \sum_x p_x \rho_x. \tag{2.5.4}$$

Para una matriz de densidad ρ se define la *entropía de von Neumann* como

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho). \tag{2.5.5}$$

Es sabido que la entropía de von Neumann limita la información accesible de un determinado sistema [55]. Algunas de sus propiedades más destacables y que requeriremos posteriormente son:

1. Pureza: $S(\rho) = 0$ para todo estado puro $\rho = |\psi\rangle \langle\psi|$.
   Demostración: trivial por la definición. □

2. Invarianza: $S(U\rho U^*) = S(\rho)$ para toda transformación unitaria U.
   Demostración: obvio por la propiedad cíclica de la traza. □

3. Máximo: $0 \leq S(\rho) \leq \log_2 D$ para todo estado ρ en dimensión D. Vemos, por tanto, que como máximo puede valer el límite clásico. La igualdad se da cuando todos los autovalores son iguales.

   Demostración: consultar en [55] (cap. 7, pág.45) □

4. Para todo par de estados con matrices de densidad ρ y σ se tiene que $S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$.

   Demostración: se deduce del hecho de que si $(\lambda_i)_i$ y $(\beta_j)_j$ son los autovalores de ρ y σ respectivamente, entonces $\lambda_i \beta_j$ para todo i, j, son los autovalores de $\rho \otimes \sigma$. □

Pasemos ahora a definir la *información de Holevo* del conjunto $\mathcal{E} = \{(p_x)_x, (\rho_x)_x\}$ como

$$\mathcal{X}(\mathcal{E}) = S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S\left(\rho_x\right). \tag{2.5.6}$$

Nótese que esta cantidad se reduce a la entropía de von Neumann si $\rho_x = |\phi_x\rangle \langle\phi_x|$ es un estado puro para todo x.

Enunciemos ahora el siguiente teorema que acota la información accesible mediante la *cota de Holevo*.

Teorema 2.5.2. *(Cota de Holevo) Supongamos que Alice prepara un estado cuántico a partir del conjunto* $\mathcal{E} = \{(p_x)_x, (\rho_x)_x\}$. *Entonces,*

$$I_{acc} \leq \mathcal{X}(\mathcal{E}). \tag{2.5.7}$$

Es decir, la información de Holevo limita la cantidad de información accesible de N qubits. Una consecuencia inmediata de la cota de Holevo es que $I_{acc} \leq \log_2 N$ si estamos tratando con estados en dimensión $N = 2^n$. En otras palabras, no podemos obtener una capacidad clásica de N bits si estamos tratando con N qubits.

Demostración: consultar en [55] (cap. 7, págs. 57-59). □

Nótese además que:

1. En el caso de estados puros $\rho_x = |\phi_x\rangle \langle\phi_x|$, la cota de Holevo se reduce a $I_{acc} \leq S(\rho)$.

2. Tanto para estados puros como para mezclas estadísticas, la igualdad en la cota de Holevo se obtiene para estados ortogonales entre sí.

Una versión más simple de este teorema es consecuencia de la *cota de Nayak* [53] que es suficiente en numerosas aplicaciones, en particular, en el protocolo que propondremos en el trabajo.

Teorema 2.5.3. *Supongamos que x es una cadena de m bits que se envían codificándolos en n qubits, siendo $n < m$, e y es la cadena de bits que obtenemos al decodificarlos. Entonces, la probabilidad de que esta cadena extendida con m bits sea igual a la original viene dada por*

$$\mathcal{P}(x = y) \leq \frac{2^n}{2^m}. \tag{2.5.8}$$

Demostración: se puede consultar en [3] (Teorema 17.2). □

Se deduce, por tanto, que la probabilidad de que $x = y$ será exponencialmente pequeña cuanto más comprimamos x, es decir, será más difícil recuperar los bits originales.

Por último, exponemos un resultado más fuerte que acota también la información accesible, en particular, acota la probabilidad de obtener k bits de una cadena de n bits codificados en m qubits.

Teorema 2.5.4. *(Cota k-de-n) Para todo $\eta > 2\ln 2$ existe una constante C_η tal que si n/k es suficientemente grande, entonces la probabilidad de obtener k bits de una cadena de n bits codificados en m qubits está acotada de forma que*

$$\mathcal{P} \leq C_\eta \left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{\eta m}{n}} \right)^k . \tag{2.5.9}$$

Demostración: se puede consultar en [11] (Teorema 2). □

En particular, se deduce que la probabilidad de éxito es exponencialmente pequeña en k si $\frac{m}{n} < \frac{1}{2\ln 2} \simeq 0.721$, pues para $\frac{m}{n}$ suficientemente bajo, la cota se aproxima a 2^{-k}, que es lo que uno conseguiría si adivinara el bit de la posición k-ésima de forma aleatoria.

En el contexto mostrado por la Sección 2.5 que concluye, se enmarca el ámbito de la *Criptografía Cuántica* dentro del que desarrollaremos nuestro protocolo de seguridad empleando estados coherentes y sacando partido de todos los resultados anteriormente expuestos.

2.5.4. Tecnologías de generación, detección y transmisión de fotones

El interés por obtener técnicas que permitan la detección y la generación de fotones individuales eficientemente ha crecido en los últimos años debido al auge de la información cuántica. Actualmente, ambas son tareas complicadas y no hay una técnica aún que pueda considerarse ideal. Lo que sí que está claro, en cambio, es que para llevar a cabo la transmisión de información, la mejor vía es la que representan los fotones, ya que se mueven a la velocidad de la luz, no interaccionan con su entorno y se pueden manipular con óptica lineal, siendo los mejores candidatos para transmisiones de larga distancia. Veamos algunas de las técnicas propuestas para manipular fotones en el ámbito de las comunicaciones cuánticas, recomendando al lector para más información [16, 47].

Los canales de comunicaciones cuánticas tienen en común, al menos, un emisor (Alice), y un receptor (Bob) conectados tanto por un canal de comunicación clásico, como por uno cuántico. Respecto la implementación de un sistema de comunicaciones cuánticas, consta de una fuente de fotones individuales, un detector de fotones individuales y un medio óptico de transmisión. Todos estos componentes introducen errores y pérdidas que disminuyen el rendimiento.

La fuente de fotones individuales suele ser el *láser* [51], el cual emite luz a través un proceso de amplificación óptica basado en emisión estimulada de la radiación electromagnética (de ahí el nombre: *Light Amplification by Stimulated Emission Radiation*). Se diferencia del resto de fuentes en que emite luz con un alto grado de coherencia. En un láser para aproximar estados con fotones individuales se emiten pulsos de *estados coherentes* que se atenúan en lo posible para reducir el número medio de fotones $|\alpha|^2$ (2.1.12). En este caso, la probabilidad de que el láser

emita n fotones en el tiempo sigue una distribución de Poisson, tal y como se vio en (2.1.14). Sin embargo, mientras se emiten pulsos, es probable que se emitan también algunos vacíos, lo que llevará a obtener medidas incorrectas.

Para efectuar las medidas, los detectores de fotones individuales más utilizados son los *tubos fotomultiplicadores (PMT)* y los *fotodiodos de avalancha (APD)*. Ambos convierten la incidencia de un fotón en una señal eléctrica que es detectada, basándose en el efecto fotoeléctrico. El PMT es un tubo al vacío compuesto por un fotocátodo que emite electrones cuando en él inciden fotones de energía adecuada. Estos electrones son acelerados por un campo eléctrico y dirigidos hacia un primer ánodo (también conocido como primer dínodo), provocando la emisión de más electrones secundarios que son dirigidos hacia un segundo dínodo, y así sucesivamente, hasta que se genera un pulso detectable. Los APD, por su parte, son similares pero la absorción inicial del fotón crea un par electrón-hueco en una unión PN de un semiconductor. La multiplicación de la carga se consigue con un voltaje en inversa elevado.

En cuanto al canal óptico, se puede utilizar espacio libre o *fibra óptica* [31]. Habitualmente hecha de dióxido de silicio, ofrece una guía de ondas cerrada que protege a los fotones. Sin embargo, la transmisión de fotones a través de fibra óptica reduce la potencia de la señal debido a la atenuación y hay otros efectos como la dispersión que pueden afectar a la señal. La atenuación de la señal en comunicaciones clásicas se solventa mediante amplificadores, pero sabemos que esto no es posible en comunicaciones clásicas como consecuencia del teorema de no-clonación; por este motivo, se investiga en la creación de *repetidores cuánticos* [44].

En general, se puede apreciar que la tecnología clásica de comunicaciones permite implementar un sistema cuántico. Lo más complicado es la detección de fotones individualizada y la principal diferencia es que se investiga en la creación de repetidores cuánticos en lugar de amplificadores clásicos.

Capítulo 3

Protocolos de seguridad con estados cuánticos de la luz

La Criptografía Cuántica es un campo emergente de la Física y la Tecnología que ha atraído enormemente la atención de los investigadores, puesto que la posibilidad de intercambiar información de forma segura es un hito en la historia de las comunicaciones. Su objetivo es garantizar la confidencialidad de la información transmitida basándose en los principios de la Mecánica Cuántica: la presencia de un espía alterará los estados cuánticos que se estén transmitiendo de forma incontrolada por el *principio de incertidumbre* y el *Teorema de no clonación* imposibilita realizar copias exactas de los mismos. Por el contrario, la seguridad de la Criptografía Clásica se basa en la dificultad de resolución de ciertos problemas como la factorización, el logaritmo discreto o problemas en curvas elípticas, que ahora son vulnerables a ciertos algoritmos cuánticos, como el de Shor [66].

Expondremos en este capítulo algunos ejemplos de protocolos existentes para resolver dos problemas centrales centrales Criptografía Cuántica: *la Distribución Cuántica de Claves (QKD)* y *la autenticación de los usuarios*. Se buscará comprender el problema planteado así como las soluciones propuestas, de forma que podamos inspirarnos en ellas y tratar de mejorarlas a la hora de exponer nuestro particular protocolo en el próximo capítulo.

El capítulo se organiza tal y como se muestra a continuación:

- En primer lugar, se sientan las bases de la Distribución Cuántica de Claves (QKD) y se hace referencia a algunos de los protocolos de seguridad más famosos, en particular se explica el *BB84* [13] . De esta forma, se podrán entender correctamente las discusiones que se realizan por el canal privado y por el público, que es autenticado en este caso, con el fin de generar una clave secreta aleatoria, así como la codificación de los qubits por medio de la polarización de los fotones. Como referencia principal se emplea [39] (*Capítulos 1, 2, 3*).
- A continuación, se expone el problema que supone identificar la identidad legítima de los usuarios cuando no existe un canal público autenticado y ambos comparten una contraseña secreta p. Como ejemplo, se toma el *protocolo de comprobación de contraseñas* [29] y se muestran las ideas que nos resultarán más relevantes en nuestro desarrollo: por un lado, la utilización de *estados cuánticos simétricos* en los que codificar la información de p de manera segura y aleatoria, lo cual se garantiza mediante las cotas de información accesible ya estudiadas y la *función hash*, respectivamente; por otro lado, la propuesta de la comparación de estados mediante un *test SWAP*.

Puesto que nuestro objetivo es generalizarlo a estados coherentes, expondremos también a este respecto el esquema "llave-candado" propuesto en [6] que propone comprobar una contraseña compuesta de estados coherentes comparándolos mediante un *test* que emplea un *divisor de haz* y *detectores binarios*, es decir, capaces de distinguir el vacío de estados con uno o más fotones.

3.1. Distribución Cuántica de Claves (QKD)

Con el fin de resolver con mayor eficiencia uno de los problemas clásicos de Criptografía, el intercambio de la clave, apareció el método conocido como Distribución Cuántica de Claves (QKD) [32]. Se han publicado distintos protocolos, siendo el primero el BB84 [13]. Asimismo, varios experimentos han demostrado que es factible, siendo el primer sistema de red de QKD presentado en 2008 (Viena, Austria) [57]; existen también algunas propuestas comerciales e implementaciones por satélite, que permiten mayores distancias de transmisión [41]. No obstante, es un hecho que actualmente la distancia a la que estos protocolos de seguridad funcionan correctamente está limitada y los experimentos más recientes se centran en solucionarlo con el fin de poder mejorar la aplicación de los resultados que se han obtenido a nivel teórico [21].

El objetivo de QKD es establecer una clave secreta aleatoria suponiendo lo siguiente:

1. Alice (emisor) y Bob (receptor) tienen acceso a un canal clásico, público y autenticado.
2. Existe un canal cuántico privado inseguro, es decir, puede haber alguien espiando, Eve.
3. Alice y Bob tienen acceso a un generador de números aleatorios: generan ciertos qubits y según la base en la que midan obtendrán un resultado u otro.
4. Eve puede hacer cualquier operación que esté permitada por las leyes de la Mecánica Cuántica con el fin de engañarlos. Cada vez que Alice y Bob detecten una anomalía se la atribuirán a ella.

En este contexto, la realización física más habitual de un qubit es un fotón polarizado. De esta forma, los dos valores de un bit, 0 y 1, se pueden codificar de diferentes formas. Una posibilidad es usar dos estados de polarización ortogonales de un solo fotón de forma que se asigne a cada valor lógico uno de ellos, por ejemplo el estado de polarización horizontal o el vertical. Cualquier estado de polarización arbitrario se puede obtener como superposición de estos dos, es decir, forman una base. También podemos considerar polarización a distintos grados e incluso circular. Por ejemplo, podemos expresar la polarización diagonal (a 45°) y la polarización antidiagonal (a −45°) como

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \qquad |\swarrow\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{3.1.1}$$

También se emplea la notación $|+\rangle \equiv |\nearrow\rangle$ y $|-\rangle \equiv |\swarrow\rangle$.

Hemos visto, por tanto, que tenemos las siguientes bases en las que se trabaja habitualmente cuando se concibe el qubit como un fotón polarizado:

$$\{|0\rangle, |1\rangle\} \equiv \{|\leftrightarrow\rangle, |\uparrow\rangle\}, \qquad \{|+\rangle, |-\rangle\} \equiv \{|\nearrow\rangle, |\swarrow\rangle\}.$$

El fundamento de los protocolos QKD es la imposibilidad de medir el estado de un fotón en dos bases complementarias. El ejemplo más famoso, y el pionero, es el protocolo BB84 (Benett

y Brassard, 1984, [13]). Además, cabe mencionar como otros ejemplos: el protocolo B92 [12], el protocolo SARG04 [62] y el protocolo de Ekert [28].

Veamos, en líneas generales y a modo de ejemplo del primer protocolo de seguridad utilizando estados cuánticos de la luz, el protocolo BB84. Además, reutilizaremos algunas ideas relativas a la utilización de un canal público y otro privado para distribuir la clave a la hora de hacer nuestra particular propuesta, por lo que es útil para comprenderlo.

En primer lugar, se lleva a cabo la fase cuántica:

1. Alice escoge N bits al azar. Además, elige las N bases que va a emplear para codificarlos: $\{|0\rangle, |1\rangle\}$ o $\{|+\rangle, |-\rangle\}$. Se tienen, por tanto, 2 bases y 4 estados posibles.
2. Alice envía los N bits por el canal privado a Bob.
3. Bob escoge N bases al azar para realizar las medidas.

Seguidamente tiene lugar la fase clásica para ponerse de acuerdo:

4. Discusión pública, a través el canal público. Bob dice en qué bases ha medido y Alice le contesta cuáles son correctas; no se revelan en ningún momento los resultados. Si Bob ha escogido una base distinta a la de Alice, tiene un 50 % de posibilidades de haber acertado cada medida. Si las dos bases son las mismas, entonces los resultados coinciden.
5. Comprobación para poder detectar espías: se estima el porcentaje de bits que Bob ha medido mal, para lo cual Bob revela algunos y Alice los comprueba. Se atribuye cualquier error a un posible atacante.
6. Reconciliación y extracción de la clave.

Para la implementación de este protocolo es necesario una fuente de fotones individuales, detectores y polarizadores. Por tanto, recordemos que la tecnología clásica de comunicaciones permite implementarlo y el mayor problema se encuentra en la producción y detección de fotones individualizada, tal y como se explicó en la Sección 2.5.4.

3.2. Comprobación de contraseñas con estados simétricos

Similares a los protocolos de QKD, existen otros de comprobación de contraseñas que se implementan cuando se supone que:

- No existe un canal público autenticado.
- Existe una contraseña p privada que comparten ambos extremos.

El objetivo ahora es garantizar que los dos usuarios que comparten dicha contraseña son legítimos. Es decir, en lugar de en la distribución de la clave, se centran en comprobarla con el fin de autenticar la identidad de ambas partes. Existen varias propuestas que aprovechan las propiedades de los estados entrelazados [9, 43, 65] y otras que se basan en el protocolo BB84 [23, 27, 45].

En el presente trabajo, expondremos las ideas principales del protocolo publicado con tal fin en [29], pues serán en las que nos inspiraremos en nuestra particular propuesta. En concreto, reutilizaremos la idea de la utilización de una *función hash criptográfica* para introducir aleatoriedad en la clave finalmente elegida y la de la comparación de estados para lograr el objetivo de

la comparación de contraseñas. De hecho, esto último será lo que se lleve a cabo en el siguiente punto de esta sección particularizado al caso de estados coherentes, que serán los que finalmente utilicemos.

3.2.1. Funciones hash

Una función hash criptográfica

$$H : \{0,1\}^k \mapsto \{0,1\}^n, \quad n < k, \tag{3.2.1}$$

toma como entrada una cadena de bits x y produce otra cadena de bits de menor tamaño $H(x)$, en general, aparentemente aleatoria. Veamos algunas propiedades habituales que se piden a las funciones hash, teniendo presente antes que por "difícil" se entiende que se requiere un tiempo de cómputo, por lo menos, exponencial y, por "fácil", que como máximo consume tiempo polinomial. Se obtener más información en [5].

1. Es una *función unidireccional*, es decir, es fácil computar $H(x)$, pero muy complicado de invertir.
2. Es difícil encontrar una pareja (x, y) con $x \neq y$ tal que $H(x) = H(y)$.
3. Si $x = y$, entonces $H(x) = H(y)$.
4. Un pequeño cambio en la cadena x produce un cambio significante en el valor $H(x)$.
5. El tamaño de la cadena que produce la función hash, k, es fijo.

En Criptografía Clásica también se utilizan estas funciones como parte de la solución del problema de autenticación. Por ejemplo, en el protocolo SPEKE [37], el protocolo SSH [10] o en el propio RSA [60] cuando Alice envía el hash del mensaje en lugar del mensaje en sí. Más concretamente, es habitual recurrir a la familia de funciones hash *SHA-256*, que proporcionan salidas de 256 bits. En cualquier caso, existen muchas disponibles y nosotros no nos preocuparemos por esto a la hora de proponer el protocolo de comprobación de contraseñas, ya que cualquier ordenador es capaz de computarlas.

No obstante, los ordenadores cuánticos podrían romper la seguridad de estos protocolos clásicos. Por tanto, la idea ahora es utilizar esta idea de la función hash para autenticar a los usuarios y garantizar la seguridad basándonos en las leyes de Mecánica Cuántica.

3.2.2. Protocolo básico

La idea que se propone en [29] es crear *estados cuánticos simétricos* de dimensión $D = 2^d$

$$|\psi_j\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} e^{\frac{2\pi i j k}{N}} |\gamma_k\rangle , \quad j = 0, \ldots, N-1, \tag{3.2.2}$$

de forma que la salida del hash cuya entrada sea p y una cadena de bits aleatoria r_i, $H(p\|r_i)$, sea la representación binaria de j ($p\|r_i$ es la concatenación de las cadenas p y r_i). Se codifica así de forma aleatoria las fases de los estados que se emplearán como la contraseña a comprobar para confirmar la identidad de los usuarios.

3.2.3. Comparación de estados cuánticos

En este caso, para lograr el objetivo se comparan los estados de esta contraseña mediante el test SWAP [15], que se implementa en el circuito cuántico de la Figura 3.1 y describimos a continuación. H es la *puerta lógica cuántica* de Hadamard. Como ya comentamos en la sección

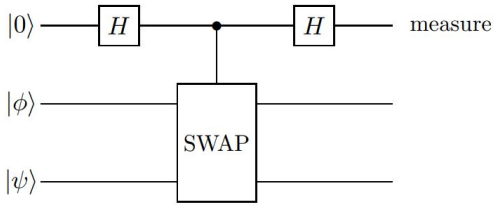


Figura 3.1: Test SWAP: circuito cuántico para comprobar si $|\phi\rangle = |\psi\rangle$. Fuente: [15].

anterior, las puertas son transformaciones unitarias y, en particular, la de Hadamard se trata de una rotación:

$$H = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|. \tag{3.2.3}$$

Entonces, si queremos comparar dos estados $|\phi\rangle$ y $|\psi\rangle$, tendremos al inicio del test el estado $|0, \phi, \psi\rangle$. Tras atravesar las dos puertas de Hadamard y antes de medir, se tiene el estado

$$\frac{1}{2}(|0,\phi,\psi\rangle + |1,\phi,\psi\rangle + |0,\psi,\phi\rangle - |1,\psi,\phi\rangle) = \frac{1}{2}|0\rangle(|\phi,\psi\rangle + |\psi,\phi\rangle) + \frac{1}{2}|1\rangle(|\phi,\psi\rangle - |\psi,\phi\rangle).$$

La probabilidad de que al medir el primer qubit sea 0 es

$$\frac{1}{2} + \frac{1}{2}|\langle\psi \mid \phi\rangle|^2. \tag{3.2.4}$$

Si $|\phi\rangle$ y $|\psi\rangle$ son ortogonales, entonces esta probabilidad es 1/2. En cambio, si son iguales, es 1.

3.2.4. Identificación de estados

Los pasos a seguir para que Alice demuestre su identidad a Bob y asegurar que ambos comparten la contraseña p de m bits son:

1. Alice y Bob generan conjuntamente una cadena aleatoria de m bits, r_i.
2. Utilizando la función hash $H(p\|r_i)$ generan una fase única para cada etapa.
3. Alice prepara el estado $|\psi_j^{r_i}\rangle_A$ de dimensión $D = 2^d$ con $d \ll n$ y se lo da a Bob.
4. Bob lo compara con el que él mismo ha generado, $|\psi_j^{r_i}\rangle_B$, mediante un test SWAP.
5. Se repite este procedimiento s veces hasta lograr el nivel de certeza deseado con nuevos r_i aleatorio.

Cabe mencionar que generar los r_i aleatoriamente es sencillo si Alice y Bob aportan cada uno un bit aleatorio, de manera alternada. Para ello, cada uno puede llevar a cabo un test SWAP con estados ortogonales, de forma que, por cómo funciona, tendrán probabilidad 1/2 de superarlo, lo que podría identificarse con el bit 1, y probabilidad 1/2 de no hacerlo, lo que sería el bit 0. Mientras que uno de los dos usuarios sea honrado, la función hash introducirá suficiente

aleatoriedad con la que podremos garantizar la seguridad del proceso.

Algunas ventajas de usar estados cuánticos son la resistencia frente a ataques de diccionario y de repetición. Los *ataques de diccionario* son aquellos en los que el atacante, en lugar de deshacer el hash, tiene acceso a una lista de hash de contraseñas problables precompilada con la que puede comparar. No obstante, para comparar debe utilizar la versión de hash de la contraseña que se esté empleando, y esto es imposible por tratarse de estados cuánticos, los cuales solo se pueden comparar una vez.

Por su parte, en los *ataques de repetición* el atacante se hace pasar por Bob ante Alice y utiliza una memoria cuántica para comunicarse después con el Bob legítimo. Se logran evitar mediante la función hash, ya que introduce cierta aleatorización impidiendo que los estados se repitan.

Por otro lado, se garantiza la protección de la contraseña mediante resultados vistos anteriormente. En particular, por la cota de Holevo (Teorema 2.5.2), sabemos que no podemos recuperar más de d bits de un estado cuántico de dimensión $D = 2^d$; por la cota de Nayak (Teorema 2.5.3) también sabemos que si $d \ll n$, tenemos una baja probabilidad de recuperar solamente unos pocos bits; y, por último, un resultado más fuerte, la cota k-de-n (Teorema 2.5.4) que limita la probabilidad de recuperar k bits de los n totales. Si $\frac{d}{n} < \frac{1}{2\ln 2} \simeq 0.72$, la probabilidad de recuperar los k bits es exponencialmente pequeña en k. Esta cota también limita igualmente la información que podría extraer de $H(p\|r_i)$.

Asimismo, si elegimos $sd \ll n$, donde s es el número de repeticiones, Eve no sería capaz de deducir nada de la contraseña, incluso si capturara todos los estados. El número de estados generados antes de cambiar la contraseña debe establecerse de forma que el número máximo de estados capturados c satisfaga $cd \ll n$.

Respecto a la implementación, este protocolo es factible con la tecnología existente: como fuente de fotones individuales se puede utilizar, por ejemplo, un láser, el estado inicial se puede transformar en el estado simétrico necesario utilizando moduladores de fase electroópticos y controlarlo también para producir la fase que se obtenga con el hash, el cual se puede computar con un ordenador clásico.

Finalmente, destaquemos que este protocolo de comprobación de contraseñas es solo un ejemplo de todos los que existen. Los estados cuánticos empleados para codificar la contraseña p y la forma de utilizar las funciones hash puede modificarse, siempre que puedan ofrecer ventajas en cuanto a la seguridad o a la implementación práctica. Esta es la razón que motiva la exposición del siguiente apartado, pues nos proporcionará la idea fundamental para generalizar el protocolo a estados coherentes, lo cual supone ciertas ventajas que veremos en el último capítulo.

3.3. Esquema "llave-candado" con estados coherentes simétricos

Centrémonos ahora en analizar cómo se puede comprobar la contraseña utilizando, en particular, estados coherentes de la luz, que serán los que nos interesarán posteriormente. Nos basaremos en los resultados de [6] al respecto, aunque notemos que no se tiene en cuenta cómo se genera aleatoriamente esta contraseña. Ampliaremos esta información en el capítulo final.

El protocolo cuántico "llave-candado" (o *lock and key*) se denomina así por el hecho de que, intuitivamente, podemos considerar una clave secreta como una llave que encaja y abre un determinado candado. Tiene su origen en [70], donde se demostró cómo utilizar sistemas mecánico-cuánticos para crear claves secretas imposibles de falsificar, pero que pueden ser validadas mediante un determinado candado. La idea principal que hay detrás de esto es utilizar, como clave secreta, una secuencia de M sistemas cuánticos, cada uno preparado en un estado seleccionado aleatoria e independientemente, de entre un conjunto de N estados cuánticos no ortogonales entre sí. En nuestro caso, siguiendo la idea de [6], consideraremos un conjunto de estados no ortogonales compuesto por estados coherentes $|\alpha_j\rangle$, es decir, la clave será el estado:

$$|\psi_{key}\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_M\rangle \,. \tag{3.3.1}$$

Cada clave cuántica $|\psi\rangle_{key}$ está asociada con un único estado cuántico $|\psi\rangle_{lock}$ (a modo de candado en la analogía establecida), compuesto por una cadena de estados coherentes idéntica, es decir $|\psi\rangle_{lock} = |\psi\rangle_{key}$. Continuando con el símil, para comprobar si una determinada llave es válida y abre la cerradura, es necesario comparar la cadena de estados de la llave con la cadena de estados del candado. El candado se abrirá solamente si hay una coincidencia total, es decir, no se puede detectar ningún estado de $|\psi\rangle_{key}$ como diferente del correspondiente en $|\psi\rangle_{lock}$. En consecuencia, un posible atacante que ignore la cadena de estados de $|\psi\rangle_{key}$ no tiene ninguna forma de falsificarla fielmente porque, además, el Teorema de no clonación 2.5.1 impide que pueda obtener una copia.

Trabajaremos con N estados coherentes simétricos equidistribuidos alrededor de un círculo tal y como se describió en (2.4.11). Es decir, supongamos que tenemos estados coherentes simétricos $|\alpha_k\rangle$ con amplitud $|\alpha|$ pública y cuyas fases se eligen aleatoria e independientemente entre valores $\frac{2\pi}{N}k$, donde $k = 0, \ldots, N-1$.

Por tanto, Alice y Bob deben comparar el estado $|\psi\rangle_{key}$ con el estado $|\psi\rangle_{lock}$. A priori, para garantizar la seguridad de la comunicación, nos interesa que:

- Alice y Bob sean capaces de comparar con éxito.
- Un espía no sea capaz de identificar la cadena de estados utilizada como clave.

Lo determinaremos en función de probabilidades en los próximos apartados. Antes, cabe destacar que la idea de aprovechar las propiedades de los estados coherentes para crear un protocolo de seguridad cuántico también se ha llevado a cabo en otras propuestas. Por ejemplo, [8] y [52].

3.3.1. Comparación de estados coherentes

Veamos el método ideado para llevar a cabo un test análogo al SWAP sin los inconvenientes que se citan en [6]: este test, o bien requiere componentes no triviales (como determinadas puertas lógicas cuánticas que dejamos fuera de nuestro estudio), o bien destruye los estados que se comparan. La alternativa propuesta se fundamenta en lo expuesto en la Sección 2.2.

Se trata de utilizar un divisor de haz 50 : 50 como el de la Figura 2.2 de manera que las entradas sean estados coherentes

$$|\alpha\rangle_0 \quad \text{y} \quad |\beta\rangle_1 \,, \tag{3.3.2}$$

donde $\alpha = |\alpha|e^{i\phi_1}$ y $\beta = |\beta|e^{i\phi_2}$, y las salidas

$$\left|\frac{\alpha+\beta}{\sqrt{2}}\right\rangle_2 \quad \text{y} \quad \left|\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_3 . \tag{3.3.3}$$

Además situaremos un detector de fotones a la salida de los puertos 2 y 3, con lo cual, sabremos con certeza que si los estados son iguales, no se producirá ninguna detección en el detector 3. Estamos, por supuesto, suponiendo de momento que el detector es ideal, de eficiencia la unidad y ruido (o *medidas oscuras*) despreciable. Más adelante incluiremos esto para generalizar el resultado.

El test, por tanto, consiste en que Alice y Bob preparen por su cuenta un estado coherente y lo hagan incidir en el puerto 0 y 1, respectivamente. Puesto que ellos conocen la contraseña secreta para preparar dichos estados convenientemente, deberán siempre superar el test (es decir, 0 detecciones en 3). Por tanto, lo que nos interesa es determinar con qué probabilidad dos estados aún siendo distintos superarán el test, es decir, producirán 0 fotones en la salida del puerto 3, así como determinar con qué probabilidad no se producirá ninguna lectura en ninguno de los dos detectores, aún siendo iguales los estados incidentes. Estos cálculos son sencillos gracias a que el número de fotones de los estados coherentes sigue una distribución de Poisson (2.1.14). Veámoslo.

La probabilidad de obtener 0 fotones en el detector 3 cuando inciden dos estados distintos es:

$$\mathcal{P}\left(|0\rangle_3\right) = \exp\left\{-\frac{1}{2}|\alpha-\beta|^2\right\}. \tag{3.3.4}$$

Esta es, entonces, la probabilidad de que Eve supere el test probando con un estado distinto. Por tanto, la probabilidad de éxito para Alice y Bob en la tarea de detectar al espía (porque el test será fallido) es:

$$\mathcal{P}_{\text{éxito, det.}} = 1 - \mathcal{P}\left(|0\rangle_3\right) = 1 - \exp\left\{-\frac{1}{2}|\alpha-\beta|^2\right\}. \tag{3.3.5}$$

Esto mismo se puede cuantificar en términos del desfase $\delta = \phi_2 - \phi_1$ si trabajamos con estados simétricos equidistribuidos alrededor de un círculo como se vio en (2.4.11). Entonces, en ese caso $|\alpha| = |\beta|$ y se tiene que:

$$|\alpha-\beta|^2 = (\alpha-\beta)\overline{(\alpha-\beta)} = 2|\alpha|^2 - |\alpha|^2\left(e^{i\delta}+e^{-i\delta}\right) = 4|\alpha|^2\sin^2\left(\frac{\delta}{2}\right). \tag{3.3.6}$$

Por tanto, podemos reescribir la probabilidad de éxito de Alice y Bob en la detección de un atacante que utiliza un estado coherente de igual amplitud para engañarlos como

$$\mathcal{P}_{\text{éxito, det.}} = 1 - \exp\left\{-2|\alpha|^2\sin^2\left(\frac{\delta}{2}\right)\right\}, \tag{3.3.7}$$

con lo que a mayor desfase (más cercanos a la ortogonalidad), mayor probabilidad de éxito. Entonces, a Eve le interesará atacar con estados lo menos ortogonales posibles a los que Bob y Alice estén utilizando.

3.3.2. Probabilidad de superar el test con un estado cuántico cualquiera

Consideremos ahora el caso en que Eve decide atacar con un estado que no es coherente, pues recordemos que puede realizar cualquier medida que esté permitida por las leyes de la Física

Cuántica, sin necesidad por tanto de restringirse a utilizar estados coherentes. Seguiremos el razonamiento de [6].

Podría pensar en preparar un estado cuántico general donde los estados de cada posición de la cadena de $|\psi_{key}\rangle$ pudieran quizá estar entrelazadas. Sin embargo, notemos que, debido a que las fases de los estados coherentes en cada posición de la cadena de $|\psi\rangle_{lock}$ son aleatorias y la comparación se realiza para cada posición de la cadena individualmente, Eve no obtendrá ventaja alguna si utiliza estados entrelazados.

Entonces, suponiendo que los estados que componen la clave no están entrelazados y que, como en el apartado anterior, el atacante no dispone de ninguna copia de la contraseña, este puede preparar un estado general

$$\int_{-\infty}^{\infty} d^2\beta\, P(\beta)\, |\beta\rangle\langle\beta|,$$

donde $d^2\beta = d\beta_r d\beta_i$ con $\beta_r = \mathrm{Re}\,\beta$ y $\beta_i = \mathrm{Im}\,\beta$, y $P(\beta)$ es la función P de Glauber-Sudarshan, que describe el espacio de fases de un sistema cuántico en el espacio de fases de la formulación cuántica; en Óptica Cuántica cualquier estado se puede escribir en esta forma haciendo una elección adecuada, aunque a veces muy astuta (para mayor información, consultar [1] y [2]). El adversario, por tanto, elige $P(\beta)$ de forma que la probabilidad de superar el test de comparación sea lo más alta posible.

La probabilidad de superar el test para un estado determinado de la cadena que compone $|\psi\rangle_{lock}$, es decir, para $|\alpha_j\rangle = \left||\alpha|e^{i\theta}\right\rangle$, es, en promedio,

$$\mathcal{P}_{superar} = 1 - \mathcal{P}_{éxito} = \frac{1}{2\pi}\int_0^{2\pi} d\theta \int_{-\infty}^{\infty} d^2\beta\, P(\beta)\, \exp\left(-\frac{1}{2}\left||\alpha|e^{i\theta} - \beta\right|^2\right), \tag{3.3.8}$$

donde integramos en θ porque la fase es elegida al azar con distribución uniforme. Por simplicidad, el número N de posibles ángulos de fases es infinito en la expresión anterior, pero también se podría calcular $p_{superar}$ para un cierto N. Tomando $\beta = |\beta|e^{i\theta_\beta}$, se tiene

$$\begin{aligned}
\mathcal{P}_{superar} &= \frac{1}{2\pi}\int_0^{2\pi} d\theta \int_{-\infty}^{\infty} d^2\beta\, P(\beta)\, \exp\left(-\frac{1}{2}\left||\alpha|e^{i\theta} - \left|\beta\right|e^{i\theta_\beta}\right|^2\right) \\
&= \frac{1}{2\pi}\int_{-\infty}^{\infty} d^2\beta\, P(\beta) \int_0^{2\pi} d\theta\, \exp\left[-\frac{1}{2}\left(|\alpha|^2 + |\beta|^2 - 2|\alpha\beta|\cos\left(\theta - \theta_\beta\right)\right)\right] \\
&= \int_{-\infty}^{\infty} d^2\beta\, P(\beta)\, \exp\left[-\frac{1}{2}\left(|\alpha|^2 + |\beta|^2\right)\right] I_0(|\alpha\beta|),
\end{aligned} \tag{3.3.9}$$

donde I_0 es la función de Bessel modificada de primera especie. Entonces, se demuestra que, para amplitudes bajas, $|\alpha| \leq \sqrt{2}$, la probabilidad de superar el test es

$$\mathcal{P}_{superar} = \exp\left(-\frac{1}{2}|\alpha|^2\right), \tag{3.3.10}$$

de forma que se maximiza si se toma el vacío (amplitud nula). Esto cuadra con lo que vimos en la Figura 2.1 sobre la relación de incertidumbre entre la amplitud y la fase: el vacío tiene amplitud nula.

En cambio, para amplitudes más altas, $|\alpha| > \sqrt{2}$, la máxima probabilidad tiene lugar cuando el atacante elige $|\beta| \simeq |\alpha|$. Aproximando $I_0(|\alpha\beta|) \sim e^{|\alpha\beta|}/\sqrt{2\pi|\alpha\beta|}$, se llega a que

$$\mathcal{P}_{superar} \sim \frac{1}{\sqrt{2\pi}|\alpha|}. \tag{3.3.11}$$

Con lo cual, la probabilidad de que el atacante pase el test para los M estados que componen la cadena es:

$$\mathcal{P}_{superar,M} = \begin{cases} \exp\left(-\frac{M}{2}|\alpha|^2\right), & \text{si} \quad |\alpha| \leq \sqrt{2} \\ \\ \sim \left(\frac{1}{\sqrt{2\pi}|\alpha|}\right)^M & \text{si} \quad |\alpha| > \sqrt{2}. \end{cases} \tag{3.3.12}$$

Nos interesa, por tanto, con el objetivo de garantizar la seguridad en la comunicación entre Alice y Bob que $\mathcal{P}_{superar,M}$ sea lo más baja posible, luego esto nos proporciona un criterio para elegir la longitud M de la clave.

3.3.3. Obtención de información a partir de una copia de la clave

Supongamos ahora que Eve tiene acceso a una o varias copias de la clave, $|\psi_{key}\rangle$. Veamos que prácticamente no podrá extraer información de ella.

Es claro que, si el atacante se hiciera con una copia de la clave, podría superar con éxito el test de comparación. Sin embargo, ese caso será fácilmente detectable por los usuarios legítimos, ya que notarán que una de las copias de la clave ha desaparecido. Por tanto, la mejor opción para el espía es tratar de extraer la información que contienen las copias a las que tiene acceso, sin utilizarlas tal cual, pues se pondría en evidencia. Además, notemos que, si la clave fuera clásica, podría clonarla sin problema pero, en este caso, el Teorema de no clonación 2.5.1 lo impide.

Para lograr el objetivo de esta sección, recordemos lo expuesto en la Sección 2.5.3 y apliquémoslo a nuestro caso particular: la máxima información que un adversario puede obtener realizando medidas en una de las copias de la clave se denomina información accesible (2.5.3) y está limitada por la cota de Holevo (Teorema 2.5.2). En este caso, tal y como se hizo en (2.5.4), el estado de la contraseña según la información disponible para el adversario antes de que mida es

$$\rho_{key} = \sum_n p_n \rho_n, \tag{3.3.13}$$

donde ρ_n son las matrices de densidad de los estados posibles de las contraseña y p_n sus respectivas probabilidades. Puesto que los M estados de la cadena de la contraseña son $|\alpha_j\rangle = \big||\alpha| \exp\{i\frac{2\pi k}{N}\}\big\rangle$, con
$k = 0, 1, \ldots, N-1$, hay N^M posibles estados puros ρ_n que podría tener la clave, todos ellos equiprobables, con

$$p_n = 1/(N^M). \tag{3.3.14}$$

Entonces, aplicando la cota de Holevo (2.5.2) a este caso en particular, la información accesible sobre en cuál de esos N^M estados está la contraseña, está acotada por

$$I_{acc} \leq \chi\left(\rho_{key}\right) = S\left(\rho_{key}\right) - \sum_n p_n S\left(\rho_n\right), \tag{3.3.15}$$

donde $S\left(\rho_{key}\right) = -\operatorname{Tr}\left(\rho_{key} \log_2 \rho_{key}\right)$ es la entropía de von Neumann (2.5.5) de ρ_{key}. Además, ya vimos que la cantidad $\sum_n p_n S\left(\rho_n\right)$ es siempre positiva o cero y, cuando los estados ρ_n son

puros, como es el caso, es cero. Por tanto, concluimos que la entropía de von Neumann limita la información accesible.

Particularicemos aún más: si nos centramos en uno de los estados que componen la cadena de la contraseña, $|\alpha_j\rangle$, $j = 1, \ldots, M$, la matriz de densidad según la información disponible a priori antes de la medida es

$$\rho_{single} = \frac{1}{N} \sum_{k=0}^{N-1} \left| |\alpha| e^{ik2\pi/N} \right\rangle \left\langle |\alpha| e^{ik2\pi/N} \right| . \tag{3.3.16}$$

Para este estado la entropía de von Neumann, se demuestra en [6] que es

$$S\left(\rho_{single}\right) = \sum_{m=0}^{N-1} \frac{1}{NK_m^2} \log_2 \left(NK_m^2\right), \tag{3.3.17}$$

donde

$$K_m^{-2} = \sum_{k=0}^{N-1} \exp\left\{-|\alpha|^2[1 - \exp(ik2\pi/N)] + imk2\pi/N\right\}. \tag{3.3.18}$$

A la vista de las expresiones, deducimos que $S\left(\rho_{single}\right)$ crece más rápidamente cuanto menor sea N y que

$$\lim_{|\alpha|\to\infty} S\left(\rho_{single}\right) = \log_2 N, \tag{3.3.19}$$

que es justamente el límite clásico, tal y como vimos en la Sección 2.5.3. Por tanto, la idea es crear cada uno de los estados $|\alpha_j\rangle$ que componen la cadena de la contraseña de manera que la información accesible sea mucho menor que la almacenada, la cual, como acabamos de ver, para $|\alpha|$ suficientemente grande tiende a $\log_2 N$, que es justamente el límite clásico que expusimos en la Sección 2.5.3. Es decir, nos interesa que

$$S(\rho_{single}) \ll \log_2 N. \tag{3.3.20}$$

Finalmente, de analizar la entropía estado a estado pasamos a generalizar al estado producto tensorial que compone la contraseña $|\psi_{key}\rangle$ (3.3.1). Suponiendo que hay T copias disponibles de $|\psi_{key}\rangle$ públicas, entonces, por lo expuesto anteriormente en (3.3.14),

$$\rho_{public} = \frac{1}{N^M} \sum_{k=0}^{N-1} \left| \alpha e^{ik2\pi/N} \right\rangle \left\langle \alpha e^{ik2\pi/N} \right| , \tag{3.3.21}$$

y el adversario podrá obtener, como mucho, $TS(\rho_{public})$ bits de información midiendo en todas las copias. Por tanto, nos interesa asegurar, asimismo, que

$$TS(\rho_{public}) \ll M \log_2 N. \tag{3.3.22}$$

A partir de las expresiones (3.3.17) y (3.3.18), se puede ver que para $|\alpha| = 0$, $\rho_{single} = |0\rangle\langle 0|$. Puesto que solo hay un posible estado, la información almacenada en $|\psi_{key}\rangle$ es cero en este caso. La entropía de von Neumann y la información accesible de $|\psi_{key}\rangle$ son también cero. En consecuencia, se debe elegir $|\alpha| > 0$, pero no demasiado alto para un cierto número de estados N, tal y como se aprecia en la figura, donde confirmamos que la información accesible para cada estado que compone la cadena de la contraseña tiende a $\log_2 N$ cuando $|\alpha|$ es lo suficientemente grande.

Capítulo 4

Protocolo de comprobación de contraseñas con estados coherentes simétricos

Los protocolos de seguridad mencionados hasta ahora han demostrado tener ciertas ventajas respecto a los clásicos, pero aún existen ciertas limitaciones prácticas en las cuales se sigue investigando, relativas a la generación y detección de fotones o a las distancias de transmisión. Por eso, se investiga y se proponen diversas alternativas y mejoras de los resultados ya existentes, como son algunos de los ejemplos que hemos expuesto o mencionado. El motivo de la elección de estados coherentes se basa en las ventajas que presentan frente a otras posibilidades como utilizar fotones individuales, a lo cual han recurrido los protocolos anteriormente expuestos. Enumeremos, por tanto, estas ventajas a partir de lo que se expuso en la Sección 2.1.

- Los estados coherentes no son ortogonales entre sí (2.1.3) y podemos tenerlos lo más alejados posibles de esa condición eligiendo amplitudes y desfases pequeños. Por tanto, no se pueden discriminar sin ambigüedad con probabilidad 1. Además por ser simétricos podemos acotar dicha probabilidad convenientemente. Se dificulta la posibilidad de clonación, por lo visto en las Secciones 2.4 y 2.5.

- Cuando trabajamos con estados coherentes, estamos utilizando una superposición de estados de Fock con número medio de fotones $|\alpha|^2$ (2.1.12), de forma que tomando $|\alpha|^2 > 1$ se mejora la probabilidad de detección. Esto solventa en gran medida el problema que supone la detección individualizada de fotones que advertimos en la Sección 2.5.4, así como la ineficiencia de los detectores. Además, también vimos que se generan fácilmente mediante un láser; en cambio, la producción de fotones individuales es mucho más complicada.

- Los estados coherentes son los estados más parecidos a los clásicos en el sentido de que presentan mínima incertidumbre (2.1.19), lo que permite modular según convenga su fase y su amplitud, lo cual veremos que resulta imprescindible para garantizar la seguridad.

Además, otra razón a favor de utilizar estados coherentes es que la polarización de los fotones en que se codifican los qubits en algunos de los protocolos anteriores presenta inestabilidad en fibra óptica. El último cambio que haremos es consecuencia de los inconvenientes ya explicados que presenta el test SWAP. Por tanto, utilizaremos el test análogo propuesto en [6] que los evita sacando partido de las propiedades mecánico-cuánticas de los divisores de haz expuestas en la Sección 2.2.

Respecto a la simetría, se elige así porque permite obtener expresiones cerradas más sencillas y manejables, particularmente útiles para acotar la probabilidad de discriminación sin ambigüedad, tal y como vimos en la Sección 2.4.

En este capítulo proponemos nuestro particular protocolo de comprobación de contraseñas. El problema de seguridad que tratamos de resolver con él, suponiendo que la comunicación es completamente insegura, consiste en lo siguiente: suponemos que ambos extremos comparten una contraseña p privada pero no disponen ni de un canal público autenticado ni de un canal privado seguro, por lo que en principio no tenemos garantizado que su identidad sea legítima. Para identificarse (en particular, Alice ante Bob, siendo el otro caso simétrico), inspirándonos en la idea de [29] y en el escenario "llave-candado" de [6], propondremos crear a partir de p y de una cadena aleatoria de bits r_i, la contraseña $|\psi\rangle_{key}$ que deberán comparar. Esta, como sabemos, consta de una cadena de M estados coherentes simétricos de amplitud $|\alpha|$ que se eligen de entre un conjunto con un total de N, siendo tanto $|\alpha|$ como N públicos, por lo que resulta fundamental seleccionar de forma aleatoria las fases a partir del hash de $p\|r_i$, porque, de hecho, supondremos también que se conocen las máquinas que tenemos para la implementación y cómo se están poniendo en funcionamiento. Asimismo, expondremos las garantías relativas a su seguridad de forma justificada, incluso en algunos casos en que Eve pueda deshacer la función hash.

Recordemos que todo ello se recoge de forma resumida en el diagrama de la Figura 1 mostrado en la introducción del trabajo y que como ejemplo más intuitivo para entender el problema que se plantea y se trata de resolver, expusimos también que podemos suponer que $|\psi\rangle_{key}$ protege una tarjeta de crédito y p es la contraseña que se establece físicamente cuando se solicita en el banco, la cual se supone que funciona. Lo que hay que hacer, por tanto, es establecer una forma de demostrar que al utilizarla para pagar, el usuario es legítimo.

En este capítulo, en definitiva, mostramos las aportaciones propias del trabajo a la hora de crear un protocolo de seguridad, inspirándonos en las ideas referencias y reutilizando algunos desarrollos. Con este fin, la organización del capítulo es la siguiente:

- Antes de entrar en materia, resumiremos los *tipos de ataque* que hemos visto en el capítulo anterior, además de añadir otros que consideramos necesario que también hay que controlar. Quedará así por fin claro el problema al que nos enfrentamos y que resolvemos mediante nuestro protocolo, que pasaremos a detallar.

- En primer lugar, proponemos cómo generar la contraseña $|\psi\rangle_{key}$ de forma aleatoria. La clave está en codificar las fases de los estados coherentes mediante una función hash que tenga como entradas p y una cadena de bits aleatorios r_i. Asimismo, analizaremos cuántas veces puede reciclarse a partir de la entropía de von Neumann. También aplicaremos para garantizar la seguridad los resultados obtenidos acerca de la máxima probabilidad de discriminación sin ambigüedad (medidas USD).

- Añadiremos más resultados relativos al test de comparación de estados coherentes mediante divisores de haz de forma que contemplemos otros posibles ataques, teniendo en cuenta que los detectores pueden fallar y la probabilidad promedio de que el atacante supere el test. Además, daremos algunas justificaciones de que los resultados son óptimos y factibles.

- Los cálculos realizados en el capítulo anterior sobre la probabilidad de superar el test con un estado cuántico cualquiera, obtener información a partir de una copia de la clave y posibilidad de clonación (Secciones 3.3.2 y 3.3.3) se pueden aplicar tal cual. Por tanto,

advertiremos al lector de que no los repetiremos, pero los usaremos para tener aún más garantías de la seguridad, sin necesidad de realizar modificaciones.

- En base a todo ello, propondremos la elección óptima de la amplitud y el número de estados, para lo que habrá que analizar las expresiones gráficamente. Además, veremos cómo elegir el tamaño de la salida de la función hash y el número de veces que podremos reciclar la contraseña $|\psi\rangle_{key}$. Garantizaremos así que el protocolo es seguro si las elecciones son adecuadas.

- Finalmente, haremos alusión a algunos detalles a tener en cuenta a la hora de implementarlo en la práctica, como la eficiencia de los detectores, las medidas oscuras, etc. Además, veremos que es posible aplicarlo de forma segura con amplitudes moderadas, que son las que a día de hoy se han logrado detectar mejor en óptica integrada, garantizando así que su puesta en marcha es factible.

4.1. Modelos de ataque

Antes de exponer el protocolo, conviene mostrar en esta sección los tipos de ataque que puede un espía llevar a cabo. Ya hemos visto al estudiar el esquema "llave-candado" [6] que existe la posibilidad de que se supere el test de comparación con estados falsos, de que se obtenga información a partir de las copias de la clave o incluso de que esta se pueda clonar. No obstante, existen también otros ataques que añadiremos y trataremos de evitar, junto con los anteriores, en el presente capítulo, garantizando así la confidencialidad en la medida de lo posible. Asimismo, los relacionaremos con el modelo de la tarjeta de crédito que venimos empleando para comprender el problema.

Como sabemos, suponemos que es Alice la que se identifica ante Bob. Por tanto, queremos evitar dos tipos de ataque consistentes en que:

1. Eve se haga pasar por Alice, lo cual es análogo a que con una tarjeta de crédito falsa se logre sacar dinero del cajero.

2. Eve se haga pasar por Bob, que se puede identificar con la posibilidad de que utilizando un cajero falso se lea información de la tarjeta para después utilizarla en uno de verdad y obtener dinero.

   Este caso también incluye la posibilidad de que Eve esté escuchando el canal y es análogo al hecho de que se coloque una antena en el cajero con la que obtener información de la tarjeta para después poder utilizarla.

Los ataques de diccionario y de repetición que mencionábamos al exponer el protocolo de comprobación de contraseñas con estados cuánticos simétricos en la Sección 3.2 se incluyen en los de primer y segundo tipo, respectivamente.

Por otra parte, para lograr el objetivo de solventar estos tipos ataques hay que evitar, respectivamente:

1. La falsificaciones de estados.

2. La recuperación de información de las copias de la contraseña disponibles.

Respecto al primero de los casos, hemos visto en la Sección 3.3.2 que la mejor falsificación para superar el test de comparación consiste en emplear el *vacío*, lo cual equivaldría a no meter ninguna tarjeta en el cajero y que se consigua extraer dinero. Además, profundizaremos en el estudio de dicho test teniendo en cuenta otras posibilidades como obtener una medida nula en ambos detectores o utilizar uno de los N estados coherentes que se sabe públicamente que se están empleando (Sección 4.3).

En cuanto al segundo escenario, nos interesa cuantificar cuánta información puede obtener Eve cuando se hace pasar por Bob o, análogamente por el cajero o utilizando una antena. Para ello, recurriremos a los resultados expuestos anteriormente de Teoría de la Información Cuántica. En particular será necesario acotar la entropía de von Neumann de cada uno de estados, de la contraseña en su totalidad, así como de todas las copias disponibles (Sección 4.2.1). También buscaremos minimizar la probabilidad máxima de identificación sin ambigüedad (Sección 4.2.2) y ampliaremos lo que ya conocíamos por el capítulo anterior de la posibilidad de clonación (Sección 4.2.3).

4.2. Generación aleatoria y reutilización de la contraseña en el esquema "llave-candado"

En primer lugar, en nuestro protocolo queremos asegurar que la generación de la contraseña propuesta en el protocolo "llave-candado" de [6],

$$|\psi_{key}\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_M\rangle\,, \quad |\alpha_j\rangle = |\alpha_j| e^{i\phi_j}, \quad \phi_j = \frac{2\pi j}{N}, \quad j = 0, \ldots, N-1,$$

es aleatoria para evitar que Eve realice ataques de repetición en caso de tener una memoria cuántica.

Como adelantábamos, inspirándonos en la idea de [29], lo haremos a partir de la clave p compartida que supondremos que existe y es una cadena s bits, sin revelar ni esta ni $|\psi_{key}\rangle$ en ningún momento; sí que son públicos $|\alpha|$ y N. Supondremos también que tienen acceso a un canal público y a un canal privado inseguros y no autenticados. Los pasos a seguir son los siguientes, suponiendo que Alice trata de demostrar su identidad a Bob (el otro caso es simétrico):

1. Por el canal público, Alice y Bob eligen una cadena aleatoria de t bits r_i tal que $s+t=k$. Para ello, cada uno aporta un bit aleatorio, de manera alternada, que escogen al azar realizando cada uno por su cuenta un test SWAP con estados ortogonales. Ya sabemos que tendrán probabilidad $1/2$ de superarlo, lo que podría identificarse con el bit 1, y probabilidad $1/2$ de no hacerlo, lo que sería el bit 0.

2. Sea la función hash $H : \{0,1\}^k \mapsto \{0,1\}^n, \quad n < k$. Cada uno por su cuenta computa $H(p\|r_i)$, que sabemos introducirá suficiente aleatoriedad siempre que uno de los dos haya sido honesto al elegir los bits de r_i aleatoriamente. Además, solo si Alice y Bob son legítimos obtendrán el mismo valor. $H(p\|r_i)$ se considera que es la representación binaria de j, de forma que habremos codificado así las fases de los estados coherentes de $|\psi_{key}\rangle$.

3. Con esta información, Alice y Bob pueden generar de forma independiente el correspondiente $|\alpha_j\rangle_A$ y $|\alpha_j\rangle_B$, respectivamente. Esta tarea se puede llevar a cabo mediante la atenuación de los pulsos emitidos por un láser para seleccionar las amplitudes. Para modular las fases, por su parte, se requiere establecer una referencia de fase (por ejemplo,

compartiendo una señal de láser que funcione como oscilador local [73]) con respecto a la cual se empleen moduladores electroópticos [50]. Estos se basan en el efecto Pockels que permite la modificación de la fase del haz incidente gracias a una variación del índice de refracción del material proporcional al campo eléctrico aplicado. En concreto, habitualmente el material del modulador es el niobato de litio, $LiNbO_3$.

4. Para comprobar que $|\alpha_j\rangle_A$ y $|\alpha_j\rangle_B$ coinciden, por el canal privado, Alice le envía el estado que ha generado y Bob lo compara con el suyo usando la técnica del divisor de haz que se proponía en [6]. Si Alice es ella, se debe superar el test con casi toda probabilidad, pues así lo demostraremos en lo que sigue eligiendo $|\alpha|$ y N adecuados. Por tanto, si no se supera, pensaremos que hay un espía, con lo cual, se rechazará la contraseña.

Este procedimiento, resumido en el diagrama de la Figura 1, se debe realizar para los M estados que componen la cadena $|\psi_{key}\rangle$. Si se logra superar el test con todos ellos, podremos confirmar que es segura y que los usuarios son legítimos. Superado este procedimiento, Alice y Bob pueden aprovechar a generar varias copias de $|\psi_{key}\rangle$, supongamos que T, lo que marca el número de veces que reutilizarán esta clave.

Eve puede intentar diversos ataques pero va a estar muy limitada al no poder identificar los estados, extraer la información contenida, clonarlos o deshacer la función hash, lo cual supondremos también que puede conseguir, pero que resultará indiferente por las acotaciones expuestas.

4.2.1. Extracción de información

Ya hemos analizado la entropía de von Neumann de cada estado individual de la contraseña, por lo que se elegirá $|\alpha|$ y N de forma que $S(\rho_{single}) \ll \log_2 N$ (3.3.20). Por tanto, Eve apenas podrá obtener información estado a estado. Además, si consideramos el estado de la contraseña antes de medir (3.3.21) y las T copias disponibles, querremos que $TS(\rho_{public}) \ll M \log_2 N$ (3.3.22). Es decir, esta desigualdad nos proporciona un criterio para elegir el número de veces T que se debe reutilizar $|\psi_{key}\rangle$: habrá que cambiarla cuando deje de cumplirse.

Ambas cotas se deducen de la cota de Holevo. Existen, como sabemos, otras útiles para acotar la probabilidad de extracción de información por parte de Eve: por la cota de Nayak (Teorema 2.5.3) también sabemos que si $\log_2 N \ll n$, tenemos una baja probabilidad de recuperar solamente unos pocos bits; y, por último, un resultado más fuerte, la cota k-de-n (Teorema 2.5.4) que permite recuperar k bits de los n totales. Si $\frac{N}{n} < \frac{1}{2\ln 2} \simeq 0.72$, la probabilidad de recuperar los k bits es exponencialmente pequeña en k. Esta cota también limita igualmente la información que se podría extraer de $H(p\|r_i)$. Por tanto, conviene elegir

$$M \log_2 N \ll n \tag{4.2.1}$$

para garantizar la seguridad. Es decir, que la cantidad de información almacenada en los estados coherentes que componen la contraseña sea suficientemente menor que el número de bits codificados.

4.2.2. Identificación de estados coherentes simétricos

Hasta ahora hemos estudiado la probabilidad de que con un divisor de haz 50 : 50 Alice y Bob sean capaces de identificar la presencia de un atacante. Por tanto, esta tarea para ellos es importante y nos interesa que la probabilidad de éxito en la comparación de estados sea alta. No obstante, esto no evita que Eve supere el test si es capaz de identificar los estados que componen

$|\psi_{key}\rangle$ y prepararlos por su cuenta, lo cual podría lograr realizando medidas de discriminación sin ambigüedad mediante procedimientos experimentales como el demostrado en [68], basado en los resultados teóricos de [20] que ya expusimos.

Por eso, en esta sección estudiaremos la máxima probabilidad de discriminación sin ambigüedad $\mathcal{P}_D^{(N)}$, siguiendo los resultados ya expuestos en la Sección 2.4. Vimos que, en el caso de estados coherentes simétricos equidistribuidos en un círculo dicha probabilidad se expresaba, según (2.4.14):

$$\mathcal{P}_D^{(N)} = N \min_{k=0,\dots,N-1} |c_k|^2.$$

Es decir, realizando medidas permitidas por la Mecánica Cuántica, Eve puede identificar sin ambigüedad los estados que se envían Alice y Bob con una probabilidad máxima $\mathcal{P}_D^{(N)}$, que intentaremos minimizar en lo posible para garantizar la seguridad en la comunicación. Entonces, la máxima probabilidad con que conseguiría identificar sin ambigüedad los M estados de la cadena $|\psi_{key}\rangle$ es $\left(\mathcal{P}_D^{(N)}\right)^M$.

Veremos posteriormente que se tiene una probabilidad máxima muy baja eligiendo convenientemente $|\alpha|$, N, y M, por lo que este caso podrá dejar de preocuparnos.

4.2.3. Seguridad frente a clonación y ataques con almacenamiento

La probabilidad que existe de que se puedan clonar los estados de $|\psi_{key}\rangle$ debido a que tanto $|\alpha|$ como N son públicos, está acotada y la demostración, que omitiremos pues se escapa de los objetivos del trabajo, puede consultarse en [63]. Lo que nos interesa es que podemos asegurar que mediante este ataque, Eve tampoco podrá obtener información.

En definitiva, hemos generado una contraseña cuya seguridad depende de su entropía. Además, por tratarse de un sistema cuántico, solo se puede comprobar cada estado una vez. Así, se evitan incluso los ataques de diccionario aún cuando la elección de p es mala (es habitual que la gente escoja 12345, su fecha de cumpleaños o el nombre de su mascota). Esto supone una notable diferencia con lo que ocurre en Criptografía Clásica que cabe mencionar. En este caso, este tipo de elecciones se pueden acabar descifrando, aunque se guarden los hash de las contraseñas y no las contraseñas en sí. Para solucionarlo, se recurre a añadir bits aleatorios que se conocen con el nombre de *sal criptográfica* [64]. No obstante, la seguridad que ofrecen las leyes de la Mecánica Cuántica es mayor.

En consecuencia, en nuestro protocolo gracias a estos resultados podremos reducir la longitud de la contraseña p (s bits), así como la de r_i (t bits), de forma que también se reducirá la salida del hash, pues $n < s + t = k$ y podremos escoger con mayor libertad N y M de forma que $M \log_2 N \ll n$, tal y como exigían las cotas anteriores.

Además, para mayor seguridad conviene separar un tiempo prudencial las comparaciones que se realicen con el divisor de haz para evitar la posibilidad (aunque poco realista) de que Eve disponga de una memoria cuántica.

4.3. Más resultados relativos a la comparación de estados coherentes

Debido a que siempre suponemos que el canal es inseguro pudiendo haber un atacante, Eve, y que tanto $|\alpha|$ como N son conocidos, nos interesa tenerlo en cuenta para determinar tanto la probabilidad de éxito al realizar el test de comparación de $|\psi_{key}\rangle$ si los usuarios son legítimos como la probabilidad de detección de la presencia de un usuario no legítimo al llevarlo a cabo.

Entonces partiendo de los cálculos de [6] expuestos en la Sección 3.3.1, los ampliaremos al cálculo del caso promedio. Finalmente, lo terminaremos de generalizar teniendo en cuenta que se han de realizar tantas comparaciones como longitud tenga la cadena $|\psi\rangle_{key}$, es decir, M. Además, llevaremos a cabo algunas justificaciones adicionales para comprobar que los resultados son óptimos y factibles.

En primer lugar, para comprobar que este test propuesto en [6] es realizable, utilicemos lo expuesto anteriormente sobre los divisores de haz. Ya sabemos que al interferir dos estados coherentes no se produce entrelazamiento y a la salida se producen también estados coherentes cuyas amplitudes son las que se esperarían en Óptica Clásica, tal y como se muestra en (2.2.6).

Imponiendo la condiciones que deben cumplir los coeficientes de reflexión y transmisión (2.2.4) y la de que el divisor de haz sea $50:50$ (2.2.5), se llega a que, para obtener a la salida las amplitudes deseadas (2.2.6) con el fin de poder comparar estados, debemos usar un divisor de haz tal que

$$(t, r) = \left(\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) \quad \text{y} \quad (t', r') = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right).$$

Confirmamos así que el test es factible y, si los estados son iguales (misma amplitud y misma fase), no se detectarán fotones en el puerto 3. En otras palabras, si se detectan fotones en el puerto 3, sabemos con certeza que los estados incidentes son distintos.

Pasemos ahora a estudiar las probabilidades de éxito con detalle. Notemos que la probabilidad de éxito en la detección de usuarios no legítimos (3.3.5) se puede expresar en términos del producto escalar utilizando (2.1.4) como

$$\mathcal{P}_{\text{éxito, det.}} = 1 - |\langle \alpha \mid \beta \rangle|. \tag{4.3.1}$$

Esta expresión resulta interesante porque se trata del límite IDP (2.4.1), luego, concluimos que la discriminación establecida con este test es la óptima para dos estados coherentes (recordemos que los estados no ortogonales no se pueden distinguir sin ambigüedad, Sección 2.4 y el límite IDP representa la máxima probabilidad de lograrlo).

Puesto que los estados coherentes sabemos que no son ortogonales entre sí (2.1.3), deducimos que:

$$|\langle \alpha \mid \beta \rangle| \begin{cases} \neq 0 \\ \simeq 0 \Leftrightarrow |\alpha - \beta| \gg 1, \end{cases} \tag{4.3.2}$$

luego, cuanto más diferentes sean, es decir, más cercanos a la ortogonalidad estén, mayor será la probabilidad de éxito en distinguirlos.

También debemos incluir el caso en que no se detecte ningún fotón en ninguno de los detectores (cuando inciden dos estados distintos o dos estados iguales). Puesto que los estados

coherentes son bastante "clásicos", al atravesar un divisor de haz tenemos un estado separable (no hay entrelazamiento). Por tanto, podemos considerar ambas detecciones como sucesos independientes y tenemos:

$$\mathcal{P}(|0\rangle_2, |0\rangle_3) = \exp\left\{\frac{1}{2}\left(-|\alpha-\beta|^2\right)\right\}\exp\left\{\frac{1}{2}\left(-|\alpha+\beta|^2\right)\right\}. \tag{4.3.3}$$

Puesto que trabajamos con estados simétricos de igual amplitud, se llega finalmente a:

$$\mathcal{P}(|0\rangle_2, |0\rangle_3) = \exp\{-2|\alpha|^2\}, \tag{4.3.4}$$

que tiende a 0 exponencialmente para $|\alpha| > 1$. Además, en caso de que no haya ningún atacante, es decir, los usuarios del test sean legítimos (solamente Alice y Bob), este es el único caso que les puede llevar a descartar la medida. Por tanto, la probabilidad de éxito al realizar el test de comparación en el caso de que los usuarios sean legítimos es

$$\mathcal{P}_{\text{éxito, leg.}} = 1 - \mathcal{P}(|0\rangle_2, |0\rangle_3) = 1 - \exp\{-2|\alpha|^2\}. \tag{4.3.5}$$

También podría ocurrir que Eve atacara con un estado distinto $|\beta\rangle$ y obtuviera una medida $(|0\rangle_2, |0\rangle_3)$. Si $|\alpha| > \sqrt{2}$ podemos aplicar (4.3.4) porque, como hemos visto en la Sección 3.3.2, la forma que tiene el espía de maximizar la probabilidad de superar el test es utilizar un estado de igual amplitud o muy parecida, $|\alpha| \simeq |\beta|$. En ese caso, aunque la fase elegida sea otra, no afecta al desarrollo pues al calcular $|\alpha-\beta|^2 + |\alpha+\beta|^2$ los términos asociados a los desfases se anulan. Por otro lado, si fuera $|\alpha| \leq \sqrt{2}$, habría que aplicar la expresión (4.3.3). Queda, por tanto, así controlada la probabilidad de obtener una medida nula en ambos detectores en cualquier caso que se pueda dar. No obstante, atribuiremos este caso a fallos en los detectores, por lo que se estudiará en más detalle en la Sección 4.5.

En resumen, a la hora de utilizar el test del divisor de haz 50 : 50 con estados incidentes coherentes simétricos equidistribuidos alrededor de un círculo como se describe en (2.4.11), se tienen dos posibles casos:

- Si los usuarios son legítimos, la probabilidad de éxito en superar el test es

$$\mathcal{P}_{\text{éxito, leg.}} = 1 - \exp\{-2|\alpha|^2\}.$$

- Si hay un usuario no legítimo que pretende superar el test con un estado coherente, se podrá detectar su presencia con una probabilidad

$$\begin{aligned}\mathcal{P}_{\text{éxito, det.}} &= 1 - \exp\left\{\frac{-1}{2}|\alpha-\beta|^2\right\} = 1 - |\langle\alpha \mid \beta\rangle| \\ &= 1 - \exp\left\{-2|\alpha|^2 \sin^2\left(\frac{\delta}{2}\right)\right\},\end{aligned}$$

  donde la última igualdad se da en caso de que Eve ataque con un estado coherente de la misma amplitud y δ es el desfase entre ambos estados.

Estamos suponiendo hasta ahora que Eve ataca sin conocer la clave eligiendo un estado cualquiera o un estado con la misma amplitud. Pero, aparte de $|\alpha|$, el número de estados coherentes disponibles y equidistribuidos alrededor del círculo, N, también es público, así que supongamos ahora que hace también uso de este conocimiento. Generalicemos la probabilidad de éxito en el caso de que decida escoger uno de ellos al azar para superar el test, incluyendo la aleatoriedad

que esto supone.

Recordemos que se eligen N estados coherentes de la misma amplitud y se disponen en círculo de radio su amplitud, equiespaciados $\phi_k = \frac{2\pi}{N}k\ rad$, $k = 0, \dots, N-1$. A partir de (3.3.7) se deduce que el peor de los casos se tiene cuando Eve escoge el desfase es el mínimo, es decir, tal que $\delta = \frac{2\pi}{N}$ y, el mejor, cuando elige el máximo, $\delta = \pi$. Nos resulta útil, entonces, calcular la probabilidad promedio de éxito al comparar dos estados distintos elegidos del círculo al azar. Para ello, sacaremos partido, en primer lugar, de la expresión (4.3.1).

Es obvio que $|\langle\alpha \mid \beta\rangle| = |\langle\beta \mid \alpha\rangle|$. Además, suponemos que todos los estados son equiprobables, con probabilidad de ser escogidos $\frac{1}{N}$. Necesitamos calcular el solapamiento promedio, $\overline{|\langle\alpha \mid \beta\rangle|}$, para lo cual basta escoger uno de los N estados, $|\alpha_0\rangle = \alpha e^{i\phi_0}$ y compararlo con los $N-1$ estados restantes, $|\alpha_k\rangle = |\alpha|e^{i\phi_k}$, $\phi_k = \frac{2\pi}{N}k$, $k = 1, \dots, N-1$. Es decir, hay que calcular $|\langle\alpha_0 \mid \alpha_k\rangle|$, $\forall k = 1, \dots, N-1$, y para hallar el promedio buscado, sumar y dividir entre $N-1$. Nótese que, debido a que los N estados son indistinguibles y equiprobables, da igual cuál sea el estado de partida $|\alpha_0\rangle$ (es decir, para las N posibles elecciones se obtienen los mismos resultados). Entonces

$$\overline{|\langle\alpha \mid \beta\rangle|} = \frac{1}{N-1}\sum_{k=1}^{N-1}\exp\Big\{-2|\alpha|^2\sin^2\left(\frac{\pi}{N}k\right)\Big\}, \tag{4.3.6}$$

con lo cual, la probabilidad promedio de éxito en la detección de un atacante que emplea para engañar a los usuarios legítimos uno de los N estados coherentes simétricos es

$$\overline{\mathcal{P}}_{\text{éxito, det.}} = 1 - \overline{|\langle\alpha \mid \beta\rangle|} = 1 - \frac{1}{N-1}\sum_{k=1}^{N-1}\exp\Big\{-2|\alpha|^2\sin^2\left(\frac{\pi}{N}k\right)\Big\}, \tag{4.3.7}$$

que aumenta con $|\alpha|$.

Nótese que estamos restringiendo las fases posibles a las posibles para cierto N. Pero, si Eve decide atacar utilizando otra cualquiera en el intervalo $[0, 2\pi)$, tendremos que cambiar la suma por una integral:

$$\overline{\mathcal{P}}_{\text{éxito, det.}} = 1 - \overline{|\langle\alpha \mid \beta\rangle|} = 1 - \frac{1}{2\pi}\int_0^{2\pi}\exp\{-2|\alpha|^2\sin^2\theta d\theta\} = 1 - e^{-|\alpha|^2}I_0(|\alpha|^2), \tag{4.3.8}$$

donde I_0 es la función de Bessel modificada de primera especie. Esta probabilidad la habíamos aproximado anteriormente mediante (3.3.10) y (3.3.11).

Para acabar, tengamos en cuenta que hay que realizar M comparaciones y que, en todas ellas, se debe superar el test para validar la $|\psi_{key}\rangle$. Entonces, analicemos de nuevo los dos casos que pueden darse:

- Si los usuarios son legítimos, la probabilidad de éxito en superar el test es

$$\mathcal{P}_{\text{éxito, leg., M}} = 1 - \exp\{-2M|\alpha|^2\}. \tag{4.3.9}$$

- Si hay un usuario no legítimo que pretende superar el test con estados coherentes, la probabilidad de detectar su presencia viene dada por

$$\begin{aligned}\mathcal{P}_{\text{éxito, det., M}} &= 1 - \exp\left\{\frac{-M}{2}|\alpha-\beta|^2\right\} = 1 - |\langle\alpha \mid \beta\rangle|^M \\ &= 1 - \exp\left\{-2M|\alpha|^2\sin^2\left(\frac{\delta}{2}\right)\right\},\end{aligned} \tag{4.3.10}$$

donde la última igualdad se da para el caso de que Eve ataque con un estado coherente de la misma amplitud. Por otro lado, se aplica

$$\overline{\mathcal{P}}_{\text{éxito, det., M}} = 1 - \left[\frac{1}{N-1}\sum_{k=1}^{N-1} \exp\left\{-2|\alpha|^2 \sin^2\left(\frac{\pi}{N}k\right)\right\}\right]^M \tag{4.3.11}$$

en caso de que Eve ataque eligiendo al azar uno de los N estados coherentes del círculo seleccionado y, en caso de que lo haga seleccionando la fase al azar en el intervalo $[0, 2\pi)$:

$$\overline{\mathcal{P}}_{\text{éxito, det., M.}} = 1 - \left[e^{-|\alpha|^2} I_0(|\alpha|^2)\right]^M, \tag{4.3.12}$$

que habíamos aproximado anteriormente mediante (3.3.10) y (3.3.11).

4.4. Elección óptima de la amplitud y el número de estados

Los resultados que acabamos de exponer, así como las Secciones 3.3.2 y 3.3.3 que hemos reutilizado y omitido en el capítulo, nos proporcionan los criterios de elección de la amplitud de los estados coherentes, así como del número de ellos que debemos utilizar para la creación de la contraseña $|\psi_{key}\rangle$.

A modo de síntesis, buscamos garantizar:

1. Éxito en la comparación de estados coherentes, tanto en el caso de que haya un atacante como en el caso de que no, para lo cual debemos maximizar en lo posible las expresiones (4.3.9), (4.3.10), (4.3.11) y (4.3.12).

2. Minimizar la probabilidad de superar el test con un estado cuántico cualquiera, (3.3.12), expresión que recordemos que aproxima a (4.3.12).

3. Baja probabilidad de identificación de estados coherentes, es decir, minimizar (2.4.14).

4. Estados componentes de la cadena de la contraseña cuya información accesible sea menor que la almacenada $S(\rho_{single}) \ll \log_2 N$.

5. La información accesible de las copias disponibles de la contraseña sea también menor que la almacenada $TS(\rho_{public}) \ll M \log_2 N$, donde T podemos interpretarlo como el número de veces que se recicla la contraseña $|\psi_{key}\rangle$.

6. $M \log_2 N \ll n$ (4.2.1), donde n es el tamaño de la salida de la función hash que utilicemos. La longitud k de la concatenación $p\|r_i$ está relacionada también con esta expresión debe cumplirse que $n < k$.

7. Amplitudes pequeñas o moderadas y N suficientemente alto por la incertidumbre en la medida: cuanta menos ortogonalidad haya, más difícil serán tanto la posibilidad de clonación (Teorema 2.5.1) como realizar una medida de discriminación sin ambigüedad.

8. Separación de las comparaciones de estados de estados coherentes un tiempo prudencial para evitar la posibilidad (poco realista) de que Eve posea una memoria cuántica.

Puesto que sabemos cómo generar los estados coherentes por lo expuesto anteriormente en la Sección 4.2, pasemos a elegir con qué características ópticas crearlos. Debido a que las expresiones obtenidas son complejas de analizar analíticamente, lo haremos gráficamente, comparando

esencialmente amplitudes $|\alpha|$ entre 0 y 4, número de estados N entre 4 y 20 y longitud de la contraseña $M = 5, 10, 15, 20, 30$. El motivo de esta elección a priori es que, a partir de las deducciones anteriores, intuimos que los valores de amplitud no deben ser altos, mientras que N y M, sí. En cualquier caso, veremos que todas las gráficas presentan una tendencia clara que nos permitiría extrapolar trivialmente los resultados a otros valores.

Seguiremos el orden marcado por las secciones anteriores para mostrar progresivamente las gráficas correspondientes a cada situación a tener en cuenta, junto con algunos comentarios introductorios que repetiremos de forma más general finalmente. Así, obtendremos un análisis conjunto con el que extraer conclusiones respecto a la elección óptima de los parámetros que intervienen.

4.4.1. Probabilidad de éxito al realizar el test de comparación de $|\psi_{key}\rangle$ entre usuarios legítimos

En primer lugar, mostramos en la Figura 4.1 la representación de la probabilidad de éxito al realizar el test de comparación entre usuarios legítimos (4.3.9) en función de $|\alpha|$ para varios valores de la longitud de la contraseña, M. Podemos ver que a mayor amplitud, mayor probabilidad de éxito en la tarea de comparación mediante el test propuesto con el divisor de haz, tendiendo finalmente a la unidad para amplitudes $|\alpha| > 2$.

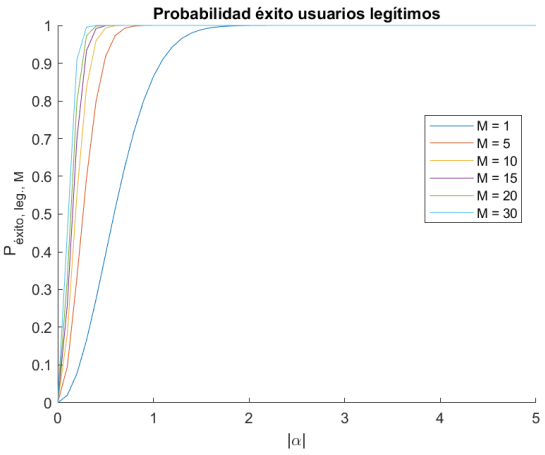


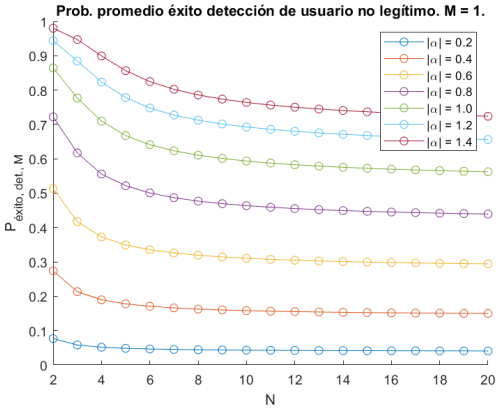
Figura 4.1: Probabilidad de éxito al realizar el test de comparación de $|\psi_{key}\rangle$ entre usuarios legítimos, $\mathcal{P}_{\text{éxito, leg., M}}$ (4.3.9) para $M = 1, 5, 10, 15, 20, 30$.

Recordemos que esta probabilidad hacía referencia a no obtener una medida nula en ambos detectores. Esto es lo único que puede llevar a descartar el protocolo si los usuarios son legítimos, de ahí el nombre de esta sección, pero también puede darse este caso cuando un atacante trata de superar el test con un estado falso.

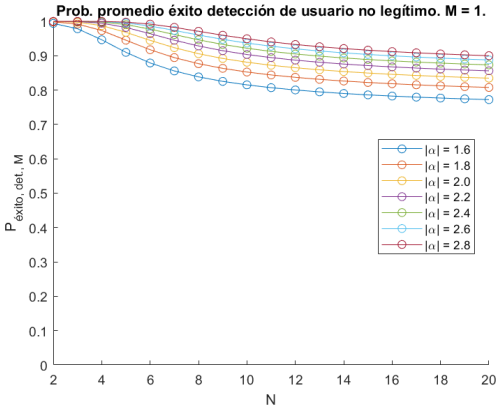
Este hecho debemos tenerlo presente antes de pasar a la siguiente sección, pues la probabilidad total de detección incluye tanto este caso como el que pasaremos a mostrar. No obstante, cabe destacar que dicha posibilidad de medida nula la consideraremos un fallo de los detectores y la analizaremos con mayor detalle al incluir el tratamiento realista en la Sección 4.5.

4.4.2. Probabilidad promedio de éxito en la detección de un atacante que emplea uno de los N estados disponibles para superar el test

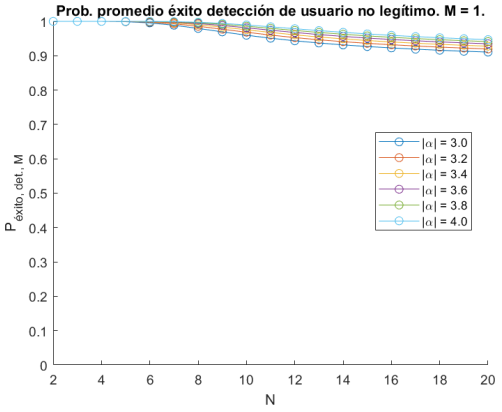
En segundo lugar, en las nueve figuras siguientes representamos la probabilidad promedio de éxito en la detección de un atacante mediante el test de comparación (3.3.12) en función de N para distintos valores de M y de $|\alpha|$. Se aprecia que crece con $|\alpha|$ y más rápidamente cuanto mayor sea M, tendiendo finalmente a la unidad si $|\alpha| > 1.4$ y $M > 5$.



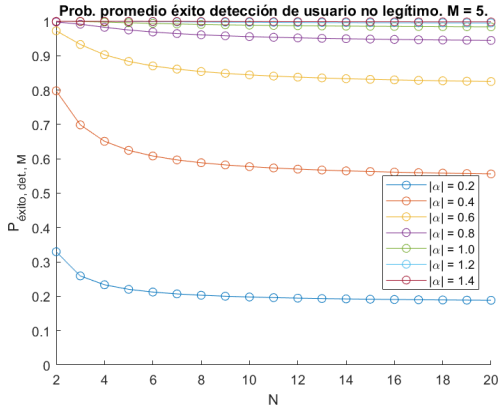
(a) $M = 1$ y $|\alpha| = 0.2, 0.4, \ldots, 1.4$.



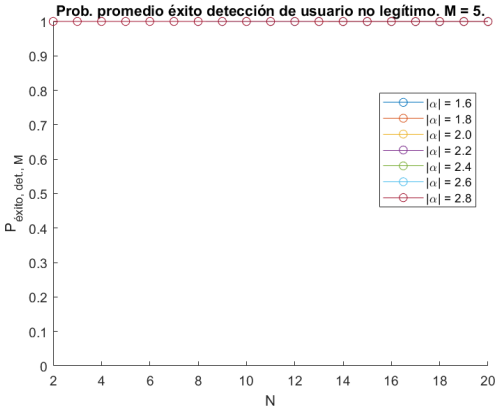
(b) $M = 1$ y $|\alpha| = 1.6, 1.8, \ldots, 2.8$.



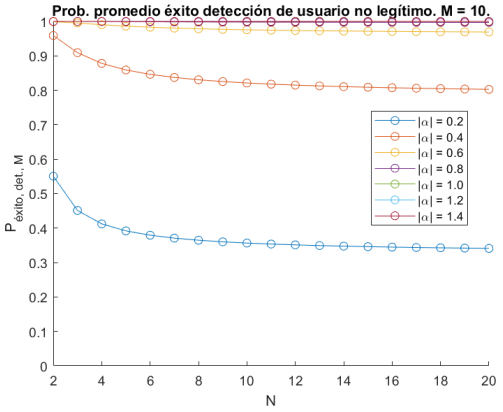
(c) $M = 1$ y $|\alpha| = 3.0, 3.2, \ldots, 4.0$.



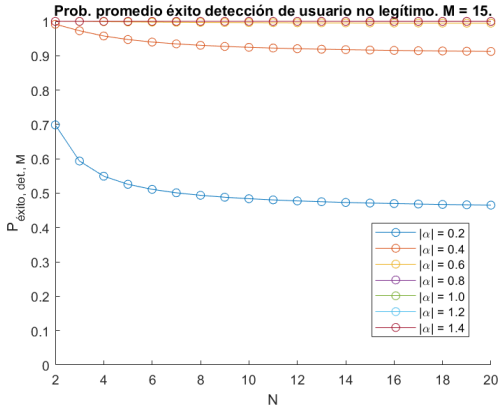
(d) $M = 5$ y $|\alpha| = 0.2, 0.4, \ldots, 1.4$.



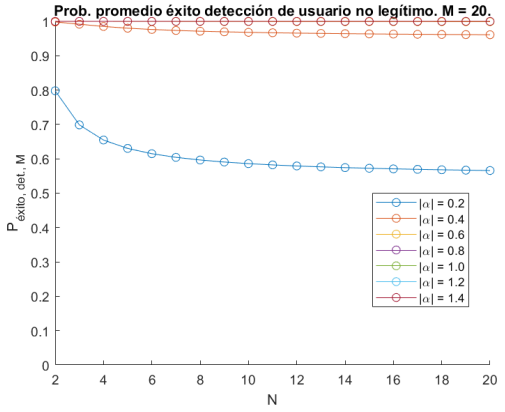
(e) $M = 5$ y $|\alpha| = 1.6, 1.8, \ldots, 2.8$.



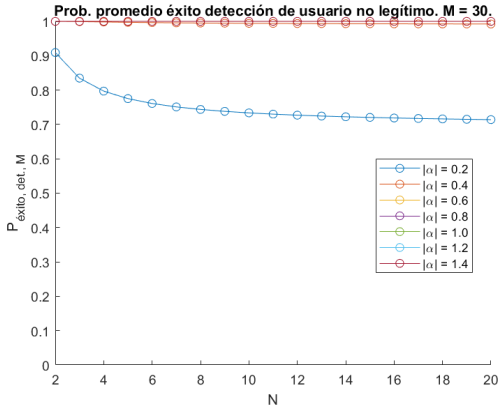
(f) $M = 10$ y $|\alpha| = 0.2, 0.4, \ldots, 1.4$.



(g) $M = 15$ y $|\alpha| = 0.2, 0.4, \ldots, 1.4$.



(h) $M = 20$ y $|\alpha| = 0.2, 0.4, \ldots, 1.4$.

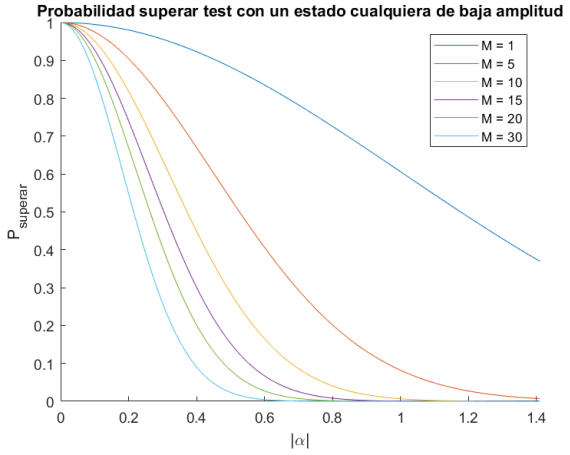


(i) $M = 30$ y $|\alpha| = 0.2, 0.4, \ldots, 1.4$.

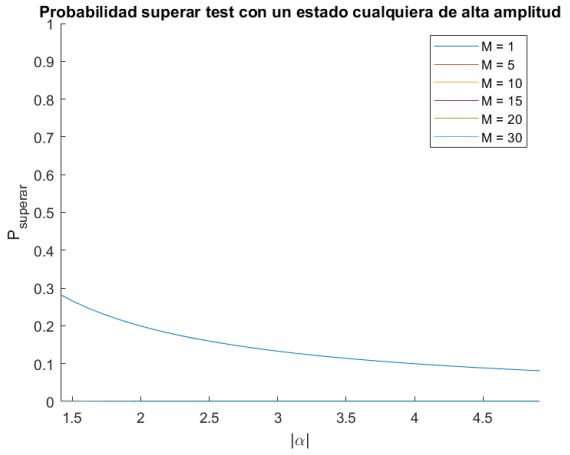
Figura 4.2: Probabilidad promedio de éxito en la detección de un atacante mediante el test de comparación de de $|\psi_{key}\rangle$, $\overline{P}_{\text{éxito, det., M}}$ (4.3.11).

4.4.3. Probabilidad de superar el test de comparación de $|\psi_{key}\rangle$ con un estado cuántico cualquiera

A continuación en la Figura 4.3, representamos la probabilidad de que un atacante supere el test utilizando cualquier estado cuántico (3.3.12) en función de $|\alpha|$ para distintos valores de M. Vemos que se hace nula a medida que aumenta $|\alpha|$ y lo hace más rápidamente cuanto mayor sea M.



(a) $M = 1, 5, 10, 15, 20, 30$ y $|\alpha| \leq \sqrt{2}$.

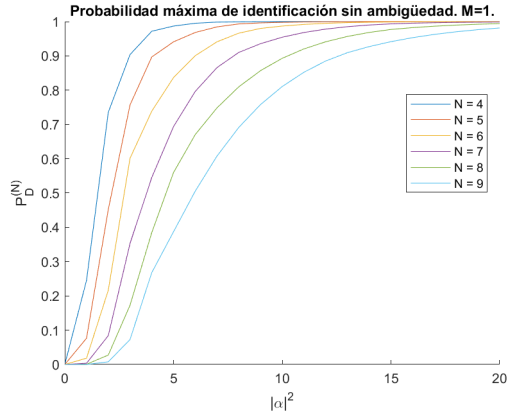


(b) $M = 1, 5, 10, 15, 20, 30$ y $|\alpha| > \sqrt{2}$.

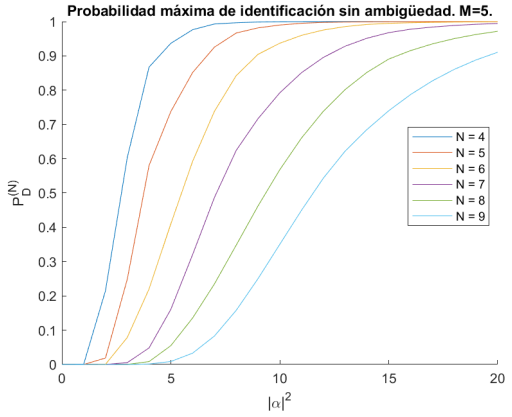
Figura 4.3: Probabilidad de superar el test de comparación de $|\psi_{key}\rangle$ con un estado cuántico cualquiera, $\mathcal{P}_{superar}$ (3.3.12).

4.4.4. Probabilidad máxima de identificación sin ambigüedad de los estados coherentes componentes de $|\psi_{key}\rangle$

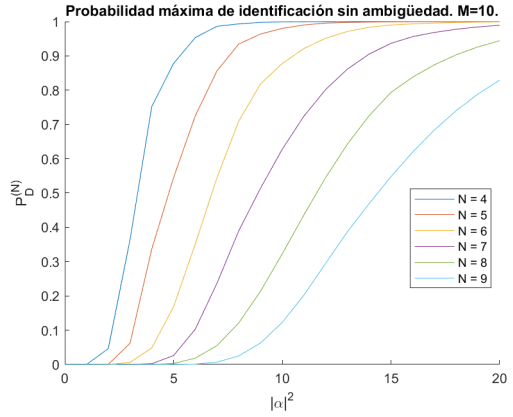
En las próximas figuras, representamos la probabilidad máxima de discriminación de los estados coherentes (2.4.14) en función de $|\alpha|^2$ para distintos valores de M y N. Vemos que decrece con la amplitud más rápidamente cuanto mayores sean N y M. Además, notemos que tiende a anularse para determinados valores por los que nos decantaremos finalmente, pues es lo que nos interesa.



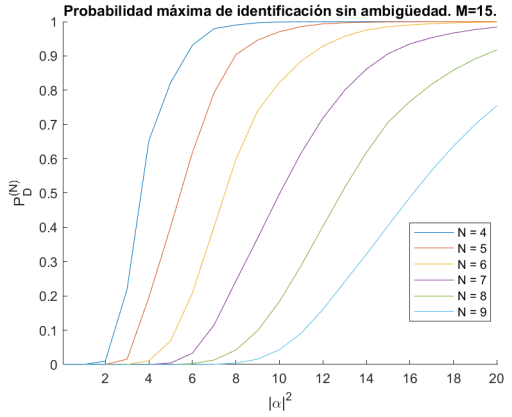
(a) $M = 15$ y $N = 4, \ldots, 9$.



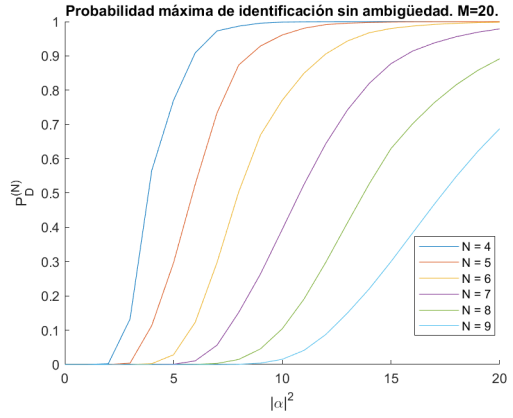
(b) $M = 5$ y $N = 4, \ldots, 9$.



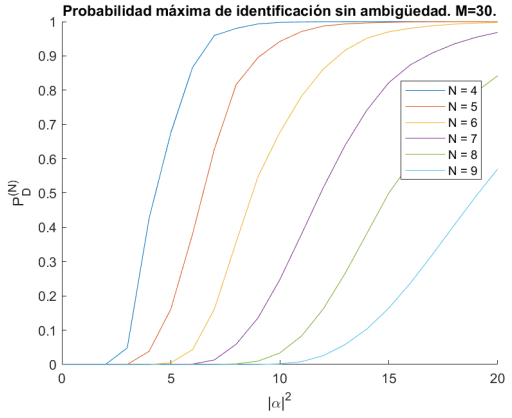
(c) $M = 10$ y $N = 4, \ldots, 9$.



(d) $M = 15$ y $N = 4, \ldots, 9$.

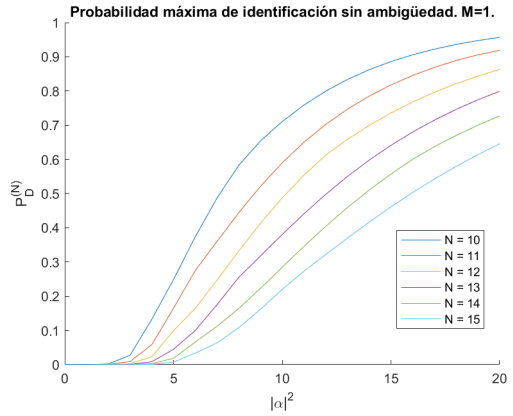


(e) $M = 20$ y $N = 4, \ldots, 9$.

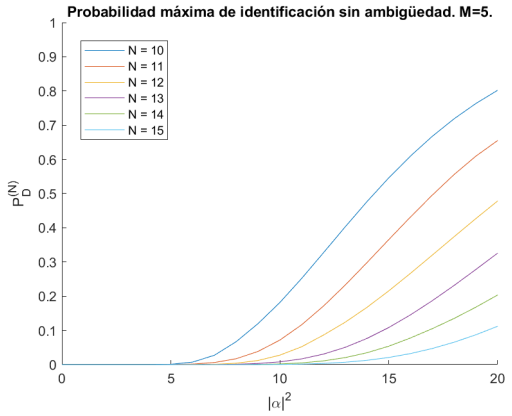


(f) $M = 30$ y $N = 4, \ldots, 9$.

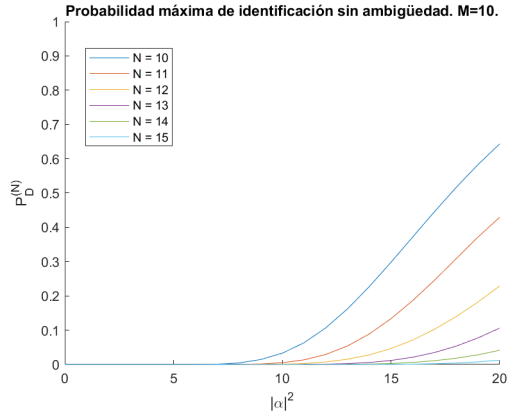
Figura 4.4: Probabilidad máxima de identificación sin ambigüedad de los estados coherentes componentes de $|\psi_{key}\rangle$, $\mathcal{P}_D^{(N)}$ (2.4.14).



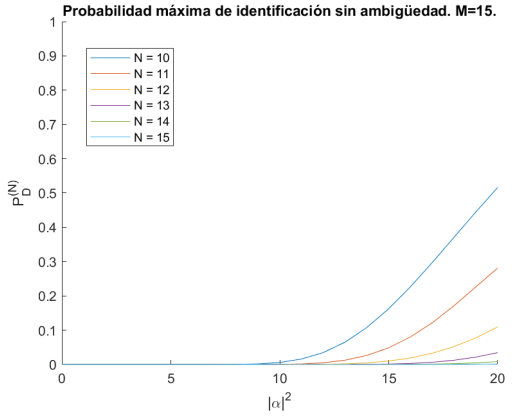
(g) $M = 1$ y $N = 10, \ldots, 15$.



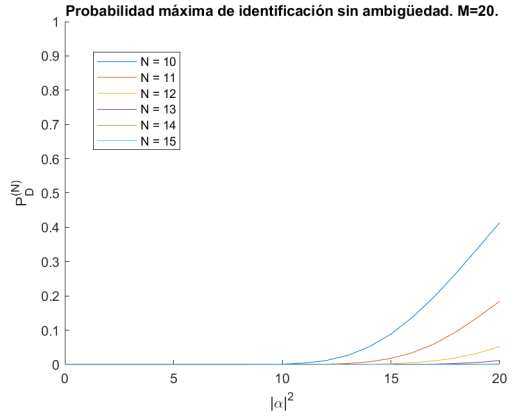
(h) $M = 5$ y $N = 10, \ldots, 15$.



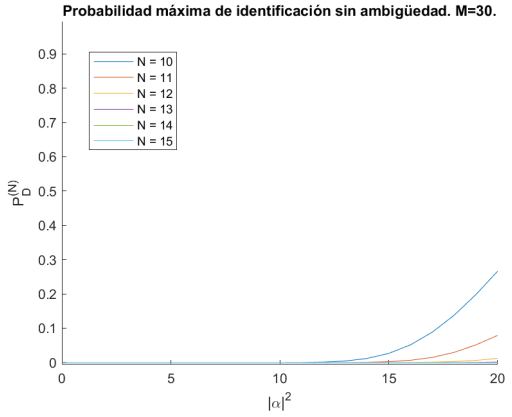
(i) $M = 10$ y $N = 10, \ldots, 15$.



(j) $M = 15$ y $N = 10, \ldots, 15$.

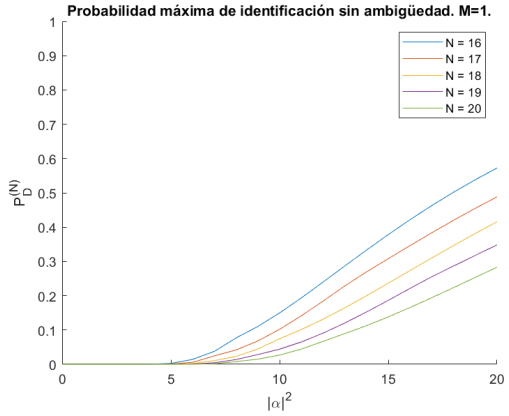


(k) $M = 20$ y $N = 10, \ldots, 15$.

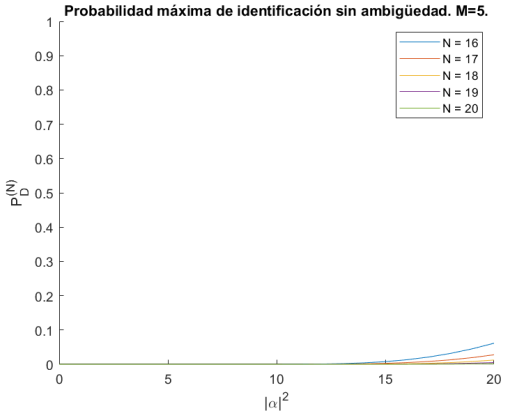


(l) $M = 30$ y $N = 4, \ldots, 9$.

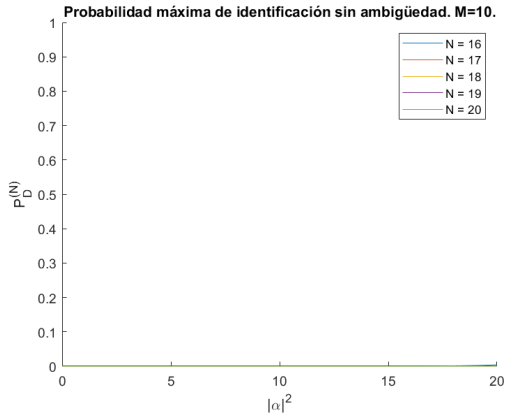
Figura 4.4: Probabilidad máxima de identificación sin ambigüedad de los estados coherentes componentes de $|\psi_{key}\rangle$, $\mathcal{P}_D^{(N)}$ (2.4.14).



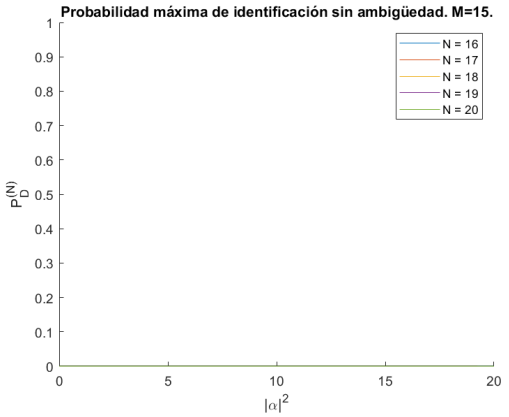
(m) $M = 1$ y $N = 16, \ldots, 20$.



(n) $M = 5$ y $N = 16, \ldots, 20$.



(ñ) $M = 10$ y $N = 16, \ldots, 20$.

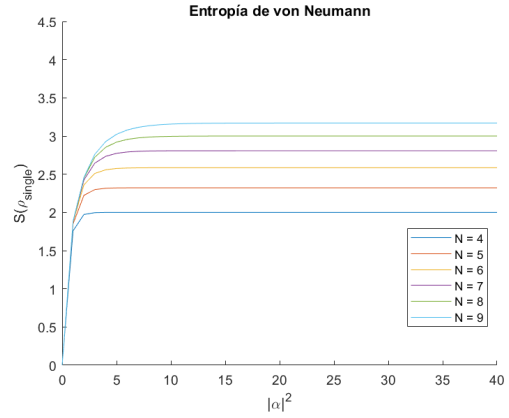


(o) $M = 15$ y $N = 16, \ldots, 20$.

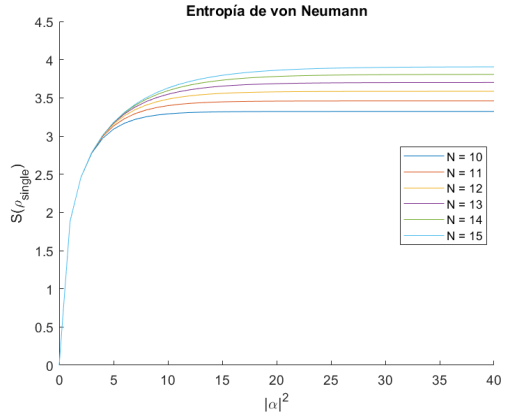
Figura 4.4: Probabilidad máxima de identificación sin ambigüedad de los estados coherentes componentes de $|\psi_{key}\rangle$, $\mathcal{P}_D^{(N)}$ (2.4.14).

4.4.5. Entropía de von Neumann de cada estado coherente de $|\psi_{key}\rangle$

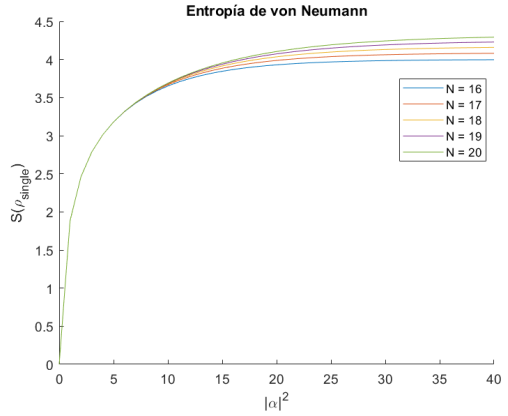
Por último, hemos representado la entropía de von Neumann de un estado coherente de la contraseña (3.3.17) en función de $|\alpha|^2$ para distintos N. Apreciemos que crece con la amplitud más lentamente cuanto mayor sea N, así como la tendencia a $\log_2 N$ deducida en (3.3.19).



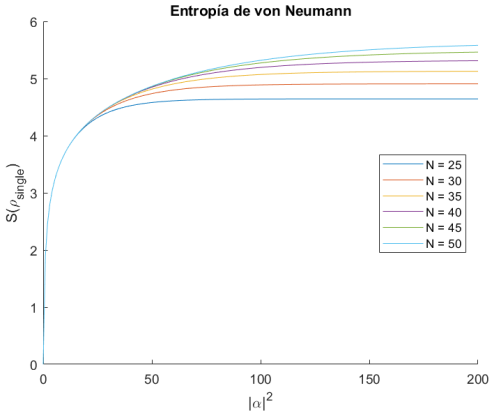
(a) $N = 4, \ldots, 9$.



(b) $N = 10, \ldots, 15$.



(c) $N = 16, \ldots, 20$.



(d) $N = 25, 30, \ldots, 50$.

Figura 4.5: Entropía de von Neumann de cada estado coherente de $|\psi_{key}\rangle$, $S(\rho_{single})$ (3.3.17).

4.4.6. Elección óptima de $|\alpha|$, N, M

Teniendo en cuenta todo lo anterior, estamos por fin en condiciones de extraer conclusiones generales acerca de la elección óptima de la amplitud $|\alpha|$, el número de estados N y la longitud de la contraseña M con el fin de garantizar la seguridad del protocolo propuesto.

En primer lugar, a partir de la Figura 4.1 deducimos que a mayor amplitud, mayor probabilidad de éxito en la comparación $\mathcal{P}_{\text{éxito, leg., M}}$ y esta crece más rápidamente cuanto mayor sea M. Respecto a la tendencia, se observa que en general, $\mathcal{P}_{\text{éxito, leg., M}} \longrightarrow 1$ para $|\alpha| > 2$, y la convergencia es más rápida cuanto mayor sea M. En consecuencia, nos conviene elegir M lo más alto posible porque nos permite escoger valores de $|\alpha|$ más bajos (que ya vimos que era lo recomendable tanto por razones prácticas como por el Teorema de no clonación 2.5.1 con los que obtener altas probabilidades de éxito.

Por otra parte, de la Figura 4.2 se deduce, de nuevo, que $\mathcal{P}_{\text{éxito, det., M}}$ crece con la amplitud y más rápido cuanto mayor sea M. En cuanto a la tendencia, se aprecia que para un determinado valor de $|\alpha|$ bajo y fijo, $\mathcal{P}_{\text{éxito, det., M}}$ decrece hacia un determinado valor a medida que aumenta N. En particular, si $|\alpha| > 1.4$ y $M > 5$ es obvio que $\mathcal{P}_{\text{éxito, det., M}} \longrightarrow 1$. Por tanto, nos interesa tomar M lo más alto posible por la misma razón que antes.

Analizando ahora la Figura 4.3, vemos que $\mathcal{P}_{superar}$ decrece hacia 0 con $|\alpha|$ y lo hace más rápido cuanto mayor sea M. Aún más notable es esto en la Figura 4.3b con valores $|\alpha| > \sqrt{2}$; de hecho, para $M > 1$ es despreciable. En consecuencia, concluimos de nuevo que nos conviene tomar M lo más alto posible porque permite escoger valores de la amplitud más bajos con los que lograr una probabilidad de superar el test por parte del atacante prácticamente nula.

En lo que respecta a la Figura 4.4, cabe destacar que la máxima probabilidad de discriminación sin ambigüedad decrece con la amplitud y lo hace más rápido cuanto mayor sea el número de estados. Esta velocidad de decrecimiento de $\mathcal{P}_D^{(N)}$ aumenta, además, con la longitud de la contraseña. En cuanto a la tendencia, para valores de la amplitud suficientemente altos siempre $\mathcal{P}_D^{(N)}$ converge hacia 1. No obstante, para valores de $|\alpha|$ suficientemente bajos y para un cierto M, existe un intervalo de valores de la amplitud en el que $\mathcal{P}_D^{(N)}$ es despreciable. Por tanto, confirmamos que nos interesa tomar N alto, así como $|\alpha|$ bajo y M también lo más alto

posible.

Por último, a la vista de la Figura 4.5 apreciamos la tendencia a $\log_2 N$ deducida en (3.3.19). Además, la entropía de von Neumann (que, recordemos, limita la información accesible) crece con la amplitud; pero este crecimiento es más lento cuanto mayor es N. Por tanto, esto cuadra con lo deducido hasta ahora acerca de la conveniencia de tomar valores de la amplitud bajos y del número de estados suficientemente altos. En particular, nos interesa buscar la región en que se cumpla $S(\rho_{single}) \ll \log_2 N$, tomando un $|\alpha|$ bajo y un N adecuado a partir de las gráficos.

Entonces, teniendo esto último en cuenta para elegir $|\alpha|$ y N adecuadamente de manera que se limite la información accesible de los estados y con la garantía de que tomando M suficientemente alto tendremos, para dichos $|\alpha|$ y N, $\mathcal{P}_{\text{éxito, leg., M}} \longrightarrow 1$, $\overline{\mathcal{P}}_{\text{éxito, det., M}} \longrightarrow 1$, $\mathcal{P}_D^{(N)} \longrightarrow 0$ y $\mathcal{P}_{superar} \longrightarrow 0$.

De esta forma, se seleccionan los valores de $|\alpha|$, N y M y a partir de ellos se debe ajustar, por un lado, la salida de la función a hash a utilizar teniendo en cuenta que $M \log_2 N \ll n$ (4.2.1), donde $n < k$ siendo k la longitud de $p\|r_i$; y, por otro lado, el número de veces T que se puede reutilizar la contraseña $|\psi\rangle_{key}$, pues $TS(\rho_{single}) \ll M \log_2 N$ (3.3.22). Así, la contraseña está protegida por su entropía, siendo segura incluso ante malas elecciones de p.

En definitiva, hemos visto que la M es un factor limitante y que cuanto mayor sea, mejor. Pero, por otro lado, esto aporta más información al atacante, así que la parte más complicada del proceso es escoger un M que acote como acabamos de exponer la entropía de von Neumann.

Concluimos que se puede garantizar la seguridad en la comunicación mediante este protocolo, siempre y cuando se elijan adecuadamente el conjunto de estados coherentes, la función hash, la contraseña $|\psi_{key}\rangle$ y el número de veces que se recicla, además de separar las comparaciones un tiempo prudencial.

4.5. Tratamiento no ideal

Hasta ahora hemos podido ver cómo tanto el protocolo propuesto como cualquier otro de seguridad con estados cuánticos son realizables experimentalmente con instrumentos ópticos sencillos y que se utilizan en la actualidad en numerosas aplicaciones, como son los divisores de haz, detectores, polarizadores, el láser o la fibra óptica. Sin embargo, hemos supuesto que son ideales y en la práctica esto no ocurre así, pues entran en juego la *eficiencia* de los detectores y el ruido, así como las *pérdidas* a través del canal, entre otros inconvenientes como las *medidas oscuras* que conllevan, por ejemplo, a que a día de hoy el problema de la distribución cuántica de claves a largas distancias esté aún abierto. Esto puede apreciarse con más detalle en algunas de las últimas propuestas más recientes [18], [69], [71] y [72], estando las dos últimas particularizadas al caso de estados coherentes. También existen otras complejas propuestas actuales centradas en solucionar el problema del ruido en el canal como [42] y [26]. Valgan estas citas como ejemplos del carácter puntero de esta tecnología cuántica y justificación de las limitaciones que nos impiden abordar con detalle el caso no ideal.

No obstante, sí que nos gustaría garantizar, en líneas generales, que nuestro particular protocolo con estados coherentes puede implementarse eficientemente en la realidad. Para ello, analizaremos algunos de los problemas que surgen al tratar el caso no ideal, tratando de demos-

trar que las fórmulas deducidas que garantizan la seguridad del protocolo se pueden modificar y adaptar para tenerlos en cuenta.

4.5.1. Eficiencia finita en los detectores y pérdidas

En primer lugar, caractericemos la *eficiencia* de los detectores η, que se define como la probabilidad de un fotodetector de detectar la presencia de un fotón, es decir $\eta \in [0,1]$ siendo $\eta = 1$ el caso ideal que tratábamos anteriormente. El efecto físico de la eficiencia es equivalente a una reducción de la amplitud del estado coherente en un factor $\sqrt{\eta}$. Entonces, para incluirlo en las fórmulas anteriores, basta multiplicar la amplitud de salida por un factor $\sqrt{\eta}$.

Por tanto, Alice y Bob pueden compensar este efecto incrementando el valor inicial de la amplitud de los estados elegidos: $\alpha \to \alpha/\sqrt{\eta}$. Es decir, no haría falta atenuar tanto la salida del láser que, en principio, produce altas amplitudes. En consecuencia, Alice y Bob no tendrían por qué preocuparse de la eficiencia de sus detectores, pero sí del que tenga Eve, ya que podría ser mejor. Concluimos que, para una mayor exactitud, en las fórmulas deducidas anteriormente debemos multiplicar las amplitudes de los estados coherentes de salida por un factor $\sqrt{\eta_{espía}}$, que representa la eficiencia del detector del atacante, y que podremos suponer que vale 1 en el peor de los casos.

Respecto a la pérdida que tiene lugar en el canal, es decir, la *atenuación* que se produce en la fibra óptica que ya explicamos en la Sección 2.5.4, podemos suponer por simplicidad que está también incluida en el término $\sqrt{\eta_{espía}}$. Recordemos que vimos también que la atenuación en comunicaciones clásicas se solventa mediante amplificadores y que esto no es posible en un escenario cuántico debido al Teorema de no clonación 2.5.1, motivo por el cual se investiga en la creación de repetidores cuánticos [44].

4.5.2. Medidas oscuras

Otro problema que podemos analizar es el del ruido entendido como la perturbación que causan los falsos clicks en los detectores, es decir, los que se producen aún cuando no inciden fotones. Esto se conoce también como medidas oscuras o *dark counts*. Generalmente los falsos clicks tienen origen térmico y, por tanto, pueden reducirse en gran medida mediante el uso de detectores refrigerados.

La probabilidad de que se produzca una cuenta oscura, $\mathcal{P}_{dark}$ es la probabilidad de que se produzca una detección condicionada a que no haya incidido ningún fotón:

$$\mathcal{P}_{dark} = \mathcal{P}(\text{“Click”}\,|\,\text{“No fotón”}).$$

Nos gustaría que estuviera acotada por una cantidad muy pequeña, $\varepsilon > 0$, es decir $\mathcal{P}_{dark} \leq \varepsilon$. Se ha demostrado en [49] que se pueden lograr valores tan bajos como $\mathcal{P}_{dark} \simeq 10^{-8}$. Sin embargo, estos resultados tan bajos se obtienen para fotodetectores que funcionan con superconductores y son de enorme tamaño, lo cual no nos interesa en la práctica; en nuestro caso, atendiendo las hojas de especificaciones de los detectores disponibles en los laboratorios, consideraremos $\mathcal{P}_{dark} \simeq 10^{-5}$. Para ajustarlo, debemos caracterizarlo experimentalmente tapando la entrada del detector y contando las medidas que se producen.

Entonces, la probabilidad de obtener una medida correcta ha de modificarse teniendo en cuenta que debe producirse a la vez que no haya habido una cuenta oscura. Es decir, las expresiones obtenidas relacionadas con la detección de fotones deben multiplicarse por un factor

$(1-\mathcal{P}_{dark})^M$, que será prácticamente 1 si logramos ajustar bien el sistema de forma que se minimice la probabilidad de falsos clicks.

Es posible además que también fallen alguno o ambos detectores, produciéndose una medida $(|0\rangle_2, |0\rangle_3)$. Esta probabilidad ya la hemos calculado en caso de que Alice y Bob sean legítimos (4.3.4), señalando que esta expresión también es válida si Eve atacara con un estado de amplitud $|\beta| \simeq |\alpha|$, cuando $|\alpha| > \sqrt{2}$. Si no estamos en este caso, hay que aplicar (4.3.4). No obstante, por las limitaciones de los dispositivos actualmente disponibles en los laboratorios de óptica integrada se requiere que para poder realizar detecciones correctamente, las amplitudes no sean tan bajas, en torno a $|\alpha|^2 = 5$ ó 10, por ejemplo. Para otros sistemas, $|\alpha|^2 = 20$ también podría ser interesante. Por tanto, nos basta considerar (4.3.3) para tener este efecto en cuenta; pasemos a compararlo con $\mathcal{P}_{dark}$. En la Figura 4.6 se ha representado $\mathcal{P}(|0\rangle_2, |0\rangle_3)$ a partir de la ecuación (4.3.4).

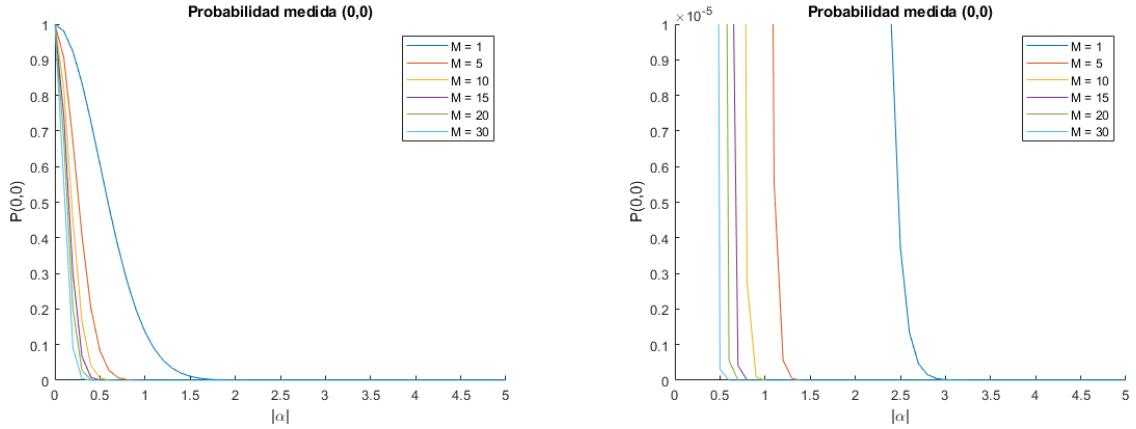


Figura 4.6: A la izquierda representación de $\mathcal{P}(|0\rangle_2, |0\rangle_3)$ calculada a partir de (4.3.4). A la derecha una ampliación de la gráfica de la izquierda para poder observar dónde $\mathcal{P}(|0\rangle_2, |0\rangle_3) \leq \mathcal{P}_{dark} \simeq 10^{-5}$.

Es evidente, por tanto, que en el caso que nos interesa en la práctica, $|\alpha|^2 = 5, 10$ ó 20, la probabilidad de que se obtenga una medida nula es despreciable para cualquier M, incluso es menor que la de que tenga lugar una cuenta oscura. En definitiva, si ajustamos correctamente el detector para que $\mathcal{P}_{dark} \simeq 10^{-5}$, podremos considerar despreciables ambos efectos.

En resumen, el test de comparación de estados coherentes tratándolo en el caso real puede producir los siguientes resultados, teniendo en cuenta que por test "positivo" consideramos que Alice y Bob hayan tenido éxito en su tarea, y recordando que en el puerto 3 del divisor de haz se obtiene la diferencia de las amplitudes de los estados incidentes:

- Test positivo: no hay click en el puerto 3 cuando los estados incidentes son iguales.
- Test negativo: puede producirse por dos razones.
  - Falso positivo: no hay click en el puerto 3 aún cuando inciden estados diferentes. Esto no lo consideraremos como tal ruido porque no es un fallo del detector si ocurre que sí que hay clicks en el detector 2, probabilidad que ya lo hemos cuantificado mediante (3.3.4). Pero, consideraremos un fallo posible en la práctica de los detectores el hecho de que no haya detecciones en ninguno de los casos, lo cual acabamos de ver que se calcula con (4.3.4).

- Falso negativo: hay click en el puerto 3 aún cuando los estados son iguales, es decir, tiene lugar una medida oscura cuya probabilidad $\mathcal{P}_{dark}$ ya hemos analizado.

Cabe mencionar que también existen otros problemas que surgen en la práctica aunque un análisis profundo de ellos se escapa de los objetivos del trabajo. Por ejemplo, el *tiempo muerto* del detector, es decir, el intervalo de tiempo que tiene lugar tras la detección de un fotón y en el cual no es posible detectar ningún otro. Esto limita el ritmo máximo de conteo. También hay que tener en cuenta la incertidumbre en la sincronización de los eventos de fotones registrados (*timing jitter*, del orden de cientos de picosegundos por detección de un fotón). Una forma de aliviar estos problemas es utilizar dispositivos de óptica integrada que permiten realizar detecciones convenientemente si utilizamos amplitudes como $|\alpha|^2 = 5, 10$ o 20. Igualmente, se caracterizan experimentalmente y deben incluirse en los cálculos para ajustarlos a la realidad.

En particular, podemos comprobar, finalmente, que con estos valores de la amplitud es posible garantizar la seguridad basándonos en los resultados ya expuestos. Si nos fijamos en las gráficas de la sección anterior y razonamos como hasta ahora, se puede comprobar que es posible elegir N y M adecuados. Más concretamente, si tomamos $M \geq 5$, basta escoger $N \geq 14$ si $|\alpha|^2 = 5$; $N \geq 18$ si $|\alpha|^2 = 10$; y $N \geq 35$ si $|\alpha|^2 = 20$. Respecto a la salida de la función hash en estos casos, recordemos que debe cumplir que $M \log_2 N \ll n$ (4.2.1) y esto es factible seleccionando el menor valor posible de N, pues suele ser $n = 128$ ó 256. Además, nótese que solamente ha hecho falta aumentar N e incluir una gráfica conteniendo valores mayores que 20 para el estudio de la entropía de von Neumann si $|\alpha|^2 = 20$ (Figura 4.5d), por lo que deducimos definitivamente que el protocolo propuesto es seguro y realizable con la tecnología actual.

Teniendo todo en cuenta, hemos incluido en nuestro desarrollo la posibilidad de que los detectores fallen cuando realizamos un tratamiento no ideal de nuestro protocolo, habiendo concluido que puede despreciarse si ajustamos convenientemente $\mathcal{P}_{dark}$ atendiendo a las especificaciones de los aparatos empleados, y tomando los siguientes valores de las amplitudes: $|\alpha|^2 = 5, 10$ o 20, las cuales también permiten una elección de N y M adecuada.

Conclusiones

A la vista de lo expuesto en este trabajo, es evidente que la Óptica Cuántica está íntimamente relacionada con la Teoría de la Información Cuántica. Por tanto, es un trabajo que entronca perfectamente con asignaturas del Grado en Física, especialmente Física Cuántica, Mecánica Cuántica y Óptica Cuántica, así como Electromagnetismo, Óptica y Mecánica Teórica, sobre todo a la hora de exponer los resultados previos.

Además, cabe destacar otras asignaturas de Matemáticas a cuyos conocimientos se ha debido recurrir, como son las relativas a Análisis Real y Complejo, Probabilidad y Estadística, además de Criptografía. Por último, es importante mencionar los conocimientos de manejo de programas informáticos de cálculo numérico y representación gráfica que se han proporcionado a lo largo de estos años de estudio y que han permitido obtener las conclusiones pertinentes.

Teniendo todo en cuenta, ha resultado fundamental la capacidad de razonamiento, planteamiento y resolución de problemas de forma rigurosa y abstracta que se ha adquirido a lo largo del Grado para adaptarse a emplear técnicas y resultados de otras ramas de la Ciencia que han intervenido, como la Teoría de la Información o las Comunicaciones.

En particular, se han aprovechado todos estos conocimientos para detallar un protocolo de comprobación de contraseñas con estados coherentes cuya seguridad se basa en las leyes de la Física, al contrario de lo que ocurre en Criptografía Clásica, donde se recurre a problemas matemáticos computacionalmente difíciles de resolver.

Suponiendo una comunicación completamente insegura y que los dos usuarios comparten una contraseña privada p de s bits, hemos demostrado cómo autenticar su identidad es posible generando a partir del hash de p y una cadena de bits aleatorios, una contraseña de estados coherentes simétricos que se comparan mediante un test que emplea un divisor de haz. El motivo de utilizar estados coherentes es que presentan numerosas ventajas frente a la generación y detección de fotones individuales que utilizan otros protocolos de seguridad existentes, como el BB84 [13] o en el que nos hemos inspirado, [29]. Además, el hecho de que sean simétricos permite obtener expresiones cerradas más sencillas y manejables, particularmente útiles para acotar la probabilidad de discriminación sin ambigüedad.

En resumen, suponiendo que es Alice quien demuestra su identidad a Bob (siendo el otro caso simétrico), los pasos a seguir que hemos propuesto se muestran en el diagrama de la Figura 1 y son:

1. Alice y Bob eligen una cadena aleatoria de t bits r_i tal que $s + t = k$, para lo cual pueden recurrir a realizar de forma independiente y alternada un test SWAP con estados ortogonales.

2. Utilizando una función hash $H : \{0,1\}^k \mapsto \{0,1\}^n$, $n < k$, computa cada uno por su cuenta $H(p\|r_i)$, que sabemos que introducirá suficiente aleatoriedad y solo dará el mismo valor si ambos usuarios son legítimos. Por tanto, se propone considerar $H(p\|r_i)$ como la representación binaria de las fases de los M estados coherentes simétricos $|\alpha_j\rangle = |\alpha_j|e^{i\phi_j}$, $j = 0, \ldots, N-1$ que compondrán la cadena de la contraseña $|\psi\rangle_{key}$ que tratan de generar aleatoriamente y comprobar. El hecho de que la fase se escoja al azar es fundamental porque, recordemos, la comunicación es completamente insegura y tanto $|\alpha|$ como N son públicos, además de conocerse qué dispositivos se emplean y cómo se ponen en funcionamiento.

3. Conociendo esta información, Alice y Bob podrán generar de forma independiente el correspondiente estado coherente, $|\alpha_j\rangle_A$ y $|\alpha_j\rangle_B$ respectivamente. Para ello deberán disponer de un láser y una refrencia de fase, así como de un modulador electroóptico.

4. Para llevar a cabo la tarea de comprobación en sí que demostrará si su identidad es legítima, Alice le envía a Bob el estado que ha generado y este lo compara con el suyo usando el test análogo al SWAP que hemos expuesto para estados coherentes mediante un divisor de haz.

5. Este procedimiento se debe realizar para los M estados que componen la cadena $|\psi\rangle_{key}$. Cualquier fallo se atribuye a un atacante y lleva a rechazar la contraseña.

Con el fin de garantizar la seguridad, hemos tratado de hacer frente a los dos posibles ataques, identificándolos con un modelo más intuitivo consistente en emplear una tarjeta de crédito como $|\psi\rangle_{key}$:

- Falsificar estados (análogamente, utilizar una tarjeta de crédito falsa para obtener dinero).
- Obtener información de la contraseña (mediante un cajero falso, leer la información de la tarjeta o colocar una antena cercana al cajero con el mismo fin).

Para evitar lo primero, se han demostrado varios resultados relativos a que un espía no podrá superar el test sea cual sea el estado con el que lo intente: un estado coherente de entre los N posibles, un estado cualquiera o el vacío, siendo, como vimos, este último el mejor y que en el modelo de la tarjeta de crédito, consistiría en no meter ninguna tarjeta en el cajero y conseguir sacar dinero. Por otro lado, para evitar el segundo ataque, hemos recurrido a las cotas de información accesible, a la entropía de von Neumann, a las medidas de discriminación sin ambigüedad y al Teorema de no clonación. Es decir, hemos buscado lograr:

- Éxito en la comparación de estados coherentes, tanto en el caso de que haya un atacante como en el caso de que no, permitiendo detectarlo.
- Baja probabilidad de identificación sin ambigüedad de estados coherentes, así como de clonación.
- Acotar la información accesible de los estados componentes de la cadena de la contraseña por debajo de la almacenada.

Además, hemos garantizado que la generación de $|\psi\rangle_{key}$ es aleatoria y que el número de veces que puede reciclarse también está acotado por dichos resultados, de manera que se logra basar la seguridad de $|\psi\rangle_{key}$ en su entropía y no en la dificultad de resolver algún problema matemático complejo como ocurre en Criptografía Clásica. Esto implica que esta contraseña es segura incluso aunque se hagan elecciones inadecuadas de p (por ejemplo, 12345, la fecha de

cumpleaños, etc.), pues una de las ventajas de usar estados cuánticos es que aunque un atacante los almacene solo puede acceder una vez a ellos, lo cual no ocurre en el caso clásico.

Teniendo todo en cuenta y tras haber realizado algunos experimentos numéricos cuyas gráficas hemos mostrado, concluimos que se puede garantizar la seguridad de este protocolo, siempre y cuando los estados coherentes, la función hash y el número de veces que se recicla la contraseña se elijan convenientemente.

Asimismo, se ha incluido el caso no ideal en que los detectores puedan producir medidas oscuras o ser ineficientes, lo cual equivale a una reducción de la amplitud en un factor η que hemos solventado poniéndonos en el peor de los casos en que Eve disponga de máxima eficiencia, es decir, $\eta = 1$. También hemos considerado el caso en que los valores de las amplitudes de los estados coherentes empleados son los que actualmente producen buenos resultados en las detecciones empleando elementos de óptica integrada.

En particular se han escogido las siguientes condiciones razonables:

- $M \geq 5$, siendo M la longitud de $|\psi\rangle_{key}$.
- Por limitaciones técnicas, $|\alpha|^2 = 5$ ó 10. En el primer caso, habría que escoger $N \geq 14$ y en el segundo, $N \geq 18$.
- La salida de la función hash n debe cumplir que $M \log_2 N \ll n$, lo cual es factible pues suele ser $n = 128$ ó $n = 256$. Esto determina también la longitud k de la concatenación $p\|r_i$, pues debe cumplirse que $n < k$.

  (Con estas dos elecciones se puede despreciar tanto la probabilidad de obtener medidas nulas en ambos detectores como la probabilidad de obtener medidas oscuras.)
- El número de veces T que puede reciclarse $|\psi\rangle_{key}$ debemos escogerlo de forma que se cumpla que $TS(\rho_{public}) \ll M \log_2 N$.
- Un tiempo de separación prudencial entre las comparaciones de estados coherentes con el fin de evitar la posibilidad (poco realista) de que el espía posea una memoria cuántica.

Con ello se ha demostrado que el protocolo propuesto, que generaliza las ideas de [29] y [6], es seguro incluso en la práctica y puede llevarse a cabo con la tecnología disponible a día de hoy.

Para finalizar indicar que a lo largo de este trabajo se espera haber dejado claros los conocimientos necesarios para poder comprender otros protocolos similares o futuros avances en este campo puesto que, a pesar de haber mencionado algunos de ellos, la activa investigación que se realiza al respecto imposibilita estar completamente actualizado. Asimismo, se espera haber despertado el interés por esta novedosa y puntera aplicación de la Física cuyo futuro resulta tan prometedor, así como invitar a la reflexión a este respecto.

Bibliografía

[1] L. Cohen, Generalized Phase-Space Distribution Functions, *J. Math. Phys.* **7**, 781–786 (1966).

[2] L. Cohen, Quantization problem and variational principle in the phase space formulation of quantum mechanics, *J. Math. Phys.* **17**, 1863–1866 (1966).

[3] U. Vazirani, *Quantum Computing, CS 294. Lecture 17: Quantum Random Access Codes and Aplications*, Berkeley University Lectures (2009).

[4] S. Aaronson, The limits of quantum, *Sci. Am.* **298**, 62–69 (2008).

[5] S. Al-Kuwari, J.H. Davenport, and R.J. Bradfor, Cryptographic hash functions: Recent design trends and security notions, *IACR Cryptology ePrint Archive* **565**, (2011).

[6] E. Andersson, M. Curty, and I. Jex, Experimentally realizable quantum comparison of coherent states and its applications, *Phys. Rev. A* **74**, 022304 (2006).

[7] F. Arute et al, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505–510 (2019).

[8] G. A. Barbosa, J. van de Graaf, P. Mateus, and N. Paunković, Quantum key distribution by phase flipping of coherent states of light, https://arxiv.org/abs/1609.07064 (2017).

[9] H. Barnum et al, Authentication of quantum messages, *Proceedings of The 43rd Annual IEEE Symposium on Foundations of Computer Science*, 449–458 (2002).

[10] D. J Barrett, R. E. Silverman, and R. G. Byrnes, *SSH, The Secure Shell: The Definitive Guide*, O'Reilly Media, 2nd edition (2005).

[11] A. Ben-Aroya, O. Regev, and R. de Wolf, A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs, *Foundations of Computer Science, Annual IEEE Symposiumon*, 477–486 (2008).

[12] C. H. Benett, Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* **68**, 3121–3124 (1992).

[13] C. H. Benett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (1984).

[14] N. Bloembergen, *Nonlinear Optics*, World Scientific Publishing (1996).

[15] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Quantum fingerprinting, *Phys. Rev. Lett.* **87**, 167902 (2001).

[16] G. S. Buller and R. J. Collins, Single-photon generation and detection, *Meas. Sci. Technol.* **21**, 012002 (2009).

[17] P. N. Butcher and D. Cotter, *The Elements of Nonlinear Optics*, Cambridge University Press (1990).

[18] Y. Cao, et al, Long-distance free-space measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **125**, 260503 (2020).

[19] A. Chefles, Unambiguous discrimination between linearly independent quantum states, *Phys. Lett. A* **239**, 339–347 (1998).

[20] A. Chefles and S. M. Barnett, Optimun unambiguous discrimination between linearly independent symmetric states, *Phys. Lett. A* **250**, 223–229 (1998).

[21] J.-P. Chen et al, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).

[22] D. Petz, Entropy, von Neumann and the von Neumann Entropy, in *John von Neumann and the Foundations of Quantum Physics*, M. Redei and M. Stoeltzner (Eds.), Springer (2001).

[23] I. Damgaard et al, Improving the security of quantum protocols via commit-and-open, in *Lecture Notes in Computer Science*, **677**, 408–427, Springer (2009).

[24] D. Dieks, Overlap and distinguishability of quantum states, *Phys. Lett. A* **126**, 303–306 (1988).

[25] D. P. DiVincenzo, The physical implementation of quantum computation, *Fortschr. Phys.* **48**, 771–783 (2000).

[26] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, Quantum key distribution overcoming extreme noise: Simultaneous subspace coding using high-dimensional entanglement, *Phys. Rev. Applied* **15**, 034003 (2021).

[27] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, Quantum identification system, *Phys. Rev. A* **60**, 149–156 (1999).

[28] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661–663 (1991).

[29] J. C. Garcia-Escartin and P. Chamorro-Posada, Simple quantum password checking, *Phys. Rev. A* **91**, 062310 (2015).

[30] C. Gerry, *Introductory Quantum Optics*, Cambridge University Press (2004).

[31] A. Ghatak and K. Thyagarajan, *Introduction to Fiber Optics*, Cambridge University Press (1998).

[32] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145–195 (2002).

[33] R. J. Glauber, The quantum theory of optical coherence, *Phys. Rev.* **130**, 2529–2539 (1963).

[34] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, *Probl. Inf. Transm.* **9**, 177–183 (1973).

[35] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Unambiguous quantum measurement of nonorthogonal states, *Phys. Rev. A* **54**, 3783–3789 (1996).

[36] I. D. Ivanovic, How to differentiate between non-orthogonal states, *Phys. Lett. A* **123**, 257–259 (1987).

[37] D. P. Jablon, Strong password-only authenticated key exchange, *ACM SIGCOMM Comput. Commun. Rev.* **26**, 5–26 (1996).

[38] J. R. Klauder and E. C. G. Sudarshan, *Fundamentals of Quantum Optics*, Dover (2006).

[39] C. Kollmitzer and M. Pivk, *Applied Quantum Cryptography*, Springer (2010).

[40] R. Landauer, Information is physical, *Phys. Today* **44**, 23–29 (1991).

[41] O. Lee and T. Vergoossen, An updated analysis of satellite quantum-key distribution missions, https://arxiv.org/abs/1909.13061 (2019).

[42] X.-H. Li, F-G. Deng, and H.-Y. Zhou, Efficient quantum key distribution over a collective noise channel, *Phys. Rev. A* **78**, 022321 (2008).

[43] X. Li and D. Zhang, Quantum information authentication using entangled states, in *International Conference on Digital Telecommunications*, 64 (2006).

[44] Z.-D. Li et al, Experimental quantum repeater without quantum memory, *Nat. Photonics* **13**, 644–648 (2019).

[45] D. Ljunggren, M. Bourennane, and A. Karlsson, Authority-based user authentication in quantum key distribution, *Phys. Rev. A* **62**, 022305 (2000).

[46] R. Loudon, *The Quantum Theory of Light*, Oxford University Press, 3rd edition (2000).

[47] X. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, Experimental generation of single photons via active multiplexing, *Phys. Rev. A* **83**, 043814 (2011).

[48] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University (1995).

[49] F. Marsili, et al, Detecting single infrared photons with 93 % system efficiency, *Nat. Photonics* **7**, 210–214 (2013).

[50] B.Y. Martínez Pérez, Modulación de coherencia óptica con dispositivos electro-ópticos con aplicaciones en detección de campos eléctricos, Proyecto Final, Universidad de las Américas Puebla (2012).

[51] P. W. Milonni and J. H. Eberly, *Laser Physics*, John Wiley & Sons (2008).

[52] R. Namiki and T. Hirano, Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection, *Phys. Rev. A* **74**, 032302 (2006).

[53] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in *Proc. of the 40th Annual Symposium on Foundations of Computer Science*, 477–486 (1999).

[54] NIST, *Report on Post-Quantum Cryptography*, NISTIR 8105 (2016). https://csrc.nist.gov/publications/detail/nistir/8105/final

[55] C. Palazuelos, *Introduction to Quantum Information Theory*, Semantic Scholar (2015).

[56] E. Pednault, J. Gunnels, D. Maslov, and J. Gambetta, *On "quantum supremacy"*, IBM research blog: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[57] M. Peev et al, The secoqc quantum key distribution network in Vienna, *New J. Phys.* **11**, 075001 (2009).

[58] A. Peres, How to differentiate between non-orthogonal states, *Phys. Lett. A* **128**, 19 (1988).

[59] IBM Research, *IBM quantum system one*, in https://www.research.ibm.com/quantum-computing/system-one/

[60] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining public key signatures and public key cryptosystems, *Commun. ACM* **21**, 120–126 (1978).

[61] O. Rosas-Ortiz, Coherent and squeezed states: introductory review of basic notions, properties and generalizations, in *Integrability, Supersymmetry and Coherent States. A Volume in Honor of Professor Veronique Hussin*, S. Kuru et al (Eds.), pages 187–230, Springer (2019).

[62] V. Scarani et al, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations, *Phys. Rev. Lett.* **92**, 057901 (2004).

[63] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Quantum cloning, *Rev. Mod. Phys.* **77**, 1225–1256 (2005).

[64] Defuse Security, *Salted password hashing-doing it right*, in https://crackstation.net/hashing-security.htm

[65] B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo, Quantum key distribution and quantum authentication based on entangled state, *Phys. Lett. A* **281**, 83–87 (2001).

[66] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26**, 1484–1509 (1997).

[67] Toshiba, *Toshiba qkd system*, in https://www.toshiba.co.jp/qkd/en/index.htm

[68] S. J. van Enk, Unambiguous state discrimination of coherent states with linea optics: Application to quantum cryptography, *Phys. Rev. A* **66**, 042313 (2002).

[69] B.-X. Wang et al, Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber, *Opt. Express* **28**, 12558–12565 (2020).

[70] S. Wiesner, Conjugate Coding, *SIGACT News* **15**, 78–88 (1983).

[71] F. Xu et al, Experimental quantum fingerprinting with weak coherent pulses, *Nat. Commun.* **6**, 8735 (2015).

[72] H.-L. Yin and Z.-B. Chen, Coherent-state-based twin-field quantum key distribution, *Sci. Rep.* **9**, 14918 (2019).

[73] A. Zaidi et al, *Mathematical modeling of hardware impairments*, in *5G Physical Layer*, by A. Zaidi et al (Eds.), pages 87–118, Academic Press (2018).

[74] B. Zygelman, *A First Introduction to Quantum Computing and Information*, Springer (2018).