Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Física

PRUEBA DE CONCEPTO DE CRIPTOGRAFÍA CUÁNTICA

Autor: Juan Marcos Arranz Díez
Tutores: Juan Carlos García Escartín y Luis Miguel Nieto Calzada
2022

Índice general

Abstract

The purpose of this work is to introduce the field of *quantum key distribution* through an experimental proof of concept, as well as its motivations and strong points against classical squemes. The BB84 protocol is described, illustrating the philosophy behind these cryptographic systems, as well as the COW protocol, from which a prototype is built in the laboratory. In spite of the simplicity of its configuration, the error rates found are acceptable and show the convenience of using this protocol in practice.

Resumen

El objetivo de este trabajo es presentar el campo de la *distribución cuántica de claves* a través de una prueba de concepto experimental, así como sus motivaciones y puntos fuertes frente a esquemas clásicos. Se describe el protocolo BB84, que ilustra la filosofía de estos sistemas criptográficos, así como el protocolo COW, del cual se construye un prototipo en el laboratorio. Pese a su sencilla configuración, las tasas de errores encontradas son aceptables y muestran la conveniencia de usar este protocolo en la práctica.

Introducción

A lo largo de la historia el ser humano ha sentido la necesidad de comunicarse de forma secreta, de lo cual existe pruebas que se remontan hasta la época de la Grecia clásica [19]. Sin embargo, no sería hasta el siglo XX cuando esta ciencia del cifrado de mensajes, la criptografía, sufriese un desarrollo inmenso frente a todas las técnicas utilizadas previamente durante siglos.

Con la llegada de técnicas modernas de análisis y de los ordenadores se descartaron los esquemas clásicos en codificación, basados en el desconocimiento de terceras personas tanto del mensaje cifrado como del algoritmo empleado para ello. Los protocolos de cifrado utilizados en la actualidad ya no se basan en la ocultación de los métodos, favoreciendo en su lugar aquellos modelos que, si se desconoce la clave criptográfica secreta que utilizan, son extremadamente difíciles de romper computacionalmente. Esto, sin embargo, podría cambiar en un futuro no muy lejano con la aparición de tecnologías como los ordenadores cuánticos capaces de resolver de forma eficiente algunos problemas, como puede ser la factorización en números primos, posible siguiendo el algoritmo descubierto en 1994 por Peter Shor [12, págs. 7-8].

Estos fallos de seguridad motivan la búsqueda de procesos para compartir claves que puedan garantizar la transmisión confidencial de información. La distribución cuántica de claves intenta satisfacer esta necesidad a través del uso de sistemas físicos que, debido a las limitaciones impuestas por las leyes de la Física, permitan compartir claves de forma secreta [2]. En la actualidad existen diversos protocolos de estas características, y aunque la seguridad de algunos de ellos está demostrada solamente bajo ciertas suposiciones, pueden llevarse a cabo en la práctica utilizando sistemas estándar de telecomunicaciones a través de fibra óptica.

Este trabajo pretende ser una introducción a la distribución cuántica de claves a través de la construcción de un prototipo experimental. En el Capítulo 1 se introduce el campo de la criptografía y se define el *qubit* o bit cuántico. También se demuestra el teorema de no clonación, que muestra la ventaja de utilizar sistemas cuánticos en lugar de clásicos. En el Capítulo 2 se exponen algunos mecanismos de generación y detección de fotones, que resultan esenciales para la implementación de protocolos de distribución cuántica de claves, dos de los cuales se desarrollan en el Capítulo 3. En el Capítulo 4 se describen los instrumentos y el montaje experimental utilizados en la prueba de concepto que motiva este trabajo y que, junto con los resultados mostrados en el Capítulo 5, componen la parte original del mismo. Por último, en el Capítulo 6 se resume el trabajo realizado y se exponen las conclusiones a las que se ha llegado.

Capítulo 1

Conceptos previos

1.1. Criptografía

La criptografía es el estudio y aplicación de técnicas para la comunicación de información de forma segura, a salvo de agentes externos que pretendan obtenerla o modificarla. Algunas de sus principales aplicaciones [7] son:

- Confidencialidad: garantizar que solamente el emisor y el receptor pueden leer el mensaje.
- Autenticación: el proceso de demostrar la identidad de uno mismo.
- Integridad: asegurar que el mensaje recibido por el receptor no ha sido alterado respecto al original.
- No repudio: un mecanismo para probar que efectivamente el emisor envió el mensaje.
- Intercambio de claves: un método para compartir claves criptográficas entre emisor y receptor.

El proceso de comunicación comienza con el mensaje legible o *texto en claro*, que se somete a un proceso de *cifrado* y que normalmente requiere de una *clave*. El resultado, el *texto cifrado*, se transmite al receptor que vuelve a convertir el mensaje en texto en claro mediante el proceso de *descifrado*. El proceso de cifrado y descifrado es particular para cada protocolo criptográfico y clave criptográfica utilizada.

Es práctica habitual referirse al emisor y receptor por los nombres *Alicia* y *Bob* respectivamente. En el caso de que exista un espía, un agente que intenta conocer el mensaje transmitido, utilizaremos para él el nombre de *Eva*.

Existen varias formas de clasificar los distintos algoritmos criptográficos; la siguiente es una de ellas:

- Criptografía de cifrado simétrico: utiliza una única clave para el cifrado y descifrado. Se emplea principalmente para garantizar privacidad y confidencialidad. Alicia y Bob aplican la misma clave para convertir el texto en claro en cifrado y volverlo a transformar en texto en claro. Para esta configuración tanto Alicia como Bob

deben conocer la clave, que debe ser secreta: el mayor problema surge entonces de la distribución de esta.

Un ejemplo interesante es el de la "libreta de un solo uso" (*one-time pad* en inglés). Con este sistema Alicia cifra su mensaje, una cadena de bits, con una clave generada aleatoriamente de la misma longitud que el mensaje de la siguiente forma: para cada bit m_n del mensaje se toma el bit k_n de la clave y se suman, $s_n \equiv m_n + k_n \mod 2$. El mensaje cifrado $\{s_n\}_{n=1}^{N}$ se envía a Bob, que resta la clave bit a bit para recuperar el mensaje original. Este sistema criptográfico posee, teóricamente, seguridad perfecta en términos de teoría de la información [15]; en particular, el conocimiento del texto cifrado no ofrece información adicional sobre el contenido del texto en claro. Sin embargo, la necesidad de que la clave tenga la misma longitud que el mensaje hace que su uso no sea práctico.

- Criptografía de clave pública o cifrado asimétrico: utiliza una clave para el cifrado y otra clave para el descifrado. Se usan comúnmente para autentificación, no repudio e intercambio de claves. La seguridad de este tipo de cifrados se basa en la complejidad de ciertas *funciones de un solo sentido*: es fácil calcular $f(x)$ dada la variable x, pero obtener x conocido $f(x)$ es difícil. Por *difícil* se quiere decir que el tiempo necesario para realizar la operación aumenta con el número de bits en la entrada x de forma exponencial en lugar de polinómica.

  Uno de los cifrados más conocidos dentro de esta clasificación, y también uno de los primeros, es el cifrado RSA. Si Bob quiere recibir un mensaje cifrado con un sistema de clave pública, debe elegir primero una clave *privada*, que mantiene oculta, y con ella genera una clave *pública*, que muestra a terceros. Si Alicia quiere comunicarse con Bob, usará la clave pública anunciada para cifrar su mensaje y Bob utilizará su clave privada para descifrarlo. En particular, el cifrado RSA se basa en la dificultad computacional para realizar la factorización de grandes números enteros en sus factores primos. Puede entenderse esta *asimetría* de la siguiente manera: considérense los dos números primos 94999 y 100103. Para un humano es fácil calcular $94999 \times 100103 = 9509684897$; de forma similar, saber que 94999 es un factor de 9509684897 permite encontrar con facilidad el otro factor primo. Esto cambia cuando sólo se conoce el valor de 9509684897 y quiere hallarse su descomposición, una tarea mucho más compleja. Lo mismo ocurre para un ordenador: para órdenes de magnitud mucho mayores no existe, hasta la fecha, un algoritmo capaz de factorizar "en poco tiempo" un número entero. Esta falta de algoritmos rápidos es la que motiva su uso; a diferencia del *one-time pad*, no existe ninguna demostración acerca de su seguridad.

- Funciones resumen o extracto (*hash functions*): consiste en la utilización de funciones matemáticas para generar un valor *hash* de longitud fija basado en el texto en claro de forma que no se pueda determinar ni el contenido ni la longitud original de este. Suelen emplearse para crear una huella digital del contenido de un archivo para probar que no ha sido modificado por terceros. Un ejemplo de este tipo de sistemas es el *Secure Hash Algorithm* o *SHA*.

1.2. El *bit* y el *qubit*

El *bit* clásico es el concepto fundamental dentro de la computación clásica y la teoría de la información. Un bit posee dos estados, 0 y 1, y puede examinarse para determinar en qué estado se encuentra el bit. De forma análoga se define el *bit cuántico* o *qubit* (*quantum bit*), donde los estados 0 y 1 se sustituyen por dos estados cuánticos $|0\rangle$ y $|1\rangle$, elegidos de tal modo que sean ortonormales y formen una base de estados (por ejemplo, en un sistema cuántico de dos estados). Una de las principales diferencias entre el bit clásico y el qubit es que este último puede encontrarse en una superposición lineal de estados,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{bmatrix}1\\0\end{bmatrix} + \beta \begin{bmatrix}0\\1\end{bmatrix}, \quad \text{con } \alpha, \beta \in \mathbb{C} \text{ y } |\alpha|^2 + |\beta|^2 = 1.$$

Debido a esto, existe una cantidad infinita de estados accesibles para el qubit. Sin embargo, a diferencia de un bit clásico no es posible determinar el estado cuántico de un qubit desconocido, es decir, no pueden hallarse α y β.

En Mecánica Cuántica una medida está representada por un observable: un operador lineal hermítico. Aquí basta con considerar la pareja de operadores de medición

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \quad M_1 = |1\rangle\langle 1| = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}. \tag{1.1}$$

La probabilidades de encontrar el qubit en el estado $|0\rangle$ ó $|1\rangle$ son, respectivamente,

$$P(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \begin{bmatrix}\alpha^* & \beta^*\end{bmatrix} \begin{bmatrix}\alpha\\0\end{bmatrix} = \alpha^*\alpha = |\alpha|^2, \quad P(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = |\beta|^2$$

y el estado del sistema tras la medida será

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}},$$

que en este caso será el estado $|0\rangle$ si $m = 0$ y $|1\rangle$ si $m = 1$. Más adelante aparecerá también la base formada por los kets

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

para los cuales se tienen los operadores

$$M_+ = |+\rangle\langle +| = \frac{1}{2}\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}, \quad M_- = |-\rangle\langle -| = \frac{1}{2}\begin{bmatrix}1 & -1\\-1 & 1\end{bmatrix}. \tag{1.2}$$

De la misma forma que pueden tenerse varios bits clásicos, también es posible disponer de varios qubits. Para dos bits existen cuatro posibles estados: 00, 01, 10 y 11. En el caso de dos qubits se realiza un producto tensorial para obtener una base de estados formada por cuatro elementos, $|00\rangle, |01\rangle, |10\rangle$ y $|11\rangle$, de forma que el estado del sistema de dos qubits puede escribirse como combinación lineal de estos cuatro elementos[1].

[1] Existen estados que no pueden escribirse como producto tensorial de estados de qubits individuales, pero estos no resultan relevantes dentro de este trabajo.

1.3. El teorema de no clonación

El estado de un sistema de qubits (o un sistema regido por la Mecánica Cuántica) queda modificado tras un proceso de medición, lo cual impide que, en general, pueda volver a recuperarse o llegar a conocer toda la información necesaria para describir su estado inicial. Sin embargo, es posible actuar de forma reversible sobre un sistema mediante la aplicación de un operador unitario U. Como $U^\dagger U = \mathbb{1}$, la aplicación consecutiva de estos operadores revierte el sistema a su estado original.

Teniendo en cuenta lo anterior, cabe preguntarse si es posible realizar una copia de un estado cuántico desconocido. En el caso clásico la respuesta es afirmativa: es posible interceptar información clásica, es decir, en forma de bits clásicos. Estos bits se pueden examinar o copiar y reenviarlos sin modificar la información original. En el caso cuántico, en cambio, esto resulta ser imposible, lo cual elimina una importante vía de posible espionaje si se utiliza un sistema cuántico para transmitir información.

Se presenta a continuación una demostración elemental de este resultado [12, *Box* 12.1]. Para ello se considera un sistema A, que se encuentra en un estado puro $|\psi\rangle$ y que quiere copiarse en un sistema B, inicialmente en un estado puro $|s\rangle$, ambos normalizados. En conjunto se tiene un estado inicial

$$|\psi\rangle \otimes |s\rangle \,.$$

Imagínese que mediante la aplicación de algún operador unitario U se puede realizar la copia, de forma que

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \,,$$

y que esto ocurre para dos estados puros concretos $|\psi\rangle$ y $|\chi\rangle$, es decir,

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \quad \text{y} \quad U\left(|\chi\rangle \otimes |s\rangle\right) = |\chi\rangle \otimes |\chi\rangle \,. \tag{1.3}$$

Realizando el producto interno de las dos ecuaciones en (1.3) se obtiene

$$(\langle\psi| \otimes \langle s|)U^\dagger U(|\chi\rangle \otimes |s\rangle) = \langle\psi|\chi\rangle \langle s|s\rangle = \langle\psi|\chi\rangle \tag{1.4}$$

$$(\langle\psi| \otimes \langle\psi|)(|\chi\rangle \otimes |\chi\rangle) = \langle\psi|\chi\rangle^2 \tag{1.5}$$

y considerando la igualdad de (1.4) y (1.5), se tiene que

$$\langle\psi|\chi\rangle = \langle\psi|\chi\rangle^2 \,.$$

Ahora bien, la ecuación $x^2 = x$ sólo tiene dos soluciones, $x = 0$ y $x = 1$, lo cual quiere decir que o bien $|\psi\rangle = |\chi\rangle$ o bien $|\psi\rangle$ y $|\chi\rangle$ son ortogonales. Esto implica que un dispositivo de copia solamente es capaz de clonar estados ortogonales y por lo tanto no puede existir un dispositivo de copia de un sistema cuántico en general. De hecho, si se trabajase con dos estados perfectamente ortogonales la situación coincidiría con un límite clásico, pero la posibilidad de trabajar con combinaciones lineales de estos dos estados es la que separa el caso clásico del cuántico.

Capítulo 2

Generación y detección de fotones

La generación y detección de fotones resultan ser esenciales dentro de la distribución cuántica de claves. El fotón individual permite codificar con facilidad un qubit considerando como bases ortogonales a las formadas por dos polarizaciones perpendiculares del mismo. Mientras que el desarrollo tecnológico de los detectores de fotones individuales ha avanzado lo suficiente como para que estos se encuentren disponibles comercialmente, los emisores de fotones individuales existentes no resultan viables en la práctica; en general se prefiere usar pulsos de láser atenuados, algo mucho más sencillo de conseguir con la tecnología del presente [1]. En este capítulo se describirán estos pulsos de láser, así como una clase particular de detector de fotones, ambos empleados en la realización experimental de este trabajo.

2.1. Pulsos de láser atenuados

La luz emitida por un láser se encuentra en un estado coherente de la radiación [10], que es de la forma

$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{2.1}$$

Los estados coherentes $|\alpha\rangle$ son autoestados del operador aniquilación a con autovalor α, que recibe el nombre de amplitud y se corresponde con la amplitud compleja del campo electromagnético clásico; los estados $|n\rangle$ son los llamados estados de Fock, autoestados del hamiltoniano cuántico de radiación donde n representa el número de fotones existente. Un estado coherente no contiene un único fotón, sino que su número de fotones sigue una distribución de Poisson de parámetro $\mu := |\alpha|^2$. La probabilidad de que un estado del tipo (2.1) tenga n fotones[1] es de

$$P(n, \mu) = |\langle n|\alpha\rangle|^2 = \frac{\mathrm{e}^{-\mu}\mu^n}{n!}. \tag{2.2}$$

En particular, tanto el valor medio como la varianza del número de fotones n tienen valor igual a μ, por lo que este parámetro recibe aquí el significado de número medio de

[1] Esta es la probabilidad de que al medir el número de fotones de un estado coherente se obtenga el resultado n; no debe confundirse con la probabilidad de que un pulso contenga n fotones, pues este número no está definido para los estados coherentes.

fotones. Cabe destacar también que $P(0,\mu) = \mathrm{e}^{-\mu} \neq 0$, es decir, la probabilidad de no detectar ningún fotón en un estado coherente es mayor que cero.

En lo que sigue se considerarán estados coherentes que representen a pulsos láser con una misma duración finita T, de forma que la amplitud puede escribirse como $\alpha = \lambda T$ para cierta tasa de generación de fotones por segundo λ y permite dar a $\mu = |\alpha|^2$ el significado de número medio de fotones esperados dentro del pulso.

Puesto que los pulsos láser se emplean como sustitutos de estados con un único fotón, es deseable que el número medio de fotones sea lo más pequeño posible (en particular se busca que $\mu < 1$). Resulta interesante considerar la probabilidad de que un pulso no vacío esté formado por más de un fotón, que se corresponde con

$$P(n > 1 \mid n > 0, \mu) = \frac{1 - \mathrm{e}^{-\mu}(1+\mu)}{1 - \mathrm{e}^{-\mu}}. \tag{2.3}$$

Para obtener pulsos láser con estas características pueden emplearse, por ejemplo, un láser en modo de onda continua junto con un modulador de intensidad, que convertirá la señal óptica en pulsos, y un atenuador que reduzca la intensidad y con ella el número medio de fotones de cada uno de los pulsos. Esta configuración fue la recreada en la parte experimental del presente trabajo, como se expondrá en el Capítulo 4.

2.2. Detección de fotones

Existen diferentes tipos de detectores de fotones, desde tubos fotomultiplicadores a los basados en materiales superconductores que operan a temperaturas de unos pocos Kelvin. Aquí solamente se describirá el principio físico detrás del detector utilizado en los experimentos: el fotodiodo de avalancha (*avalanche photodiode*, APD) [1].

Los detectores APD están compuestos por semiconductores en una unión p-n operando en un modo de polarización inversa. Cuando el campo eléctrico en la unión es lo suficientemente intenso como para superar el potencial umbral de ruptura, un portador en la capa de conducción puede adquirir la energía cinética necesaria para crear nuevas parejas electrón-hueco. Los portadores liberados en esta ionización por impacto podrá a su vez crear más parejas electrón-hueco, provocando así una avalancha de portadores de carga. Un ejemplo de este mecanismo puede verse en la Figura 2.1.

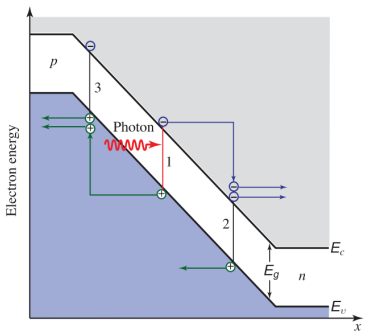

Figura 2.1: Esquema del proceso de multiplicación de portadores en una unión convencional [13].

En estas condiciones, un portador individual generado por la absorción de un fotón es capaz de generar el proceso de avalancha, de forma que la corriente resultante crece hasta un valor de saturación. Es por eso que estos detectores funcionan de forma binaria, ya que la corriente generada no depende del número de fotones recibidos. Cuando el semiconductor se encuentra en este modo de operación, también llamado modo Geiger, actúa como un contador de fotones y se denomina diodo de avalancha de fotones individuales o SPAD (*single-photon avalanche diode*).

Para cuantificar el funcionamiento de un contador de fotones se estudian diferentes parámetros que caracterizan su funcionamiento y sus limitaciones:

- El **rango espectral** en el que el contador puede detectar fotones dependerá tanto de la clase de detector como del material que lo compone. La energía de un fotón debe ser mayor que la energía de *gap* E_g que separa las bandas de valencia y de conducción del semiconductor para así poder crear una pareja electrón-hueco. El detector aquí empleado está constituido por el semiconductor InGaAs, que sitúa el rango espectral de longitudes de onda entre los 900 y 1700 nm.
- El **tiempo muerto** o de recuperación es el intervalo temporal que sigue a la absorción de un fotón y durante el cual el detector no es capaz de registrar la llegada de otros fotones. En ocasiones los causantes de un mayor tiempo muerto serán los componentes electrónicos involucrados en la detección y no el material semiconductor. Pese a todo esto, es una práctica común aumentar el tiempo muerto para este tipo de contadores, lo que permite evitar pulsos secundarios que puedan provocar detecciones ficticias.
- La **tasa de cuentas oscuras** de un contador es el número de detecciones falsas o erróneas por unidad de tiempo, debidas tanto a ruido externo al detector o a las propiedades y defectos del material. Suele considerarse como cuenta oscura todo evento de detección que no se deba a un fotón, siendo una de sus causas principales la excitación térmica de un portador.
- La **eficiencia de detección** η es la probabilidad de registrar una cuenta cuando un fotón llega al detector. Una eficiencia alta es a veces deseable, pero utilizar un valor menor puede ayudar a reducir la cantidad de ruido y de cuentas oscuras.
- La **fluctuación del retardo** es la variación del tiempo transcurrido entre la absorción de un fotón y la generación de un pulso eléctrico por parte del detector. Esta variación debe ser lo más pequeña posible para poder registrar un evento de detección en la ventana temporal que le corresponde.

Más allá de estos parámetros existe otra característica del funcionamiento de los detectores SPAD: el mecanismo de **extinción** de avalanchas

Para poder detectar otro fotón resulta necesario extinguir la avalancha de portadores y devolver el contador a un estado en el que pueda detectar fotones. Esto se logra reduciendo el potencial de polarización por debajo del umbral para más adelante devolverlo al nivel de operación original. Existen dos formas principales de lograr este reinicio: la primera es un modo de detección continua (*free-running*) que realiza la extinción cuando se detecta un aumento en la corriente producida por una avalancha; la segunda es el llamado *modo puerta*, que consiste en elevar el potencial por encima del umbral de ruptura sólo cuando se espera un fotón y de la que se darán más detalles en la Subsección 4.1.6.

Capítulo 3

Distribución cuántica de claves (QKD)

La distribución cuántica de claves, también conocida por sus siglas en inglés, QKD (*quantum key distribution*) es el principal ámbito de desarrollo del campo de la criptografía cuántica. Su objetivo no es la utilización de un canal o sistema cuántico para la transmisión de información, sino para el intercambio de una serie aleatoria de bits, es decir, una clave. La Mecánica Cuántica permite determinar si un agente externo ha podido interceptar esta clave y, en el caso de poder asegurar que esta clave es realmente secreta, puede emplearse dentro de un canal clásico para transmitir información de manera segura. En general, un protocolo de distribución cuántica tiene tres elementos esenciales:

- Un **canal privado**, cuántico y no seguro para la distribución de una clave. La información enviada a través de este canal se realiza mediante algún sistema cuántico, por ejemplo un qubit, en un estado particular. Si un agente externo quiere conocer lo que ocurre dentro de este canal deberá medir estos sistemas, que se verán modificados por el propio acto de medición. Cada protocolo de QKD debe utilizar un conjunto de sistemas y estados cuánticos que permitan detectar la presencia de terceras personas, la cual puede determinarse, por ejemplo, a partir de un aumento inevitable en la tasa de errores que solamente puede deberse a esta presencia.
- Un **canal público**, clásico y autenticado. Este canal es utilizado por Alicia y Bob para intercambiar información y verificar la integridad de la clave intercambiada por el canal cuántico. No es necesaria privacidad en este punto, pero sí es esencial la autenticación de las identidades de emisor y receptor para evitar ataques de tipo "hombre en el medio"[1] (*man-in-the-middle*).
- Un **generador de números aleatorios** para evitar cualquier tipo de sesgo a la hora de la creación de la clave.

En las secciones que siguen se describirán dos protocolos de distribución cuántica de claves. El primero de ellos, llamado BB84, permitirá ilustrar todas las etapas de las que consta un proceso de distribución cuántica de claves. El segundo, el protocolo COW, es

[1] En este tipo de ataques Eva finge ser Bob ante Alicia y viceversa, enviando a cada uno de ellos la información que ella desee y haciéndoles creer que están comunicándose de forma secreta.

más sencillo de configurar experimentalmente y es el objeto principal de estudio de este trabajo. El capítulo termina analizando algunos posibles ataques a estos protocolos.

3.1. El protocolo BB84

El protocolo BB84, ideado por Charles H. Bennett y Gilles Brassard en 1984 y a los que debe su nombre, fue el primer protocolo diseñado para la distribución cuántica de claves y se basa en los siguientes cuatro estados de un qubit:

$$|1\rangle\,, \quad |0\rangle\,, \quad |+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Denominamos base X a la formada por $|0\rangle$ y $|1\rangle$, y base Z a la formada por $|+\rangle$ y $|-\rangle$ (estos dos kets son claramente ortogonales). Resulta útil asociar estos cuatro estados con orientaciones particulares de la polarización de un único fotón, el cual se usa habitualmente como representante de un qubit. Así, elegido un eje de coordenadas, los kets $|0\rangle$ y $|1\rangle$ se identifican con polarizaciones de 0 ($\leftrightarrow$) y $\frac{\pi}{2}$ ($\updownarrow$) respectivamente, mientras que $|+\rangle$ y $|-\rangle$ se corresponden con $\frac{\pi}{4}$ ($\swarrow\!\!\nearrow$) y $\frac{3\pi}{4}$ ($\nwarrow\!\!\searrow$).

La elección de estas bases se debe a lo siguiente: si un qubit se mide con la base incorrecta, el estado tras la medida podrá ser uno de los elementos de la base utilizada con la misma probabilidad e independientemente del valor original. Si, por ejemplo, Alicia decide enviar un qubit en un estado $|0\rangle$ y Eva decide medir con la base Z, es decir, con los operadores descritos en (1.2), la probabilidad de encontrar un estado $|+\rangle$ o $|-\rangle$ es la misma:

$$P(+ \mid 0) = \langle 0|M_+^\dagger M_+|0\rangle = \frac{1}{2} = \langle 0|M_-^\dagger M_-|0\rangle = P(- \mid 0).$$

En este caso, Eva ha fallado al intentar obtener información sobre el qubit enviado por Alicia y ha modificado su estado, que ahora pertenece a una base distinta a la elegida por Alicia. Posteriormente, Alicia y Bob podrán de esta forma detectar y determinar la presencia de un espía.

El protocolo consta de varias etapas descritas a continuación; en la Tabla 3.2 se encuentra un ejemplo con cada de una de estas fases.

3.1.1. Transmisión de fotones

El protocolo comienza con Alicia como emisor y Bob como receptor en cada lado del canal cuántico. Alicia escoge de forma aleatoria e independiente dos cadenas de bits clásicos de longitud m. La primera cadena será la *clave en bruto*, que representa el valor de los bits que enviará a Bob, mientras que los bits de la segunda cadena indicarán la base a elegir para cada bit. Ambos deben compartir una asignación particular con la que Alicia envía los fotones a Bob, como la mostrada en la Tabla 3.1.

Con la ayuda de polarizadores lineales Alicia es capaz de preparar los qubits eligiendo la polarización de sus fotones de acuerdo con la asignación acordada. Por su parte, Bob elige otra cadena aleatoria de bits de longitud m para sus elecciones de base, con las que medirá cada fotón que reciba. Tras la medida, Bob mantiene en secreto los resultados que ha obtenido, que en general no coincidirán con los enviados por Alicia: en un caso

		Bit	
		0	1
Base	0 (X)	$\|0\rangle$	$\|1\rangle$
	1 (Z)	$\|+\rangle$	$\|-\rangle$

Tabla 3.1: Ejemplo de asignación de bits con las bases y los estados de un qubit.

ideal los bits correctos serán aproximadamente un 50 % del total, pero la cantidad será menor debido a fallos en el sistema, ruido en los detectores, la presencia de Eva, etc.

3.1.2. Discusión pública

Tras la intercambio cuántico de bits, Alicia y Bob deben hablar a través del canal público **autenticado** para decidir cómo tratar los bits que posee cada uno. Toda comunicación aquí realizada debe estar autenticada, por ejemplo siguiendo el esquema de Wegman-Carter [18]. Para la autenticación es sin embargo necesario que Alicia y Bob tengan una clave secreta compartida que hayan intercambiado fuera del protocolo QKD. Pueden "hacer crecer" esta clave tanto como quieran a partir de los bits intercambiados, pero la clave inicial es indispensable.

La discusión comienza con un proceso de **cribado** (*sifting*). Alicia desconoce qué fotones ha conseguido detectar Bob, ya que debido a las pérdidas y fallos del sistema solamente una pequeña fracción de los fotones enviados se detectan en el laboratorio de Bob. Es por esto que Bob anuncia a través del canal público en qué instantes ha recibido un fotón y qué base ha utilizado para medirlos, pero no los resultados de la medida. Conocida esta información, Alicia puede descartar los bits que Bob no haya recibido o que haya medido en la base incorrecta, y comunica esto último a Bob, que hace lo propio con su clave. Con esto termina la fase de cribado y tanto Alicia como Bob comparten una clave secreta, la llamada clave cribada, la cual puede contener errores.

La siguiente fase es la de **reconciliación**, que se divide en dos grandes partes. La primera es la estimación de la proporción de errores en la clave cribada. Un cálculo sencillo de esta proporción suele realizarse comparando un subconjunto de bits elegidos aleatoriamente. Alicia y Bob comparan esta cadena de cierta longitud r y comprueban el número de errores e, obteniendo así una probabilidad estimada de errores de

$$p = \frac{e}{r}.$$

Los bits usados para esta comprobación deben hacerse públicos, por lo que deben ser desechados. En el caso de que p supere cierto umbral $p_{\text{máx}}$, ya se deba a ruido en el canal o a la presencia de Eva, la clave cribada es descartada y el protocolo comienza de nuevo, esta vez en un canal cuántico diferente. El umbral puede tomarse, por ejemplo, con valor $p_{\text{máx}} = 0{,}11$ [8, pág. 31].

La segunda parte de la reconciliación consiste en la corrección de errores. Las diferencias entre las claves cribadas de Alicia y Bob se deben a la *tasa de error de bit cuántico* o QBER del canal. El valor del QBER, p, es la probabilidad de que un bit recibido por Bob haya cambiado respecto al bit enviado por Alicia, de forma que si la clave cribada tiene longitud n, el número de errores promedio es de np. El objetivo de esta fase es

corregir los errores en la clave de Bob sin revelar tanta información como para que Eva pueda reconstruir la clave. La descripción de estas técnicas de reconciliación exceden el objetivo de este trabajo y pueden consultarse en [8, págs. 33-39]. El último paso a realizar consiste en la **amplificación de privadad**, que tiene por finalidad la obtención de información compartida y secreta a partir de un cuerpo mayor de información que es parcialmente secreta.

Transmisión cuántica														
Bits aleatorios de Alicia	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Bases aleatorias de envío	X	Z	X	X	X	X	X	Z	Z	X	Z	Z	Z	X
Fotones enviados por Alicia	↕	↖↘	↔	↕	↕	↔	↔	↖↘	↗↙	↕	↖↘	↗↙	↗↙	↕
Bases aleatorias de medida	Z	Z	X	X	Z	Z	X	Z	X	Z	Z	Z	Z	X
Bits detectados por Bob		1		1	0	0	0		1	1	1		0	1
Discusión pública														
Bob anuncia las bases para bits recibidos		Z		X	Z	Z	X		X	Z	Z		Z	X
Alicia señala las bases correctas		OK		OK			OK				OK		OK	OK
Clave cribada		1		1			0				1		0	1
Bob revela bits elegidos aleatoriamente				1									0	
Alice los confirma				OK									OK	
Resultado														
Bits secretos restantes		1					0				1			1

Tabla 3.2: Ejemplo de intercambio de clave mediante el protocolo BB84.

Con la ayuda del ejemplo que aparece en la Tabla 3.2 puede resumirse todo el protocolo en unas pocas líneas:

1. Alicia genera aleatoriamente una sucesión de bits y de bases de polarización.
2. Alicia envía a Bob los fotones con la orientación que marcan sus bits y bases elegidas.
3. Bob elige aleatoriamente las bases con las que medirá los fotones entrantes.
4. Bob detecta algunos de los fotones enviados por Alicia; aquellos que no consigue detectar se han dejado en blanco dentro de la Tabla.
5. Bob anuncia las bases con las que ha medido los bits detectados.
6. Alicia señala qué bits han sido medidos con la base correcta.
7. El resultado es la clave cribada. Para comprobar la presencia de un atacante Bob puede, por ejemplo, revelar algunos de sus bits para que Alicia los compruebe.
8. Tras aplicar las técnicas oportunas Alicia y Bob comparten una cadena de bits secretos.

3.2. El protocolo COW

El protocolo *coherent one-way* (COW) busca ser un sistema de QKD con una fácil implementación en la práctica [17]. Para ello, los bits secretos se obtendrán a partir de una medición lo más sencilla posible: el tiempo de llegada de un pulso láser. La seguridad se obtendrá midiendo la coherencia cuántica entre ciertos pulsos, pues se atribuirá la pérdida de esta coherencia a la presencia de Eva al intentar ganar información sobre los

bits compartidos. Por último, la configuración será simple gracias al uso de un número reducido de elementos estándar de telecomunicaciones: la fuente de señal será un láser atenuado viajando a través de fibra óptica y los bits estarán codificados en intervalos de tiempo, que no se verán afectados por efectos de polarización de la fibra. A continuación se describirá cada una de las partes del sistema, que quedan resumidas en el esquema de la Figura 3.1.

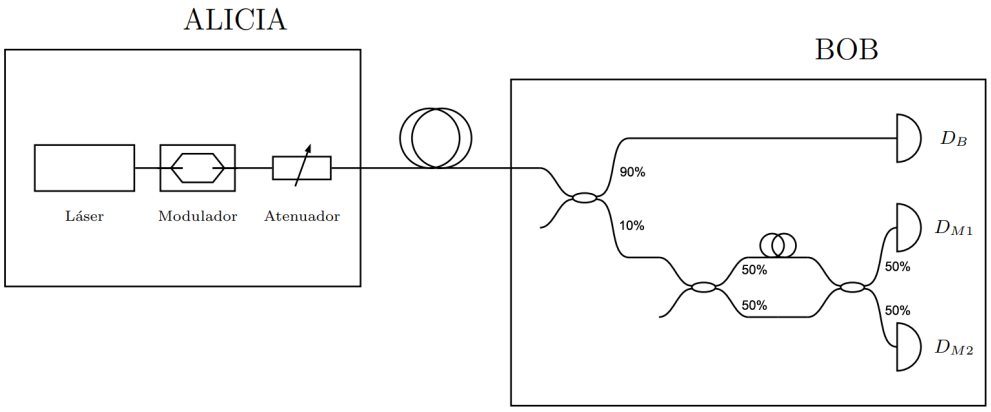

Figura 3.1: Esquema experimental del protocolo COW. Alicia emite pulsos modulados y atenuados que Bob dirige hacia uno de dos bloques: uno destinado a la obtención del tiempo de llegada de los pulsos (arriba) y otro formado por un interferómetro de monitorización para determinar la presencia de terceras personas (abajo).

3.2.1. Fuente de fotones

Para enviar el valor de un bit clásico Alicia envía dos pulsos de láser consecutivos: si el bit número k tiene valor 0 ó 1 se enviará, respectivamente, una de las siguientes parejas de pulsos:

$$|0_A\rangle = |\sqrt{\mu}e^{i\varphi_{2k-1}}\rangle_{2k-1}\,|0\rangle_{2k}\,, \tag{3.1}$$

$$|1_A\rangle = |0\rangle_{2k-1}\,|\sqrt{\mu}e^{i\varphi_{2k}}\rangle_{2k}\,. \tag{3.2}$$

Los estados $|0_A\rangle$ y $|1_A\rangle$ representan una pareja de pulsos enviados en dos instantes temporales distintos, $2k-1$ y $2k$, separados por un tiempo bien definido τ. Si el bit k tiene un valor 0, en el instante $2k-1$ se envía un pulso coherente con amplitud $\alpha = \sqrt{\mu}e^{i\varphi_{2k-1}}$, donde μ es el número medio de fotones del pulso y φ_{2k-1} es la fase del láser en ese momento; y un pulso vacío en el instante $2k$. Para el bit con valor 1 la situación es al revés: en el instante $2k-1$ se "envía" un pulso vacío y en el instante $2k$ un pulso coherente con amplitud $\alpha = \sqrt{\mu}e^{i\varphi_{2k}}$. En la Figura 3.2 puede verse un ejemplo de envío de pulsos láser.

La separación entre dos pulsos siempre estará dada por el valor τ, sin importar si los pulsos pertenecen a la misma pareja o no, es decir, la distancia temporal entre $2k-1$ y $2k$ es la misma que entre $2k$ y $2k+1$.

Para μ pequeños el producto $\langle 0_A|1_A\rangle$ es grande debido a la componente de vacío de radiación: de la expresión de un estado coherente (2.1) se veía que el coeficiente del

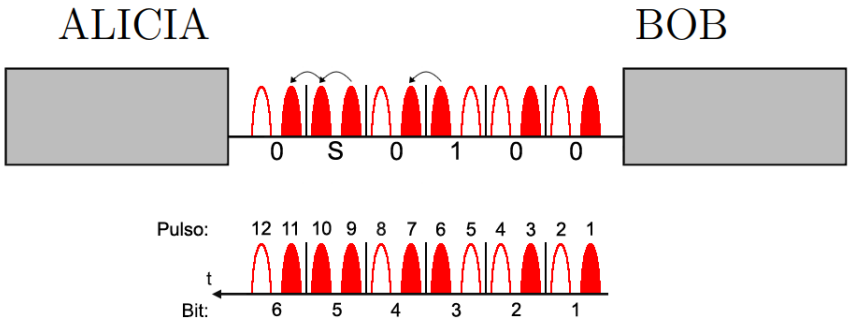

Figura 3.2: Ejemplo de envío de pulsos entre Alicia y Bob. La cadena de bits se lee de derecha a izquierda (0010S0), pues la pareja que está más a la derecha ha sido la primera en enviarse. Las flechas indican la coherencia entre dos pulsos. S hace referencia a una secuencia señuelo (Subsección 3.3.2).

estado con 0 fotones, $|0\rangle$, era no nulo. Además, gracias a que el láser opera de forma continua existirá coherencia de fase entre dos pulsos consecutivos no vacíos. Esto último será de particular interés cuando se envíen de manera consecutiva un bit 1 y un bit 0: en este caso habrá una coherencia entre el segundo pulso del bit 1 y el primero del bit 0, una coherencia de fase *a través de la separación de bits*:

$$|\sqrt{\mu}e^{i\varphi_{2k}}\rangle_{2k}\,|\sqrt{\mu}e^{i\varphi_{2k+1}}\rangle_{2k+1}\,.$$

Ya que dos pulsos vecinos pueden considerarse en fase para este sistema y solo será relevante la coherencia entre dos pulsos consecutivos, se tiene que $\varphi_j = \varphi_{j+1}$ y sin pérdida de generalidad se tomará $\varphi_j = 0$ para todos los pulsos.

3.2.2. Canal cuántico

Las parejas de pulsos se envían a Bob a través de un canal cuántico, normalmente formado por fibra óptica y caracterizado por una transmisión $t = 10^{-(\beta d+c)/10}$, siendo d la longitud del canal, β las pérdidas por unidad de longitud medidas en dB y c las pérdidas debidas a elementos que no dependen de la longitud del canal, como podrían ser conectores de fibra, también en dB. Es en este punto donde Eva podría intentar atacar el sistema, intentando ganar información de los fotones enviados antes de que los reciba Bob.

Los fotones que consigan atravesar el canal cuántico llegarán entonces a Bob. Este separará los pulsos con un acoplador no equilibrado, de forma que una proporción t_B se dirigirá a la línea de datos en la que Bob determinará si una pareja de pulsos se corresponde con un bit 0 o un bit 1 y una proporción $1 - t_B$ irán a través de la línea de monitorización, donde Bob buscará evidencia de la posible presencia de Eva.

3.2.3. Línea de datos

Los pulsos que se reciban por esta línea serán empleados para formar la clave en bruto. Para determinar el valor del bit, Bob debe distinguir dos estados no ortogonales

en su detector D_B:

$$|0_B\rangle = |\alpha\rangle_{2k-1} |0\rangle_{2k} ,$$

$$|1_B\rangle = |0\rangle_{2k-1} |\alpha\rangle_{2k}$$

donde $\alpha = \sqrt{\mu t t_B}$ es la nueva amplitud de los pulsos coherentes recibidos por Bob; el número medio de fotones de estos pulsos será $|\alpha|^2 = \mu t t_B$. En el caso de considerar un detector de fotones real con una eficiencia η, la amplitud pasa a ser $\alpha = \sqrt{\mu t t_B \eta}$.

Los dos estados que Bob puede observar, $|0_B\rangle$ y $|1_B\rangle$, no son ortogonales ya que $\langle 0_B|1_B\rangle = (\langle\alpha|0\rangle)_{2k-1} \cdot (\langle 0|\alpha\rangle)_{2k} = |\langle 0|\alpha\rangle|^2 = \mathrm{e}^{-|\alpha|^2}$, que es precisamente la probabilidad de no encontrar ningún fotón en un pulso. Esta probabilidad es no nula, por lo que aun poseyendo un detector perfecto no siempre es posible distinguir entre los dos estados. A esto debe sumarse posibles detecciones erróneas que ocurran en el detector de Bob y que podrían conllevar registrar un bit 0 cuando Alicia envió un bit 1, y viceversa. Es en estos términos que se define la QBER de este protocolo: la tasa de error de bit cuántico será la probabilidad de observar un bit distinto al enviado.

En el comienzo de la etapa de discusión pública (como se describió para el protocolo BB84, Sección 3.1) Bob anunciará estos resultados a Alicia para que pueda comenzar la fase de cribado.

3.2.4. Línea de monitorización

La proporción $1 - t_B$ de los pulsos que viajen por esta línea servirá para monitorizar la presencia de Eva. La línea de monitorización consta de un interferómetro y de dos detectores, D_{M1} y D_{M2}, que permitirán detectar una posible ruptura en la coherencia cuántica existente entre pulsos.

Sea α_j la amplitud del j-ésimo pulso que llega al interferómetro; este pulso puede pertenecer a la pareja de pulsos que representan un bit 0 o un bit 1. El valor de cada uno de estas amplitudes puede ser 0 ó $\sqrt{\mu t(1-t_B)\eta}$. En el caso de que dos pulsos consecutivos sean no nulos se tendrá la igualdad $\alpha_j = \alpha_{j+1}$.

La diferencia entre el brazo largo y el brazo corto del interferómetro es tal que a la salida se hace coincidir un pulso con el siguiente: el pulso j "recorre" el camino largo en el mismo tiempo que el pulso $j+1$ alcanza el final del camino corto, produciéndose así interferencias entre dos pulsos consecutivos. Tras atravesar el interferómetro, los pulsos que llegan a los detectores en el instante $j+1$ tienen amplitudes (calculadas en la Subsección 4.1.4)

$$|D_{M1}\rangle = \left| i\frac{\alpha_j + \alpha_{j+1}}{2} \right\rangle, \tag{3.3}$$

$$|D_{M2}\rangle = \left| \frac{-\alpha_j + \alpha_{j+1}}{2} \right\rangle. \tag{3.4}$$

Si resulta que uno de α_j ó α_{j+1} es cero, entonces $|D_{M1}|^2 = |D_{M2}|^2 = \frac{1}{2}\mu t(1-t_B)\eta$, o lo que es lo mismo, si un fotón entra en la línea de monitorización la probabilidad de encontrarlo en cada detector es la misma. Si en cambio resulta que α_j y α_{j+1} son ambos no nulos, entonces $|D_{M1}|^2 = \mu t(1-t_B)$ y $|D_{M2}|^2 = 0$, es decir, sólo uno de los detectores

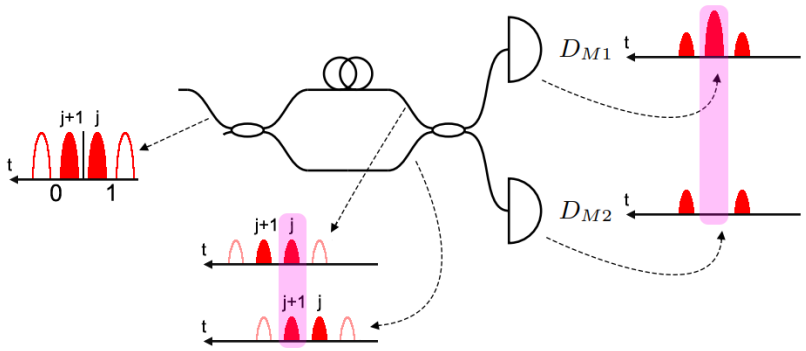

Figura 3.3: Ejemplo de interferencia entre el segundo pulso de un bit 1, denotado por j, y el primer pulso de un bit 0, denotado por $j+1$. Las flechas discontinuas indican qué señales hay en cada punto del interferómetro.

puede activarse. Este último caso es el representado en la Figura 3.3. Bob también debe anunciar en qué instantes el detector D_{M2} ha registrado un fotón.

Explicados cada uno de los elementos del sistema, el protocolo consiste de las siguientes etapas:

1. Alicia envía una serie de parejas de pulsos que correspondan a un bit o un bit 1 con igual probabilidad.
2. Tras el intercambio, Bob revela para qué bits ha obtenido detecciones en la línea de datos y cuándo el detector D_{M2} de la línea de monitorización ha registrado una cuenta.
3. Analizando las detecciones en D_{M2} Alicia puede estimar la ruptura de la coherencia gracias a la visibilidad asociada a los bits consecutivos 1-0 y calcula la información que Eva puede poseer.
4. Alicia y Bob realizan técnicas de corrección de errores y amplificación de privacidad para obtener una clave secreta.

3.3. Ataques a los protocolos QKD

El objetivo principal de la distribución cuántica de claves es poder protegerse de ataques externos a la seguridad de un intercambio de claves. Para poder afirmar que un protocolo es seguro se debe considerar que un espía no está limitado por las restricciones debidas a los instrumentos o tecnología disponibles en la actualidad, sino que su única limitación son las leyes de la física.

Existen dos clases generales de ataque que Eva puede realizar: los individuales se basan en la interacción con cada señal enviada por Alicia de forma separada, mientras que los colectivos tienen en cuenta una posible acción conjunta sobre el conjunto de señales interceptadas. Suele considerarse que Eva dispone para todas las señales de un sistema auxiliar o *ancilla* que interactúa con ellas. Estos sistemas conservan su estado en el tiempo y se deja que las señales viajen hasta Bob. Una vez que la fase de intercambio

de información ha terminado, Eva es capaz de utilizar lo que aprenda a partir de la discusión pública para realizar las mediciones óptimas sobre sus *ancillae*.

En esta sección sólo se tratará un tipo concreto de ataque, el llamado ataque por separación del número de fotones (*photon number splitting attack*, PNS) y se presentará una posible defensa ante ellos.

3.3.1. Ataque al protocolo BB84

Uno de los problemas principales de seguridad que sufre el protocolo BB84 es el uso en la práctica de pulsos de láser atenuados en lugar de fotones individuales. Si se trabaja con pulsos atenuados con número medio de fotones μ, la tasa de detección bruta de Bob [14](la probabilidad de que detecte un fotón por pulso enviado por Alicia) es

$$R_{\text{bruto}} = \sum_{n \geq 1} P(n, \mu)(1 - (1 - t\eta)^n) \approx t\eta\mu, \tag{3.5}$$

donde $(1 - (1 - t\eta)^n)$ es la probabilidad de que Bob detecte un fotón en la presencia de n fotones. La aproximación válida si $tn\eta P(n, \mu) << 1$ para todo n, lo que ocurre para pulsos atenuados $\mu < 1$.

Si Eva está restringida únicamente por las leyes de la Física, un ataque por separación del número de fotones es posible:

1. Eva cuenta el número de fotones mediante una medida cuántica no destructiva (*quantum non-demolition measurement*, QND). En esta clase de ataques el sistema a medir se acopla con otro sistema auxiliar a través de una interacción adecuada. Gracias a esta interacción los sistemas ganan correlación cuántica, de forma que el estado global será una superposición de los estados de ambos sistemas: un estado entrelazado. Estas correlaciones se mantienen de separar los sistemas. Tras la medida apropiada (y destructiva) del estado del sistema auxiliar, el resultado obtenido permite predecir en qué estado se encontrará el sistema a medir [4].

2. Si un pulso contiene un único fotón este será bloqueado, mientras que si tiene más de uno, Eva guarda un fotón en una memoria cuántica y transmite el resto a Bob a través de un canal sin pérdidas, es decir, con $t = 1$.

3. Eva espera hasta que Alicia y Bob realicen su discusión pública sobre las bases empleadas y mide los fotones correspondientes en su memoria cuántica.

Este ataque garantiza información completa acerca de la clave compartida, que ya no será secreta, y sin haber introducido error alguno en el lado de Bob.

La única restricción que Eva puede encontrarse es que debe evitar revelar su presencia; en particular, debe asegurarse de que la tasa R_{bruto} que recibe Bob no cambie: debe asegurarse de producir las mismas pérdidas que Bob se esperaría si los pulsos llegasen por el canal con pérdidas que le conecta con Alicia. Esto conlleva que el ataque PNS se debe realizar en todos los pulsos solamente cuando las pérdidas esperadas por Bob debidas a la fibra sean iguales que las introducidas por Eva al guardar y bloquear fotones. Esto ocurre cuando la transmisión t de la fibra del canal cuántico es lo suficientemente

pequeña [14] como para que

$$t\eta\mu \approx R_{bruto} \leq R^*_{bruto} = \sum_{n\geq 2} \frac{\mathrm{e}^{-\mu}\mu^n}{n!}(1-(1-\eta)^{n-1}) \approx \eta p_2. \tag{3.6}$$

Existen diferentes formas de defenderse contra este tipo de ataque. Una opción es considerar el uso de estados señuelo, creados intencionadamente con un número medio de fotones mayor, μ_s. Como Eva no podrá distinguir cuándo un pulso tiene dos o más fotones a causa de ser un señuelo o un pulso normal, Alicia y Bob pueden estudiar la distribución de estas detecciones y así determinar la presencia de Eva [9].

Otra posible solución es modificar el protocolo y utilizar el llamado SARG04, propuesto por primera vez en [14]. La diferencia frente al protocolo BB84 ocurre durante la fase clásica de cribado: Alicia no revela la base que ha utilizado, sino que anuncia públicamente una de cuatro parejas de estados no ortogonales $\mathcal{A}_{a,b} = \{|a\rangle, |b\rangle\}$ donde $|a\rangle$ pertenece a la base X, $\{|0\rangle, |1\rangle\}$ y $|b\rangle$ a la base Z, $\{|+\rangle, |-\rangle\}$, de forma que uno de los elementos de la pareja sea el estado del qubit que ha enviado. Sólo Alicia conoce qué base ha utilizado para preparar el estado: esta será la información secreta que quiere compartir con Bob: la base X será el bit 0 y la base Z será el bit 1. Bob sabe los dos estados posibles del qubit y si su medida es compatible solamente con uno de ellos, el bit será valido y anuncia este hecho; pero si la medida es compatible con ambos estados el bit es descartado. Para ilustrar mejor este protocolo puede considerarse el siguiente ejemplo:

1. Alicia envía un qubit en el estado $|0\rangle$ y anuncia la pareja $\mathcal{A}_{0,+} = \{|0\rangle, |+\rangle\}$.
2. Si Bob mide en la base X obtendrá el resultado $|0\rangle$. Sin embargo, puesto que $\langle 0|+\rangle = \frac{1}{\sqrt{2}} \neq 0$, este resultado es compatible con el estado $|+\rangle$ y Bob no puede distinguir con seguridad entre los dos.
3. Si Bob mide en la base Z puede obtener los dos resultados $|+\rangle$ y $|-\rangle$ con la misma probabilidad. Si la medida es $|+\rangle$ el resultado es de nuevo compatible con ambos elementos de $\mathcal{A}_{0,+}$, luego debe ser descartado. Sin embargo, si el resultado es $|-\rangle$, como $\langle +|-\rangle = 0$ el estado inicial solo puede haber sido $|0\rangle$. En este caso Bob anuncia que ha podido distinguir entre los dos estados, y con ello conoce el bit secreto enviado por Alicia.

Este protocolo requiere el mismo material que el BB84, y aunque esto reduce los bits compartidos a un 25 % frente al 50 % del BB84, su seguridad ante ataques de tipo PNS es demostrablemente mayor [14].

3.3.2. Ataque al protocolo COW

En la práctica debe tenerse en cuenta que un interferómetro no es perfecto. Su visibilidad se define como

$$V = \frac{p(D_{M1}) - p(D_{M2})}{p(D_{M1}) + p(D_{M2})}, \tag{3.7}$$

donde $p(D_{Mj})$ es la probabilidad de que el detector D_{Mj} se active en un instante en el que solamente D_{M1} debería activarse. Este valor será en la práctica $V < 1$, por lo que la probabilidad de que el detector D_{M2} se active cuando no deba (dos pulsos consecutivos

no vacíos) será de $\frac{1-V}{2}$ [3]. Al estar Eva limitada solamente por las leyes de la Física, puede aprovecharse de este hecho si, por ejemplo, se debe a una fase $\varphi_j \neq 0$ en el interferómetro. Ella podrá corregir sistemáticamente este error desplazando los pulsos y reproducir el valor de V añadiendo errores de una forma que le resulte beneficiosa.

La descripción del protocolo COW dada hasta ahora también lo deja expuesto ante ataques del tipo PNS: Eva puede contar los fotones en un pulso sin romper la coherencia entre dos pulsos consecutivos que pertenezcan a bits distintos, lo que no produciría errores en la línea de monitorización y le permitiría obtener prácticamente toda la información compartida – conocería todos los pulsos enviados por Alicia pero no los instantes en que Bob no detecta un fotón o tiene una cuenta oscura.

Para evitar este tipo de ataque se emplean las llamadas secuencias señuelo. La idea es la siguiente: con probabilidad f Alicia envía los pulsos $2k-1$ y $2k$ no vacíos, es decir, envía la pareja de pulsos

$$|S_A\rangle = |\sqrt{\mu}\mathrm{e}^{i\varphi_{2k-1}}\rangle_{2k-1}\,|\sqrt{\mu}\mathrm{e}^{i\varphi_{2k}}\rangle_{2k}\,.$$

Esta pareja de pulsos señuelo no representa ningún bit, de forma que si es detectado en la línea de datos se descartará durante la discusión pública. Sin embargo, si se detecta en la línea de monitorización en el instante $2k$, entonces debe detectarse solamente en D_{M1} debido a la coherencia (véase la Figura 3.3). Eva no puede pasar ahora desapercibida: si ataca de forma coherente entre bits distintos rompe la coherencia de las secuencias señuelo; si lo hace dentro de un mismo bit, entonces rompe la coherencia entre bits consecutivos; y finalmente, si ataca en un gran número de pulsos, rompe la coherencia en menos posiciones pero obtiene mucha menos información.

Para estimar cuantitativamente la cantidad de bits que Eva conoce, en teoría de la información se utiliza la llamada *información mutua* [12, Capítulo 11] entre Alicia y Eva, la cual aquí no puede presentarse formalmente pero podría tomarse como el valor [16]

$$I_{AE} = \mu(1-t) + (1-V)\frac{1+\mathrm{e}^{-\mu t}}{2\mathrm{e}^{-\mu t}}.$$

El nuevo resumen del protocolo COW junto con las secuencias señuelo es:

1. Alicia envía una serie de parejas de pulsos, que pueden ser los correspondientes a un bit 0 o a un bit 1 con una probabilidad de $\frac{1-f}{2}$ cada uno, o una secuencia señuelo con probabilidad f.

2. Tras el intercambio, Bob revela para qué bits ha obtenido detecciones en la línea de datos y cuándo el detector D_{M2} de la línea de monitorización ha registrado una cuenta.

3. Alicia le dice a Bob qué detecciones debe eliminar de su línea de datos, pues algunas se deberán a las secuencias señuelo.

4. Analizando las detecciones en D_{M2} Alicia puede estimar la ruptura de la coherencia gracias a la visibilidad asociada a los bits consecutivos 1-0 y las secuencias señuelo (en general el valor de V será distinto) y calcula la información que Eva puede poseer.

5. Alicia y Bob realizan técnicas de corrección de errores y amplificación de privacidad para obtener una clave secreta.

Capítulo 4

Descripción experimental

En este capítulo comienza la parte original de este trabajo. Aquí se presentan los instrumentos empleados en la construcción de la prueba de concepto del protocolo COW y se describe el montaje experimental realizado. Desafortunadamente, las limitaciones del material disponible no permitieron implementar la línea de monitorización debido a una muy baja visibilidad en el interferómetro, como se comentará en los siguientes apartados.

4.1. Instrumentos

4.1.1. Generador de funciones y osciloscopio

Con el generador de funciones WS8352 de *Tabor Electronics* se editaron y generaron los pulsos eléctricos para la modulación del láser de acuerdo con las señales del protocolo COW y para la sincronización con los periodos de detección del contador de fotones.

Para la visualización de estos pulsos eléctricos se utilizó el osciloscopio de muestreo PicoScope 9200A de *Pico Technology*, capaz de medir señales periódicas de muy alta frecuencia (hasta 10 GHz) y con alta resolución temporal. Las señales de los pulsos de modulación para el bit 0 y el bit 1 pueden verse en la Figura 4.1.

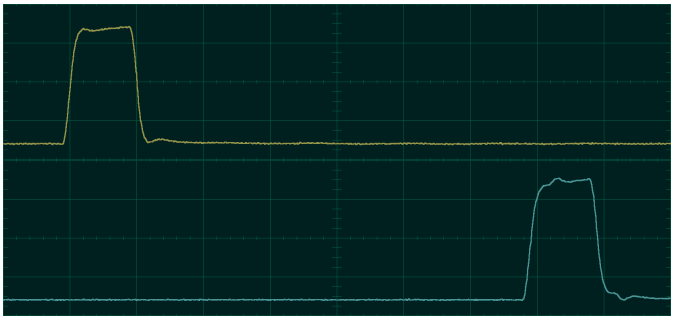

Figura 4.1: Pulsos eléctricos utilizados en la modulación, atenuados a la mitad de su amplitud para su visualización en el osciloscopio: arriba el pulso para el bit 0 (amarillo) y abajo el pulso para el bit 1 (azul). Las divisiones horizontales son de 5 ns y las verticales de 300 mV. El trazado de los pulsos ha sido ensanchado posteriormente para una mejor visualización.

4.1.2. Fibra óptica

La fibra óptica es una guía de ondas dieléctrica con forma cilíndrica y construida con un material con pérdidas bajas, como el óxido de silicio SiO_2 [6, págs. 70-75]. Tiene un núcleo central por el que se guía la luz envuelto por un revestimiento con índice de refracción ligeramente menor (Figura 4.2). Como guía de onda, la luz solamente puede propagarse siguiendo ciertos modos, soluciones de las ecuaciones de Maxwell. Cada uno de estos modos tiene una velocidad de grupo diferente, lo que lleva a causar una dispersión y un ensanchamiento en los pulsos de luz que viajan por la fibra. Para reducir esto se trabaja con fibra monomodo, que tiene un diámetro de núcleo suficientemente pequeño como para que solamente un modo pueda propagarse por ella a la longitud de onda de trabajo.

La fibra óptica utilizada, llamada SMF-28, presenta valores típicos de atenuación de 0,2 dB/km para la longitud de onda de trabajo [5]. Se usaron tramos de 2 y 10 km, así como dos latiguillos de 1 m. La atenuaciones observadas para 2 y 10 km fueron de 1,45 y 2,95 dB respectivamente. Las pérdidas a través de estas fibras ópticas serían de $0{,}2 \cdot 2 = 0{,}4$ dB y de $0{,}2 \cdot 10 = 2$ dB, atribuyéndose las atenuaciones adicionales de aproximadamente 1 dB a las conexiones entre los distintos instrumentos, que son independientes de la longitud de la fibra.

4.1.3. Acoplador 3-dB

Cuando dos guías de onda están lo suficientemente cerca, la luz puede acoplarse desde una de ellas a la otra; los detalles pueden encontrarse en [13, págs. 378-383]. Esto permite la transmisión de potencia óptica entre ambas guías, siendo una de sus aplicaciones la de acoplador En particular, un acoplador con dos puertos de entrada y dos de salida, llamado acoplador 2×2 o 3-dB, se fabrica de forma que las señales en sus puertos de entrada 1 y 2 y en sus puertos de salida 1' y 2' (Figura 4.2) siguen la relación

$$\begin{bmatrix} E_1' \\ E_2' \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & e^{i\pi/2} \\ e^{i\pi/2} & 1 \end{bmatrix} \begin{bmatrix} E_1 \\ E_2 \end{bmatrix}. \tag{4.1}$$

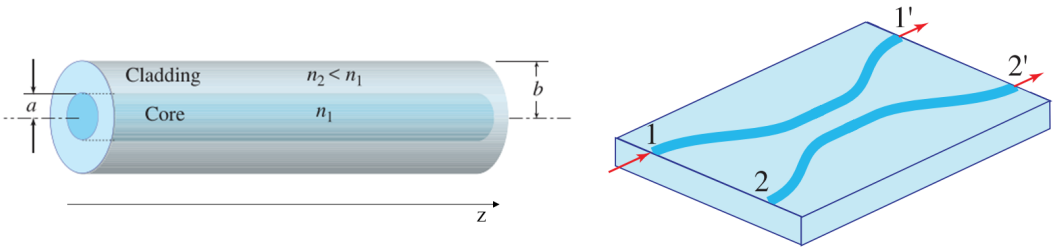

Figura 4.2: A la izquierda, representación de la estructura de un tramo de fibra óptica; la luz viaja en la dirección del eje de propagación z. A la derecha, un acoplador 3-dB [13].

4.1.4. Interferómetro

Es posible construir un interferómetro a partir de dos acopladores 3-dB. Aunque los siguientes cálculos son clásicos, los resultados siguen siendo válidos para estados

coherentes: basta con sustituir la amplitud de campo eléctrico por la amplitud de estos y las expresiones siguen siendo válidas.

Supóngase que en un acoplador introducimos una señal únicamente por una entrada: esta situación se representa con el vector

$$\begin{bmatrix} E \\ 0 \end{bmatrix}.$$

Siguiendo la expresión (4.1) en las salidas del acoplador se tendrán los campos

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \mathrm{e}^{i\pi/2} \\ \mathrm{e}^{i\pi/2} & 1 \end{bmatrix} \begin{bmatrix} E \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} E \\ \mathrm{e}^{i\pi/2} E \end{bmatrix}. \tag{4.2}$$

A continuación se conectan las salidas de este primer acoplador con las entradas del segundo, de forma que cada una de ellas ha recorrido una longitud de fibra diferente, resultando en una diferencia de fase relativa θ que puede expresarse de la siguiente manera:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\theta} \end{bmatrix} \begin{bmatrix} E \\ \mathrm{e}^{i\pi/2} E \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} E \\ \mathrm{e}^{i(\theta+\pi/2)} E \end{bmatrix}. \tag{4.3}$$

Entonces, en las salidas del segundo acoplador se tendrán los campos

$$\frac{1}{2} \begin{bmatrix} 1 & \mathrm{e}^{i\pi/2} \\ \mathrm{e}^{i\pi/2} & 1 \end{bmatrix} \begin{bmatrix} E \\ \mathrm{e}^{i(\theta+\pi/2)} E \end{bmatrix} = \frac{1}{2} \begin{bmatrix} (1-\mathrm{e}^{i\theta})E \\ i(1+\mathrm{e}^{i\theta})E \end{bmatrix} = i\mathrm{e}^{i\theta/2} \begin{bmatrix} -E\sin(\theta/2) \\ E\cos(\theta/2) \end{bmatrix}. \tag{4.4}$$

La magnitud que se mide, la potencia óptica, será proporcional al cuadrado del módulo del campo, es decir, $|E|^2 \sin^2(\theta/2)$ y $|E|^2 \cos^2(\theta/2)$.

Si la diferencia de recorridos es tal que $\theta = 0$, en una de las salidas existirá interferencia destructiva y la señal será nula, mientras que en la otra salida la interferencia será constructiva. Sustituyendo en (4.4) se tiene entonces

$$\frac{1}{2} \begin{bmatrix} 1 & \mathrm{e}^{i\pi/2} \\ \mathrm{e}^{i\pi/2} & 1 \end{bmatrix} \begin{bmatrix} E \\ \mathrm{e}^{i\pi/2} E \end{bmatrix} = \begin{bmatrix} 0 \\ \mathrm{e}^{i\pi/2} E \end{bmatrix}. \tag{4.5}$$

¿Cómo se recuperan entonces las expresiones (3.3) y (3.4) de la línea de monitorización? Volviendo a (4.3), sin pérdida de generalidad se asigna el primer elemento del vector al brazo corto y el segundo al largo. La diferencia de las longitudes de los brazos son tales que el pulso j, habiendo recorrido el brazo largo, contribuye a la amplitud en la entrada del segundo acoplador con

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ \mathrm{e}^{i(\theta+\pi/2)} \alpha_j \end{bmatrix} \tag{4.6}$$

y el pulso $j+1$, que ha recorrido el brazo corto, contribuye con

$$\frac{1}{\sqrt{2}} \begin{bmatrix} \alpha_{j+1} \\ 0 \end{bmatrix}. \tag{4.7}$$

La señal en la entrada de este acoplador será la suma de (4.6) y (4.7) y tomando de nuevo $\theta = 0$ a la salida del interferómetro se tendrá

$$\frac{1}{2} \begin{bmatrix} 1 & \mathrm{e}^{i\pi/2} \\ \mathrm{e}^{i\pi/2} & 1 \end{bmatrix} \begin{bmatrix} \alpha_{j+1} \\ \mathrm{e}^{i\pi/2} \alpha_j \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -\alpha_j + \alpha_{j+1} \\ i(\alpha_j + \alpha_{j+1}) \end{bmatrix}. \tag{4.8}$$

Se recuperan así las amplitudes de $|D_{M1}\rangle$ y $|D_{M2}\rangle$, luego puede construirse de esta manera un interferómetro para la línea de monitorización del protocolo COW (Sección 3.2).

4.1.5. Generador de pulsos coherentes débiles

En una situación ideal, un sistema de distribución cuántica de claves emplearía fuentes de fotones individuales en su implementación. En la práctica, esta tecnología está menos desarrollada que la detección de fotones individuales y, en consecuencia, muchos protocolos utilizan otro tipo de fuentes de generación de fotones. Por ejemplo, en este trabajo se usaron pulsos coherentes débiles procedentes de un láser.

En el montaje utilizado la obtención de pulsos coherentes débiles se consiguió a través de tres elementos: un láser, un modulador de amplitud y atenuadores.

Láser

El láser empleado fue un modelo FPL1009P de *Thorlabs*, un diodo láser de tipo Fabry-Perot con una longitud de onda de 1550 nm y cuyo espectro sigue la Figura 4.3, junto con un *driver* de modelo LDD-14pin-2A fabricado por *Innolume GmbH*. El láser se usó en modo de onda continua y con intensidad de corriente constante suministrada por el *driver*.

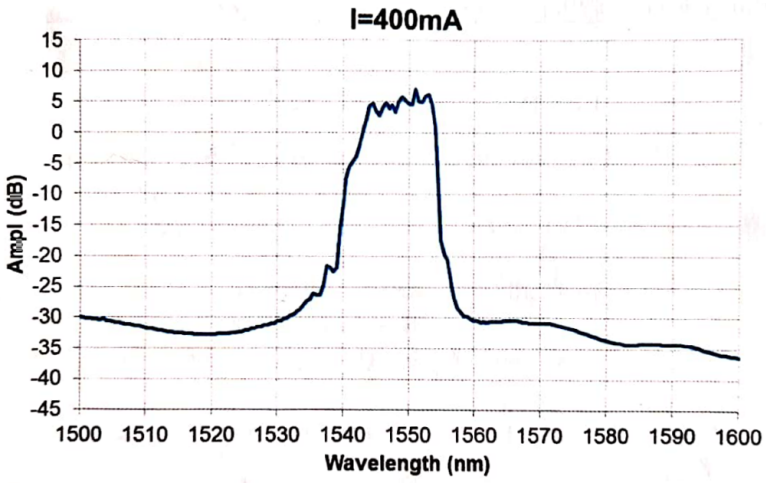

Figura 4.3: Espectro del láser FPL1009P utilizado.

Modulador de intensidad

Para la modulación del láser en pulsos se empleó un modulador de intensidad LN81S_FC de *Thorlabs*. Este modulador creado con $LiNbO_3$ consiste de un interferómetro Mach-Zehnder y utiliza el llamado efecto Pockels o efecto electroóptico lineal [13, pág. 982]. Este fenómeno describe el cambio en el índice de refracción de un medio cuando se le aplica un campo eléctrico externo. Como puede verse en la Figura 4.4, si se coloca en uno de los brazos del interferómetro un cristal en el qué se dé el efecto Pockels (como ocurre en el $LiNbO_3$), el cambio de índice de refracción provoca un cambio relativo de

fase, de forma que el sistema en su conjunto actúa como un modulador de intensidad regulable a partir del campo externo aplicado.

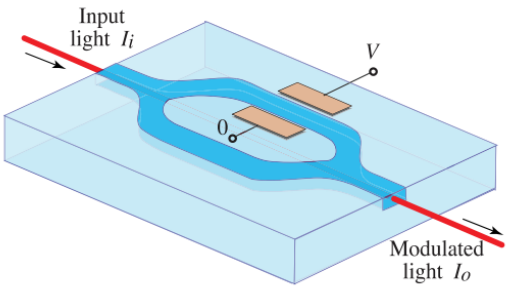

Figura 4.4: Esquema de un modulador de intensidad basado en un interferómetro Mach-Zehnder y el efecto Pockels [13].

Atenuador variable

A la salida del láser modulado se colocó un atenuador variable de modelo VOA1064-FC fabricado por *Thorlabs*. Su funcionamiento consiste en la colimación de la luz entrante por una lente. Un dispositivo de bloqueo que puede ajustarse manualmente bloquea parte de la luz, y una segunda lente vuelve a acoplar la luz en la fibra óptica de salida, como puede verse en la Figura 4.5. Aunque este atenuador variable está diseñado para una longitud de onda de 1064 nm, el principio físico permite utilizarlo también para la longitud de onda aquí empleada, aunque sufriendo mayores pérdidas.

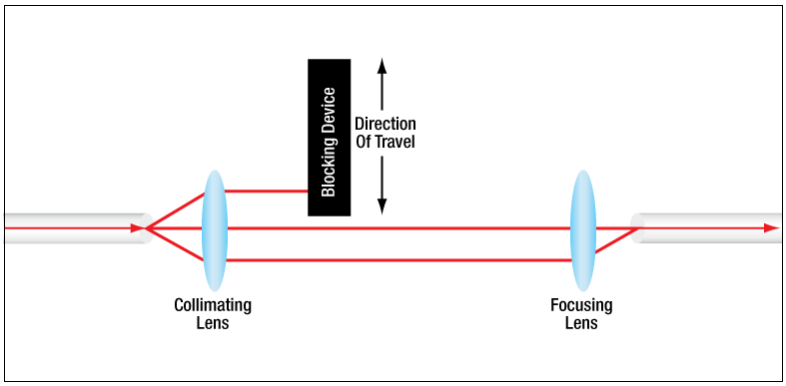

Figura 4.5: Esquema de un atenuador variable [11].

4.1.6. Contador de fotones

El detector de fotones utilizado durante los experimentos fue un modelo LINXEA SPD_A_M1_T, de *AUREA Technology*. Este detector pertenece a la familia de los fotodiodos de avalancha o APD y está basado en el semiconductor InGaAs, que presenta una buena eficiencia para el infrarrojo cercano. En particular, permite operar con eficiencias de $\eta = 10\,\%, 15\,\%, 20\,\%$ y $25\,\%$.

Este detector utiliza el modo de puertas mencionado en la Sección 2.2. Con una señal de pulsos de sincronización adecuada que tenga en cuenta los tiempos de llegada de los

fotones al contador, es posible elevar el potencial de polarización por encima del umbral solamente cuando se espere la llegada de un fotón. Esto permite evitar la aparición de cuentas oscuras o detecciones de fotones no deseados y que dejarían al contador en el tiempo muerto para recuperarse, evitando así registrar los fotones enviados en el protocolo.

Junto al modo puerta aparecen dos parámetros variables que pueden ajustarse a conveniencia: la **anchura de la puerta**, que permite variar el intervalo temporal durante el cual el detector es capaz de detectar un fotón, y el **retraso de apertura**, que permite posponer la apertura de puertas una vez se ha recibido el pulso eléctrico

Este contador está diseñado para, por un lado, registrar el número de cuentas detectadas por segundo; y por otro lado, hallar la diferencia temporal entre la apertura de puertas y un evento de detección. Esto último será lo que permita a Bob discernir qué fotones se corresponden con un bit 0 y cuáles con un bit 1.

4.2. Montaje experimental

Debido a la limitación en los instrumentos disponibles para realizar esta prueba de concepto del protocolo COW no fue posible recrear una línea de monitorización. Del espectro del láser empleado (Figura 4.3), considerando que las longitudes de onda de la luz emitida se concentran entre $\lambda_1 = 1540$ y $\lambda_2 = 1555$ nm, la anchura espectral será de

$$\Delta\nu = c_0 \left(\frac{1}{\lambda_1} - \frac{1}{\lambda_2} \right) \approx 1{,}88 \cdot 10^{12} \text{ Hz}$$

donde c_0 es la velocidad de la luz en el vacío. El tiempo de coherencia es del orden de $\tau_c \approx (\Delta\nu)^{-1}$ [13, pág. 481], y teniendo en cuenta que el índice de refracción en el núcleo de la fibra óptica es de $n \approx 1{,}46$ [6, págs. 67-68] se calcula una longitud de coherencia de

$$\ell_c = \frac{c_0}{n}\tau_c \approx \frac{c_0}{n}\frac{1}{\Delta\nu} \approx 0{,}109 \text{ mm},$$

lo que hace imposible encontrar interferencias con el interferómetro presentado en la Subsección 4.1.4. Con otro láser disponible en el laboratorio y de mayor longitud de coherencia se probaron dos interferómetros: el ya mencionado y un Michelson a partir de dos espejos adaptados para fibra óptica. Sin embargo, se registraron grandes fluctuaciones de potencia óptica y una visibilidad demasiado baja para ambos, como pudo comprobarse haciendo coincidir dos pulsos consecutivos con la ayuda del osciloscopio y un fotodetector de InGaAs de modelo DET08CFC/M, fabricado por *Thorlabs*. Debido a estas razones fue imposible recrear la línea de monitorización en el laboratorio.

La línea de datos sí que pudo implementarse en el laboratorio. De acuerdo con el esquema mostrado en la Figura 3.1, se situó el láser de longitud de onda 1550 nm seguido de un modulador de intensidad y un atenuador variable, lo que compone el montaje en la parte de Alicia. La configuración de Bob constaba simplemente del contador de fotones. Para el canal cuántico se realizó tanto una conexión directa como dos longitudes de fibra de 2002 y 10002 m.

El siguiente paso fue la creación de los pulsos eléctricos para la modulación del láser. Con el generador de funciones y la ayuda del osciloscopio se crearon series de pulsos individuales de anchura 5 ns y periodo 10010 ns, lo que supone una frecuencia de

pulsos enviados por Alicia de aproximadamente 100 kHz. Dentro de cada uno de estos periodos, el pulso de un bit 0 y el pulso de un bit 1 se separaron un total de 30 ns; esto puede apreciarse en la Figura 4.1. Con el mismo generador de funciones se crearon también los pulsos de sincronización para la apertura de puertas en el detector de Bob con la misma frecuencia que los pulsos y se suministraron al contador de fotones.

A continuación se configuró el detector con un tiempo muerto de 9,0 µs, una anchura de puerta de 55,0 ns y una eficiencia del 10 %. Esta configuración dio buenos resultados al reducir los problemas que causan las cuentas oscuras y los fotones que no se correspondiesen con los pulsos enviados. El contador fue entonces conectado directamente al atenuador variable con el objetivo de estimar la intensidad del láser y la atenuación necesarias para obtener un número de fotones por pulso menor que 1. Teniendo en cuenta que hay aproximadamente 100000 pulsos por segundo, para obtener un promedio de $\mu = 0{,}2$ fotones por pulso es necesario registrar en el contador un total de

$$100000\,\frac{\text{pulsos}}{\text{s}} \cdot 0{,}2\,\frac{\text{fotones}}{\text{pulso}} \cdot 0{,}1\,\frac{\text{detecciones}}{\text{fotón}} = 2000\,\frac{\text{detecciones}}{\text{s}}.$$

Elegidos estos parámetros debe realizarse una calibración temporal, ya que la diferencia entre pulsos es mucho mayor que la anchura de la puerta. Alicia puede, por su parte, cambiar en qué momento respecto al pulso láser envía el pulso eléctrico para abrir la puerta, mientras que Bob, desde el contador de fotones utilizado, puede retrasar la apertura de puertas respecto al pulso eléctrico recibido. Con esto, el detector de fotones queda calibrado para que pueda detectar los fotones correspondientes a bits 0 y 1 dentro de una misma anchura de puerta. A partir de pulsos de prueba enviados por Alicia, Bob también debe determinar los intervalos temporales dentro de los cuales considerará que un evento de detección se corresponde con un bit en lugar de una cuenta errónea.

Finalmente, se lleva a cabo un ajuste grueso con el atenuador variable hasta obtener un orden de magnitud al de cuentas por segundo esperado, y con la intensidad suministrada al láser por el *driver* – entre 80 y 100 mA– se logró un ajuste más fino en el número de cuentas por segundo.

Previamente a la toma de medidas con una configuración concreta se registraron las cuentas oscuras que aparecen cuando el láser se encuentra apagado, el promedio de las cuales se debe descontar del resto de medidas con el láser encendido.

Capítulo 5

Resultados experimentales

En este capítulo se exponen los resultados experimentales encontrados siguiendo el montaje explicado en el capítulo anterior. Se registró el número de fotones que llegó al detector para cada una de las parejas de pulsos del protocolo COW: bit 0, bit 1 y secuencia señuelo. También se midió la tasa de error de bit cuántico, todo ello para tres longitudes diferentes del canal cuántico.

5.1. Número de detecciones

Para caracterizar la línea de datos se enviaron durante tres minutos trenes de pulsos correspondientes a un mismo bit o a una secuencia señuelo, tal y como se han descrito en la Sección 4.2, para cada una de las longitudes del canal cuántico. En la Tabla 5.1 se recogen los totales de cuentas detectadas en cada medida. En las Figuras 5.1, 5.2 y 5.3 pueden verse los histogramas de las medidas para los tres tipos de pulso y un canal cuántico de 2002 m, mientras que en la Figura 5.4 se comparan los histogramas para el bit 0 y las tres longitudes de canal cuántico. El resto de medidas pueden encontrarse en el Anexo que acompaña a este trabajo.

	Bit 0	Bit 1	Secuencia señuelo	Cuentas oscuras
0 m, $\eta = 10\,\%$	356562	360490	664708	4003
2002 m, $\eta = 10\,\%$	325579	327181	603205	1344
10002 m, $\eta = 10\,\%$	204244	202816	374508	1443

Tabla 5.1: Número de cuentas totales en tres minutos.

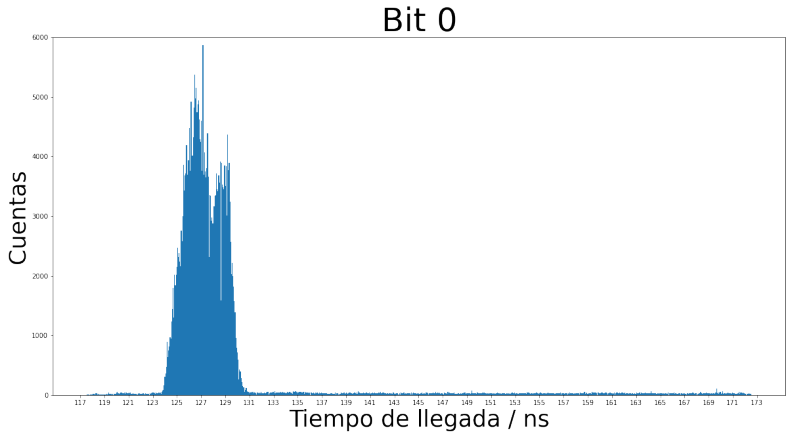

Figura 5.1: Histograma de tiempos de llegada de fotones para el canal cuántico de longitud 2002 m, bit 0.

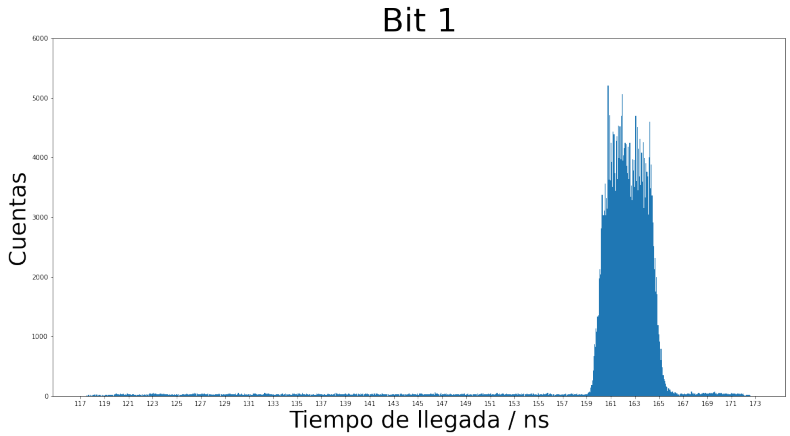

Figura 5.2: Histograma de tiempos de llegada de fotones para el canal cuántico de longitud 2002 m, bit 1.

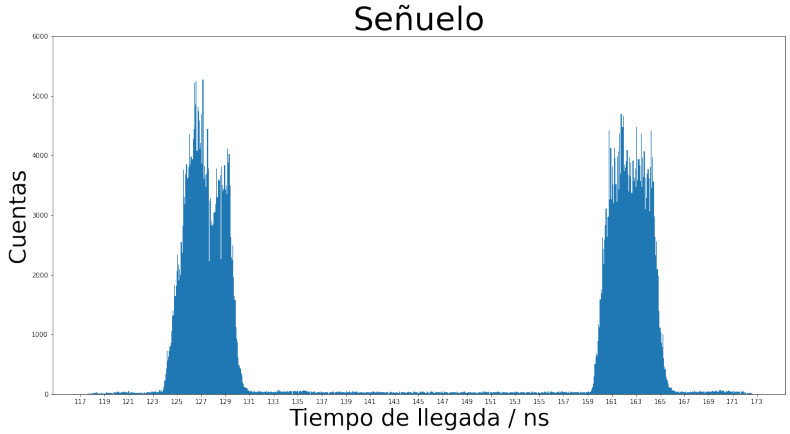

Figura 5.3: Histograma de tiempos de llegada de fotones para el canal cuántico de longitud 2002 m, secuencia señuelo.

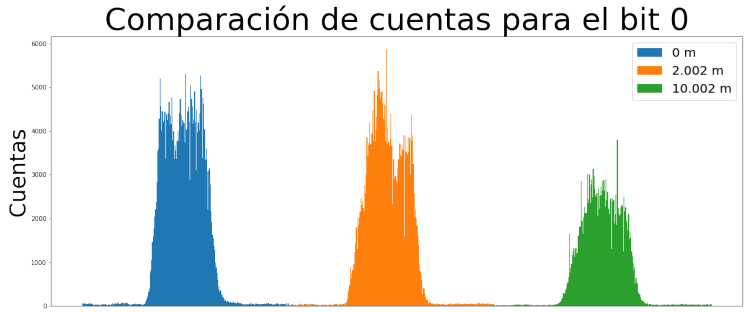

Figura 5.4: Comparación del número de cuentas y su distribución para el bit 0 y las tres longitudes de canal cuántico. Los histogramas completos han sido recortados para poder realizar una mejor comparación; para cada color, el eje x representa el tiempo de llegada de un fotón.

5.2. Tasa de error de bit cuántico: QBER

Se define el valor QBER$(1|0)$ como la probabilidad de encontrar un bit 1 cuando Alicia ha mandado un bit 0: si $N(0|0), N(1|0)$ son respectivamente los totales de bits 0 y bits 1 registrados en una medida en la que se esperaba un bit 0, entonces

$$\text{QBER}(1|0) = \frac{N(1|0)}{N(0|0) + N(1|0)}.$$

Análogamente,

$$\text{QBER}(0|1) = \frac{N(0|1)}{N(1|1) + N(0|1)}$$

y la tasa de error de bit cuántico se calcula como el promedio de estos dos valores suponiendo que ambos bits son equiprobables,

$$\text{QBER} = \frac{1}{2}\text{QBER}(0|1) + \frac{1}{2}\text{QBER}(1|0).$$

En las Tablas 5.2 y 5.3 se recogen las tasas de errores de bit cuántico y la tasa promedio de cuentas oscuras registradas para los tres canales cuánticos considerados y con una eficiencia del detector de $\eta = 10\,\%$, con la diferencia de que fueron tomadas en días distintos. Para apreciar el cambio de comportamiento que supone elegir una eficiencia mayor en el contador de fotones, se realizó una medida de la tasa de cuentas oscuras R_{oscura} con una eficiencia de $\eta = 25\,\%$ en las mismas condiciones que las medidas recogidas en la Tabla 5.2 y que resultó ser de $R_{\text{oscura}} = 89{,}414$ Hz.

	QBER$(1\|0)$ / %	QBER$(0\|1)$ / %	QBER / %	R_{oscura} / Hz
0 m	1,5086	1,3618	1,4352	22,364
2002 m	1,1414	1,0792	1,1103	7,5556
10002 m	1,1688	1,1576	1,1632	8,0320

Tabla 5.2: Medidas del QBER del protocolo COW con eficiencia $\eta = 10\,\%$.

	QBER(1|0) / %	QBER(0|1) / %	QBER / %	R_{oscura} / Hz
0 m	3,3409	3,3392	3,3400	54,394
2002 m	3,3829	3,2990	3,3409	14,552
10002 m	2,2466	2,3825	2,3145	12,290

Tabla 5.3: Medidas del QBER del protocolo COW con eficiencia $\eta = 10\,\%$, distintas condiciones de laboratorio.

5.3. Discusión de resultados

Los números totales de detecciones registradas en cada una de las medidas concuerdan con lo esperado a partir de la intensidad de los pulsos de láser atenuados. Si, como se describe en el montaje experimental en la Sección 4.2, la atenuación es tal que para una conexión directa con el contador se leen 2000 detecciones por segundo, será de esperar que después de tres minutos el número total de eventos de detección sea $2000 \cdot 180 = 360000$. Los datos experimentales recogidos en la Tabla 5.1 coinciden con esta aproximación y se observa cómo las detecciones decrecen según aumenta la longitud del canal cuántico, tal y como era de esperar debido a la atenuación no nula de la fibra óptica.

El número total de cuentas oscuras, aun siendo varias magnitudes menor que el total de detecciones, parece ser mayor para el canal cuántico directo de 0 m frente a las distancias de 2002 y 10002 m. Estas diferencias podrían deberse a un cambio en las condiciones del laboratorio, ya sea tanto de la temperatura ambiente y de los instrumentos de medida como de la iluminación, que podría contaminar la medida con fotones no provenientes del láser, que se encontraba apagado durante el recuento de las cuentas oscuras.

En cuanto a las tasas de error de bit cuántico encontradas, los bajos valores obtenidos resultan satisfactorios. Debe tenerse en cuenta que estos valores dependen de los intervalos temporales escogidos de antemano para representar cada bit. Cabe también destacar la diferencia en la anchura de estos en función de la longitud del canal cuántico, pues al aumentar esta también aumenta la dispersión que sufren los pulsos al viajar por él, provocando una mayor varianza en los tiempos de llegada tal y como se observa en la Figura 5.4.

Existen experimentos de implementaciones en el mundo real, como una conexión realizada entre las ciudades de Ginebra y Neuchâtel [16] con 150 km de fibra, atenuaciones totales de 43 dB y detectores de fotones basados en superconductores, así como en laboratorio con atenuaciones de 31 dB y contadores APD, que encuentran valores de QBER no mayores que el 6 %. Aunque los experimentos aquí realizados son con distancias y atenuadores mucho menores (2 y 10 km con atenuación de 1,45 y 2,95 dB respectivamente, Subsección 4.1.2) y no pueden compararse con estos datos, ha sido posible crear un prototipo de forma sencilla con tasas de error no mayores de 3,5 %.

La influencia de las condiciones de laboratorio quedan reflejadas en las diferencias entre los datos mostrados en las Tablas 5.2 y 5.3 y que se corresponden con medidas tomadas en días distintos. Por ejemplo, una mayor temperatura del detector podría aumentar el número de cuentas debidas a excitaciones térmicas de portadores; otra

posible causa podría ser una peor conexión entre los diferentes elementos de la fibra óptica o una mala limpieza de estos, que podrían producir pérdidas no deseadas o permitir la entrada de fotones externos.

Resultan llamativas las diferencias en los valores de R_{oscura}, que son mayores para la conexión directa que para las distancias de 2002 y 1002 m, lo cual podría abrir la posibilidad de que su causa no se deba a las condiciones ambientales sino a la propios elementos empleados para realizar la conexión.

Otra posible anomalía es la diferencia que aparece en la Tabla 5.3 de casi 1 % en el QBER del canal con 10002 m frente a los otros dos. Esto podría deberse a una mayor estabilidad del láser, pues este había estado encendido durante más tiempo antes de tomar la medida en comparación con los otros dos.

Capítulo 6

Resumen y conclusiones

Este trabajo ha servido como introducción al mundo de la distribución cuántica de claves, el campo con más desarrollo dentro de la llamada "criptografía cuántica" gracias a la posibilidad de comprobar experimentalmente una parte de los sistemas y ataques que se han ideado, todo ello utilizando instrumentos estándar dentro de la tecnología de telecomunicaciones que se posee en la actualidad.

En particular se han desarrollado dos protocolos de distribución cuántica de claves, que han permitido ilustrar los conceptos fundamentales en los que se basa. La sencillez del protocolo COW ha permitido crear un prototipo de este sistema con instrumentos que pueden encontrarse en muchos laboratorios de telecomunicaciones por fibra óptica. Aunque la falta de un interferómetro ha impedido crear una prueba de concepto completa, el trabajo ha sido una buena oportunidad para familiarizarse con el equipo utilizado, así como para aprender los fenómenos físicos detrás de cada elemento.

En cuanto a los resultados obtenidos, se ha encontrado un buen acuerdo tanto con lo predicho teóricamente como con la bibliografía, corroborando la facilidad de implementación del protocolo COW.

Mirando al futuro, con mejores instrumentos pero sin un aumento en la complejidad del sistema sería posible completar el estudio del protocolo COW, así como realizar una caracterización más completa utilizando un mayor rango de longitudes de fibra óptica para el canal cuántico y un estudio pormenorizado de todos los parámetros involucrados: eficiencia del detector, número medio de fotones por pulso, duración de cada pulso, separación entre pulsos... Tanto una mejora del equipo disponible como un mayor tiempo para la experimentación permitirían ampliar, sin mucha dificultad, el trabajo aquí realizado.

Bibliografía

[1] Buller, G. S. y Collins, R. J. «Single-photon generation and detection». *Measurement Science and Technology* 21.1 (2009), 012002.

[2] Gisin, N. y col. «Quantum Cryptography». *Reviews of Modern Physics* 74.1 (2002), 145-195.

[3] Gisin, N. y col. «Towards practical and fast Quantum Cryptography» (2004).

[4] Grangier, P., Levenson, J. A. y Poizat, J.-P. «Quantum non-demolition measurements in optics». *Nature* 396 (1998), 537-542.

[5] *Hoja de especificaciones de la fibra SMF-28*. URL: `https://www.corning.com/media/worldwide/coc/documents/Fiber/PI-1450-AEN.pdf` (visitado 13-07-2022).

[6] Keiser, G. *Optical Fiber Communications*. 3.ª ed. McGraw-Hill, 2000.

[7] Kessler, G. C. *An Overview of Cryptography*. URL: `https://www.garykessler.net/library/crypto.html` (visitado 11-07-2022).

[8] Kollmitzer, C. y Pivk, M. *Applied Quantum Cryptography*. Vol. 797. Springer, 2010.

[9] Lo, H.-K., Ma, X. y Chen, K. «Decoy State Quantum Key Distribution». *Physical Review Letters* 94.23 (2005).

[10] Loudon, R. *The Quantum Theory of Light*. 3.ª ed. OUP Oxford, 2000.

[11] *Narrowband VOAs*. URL: `https://www.thorlabs.com/NewGroupPage9.cfm?ObjectGroup_ID=6161` (visitado 11-07-2022).

[12] Nielsen, M. A. y Chuang, I. *Quantum Computation and Quantum Information*. Edición 10º Aniversario. Cambridge University Press, 2019.

[13] Saleh, B. E. A. y Teich, M. C. *Fundamentals of Photonics*. 3.ª ed. John Wiley & Sons, 2019.

[14] Scarani, V. y col. «Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations». *Physical Review Letters* 92.5 (2004).

[15] Shannon, C. E. «Communication Theory of Secrecy Systems». *The Bell System Technical Journal* 28.4 (1949), 656-715.

[16] Stucki, D. y col. «Continuous high speed coherent one-way quantum key distribution». *Optics Express* 17.16 (2009), 13326.

[17] Stucki, D. y col. «Fast and simple one-way quantum key distribution». *Applied Physics Letters* 87.19 (2005), 194108.

[18] Wegman, M. N. y Carter, J. L. «New hash functions and their use in authentication and set equality». *Journal of Computer and System Sciences* 22.3 (1981), 265-279.

[19] Willett, M. «Cryptography old and new». *Computers & Security* 1.2 (1982), 177-186.