Universidad de Valladolid

Escuela Técnica Superior de Ingenieros de Telecomunicación
Grado en Ingeniería de Tecnologías de Telecomunicación

Redes híbridas de comunicaciones clasico-cuánticas

Autor: Daniel Leiro Arroyo
Tutores: Dña. Lidia Ruiz Pérez y D. Juan Carlos García Escartín

Curso: 2024-2025

Departamento de Teoría de la Señal y Comunicaciones e Ingeniería Telemática

TÍTULO: Redes híbridas de comunicaciones clasico-cuánticas

AUTOR: Daniel Leiro Arroyo

TUTORES: Dña. Lidia Ruiz Pérez y D. Juan Carlos García Escartín

DEPARTAMENTO: Teoría de la Señal y Comunicaciones e Ingeniería Telemática

TRIBUNAL

PRESIDENTE: Pedro Chamorro Posada

SECRETARIO: Juan Carlos García Escartín

VOCAL: Julio Sánchez Curto

SUPLENTE: Juan Carlos Aguado Manzano

SUPLENTE: Maria Jesús González Morales

FECHA:

CALIFICACIÓN:

RESUMEN

Este trabajo aborda la integración de la comunicación cuántica y clásica sobre una misma infraestructura de fibra óptica. Se plantea el objetivo principal de desplegar una red híbrida que soporte un protocolo de distribución cuántica de clave (QKD) llamado BB84 para garantizar una comunicación segura mientras se mantiene un tráfico de datos convencional.

El estudio se centra en las interferencias y efectos no lineales debidos a multiplexar por longitud de onda (WDM) los canales clásicos de alta potencia con los canales cuánticos que operan a nivel de fotón único normalmente. Se comprobará de qué forma afectan al rendimiento del protocolo cuántico mediante un simulador de redes que estima la degradación de las señales cuánticas con los modelos propuestos en el trabajo y la viabilidad del protocolo, aplicando técnicas de gestión de redes como algoritmos de enrutamiento y asignación de longitud de onda (RWA) o con control dinámico de potencia.

Palabras clave: Cuántica, QKD, BB84, distribución de clave, qubit, fotón, efecto no lineal, QBER, QSNR.

ABSTRACT

This work covers the integration of quantum and classical communication over the same fiber optic infrastructure. The main objective is to deploy a hybrid network that supports a Quantum Key Distribution (QKD) protocol called BB84 to ensure secure communication while maintaining conventional data traffic.

The study focuses on interference and nonlinear effects due to wavelength division multiplexing (WDM) of high-power classical channels with quantum channels that typically operate at the single-photon level. It will be examined how these affect the performance of the quantum protocol using a network simulator that estimates the degradation of quantum signals with the models proposed in this work and the viability of the protocol applying network management techniques such as routing and wavelength assignment algorithms (RWA) or dynamic power control.

Keywords: Quantum, QKD, BB84, key distribution, qubit, photon, non-linear effect, QBER, QSNR.

ÍNDICE GENERAL

1 INTRODUCCIÓN

Un cifrado irrompible en términos de criptografía significa que, aún interceptando un criptograma, un posible adversario no pueda obtener ninguna información del mensaje original. En el año 1949, Claude Shannon demostró que el cifrado Vernam era irrompible [1] cuando se emplea una clave aleatoria tan larga como el mensaje a enviar y de un solo uso. A partir de entonces, el nuevo reto en criptografía pasó a ser la distribución de claves, es decir, en cómo proveer a ambos extremos de una comunicación cifrada las claves compartidas necesarias para el cifrado Vernam.

En el año 1984 Charles H. Bennett y Gilles Brassard publicaron un artículo titulado "*Quantum cryptography: Public key distribution and coin tossing*" [2], en el que se describe el funcionamiento del protocolo de distribución cuántica de clave denominado BB84. Este protocolo ha demostrado ser seguro contra oponentes con ilimitada capacidad de cómputo, si no se infringen las leyes fundamentales de la física aceptadas.

Para la correcta ejecución de este protocolo QKD se requiere la utilización de un canal cuántico entre emisor y receptor. Se entiende por canal cuántico un medio a través del cual poder transmitir qubits, la unidad mínima, y por tanto constitutiva, de la información cuántica. Parte de este trabajo se basa en que el canal clásico y cuántico compartan medio, de modo que se formarán varios canales en los enlaces de fibra óptica a través de multiplexación por división de longitud de onda (WDM).

El soporte físico para los qubits que transportan la clave será la polarización de fotones transmitidos mediante pulsos de luz. Para mantener la seguridad de la clave compartida, estos pulsos deben ser débiles (de pocos fotones), idealmente de uno solo. Además, las transmisiones cuánticas no podrán ser amplificadas por la propiedad de no clonación de los qubits. De modo que estudiar los efectos no deseados del medio como el ruido, los efectos dispersivos y los efectos no lineales, así como las interferencias de los canales clásicos que afectarán al canal cuántico, se vuelve fundamental en este tipo de redes que integran un protocolo de QKD.

El propósito último de este trabajo es descubrir hasta qué punto es posible desplegar un protocolo QKD de variable discreta en una red con comunicaciones clásicas sin componentes especializados y no comprometer la fiabilidad de la clave compartida. Los elementos disponibles con los que intentar mejorar las

prestaciones son escasos: variar la potencia o intensidad de las fuentes (tanto para canales clásicos como para cuánticos), caracterizar mejor el canal y los dispositivos *hardware* (para agilizar los trámites del protocolo QKD, pero sin asumir demasiado riesgo) y manipular las rutas entre nodos.

En el segundo capítulo se presentarán los conocimientos básicos de la mecánica cuántica necesarios para entender el funcionamiento del protocolo de distribución cuántica de clave BB84. Concretamente, qué son los qubits, sus principales características y bases para la codificación y medición. Además, se presenta y explica el protocolo BB84 que será estudiado a fondo en el resto del trabajo.

En el tercer capítulo, tomamos el papel de un posible atacante que pretenda descubrir la clave compartida entre dos extremos de la comunicación para comprobar en qué elementos radican las limitaciones de seguridad de nuestro protocolo. Esencialmente, se explica el ataque por división de número de fotones y su principal contramedida: el método de los estados señuelo.

Después introduzco los fundamentos de las redes con enrutamiento de longitud de onda (WRON) y los principios básicos de la técnica *Wavelength Division Multiplexing (WDM)*, para más adelante exponer un aspecto crucial que será uno de los principales elementos limitadores en nuestra red simulada, el problema de asignación de ruta y longitud de onda (RWA).

En el capítulo 5 se explora el fundamental factor limitante para el despliegue del protocolo en redes híbridas: los efectos no lineales. Principalmente, la mezcla de cuatro ondas (FWM) y la dispersión Raman. Se propondrá un modelo para cuantificar la degradación producida por estos efectos que se empleará en el simulador. Al tener clara la forma de estas interferencias se puede abordar el problema RWA de forma diferente en redes híbridas, con un trato especial a los canales cuánticos. Además, se explica en qué consiste el control adaptativo de potencia, crucial para mejorar las distancias máximas de nuestra red.

Se propondrán en el séptimo capítulo las métricas básicas empleadas para estimar el rendimiento de la red y del protocolo QKD. Estos parámetros afectan significativamente a la seguridad del protocolo, y por tanto, a la privacidad de la clave compartida.

2 INFORMACIÓN CUÁNTICA

Para transmitir información, es necesario poder elegir uno o más estados o mensajes de un conjunto de opciones distinguibles. Si aplicamos esta premisa de la forma más simple posible, obtendremos el sistema binario, donde tenemos un conjunto de dos posibles estados '0' o '1', y tomaremos uno u otro para poder reproducir un mensaje.

2.1 Superposición cuántica

Un qubit es la unidad mínima de información cuántica y, como los bits clásicos, pueden valer $|0\rangle$ o $|1\rangle$. Pero gracias a las leyes de la mecánica cuántica, también pueden encontrarse en una superposición de estos estados, que no es más que una combinación lineal de la forma:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

con $\alpha, \beta \in \mathbb{C}$, tales que $|\alpha|^2 + |\beta|^2 = 1$. Para representar los qubits se emplea la notación de Dirac, y el símbolo "$|\,\rangle$" se llama *ket*. Sirve para representar los estados cuánticos asociados a un vector en el espacio de Hilbert complejo $\mathcal{H}$.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \mathbb{C}^2, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbb{C}^2. \tag{2.2}$$

Esta será la base ortonormal *Z* o base computacional del espacio de Hilbert complejo. De esta manera, podemos definir el estado compuesto $|\psi\rangle$ como:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2. \tag{2.3}$$

Otras bases ortonormales relevantes del espacio $\mathcal{H}$ son:

$$\left\{ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix},\ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} \right\} \tag{2.4}$$

$$\left\{ |\circlearrowright\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix},\ |\circlearrowleft\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{bmatrix} \right\} \tag{2.5}$$

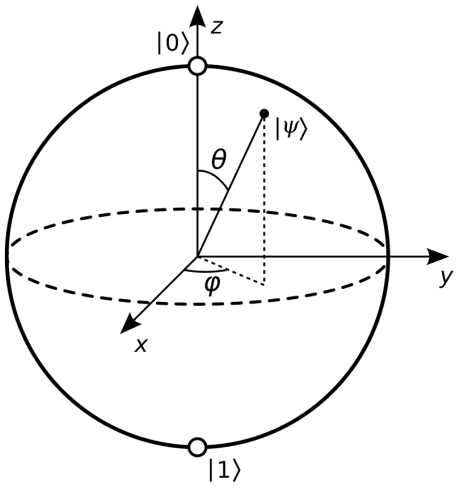

Figura 2.1: Esfera de Bloch
Fuente: Smite-Meister, 2009, Wikimedia Commons,
`https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg`

Las expresiones (2.4) y (2.5) corresponden a la base *X* e *Y* respectivamente, expresadas en función de la computacional. En el protocolo BB84 entrarán en juego dos bases, la *X* y la *Z* o computacional.

Obviando un factor de fase global $e^{i\gamma}$ (con $\gamma \in \mathbb{R}$) sin efectos observables [3], cada uno de los estados cuánticos se puede representar gráficamente como un punto de la superficie de una esfera de radio unidad, llamada esfera de Bloch (Figura 2.1)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,, \tag{2.6}$$

donde $\theta, \varphi \in \mathbb{R}$ tales que $0 \leq \theta \leq \pi$ y $0 \leq \varphi \leq 2\pi$. Se puede comprobar que se cumple la condición de normalización: $\left|\cos\left(\frac{\theta}{2}\right)\right|^2 + \left|e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\right|^2 = 1.$

2.2 Medición de qubits

Podemos inferir del apartado anterior que un qubit puede tomar un estado de un conjunto infinito de ellos. Esto es, hasta cierto punto, equivalente a decir que un solo qubit puede contener infinita información. Teóricamente se podría escribir cualquier cantidad de información en los decimales de α por ejemplo. El problema surge al intentar que el qubit reproduzca esta información.

Si tenemos un qubit en un estado de superposición con coeficientes α y β, suponemos por simplicidad que $\alpha, \beta \in \mathbb{R}$, y este estado está expresado con respecto a la base computacional ($|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$), al medir obtendríamos el valor $|0\rangle$ con probabilidad $|\alpha|^2$ o el valor $|1\rangle$ con probabilidad $|\beta|^2$. Se podría decir que

al medir un qubit se convertirá en un bit clásico con solo uno entre dos posibles valores. Para referirnos a esta conversión se utilizará la palabra 'colapsar'.

De forma análoga podemos expresar $|\psi\rangle$ en la base *X*:

$$|\psi\rangle = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|-\rangle\,. \tag{2.7}$$

De modo que al medir obtendríamos el valor $|+\rangle$ con probabilidad $|\frac{\alpha+\beta}{\sqrt{2}}|^2$ o el valor $|-\rangle$ con probabilidad $|\frac{\alpha-\beta}{\sqrt{2}}|^2$.

Será importante el caso particular en el que $\alpha = 1$ y $\beta = 0$. Se obtendrá $|0\rangle$ con probabilidad $|\alpha|^2 = 1$ al medir en la base computacional, es decir, siempre. Pero en la base *X* se obtendrá un $|+\rangle$ o un $|-\rangle$ con igual probabilidad $1/2$.

2.3 Teorema de no clonación

Pese a que al medir un estado compuesto de un qubit obtendremos un solo bit de información, este tomará un valor u otro en función a unas probabilidades definidas mediante los coeficientes de la superposición. Si pudiéramos tener copias ilimitadas de un qubit cuyos coeficientes desconocemos, podríamos averiguar α y β, con tanta precisión como queramos, tan solo calculando la media estadística de las veces que colapsa en cada uno de los estados fundamentales de la base.

Asumiremos que esta operación de clonación perfecta es posible; luego, deberá existir un operador unitario y lineal al que denominaremos U. Un operador es lineal si

$$U(\alpha|\psi\rangle + \beta|\phi\rangle) = \alpha U|\psi\rangle + \beta U|\phi\rangle \tag{2.8}$$

para estados $|\psi\rangle, |\phi\rangle$ y escalares α, β. Y es unitario si

$$U^\dagger U = I \tag{2.9}$$

donde $U^\dagger$ es el adjunto transpuesto de U e I es la matriz identidad. De esta manera, conservamos los productos internos entre vectores ($\langle U\psi|U\phi\rangle = \langle\psi|\phi\rangle$) y las normas de los estados cuánticos, es decir, las probabilidades.

Para evaluar la viabilidad de este operador, supondremos un estado $|\psi\rangle_A$ en superposición, cuyos coeficientes α y β desconocemos. Y llamaremos U al operador que copiará el estado $|\psi\rangle_A$ en el estado inicial $|0\rangle_B$.

$$U\,|\psi\rangle_A\,|0\rangle_B = |\psi\rangle_A\,|\psi\rangle_B \tag{2.10}$$

La expresión de los estados $|\psi\rangle_A\,|0\rangle_B$ no es más que un estado combinado

descrito por el producto tensorial de la forma:

$$|\psi\rangle_A \otimes |0\rangle_B = |\psi\rangle_A |0\rangle_B \tag{2.11}$$

Desarrollando, obtenemos:

$$\begin{aligned} U|\psi\rangle_A |0\rangle_B &= U(\alpha|0\rangle_A + \beta|1\rangle_A)|0\rangle_B \\ &= (\alpha|0\rangle_A + \beta|1\rangle_A)(\alpha|0\rangle_B + \beta|1\rangle_B) \\ = \alpha^2|0_A 0_B\rangle + \alpha\beta|0_A 1_B\rangle + \beta\alpha|1_A 0_B\rangle + \beta^2|1_A 1_B\rangle &. \end{aligned} \tag{2.12}$$

De otro modo, igualmente válido, obtenemos:

$$\begin{aligned} U|\psi\rangle_A |0\rangle_B &= U(\alpha|0_A 0_B\rangle + \beta|1_A 0_B\rangle) \\ &= (\alpha|0_A 0_A\rangle + \beta|1_A 1_B\rangle). \end{aligned} \tag{2.13}$$

Para que se cumpla

$$\begin{aligned} \alpha^2|0_A 0_B\rangle + \alpha\beta|0_A 1_B\rangle + \beta\alpha|1_A 0_B\rangle + \beta^2|1_A 1_B\rangle = (\alpha|0_A 0_A\rangle + \beta|1_A 1_B\rangle) \\ \alpha^2 = \alpha \qquad \beta^2 = \beta \qquad \alpha\beta = 0 \end{aligned} \tag{2.14}$$

Esto solo ocurrirá si $\alpha = 0$, $\beta = 1$ o si $\alpha = 1$, $\beta = 0$, es decir, solo podremos clonar los estados fundamentales de la base en la que trabajemos [4].

2.4 Protocolo BB84

El protocolo BB84 es el principal protocolo de distribución cuántica de clave (QKD). Permitirá que dos extremos de la comunicación, que no han intercambiado información ninguna de antemano, compartan una clave segura. Cualquier intento de escucha clandestina por parte de terceros tendrá una alta probabilidad de ser detectado por los pares legítimos.

Para lograr la distribución de clave serán necesarios:

1. Fuente de fotones: Idealmente el protocolo BB84 emplea una fuente de fotones individuales perfecta. Pero en la práctica se suelen emplear láseres enormemente atenuados.

2. Generador de números aleatorios: También pueden ser cuánticos.

3. Canal cuántico: Necesariamente inseguro, sensible a la escucha de terceros.

4. Canal clásico público: También será sensible a la escucha, pero deberá estar autenticado, es decir, los mensajes no se podrán alterar ni falsificar.

5. Receptores ópticos para medición de qubits en distintas bases.

(1). Generación y codificación de clave: Un transmisor (Alice) generará una cadena de bits aleatorios. Cada uno de estos bits será codificado en un qubit como una polarización lineal de un fotón en la base *X* o *Z* aleatoriamente.

Para la base rectilínea *Z*:

- Bits '0' de la clave serán codificados como $|0\rangle$ con fotones con polarización horizontal ($\rightarrow$).
- Bits '1' de la clave serán codificados como $|1\rangle$ con fotones con polarización vertical ($\uparrow$).

Para la base diagonal *X*:

- Bits '0' de la clave serán codificados como $|+\rangle$ con fotones con polarización a 45º ($\nearrow$).
- Bits '1' de la clave serán codificados como $|-\rangle$ con fotones con polarización a -45º ($\nwarrow$).

Clave generada (Alice)	1	1	1	1	0	1	0	0	1	0	0	1	0	0
Base de codificación (Alice)	X	X	Z	X	Z	Z	X	Z	X	X	Z	X	Z	Z
Polarización de fotones (Alice)	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\rightarrow$	$\nwarrow$	$\nearrow$	$\rightarrow$	$\nwarrow$	$\rightarrow$	$\rightarrow$

Tabla 2.1: Generación y codificación cuántica de clave.

Alice enviará estos fotones polarizados al receptor (Bob) a través de un canal cuántico.

(2). Medición: Bob escogerá, también aleatoriamente, la base de medición de cada fotón.

Clave generada (Alice)	1	1	1	1	0	1	0	0	1	0	0	1	0	0
Base de codificación (Alice)	X	X	Z	X	Z	Z	X	Z	X	X	Z	X	Z	Z
Base de lectura (Bob)	X	Z	X	Z	Z	X	X	Z	X	X	X	Z	X	Z
Bits medidos (Bob)	1	1	0	0			0	0	1	0		1		0

Tabla 2.2: Medición qubits de clave.

Debido a las imperfecciones del canal de transmisión y del receptor de Bob, este no recibirá todos los qubits transmitidos en origen.

Al medir un qubit en la base en la que no fue preparado, esté tomará el valor '1' o '0' de forma aleatoria con probabilidad $1/2$. Debido a que al expresar un estado generador de una base en términos de la otra (1.14) obtenemos las probabilidades $|\alpha|^2 = |\beta|^2 = 1/2$. Tenemos estados

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\,, \\ |1\rangle &= \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\,, \\ |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ y} \\ |-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\,. \end{aligned} \tag{2.15}$$

(3). Discusión pública: Mediante un canal público clásico vulnerable a la escucha clandestina, pero no a la alteración de mensajes, Alice y Bob se podrán de acuerdo sobre qué qubits fueron recibidos y cuáles se han medido en la base correcta. Para ello, Bob publicará su lista de bases empleadas, Alice reportará que bases son correctas y ambos descartarán los resultados en los que las bases empleadas difieran.

Bases de qubits recibidos	X	Z	X	Z			X	Z	X	X		Z		Z
Reporte de bases correctas	✓						✓	✓	✓	✓				✓
Bits restantes	1						0	0	1	0				0

Tabla 2.3: Comprobación de bases.

(4). Detección de escucha clandestina: Cualquier intento de escucha de un tercer sujeto (Eve) conlleva un riesgo alto de alterar los estados transmitidos, lo que conlleva a su vez riesgo de producir una discrepancia en los bits en los que Alice y Bob están de acuerdo.

Si Eve intercepta un estado $|+\rangle$ (base *X*) y realiza su medición en la base *Z*, el qubit colapsará en el estado $|0\rangle$ o en el estado $|1\rangle$ con igual probabilidad. Si envía el resultado a Bob y este realiza la medida en la base *Z*, el bit se descartará y la escucha no deseada pasará desapercibida. Sin embargo, si Bob mide en la base original *X*, existe una probabilidad de $1/2$ de que el resultado en el receptor difiera con el del emisor pese a que se ha medido en la misma base en la que se preparó. Esta forma de internar obtener información de la clave se llama ataque de medida y reenvío (*measure-and-resend attack*), y es el tipo de ataque más básico posible.

Si por ejemplo, Eve intercepta todos los fotones transmitidos y mide todos

ellos en la misma base, cabe esperar que leerá correctamente la mitad y alterará la mitad restante. De modo que si los retransmite, los fotones de esa primera mitad medidos correctamente por Bob tomarán el valor original, mientras que los medidos correctamente de la segunda mitad tendrán un 50 % de posibilidades de cambiar el valor original. Así que del conjunto final de bits resultante del descarte, es presumible que un cuarto de ellos hayan cambiado.

Para detectar la escucha indeseada, ambos extremos compararán un subconjunto aleatorio de los bits restantes. Si la tasa de error supera un cierto umbral se aborta el procedimiento y se descartan los bits de la clave. El umbral debe tener en cuenta el ruido introducido por el enlace y un cierto margen de error en el receptor.

Bits restantes	1						0	0	1	0				0
Subconjunto	1						0		1					
Bits originales (Alice)	1	1	1	1	0	1	0	0	1	0	0	1	0	0
Coincidencias	✓						✓		✓					

Tabla 2.4: Comprobación de errores.

El subconjunto de bits publicado no será utilizado en la clave en caso de seguir adelante con el protocolo.

(5). Reconciliación de información y amplificación de privacidad: [5] En esta última fase, Bob corrige los posibles errores de su clave para obtener una cadena de bits idéntica a la de Alice. Una posibilidad es que Alice calcule la paridad de ciertos subconjuntos de bits y envíe, por el mismo canal público, esta información a Bob. Por supuesto Eve podría obtener más información de la clave en el proceso.

Durante la amplificación de privacidad se reducirá aún más el tamaño de la clave compartida para minimizar la cantidad de información mutua que Eve podría poseer hasta el nivel de seguridad que se desee. Para este procedimiento Alice y Bob pueden acordar una función hash, también a través del canal público clásico, que aplicar a la cadena de bits compartida. Puesto que solo poseía información parcial, al aplicar la misma función hash la incertidumbre de Eve sobre la nueva clave será total.

3 CONSIDERACIONES DE SEGURIDAD

Consideremos ahora cómo un posible atacante podría interceptar información de la clave. Existen tres principales estrategias de ataque. La más básica es la llamada interceptación y reenvío, como su nombre indica, Eve capturará un fotón y lo medirá para después reenviarlo hacia Bob. Obviamente, esta técnica no es muy efectiva, principalmente porque todo el protocolo BB84 está diseñado para contrarrestarla. En cambio, con el ataque por división de número de fotones, Eve no introducirá perturbación ninguna en los qubits de Bob aprovechandose de las imperfecciones del *hardware* utilizado. Y los ataques de clonación pueden ser incluso más efectivos. En las siguientes secciones estudiaremos su impacto y sus principales contramedidas.

3.1 Ataque por división de número de fotones

Aunque se pueden emplear fuentes de fotones individuales, es caro, así que en su lugar se utilizan láseres muy atenuados, con menos de un fotón por pulso en promedio. Con intensidades de luz tan bajas, los pulsos se aproximan a la definición de un estado coherente, por ejemplo, el número de fotones seguirá una distribución de Poisson. Como consecuencia, algunos de los pulsos emitidos por la fuente contendrán más de un fotón, lo que da la posibilidad a un potencial espía para realizar el ataque por división de número de fotones (PNS: *photon number splitting attack*)[6].

La estrategia se basa en almacenar en memoria un fotón del pulso y enviar los restantes sin perturbación alguna al extremo receptor. Tras la fase de discusión pública, el atacante podía leer el qubit en la base correcta, obteniendo el mismo bit que tiene Bob. Las memorias cuánticas empleadas no existen en la práctica; es un concepto teórico para probar la seguridad del protocolo contra un atacante con recursos ilimitados.

Los pulsos de un solo fotón y los multifotónicos no son distinguibles para los extremos de la comunicación. Así pues, para la máxima seguridad del protocolo, se debe suponer el peor escenario posible: Eve obtiene información completa de los pulsos multifotónicos y todos los errores y pérdidas sufridas proceden de los pulsos de un solo fotón interceptados por Eve [7].

3.1.1 Método de los estados señuelo

Como contramedida para los ataques PNS aparece el método de los estados señuelo. Su consecuencia más importante es que se obtiene una estimación mucho más ajustada y menos pesimista sobre la cantidad de información que Eve ha podido capturar, lo cual repercute directamente en la cantidad de bits que se destilan en la etapa de ampliación de privacidad, aumentando las tasas binarias de clave compartida y aumentando también la distancia segura del enlace.

La idea principal es que Alice, además de enviar pulsos que contienen los bits de la clave, transmite también pulsos adicionales con diferentes intensidades o incluso nulas (cero fotones), equivalente a apagar el láser. Se conocen como estados de señal y estados señuelo, respectivamente. El número de fotones transmitidos en cada pulso (n) se puede modelar como una realización de una variable aleatoria con una distribución de Poisson de parámetro μ [8]:

$$P(n) = e^{-\mu}\frac{\mu^n}{n!}. \tag{3.1}$$

El parámetro μ sería el valor de intensidad que Alice puede modificar en cada pulso.

Se miden experimentalmente dos métricas clave para cada intensidad empleada [8]:

1. "Ganancia total"(Q_μ): Probabilidad con la que Bob detecta un pulso. Esta cantidad se puede expresar como la suma ponderada de las probabilidades para pulsos con n fotones

$$Q_\mu = \sum_{n=0}^{\infty} p(n|\mu)Y_n, \tag{3.2}$$

donde:

- La probabilidad de que Alice envíe n fotones con una intensidad de μ es $p(n|\mu) = e^{-\mu}\frac{\mu^n}{n!}$ (distribución de Poisson).
- Y_n es la probabilidad de detección de un pulso de n fotones por parte de Bob. Se denomina rendimiento.

Entonces al desarrollar el sumatorio obtenemos:

$$Q_\mu = Y_0 e^{-\mu} + Y_1 \mu e^{-\mu} + Y_2 \frac{\mu^2}{2!} e^{-\mu} + \dots \tag{3.3}$$

Y_0 sería el rendimiento de un pulso vacío (sin fotones), asociado a falsas detecciones en recepción llamadas conteos oscuros (*dark counts*).

2. QBER (E_μ): Tasa de error cuántico de bits. De igual forma, se puede expresar como:

$$Q_\mu E_\mu = \sum_{n=0}^{\infty} p(n|\mu) Y_n e_n = Y_0 e^{-\mu} e_0 + Y_1 \mu e^{-\mu} e_1 + Y_2 \frac{\mu^2}{2!} e^{-\mu} e_2 + \dots \quad (3.4)$$

donde:

- e_n es la tasa de error cuántico de bits (QBER) para un pulso de n fotones. Luego e_0 representa la tasa de error para un pulso vacío. Se tomará 1/2 puesto que el valor del bit procedente del conteo oscuro suele ser aleatorio.

Mediante la variación de la intensidad de cada pulso, Alice y Bob crean un gran sistema de ecuaciones lineales para Q y QE, dependientes de Y_n y e_n. Truncando el sumatorio, al despreciar los términos con elevados valores de n, aproximación razonable para pulsos muy atenuados donde $\mu \ll 1$, se obtienen Y_1 y e_1.

La seguridad del protocolo BB84 emana únicamente de los qubits obtenidos de pulsos de un solo fotón (no etiquetados). Los pulsos multifotónicos son vulnerables a ataque por división de número de fotones. Definimos

$$Q_1 = p(1|\mu) Y_1 = Y_1 \mu e^{-\mu}, \quad (3.5)$$

que representa la fracción de qubits procedentes de emisiones seguras a los que se aplica corrección de errores y amplificación de privacidad. e_1, por su parte, es la tasa de error de los qubits no etiquetados. Cuanto mayor sea esta tasa, más se deberá destilar la clave, reduciendo la longitud efectiva de esta.

3.2 Ataques de clonación

Las máquinas de clonación cuántica son construcciones teóricas utilizadas para estudiar la escucha no deseada en criptografía cuántica. Como se ha explicado en la sección 2.1.3 Teorema de no clonación, realizar una copia exacta de un qubit desconocido no es posible, pero se pueden obtener copias o clones parciales alterando el qubit original.

El ataque óptimo que Eve puede realizar en relación a la información obtenida-perturbación introducida requiere de una máquina de clonación asimétrica fase-covariante. Es asimétrica pues no todos sus clones tendrán el mismo grado de fidelidad al qubit original. Además, esta herramienta está definida para copiar con

mayor fidelidad los estados que quedan en el ecuador de la esfera de Bloch [9]:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle). \tag{3.6}$$

Para valores de parámetros realistas en los dispositivos ópticos, los ataques que utilizan máquinas de clonación suponen una mejora despreciable en comparación con las estrategias de división de número de fotones [6].

4 REDES ÓPTICAS CON ENRUTAMIENTO EN LONGITUD DE ONDA

Una *Wavelength-routed optical networks* o WRON por sus siglas en inglés, es un tipo de arquitectura de red óptica. Se compone principalmente de nodos interconectados por enlaces de fibra óptica. Los nodos de la red cuentan con transmisores y receptores para poder enviar y recibir señales. Los usuarios finales se comunican a través de canales WDM completamente ópticos llamados *lightpaths*.

4.1 Wavelength Division Multiplexing (WDM)

La multiplexación por división de longitud de onda (WDM) es una técnica empleada en las redes ópticas que permite aprovechar el ancho de banda del infrarrojo para soportar grandes volúmenes de datos. Se basa en transmitir simultáneamente en varios canales no superpuestos dentro de una misma fibra, cada uno situado en una región diferente del espectro de frecuencias, es decir, cada uno con una longitud de onda diferente. Esto permite crear multitud de fibras virtuales dentro de una misma fibra física.

Es especialmente útil en redes troncales, aumentando la tasa binaria soportada sin necesidad de establecer nuevos enlaces. Aunque requiere de dispositivos especializados en los nodos de la red, como por ejemplo multiplexores y demultiplexores ópticos para dividir o unificar los canales WDM [17].

Según la distancia entre canales adyacentes, la ITU-T (Unión Internacional de Telecomunicaciones), distingue dos tipos de técnica WDM: *Coarse Wavelength Division Multiplexing* y *Dense Wavelength Division Multiplexing*. CWDM se caracteriza por un espaciado fijo de 20nm, equivalente a 3.5 THz aproximadamente en banda O [18]. En cambio, DWDM permite espaciados desiguales entre canales con valores mucho menores, desde 12,5 GHz hasta los 100 GHz [19]. Este margen tan pequeño entre canales hace necesario transmisores con mucha estabilidad en frecuencia.

Para la banda O, donde se alojan los canales cuánticos, se utiliza CWDM.Para los canales clásicos, en cambio, se empleará DWDM con una separación de 50 GHz, equivalente a 0,4 nm en longitud de onda para la banda C. El máximo de longitudes de onda disponibles que asumiremos para muestra red de distribución de clave cuántica serán 10 en banda O (centrada en 1310 nm) y 40 en banda C

(centrados en 1550 nm).

4.2 *Ligthpaths*

Los *ligthpaths* son caminos dedicados que conectan los nodos extremos de una comunicación en una WRON para ofrecer un servicio de conmutación de circuitos virtuales. Sus características principales son:

1. Son canales WDM completamente ópticos. Sus señales no se transformarán al dominio óptico durante su trayecto.
2. Restricción de continuidad de longitud de onda: Aunque existen convertidores de longitud de onda, por definición, esta conexión ocupará un solo canal WDM en todos los enlaces de fibra que atraviese su ruta.
3. Las longitudes de onda se pueden reusar en varios *ligthpaths* siempre y cuando sus rutas no compartan ningún enlace.
4. Si no quedan longitudes de onda disponibles para una ruta dada se producirá una situación de bloqueo.

4.3 Problema RWA

El problema RWA (*Routing and Wavelength Assignment*) consiste en establecer los *lightpaths* entre los nodos finales de una comunicación. Establecer un *lightpath* se puede descomponer en dos problemas diferentes: uno de enrutamiento y otro de asignación de longitud de onda.

Los algoritmos RWA se clasifican según el tipo de tráfico [15]:

- Tráfico estático: Las peticiones de conexiones entre nodos se conocen de antemano. Se tratará de minimizar la cantidad de longitudes de onda usadas.
- Tráfico dinámico: Las solicitudes de conexión llegarán de forma secuencial. El objetivo es evitar situaciones de bloqueo, entendiendo por situación de bloqueo que una solicitud de conexión no logre ser resuelta.

En comunicaciones ópticas clásicas, los criterios más sencillos y más utilizados para el establecimiento de rutas son [15]:

- *Fixed Shortest-Path Routing*: Se escogerá el camino más corto entre dos pares origen-destino. Si las longitudes de onda a lo largo de la ruta están ocupadas la petición se bloqueará.
- *Fixed-Alternate Routing*: Los nodos almacenan una lista con multiples rutas ordenadas de la más corta a la más larga, de modo que si las longitudes de onda en una ruta están ocupadas se pasará a la siguiente. Este método es algo más complejo pero reduce drásticamente las probabilidades de bloqueo.
- Enrutamiento adaptativo: Reduce aún más la probabilidad de bloqueo, pero se necesitan protocolos de de control y señalización para mantener actualizadas las tablas de encaminamiento de los nodos de la red. Por ejemplo, *Least-Congested-Path*, que tiene información de la congestión en cada nodo de la red.

Entre los métodos de asignación de longitud de onda destacan [15]:

- *Random Wavelength Assignment*: Se toma una longitud de onda aleatoria entre las disponibles.
- *First-Fit*: Las longitudes de onda se numeran y se elige la primera disponible. El objetivo es acumular los canales ocupados en la parte baja del espectro.
- *Most-Used / PACK*: Intenta seleccionar la longitud de onda más utilizada en la red para agrupar la mayor cantidad de enlaces en la mínima cantidad de longitudes de onda. También requiere información global de la red.

5 COEXISTENCIA DE CANALES CUÁNTICOS Y CLÁSICOS

Para llevar a cabo el protocolo BB84 será necesario, como mínimo, un canal cuántico y uno clásico. Dichos canales estarán multiplexados en frecuencia y podrán convivir en una misma fibra óptica interfiriendo entre sí. Las interferencias entre canales WDM se agravan enormemente teniendo en cuenta las limitaciones del canal cuántico empleado. La mayor causa de contaminación son los efectos no lineales que convierten fotones de los canales clásicos en fotones a las longitudes de onda cuánticas.

5.1 Efectos no lineales

5.1.1 Efecto Kerr

Partiendo de la relación constitutiva del vector de desplazamiento eléctrico $\bar{D}$ [10]

$$\bar{D} = \epsilon_0 \epsilon_r \bar{E} = \varepsilon_0 \, \bar{E} + \bar{P} \tag{5.1}$$

y la respuesta de polarización lineal de un medio para un campo eléctrico E

$$\bar{P} = \varepsilon_0 \, \chi^{(1)} \, \bar{E}, \tag{5.2}$$

ambas en formato vectorial, se puede obtener

$$\epsilon_r = 1 + \chi^{(1)}, \tag{5.3}$$

siendo ϵ_r la permitividad eléctrica relativa del medio y $\chi^{(1)}$ la susceptibilidad eléctrica lineal de primer orden.

Como el índice de refracción se define como $n = \sqrt{\epsilon_r \mu_r}$ y además μ_r se aproxima a 1 en la mayoría de los materiales para frecuencias ópticas, se concluye que

$$n^2 = \epsilon_r = 1 + \chi^{(1)}. \tag{5.4}$$

Ahora, al considerar la respuesta de polarización no lineal (desarrollo de Taylor)

$$\bar{P} = \epsilon_0 [\chi^{(1)} \bar{E} + \chi^{(2)} \bar{E}^2 + \chi^{(3)} \bar{E}^3 + \dots] \tag{5.5}$$

y tomando solamente los términos de primer y tercer orden, y obviando el tercer

armónico que aparece al desarrollar, obtenemos

$$\begin{aligned} \bar{D} &= \varepsilon_0 \bar{E}(1 + \chi^{(1)} + \frac{3}{4}\chi^{(3)}|\bar{E}|^2) \quad \text{y} \\ n^2 &= \epsilon_L + \epsilon_{NL} = 1 + \chi^{(1)} + \frac{3}{4}\chi^{(3)}|\bar{E}|^2. \end{aligned} \tag{5.6}$$

Como se puede observar, el índice de refracción de la fibra mantiene una dependencia con la intensidad de luz que la atraviesa. Este fenómeno se conoce como efecto Kerr y está detrás de muchos efectos no lineales.

5.1.2 Mezcla de cuatro ondas (Four Wave Mixing)

Al introducir tres señales a diferentes frecuencias ω_0, ω_1 y ω_2 en la misma fibra, la interacción entre estas a través de la no linealidad de tercer orden por el efecto Kerr generará nuevas componentes frecuenciales en

$$\omega_3 = \pm\omega_0 \pm \omega_1 \pm \omega_2. \tag{5.7}$$

Si los canales WDM están equiespaciados por $\Delta\omega$, entonces

$$\omega_3 = -\omega_0 + \omega_1 + \omega_2 = -\omega_0 + (\omega_0 + \Delta\omega) + (\omega_0 + 2\Delta\omega) = \omega_0 + 3\Delta\omega, \tag{5.8}$$

luego puede aparecer una señal espuria que ocupará el siguiente canal si se mantiene la separación de $\Delta\omega$.

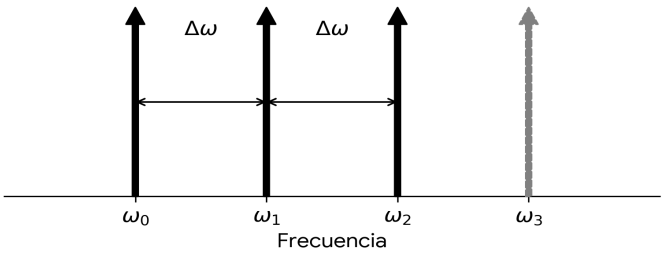

Figura 5.1: Efecto del FWM.

El efecto de la interferencia será más o menos grave según el acoplamiento de fase de las tres señales originales. En términos generales, se trata de que los pulsos ópticos no viajen juntos largas distancias, o de lo contrario, la interacción se producirá durante más tiempo [11]. Conviene, entonces, no trabajar cerca de la longitud de onda con el nulo de dispersión ($\beta_2 \to 0$), ya que en ese caso las velocidades de grupo de las diferentes componentes de frecuencia serán muy parecidas y tardarán más en desfasarse.

Como estrategia para mitigar el efecto FWM se emplean principalmente:

- Fibras con valores altos de dispersión..
- Planificación de canales: El uso de canales desigualmente espaciados en frecuencia.

Esta última será la que emplearemos para los casos de redes que implementen protocolos de QKD.

5.1.3 Dispersión Raman

La dispersión de Raman es otro efecto no lineal causado por la interacción entre los fotones y las moléculas de la fibra de sílice. Actúa dispersando la energía fotónica inelásticamente, es decir, la frecuencia o energía de los fotones cambia al ser dispersados. Con respecto a esto se distinguen dos tipos de fenómenos:

1. Ondas Stokes: El fotón incidente pierde parte de su energía para producir un fonón óptico (estado vibracional de la red cristalina de la fibra) y el fotón resultante tendrá menos energía, es decir mayor longitud de onda.
2. Ondas anti-Stokes: El fotón interacciona con una molécula ya excitada por lo que el fotón resultante será de mayor energía, es decir, con menor longitud de onda. Este fenómeno es mucho menos común, es por eso que el canal cuántico de QKD se suele situar a mayor frecuencia y menor longitud de onda que el clásico.

Además, para cada tipo de onda la dispersión puede ser estimulada o espontánea. La principal diferencia es que, en la dispersión estimulada, la onda llamada de bombeo que porta los fotones que colisionarán con las moléculas de la fibra, tiene una potencia umbral que rebasar. Si supera ese umbral el proceso se retroalimentará positivamente de forma que la nueva componente en frecuencia intensificará las oscilaciones moleculares que a su vez amplificarán la señal dispersada [12]. Esta señal podrá viajar en el sentido de la propagación o en sentido contrario a la propagación. Este efecto se puede emplear para amplificar señales, obteniendo un máximo de ganancia en 13 THz por debajo de la señal de bombeo aproximadamente [13].

Por otra parte, la dispersión espontánea es un proceso estadístico muy similar al ruido, que genera emisión de estados no coherentes, es decir, que no tienen una correlación de fase, al contrario que la dispersión estimulada. En general, este proceso tiene poca relevancia en el ámbito de comunicaciones ópticas. En cambio, para aplicaciones de QKD es más relevante la dispersión espontánea. El canal cuántico transporta señales tan débiles que es imprescindible modelar la interferencia de este proceso por minúscula que sea.

Las ecuaciones que definen la interacción entre la señal clásica de bombeo de potencia C y la señal cuántica de potencia Q, cada una en su canal WDM, en función de la distancia z son [14]:

$$\begin{aligned} \frac{dC}{dz} &= -\alpha_C C + \beta_C Q + \gamma_C CQ \\ \frac{dQ}{dz} &= -\alpha_Q Q + \beta_Q C + \gamma_Q CQ. \end{aligned} \tag{5.9}$$

α es la atenuación de la fibra, β coeficiente de dispersión Raman espontánea y γ el de estimulada. Los subíndices hacen referencia al valor de la atenuación y estos coeficientes en una frecuencia determinada donde se aloja el canal, ya sea cuántico o clásico. Por ejemplo, para la atenuación α_C se toma un valor de 0.3 dB/km, mientras que para α_Q obtenemos 0.5 dB/km (ver figura 4.2).

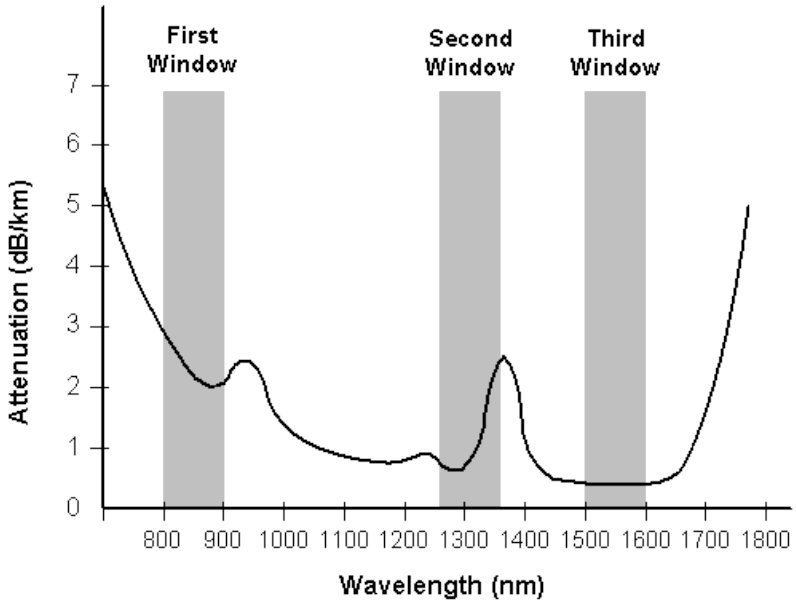

Figura 5.2: Atenuación frente a longitud de onda.

Pese a la debilidad de las transmisiones cuánticas, el canal que se sitúa en el mínimo de atenuación es el clásico. Se aloja en la banda O en torno a 1550 nm. El canal cuántico se sitúa en la banda C, en 1310 nm, en la segunda ventana de transmisión. Se eligen las frecuencias de este modo para que solo la dispersión Raman de ondas anti-Stokes afecte al canal cuántico, puesto que su efecto es mucho menor que con ondas Stokes.

Podemos despreciar el impacto en la señal de bombeo en el canal cuántico y su término de dispersión estimulada, debido a su baja potencia. Luego la potencia de dispersión Raman espontánea queda tras resolver el sistema de la forma:

$$Q(z) = \begin{cases} P_0 \beta_Q z e^{-\alpha_C z} \text{ si } \alpha_C = \alpha_Q \\ \frac{P_0 \beta_Q}{\alpha_Q - \alpha_C}(e^{-\alpha_C z} - e^{-\alpha_Q z}) \text{ si } \alpha_C \neq \alpha_Q. \end{cases} \tag{5.10}$$

Para longitudes de onda y potencias iniciales dadas, la única variable que afecta a la cantidad de luz dispersada es la distancia de propagación.

$$Z_{max} = \begin{cases} 1/\alpha_C \text{ si } \alpha_C = \alpha_Q \\ \frac{1}{\alpha_C - \alpha_Q} ln(\frac{\alpha_C}{\alpha_Q}) \text{ si } \alpha_C \neq \alpha_Q \end{cases} \tag{5.11}$$

6 ALGORITMOS RWA PARA COMUNICACIONES CUÁNTICAS

Como se ha descrito anteriormente, las interferencias entre los canales clásicos y cuánticos son muy nocivas para el protocolo BB84. Este inconveniente introduce un nivel más de complejidad al que atender. Además de la minimización de recursos utilizados y la reducción de la probabilidad de bloqueo, ahora debemos buscar soluciones de enrutamiento y asignación de longitud de onda que disminuyan la cantidad de longitud de fibra compartida por señales clásicas y cuánticas [16].

- *k-Shortest Paths y First Fit*: Combinación de métodos ya presentados. Los nodos tienen una lista con las k rutas más cortas y elegirá la primera longitud de onda disponible.

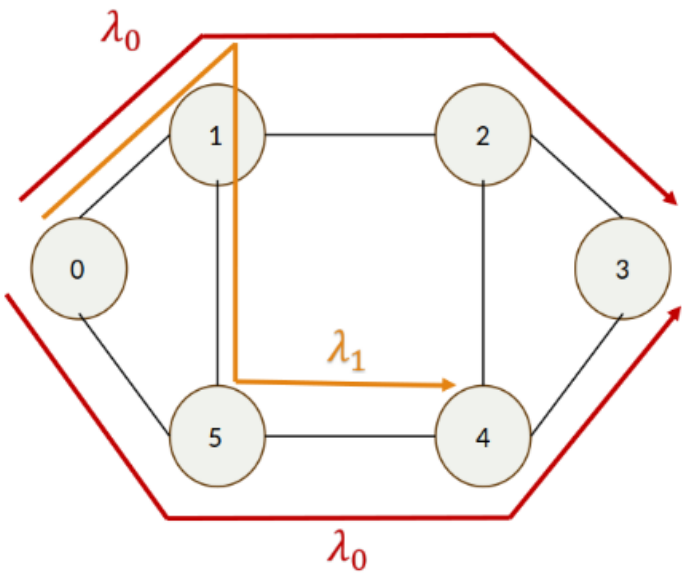

Figura 6.1: Ruta k-Shortest Path en topología simple.

- *Minimum Quantum Distance Overlap (MQDO)*: El algoritmo identifica todos los enlaces posibles entre cada par de nodos. Se marcan los enlaces de estas rutas que tienen un canal cuántico activo y se intenta establecer la ruta con la menor distancia acumulada compartida con estos. La asignación de longitud de onda se lleva a cabo mediante *First-Fit*.
- *Minimum Quantum Classical Channel Overlap (MQCCO)*: Muy similar a MQDO, solo introduce un cambio. Al calcular la distancia acumulada compar-

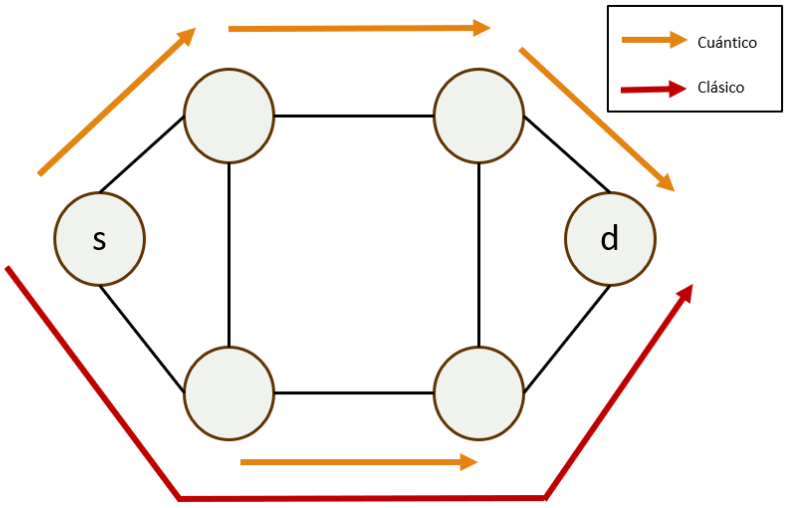

Figura 6.2: Ruta MQDO en topología simple.

tida con canales cuánticos se duplicará si estos comparten enlace de fibra con otro u otros canales clásicos.

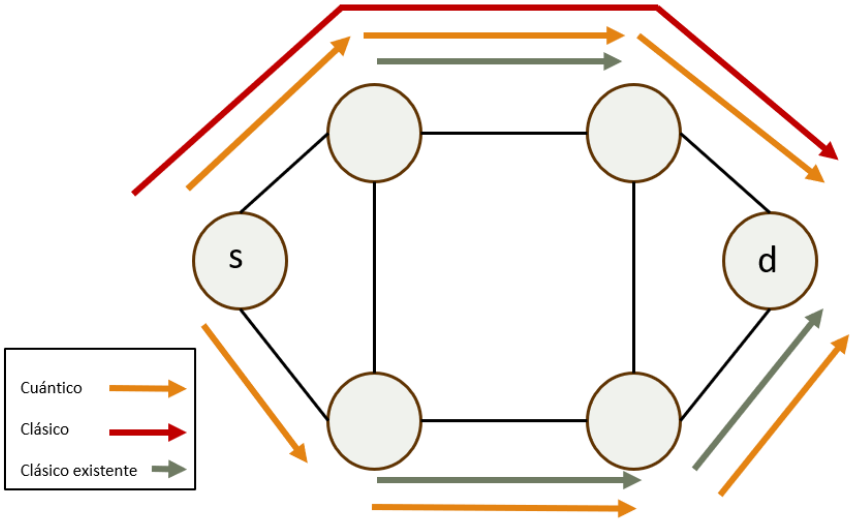

Figura 6.3: Ruta MQCCO en topología simple.

- *Quantum Totally Disjoint (QTD)*: Se pretende establecer una ruta tal que no comparta ningún enlace con un canal cuántico ya establecido. Obviamente este método generará más situaciones de bloqueo que los anteriores.

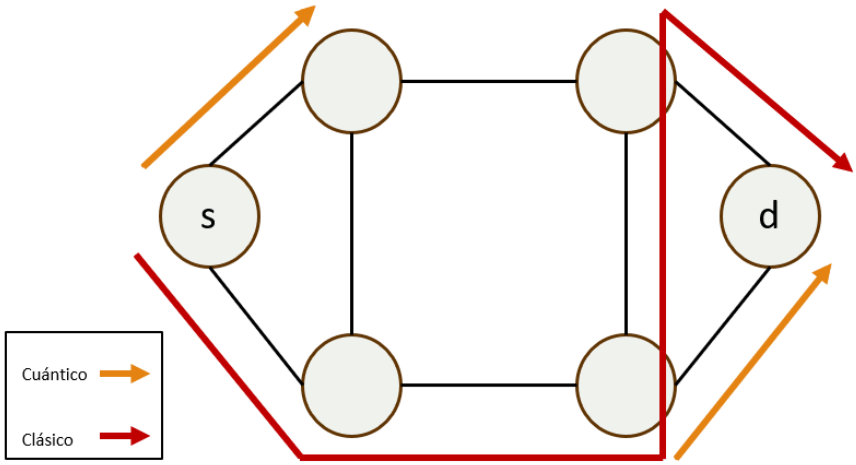

Figura 6.4: Ruta QTD en topología simple.

6.1 Control adaptativo de potencia

Muchos algoritmos de asignación de rutas y longitudes de onda incluyen esta función de control de potencia. Básicamente consiste en calcular, para los canales clásicos, la potencia mínima necesaria de transmisión, en una ruta y longitud de onda elegida, para que la relación señal-ruido en el receptor supere cierto umbral. De este modo, se reduce la acción de los efectos no lineales desfavorables.

Si se toma la expresión [16]

$$SNR = \frac{S_c}{N} = \frac{10^{-\alpha_c L_c} P_{tx,c}}{N} \tag{6.1}$$

como estimador de la relación señal-ruido en recepción, se puede calcular la potencia de transmisión como:

$$P_{tx,c} = SNR \cdot N \cdot 10^{\alpha_c L_c} \tag{6.2}$$

donde α_c es la atenuación de la fibra a la longitud de onda escogida, L_c es la longitud total de la ruta, N sería un término fijo de ruido y SNR el umbral deseado.

7 MODELADO DEL CANAL

La relación cuántica señal a ruido (QSNR), la tasa de error de bits cuánticos (QBER) y la tasa de clave secreta (R) son parámetros fundamentales en QKD porque miden la calidad física de la señal, la probabilidad de error (ligada a la seguridad) y el rendimiento práctico del protocolo.

7.1 Relación cuántica señal-ruido (QSNR)

La relación señal a ruido, SNR por sus siglas en inglés, es una métrica fundamental para medir la calidad de una señal. Su definición

$$SNR = \frac{P}{S} \tag{7.1}$$

consta de P, la potencia de la señal transmitida, y N, la potencia del ruido. Los receptores requerirán de una SNR mínima para detectar la señal de forma exitosa; por lo tanto, el denominador N está relacionado principalmente con la calidad y características del receptor. Factores como el ruido térmico y el ruido de disparo (ruido *shot*) de los fotodetectores afectan significativamente a este parámetro de rendimiento. También se debe tener en cuenta el ruido introducido por el medio de propagación durante el trayecto.

La potencia de la señal en recepción dependerá de la potencia de transmisión P_{tx}, de la atenuación α a una longitud de onda concreta (en unidades naturales de km $^{-1}$) y a la distancia del receptor L. Entonces, se toma

$$SNR = \frac{P}{N} = \frac{P_{tx}e^{-\alpha L}}{N} \tag{7.2}$$

como la calidad de la señal en recepción.

Para medir la influencia del ruido en señales cuánticas se tendrán en cuenta dos influencias principales. En primer lugar, la contribución del receptor, debido principalmente al ruido térmico, como las cuentas en oscuridad (*dark counts*): falsas detecciones que ocurren en ausencia de luz entrante. Estas pueden ser provocadas por fonones ópticos. Estos efectos quedan englobados en un término fijo N_f. Y por otro lado, la contribución al ruido de los canales clásicos, denotada como N_c.

Entonces definimos la relación señal cuántica-ruido como [REF. nuevo art.]:

$$QSNR = \frac{P_Q}{N} = \frac{P_q}{N_f + N_c}. \tag{7.3}$$

Puesto que en el canal cuántico se trabaja a nivel de fotones individuales, tomaremos la ecuación (5.10) para la potencia de la dispersión Raman espontánea, multiplicaremos por la duración de la ventana de detección ΔT elegida para nuestro protocolo QKD, para obtener unidades de energía y dividiremos por la energía de un fotón en la banda C ($E = h\nu = h\frac{c}{\lambda}$ con $\lambda =$ 1550 nm).

$$\eta \frac{P_0 \beta_Q}{\alpha_Q - \alpha_C}(e^{-\alpha_C z} - e^{-\alpha_Q z})\frac{\Delta T}{h\nu} = \gamma_{nl} P_0 (e^{-\alpha_C z} - e^{-\alpha_Q z}) \tag{7.4}$$

será el número de fotones introducidos por un solo canal clásico en la banda cuántica que el detector tomará como qubits de la clave compartida en un intervalo de detección introduciendo errores. η es la eficiencia del receptor cuántico e indica la fracción de los fotones a la entrada del fotodetector que generarán un pulso de salida, es decir, que serán detectados.

Entonces el término N_c se puede modelar como

$$\begin{aligned} N_c &= \gamma_{nl} \sum_i P_{tx,i}(e^{-\alpha_C L_i} - e^{-\alpha_Q L_i}) \\ &\text{con } \ \gamma_{nl} = \frac{\beta_Q \Delta T}{(\alpha_Q - \alpha_C) h\nu} \end{aligned} \tag{7.5}$$

donde γ_{nl} es un coeficiente no lineal que depende de la fibra empleada en el enlace y la duración de la ventana de detección, $P_{tx,i}$ la potencia de salida de la señal clásica i que comparte enlace con nuestra señal cuántica en un tramo de longitud L_i, y α_c y α_q son las atenuaciones para los canales clásicos y cuánticos respectivamente en km $^{-1}$.

De modo que definimos

$$QSNR = \frac{P_{tx,Q} e^{-\alpha_Q L_Q}}{N_f + \gamma_{nl} \sum_i P_{tx,i}(e^{-\alpha_C L_i} - e^{-\alpha_Q L_i})}. \tag{7.6}$$

Con $P_{tx,q}$ como la potencia de transmisión de la señal cuántica y L_q como la longitud total que abarca la ruta establecida para el *ligthpath* desde una fuente hasta un destino final.

7.2 Tasa de error cuántica

La QBER da cuenta de la porción de bits erróneos en la clave sobre el total de los bits compartidos. Dependiendo del número de errores obtenidos en la cuarta etapa del protocolo BB84 (”Detección de escucha clandestina”), se decide si un hipotético atacante ha obtenido suficiente información o, si por el contrario, se sigue con el protocolo. Estimar de forma precisa esta métrica será crucial para poder garantizar la seguridad de la clave compartida.

Como ya vimos en la sección 3.1.1 ”Método de los estados señuelo”los pulsos de luz emitidos por Alice contendrán un número de fotones n determinado por una variable aleatoria con distribución de Poisson con μ fotones de media. Nombraremos esta probabilidad como $p_A(n)$.

Durante el enlace de fibra, el pulso enviado experimentará atenuación en forma de pérdidas de fotones α_Q, que en la banda O tomará un valor de 0,3 dB/km aproximadamente. Definimos entonces la transmitividad del canal [6]

$$t = 10^{-\alpha_Q \frac{d}{10}} \tag{7.7}$$

como la fracción de luz o de fotones restantes después de viajar una distancia d.

En el detector del receptor se tendrán en cuenta la eficiencia cuántica del detector η y la probabilidad de cuenta oscura por ventana de detección p_d. Los valores típicos que se considerarán son $\eta = 0,1$ y $p_d = 10^{-3}$ [6].

La probabilidad de que Bob no detecte ningún fotón enviado por Alice es

$$p_B(0) = \sum_n p_A(n)(1 - t\eta)^n. \tag{7.8}$$

Entonces se pueden definir la tasa de conteo de errores y aciertos como

$$C_{ok} = \frac{1}{2}[(1 - p_B(0)(\frac{1+V}{2}) + p_B(0)p_d] \tag{7.9}$$

$$C_{err} = \frac{1}{2}[(1 - p_B(0)(\frac{1-V}{2}) + p_B(0)p_d]. \tag{7.10}$$

El factor $\frac{1}{2}$ tiene en cuenta la probabilidad de lectura en la base correcta en la que se codificó el qubit y V representa la visibilidad. La visibilidad cuantifica la claridad de los patrones de interferencia que el receptor de Bob emplea para decodificar los bits de la clave. Una $V = 1$ se considera de calidad perfecta, y con $V < 1$, aparecen errores de bits incluso cuando se mide en la base correcta. Finalmente,

la tasa cuántica de error se define [6]

$$QBER = \frac{C_{err}}{C_{err} + C_{ok}} = \frac{1}{2} - \frac{V}{2(1 + \frac{2p_d}{\mu t \eta})}. \tag{7.11}$$

Los errores introducidos por el atacante se camuflarán entre los errores ”naturales” causados por los diferentes componentes de *hardware*. Cuanta menor información haya podido interceptar Eve, mayor confianza en la clave compartida. Para asegurar una clave lo más privada posible, el valor máximo permitido de la QBER deberá reducirse. Esta condición de seguridad está críticamente ligada a la distancia del enlace donde se despliega BB84, obteniendo un rango de distancias seguras y otro de distancias inseguras donde no se puede garantizar la privacidad de la clave.

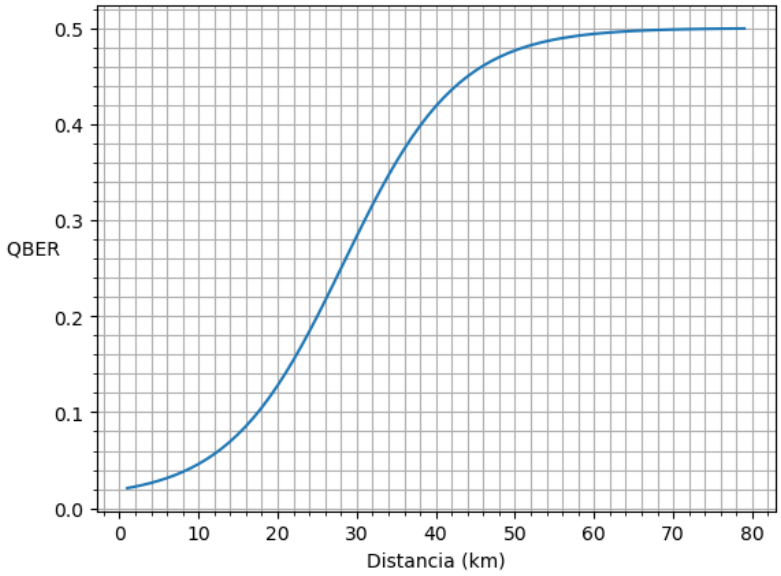

Figura 7.1: Evolución de la QBER (6.11) con la longitud del enlace.

En la gráfica de la figura 6.1 se puede observar cómo a partir de 60 km aproximadamente, la QBER toma un valor de 0,5, es decir, misma probabilidad de error que de acierto. La representación de la gráfica se ha realizado con valores de 0.1 para η, 0.98 para la visibilidad V, 10^{-3} para p_d y empleando la aproximación útil $\mu = t$ en la que suponemos que Alice ajusta la intensidad media de sus pulsos a la eficiencia esperada del canal para optimizar la tasa final de clave [20].

7.3 Tasa cuántica de clave efectiva

La tasa de clave efectiva se deriva de la diferencia entre la información mutua entre Alice y Bob ($I(A:B)$) y la información mutua entre Alice y el posible espía,

Eve ($I(A:E)$), de la forma:

$$R = I(A:B) - I(A:E). \tag{7.12}$$

La información mutua entre Alice y Bob se puede definir como [20]:

$$I(A:B) = \frac{1}{2}(\mu t\eta + 2p_d)[(1 + H(QBER)], \tag{7.13}$$

donde la función $H(\cdot)$ es la función de la entropía binaria de Shannon

$$H(x) = -x\log_2(x) - (1-x)\log_2(1-x), \tag{7.14}$$

y el resto de términos son conocidos.

$I(A:E)$ cuantifica la información que ha podido obtener Alice a través de ataques PNS (sección 3.1) en los pulsos de más de un fotón y a través de los ataques de clonación en los pulsos de un único fotón. La información obtenida en el primer caso es completa y no introduce perturbación alguna en los qubits de Bob, pero en el segundo ataque obtiene información [6]

$$I_1(D_1) = 1 - H(\frac{1}{2} + \sqrt{D_1(1-D_1)}) \tag{7.15}$$

a cambio de introducir una perturbación

$$D_1 = \frac{1-V}{2-\mu/t}. \tag{7.16}$$

De modo que queda una tasa de clave definida por:

$$R = \frac{1}{2}(\mu t\eta + 2p_d)[1 - H(QBER)] - \frac{1}{2}\mu t\eta\left[\left(t - \frac{\mu}{2}\right)I_1(D_1) + \frac{\mu}{2}\right], \tag{7.17}$$

a la que se puede restar un término más de bits consumidos en la etapa de corrección de errores [21].

8 SIMULACIONES

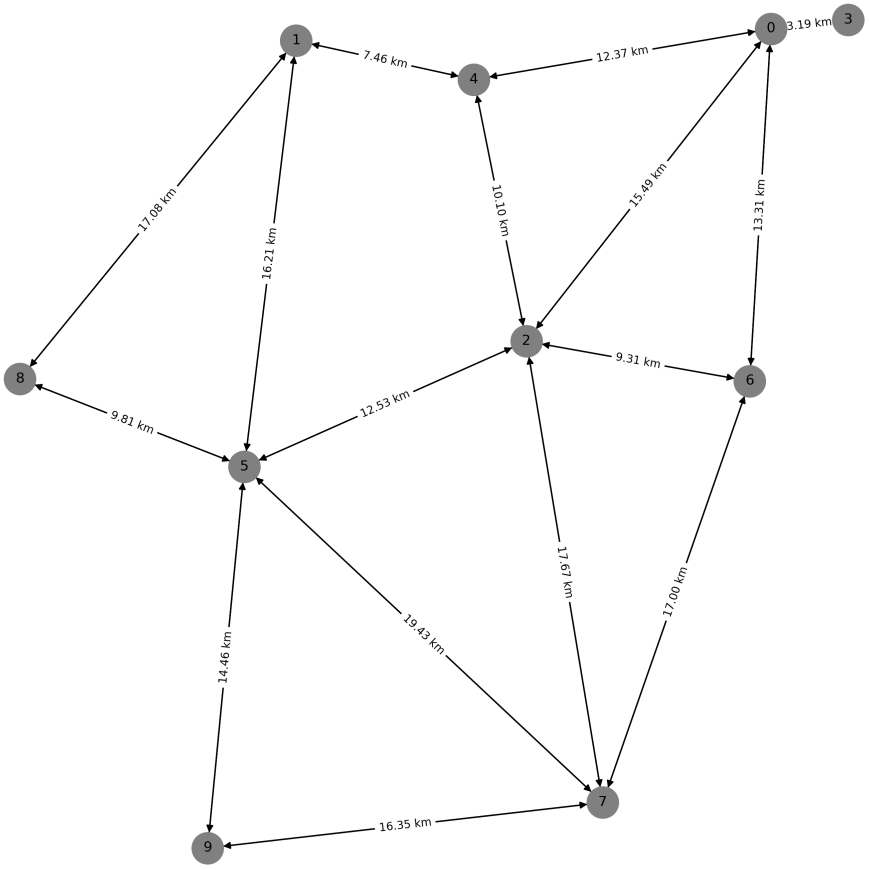

Figura 8.1: Grafo de Gabriel para topología de red simulada.

Para obtener las métricas de rendimiento, se simulará una red con una topología de grafo de Gabriel de 10 nodos. Este tipo de grafo establecerá un enlace entre dos nodos si y solo si el círculo cuyo diámetro es la línea imaginaria que une ambos nodos no contiene otro nodo en su interior. La posición de los nodos se escoge de forma aleatoria.

Como se puede ver (figuras 8.2 y 8.3) el control adaptativo de potencia mejora el rendimiento en todos los casos, gracias a que ahorra potencia innecesaria que acabaría dispersándose por el espectro de los canales cuánticos.

Ahora compararemos dos algoritmos RWA cuánticos sobre la misma topología de red. En el simulador se puede elegir el algoritmo RWA para el canal cuánti-

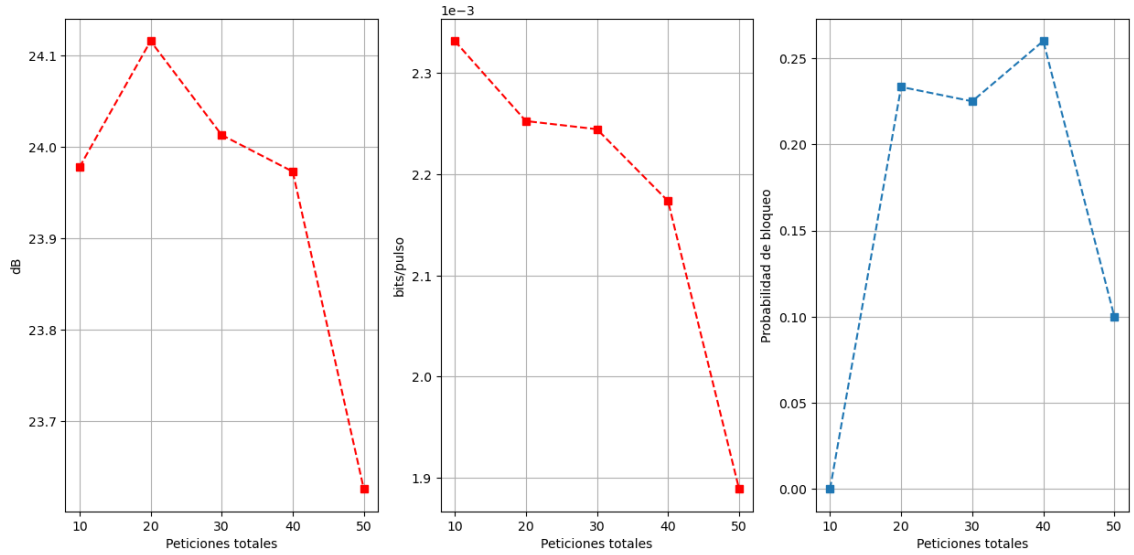

Figura 8.2: QSNR, tasa de clave media simulada y probabilidad de bloqueo media en función del número de peticiones de servicio con algoritmo k-Shortest Paths y sin control adaptativo de potencia.

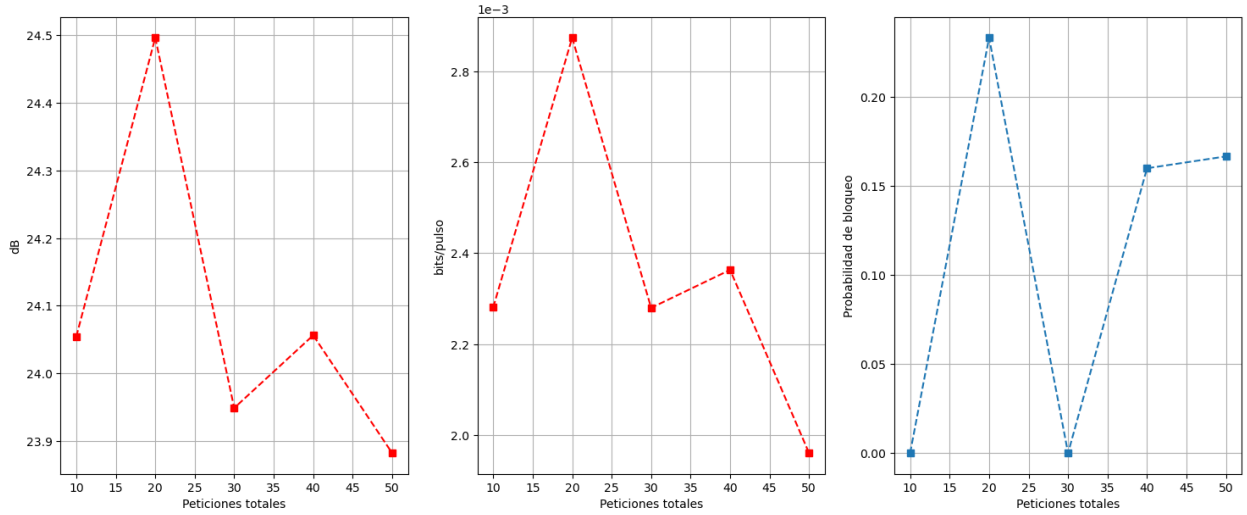

Figura 8.3: QSNR, tasa de clave media simulada y probabilidad de bloqueo media en función del número de peticiones de servicio con algoritmo k-Shortest Paths y control adaptativo de potencia.

co, para los canales de discusión pública de ambos sentidos y para los canales de datos derivados de conexiones QKD y conexiones clásicas independientes. En este caso optamos por mantener *k-shortest path* para el *ligthpath* cuántico y probar una misma estrategia de enrutamiento para todos los canales clásicos. Probaremos con las dos mas restictivas: *Minimum Quantum Classical Channel Overlap (MQCCO)* y *Quantum Totally Disjoint (QTD)*.

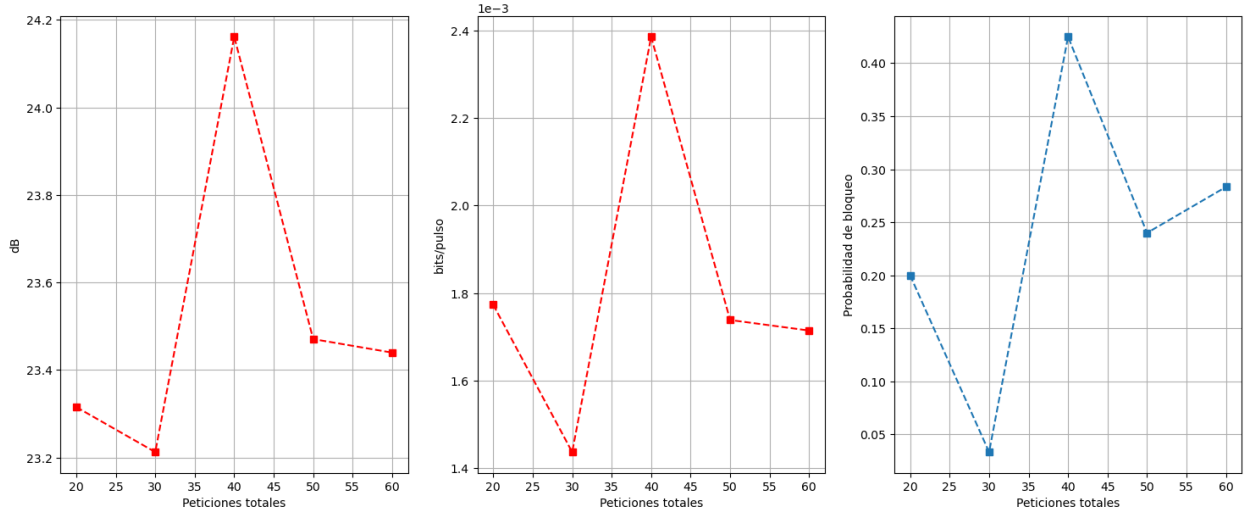

Figura 8.4: QSNR, tasa de clave media simulada y probabilidad de bloqueo media en función del número de peticiones de servicio con algoritmo MQCCO y control adaptativo de potencia.

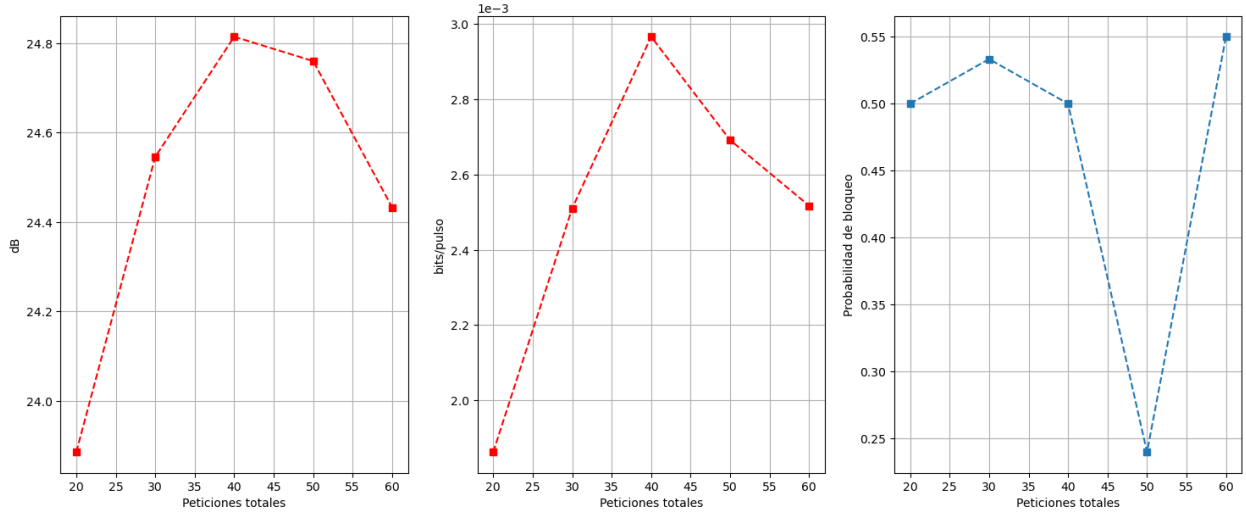

Figura 8.5: QSNR, tasa de clave media simulada y probabilidad de bloqueo media en función del número de peticiones de servicio con algoritmo QTD y control adaptativo de potencia.

El algoritmo QTD es el que más calidad de señal ofrece, pero a costa de una mayor probabilidad de bloqueo. Esta técnica es poco versátil y no muy útil en

redes que, además de las conexiones asociadas a QKD, tengan también comunicaciones clásicas independientes.

9 CONCLUSIONES

En realidad estamos lejos de que un protocolo de este tipo sustituya al cifrado asimétrico común empleado hoy en día, que nos ahorra el problema de distribuir la clave en sí. Hemos podido comprobar que desplegar un protocolo de QKD de variable discreta como lo es BB84 es viable y tiene enormes ventajas, pero también genera muchísimos problemas.

Las interferencias de los canales clásicos que portan señales con intensidades muy superiores, junto con las estrictas condiciones de seguridad de BB84 limitan severamente el alcance de estos protocolos. El alcance real, haciendo verdaderamente difícil la existencia de *ligthpaths* cuánticos que excedan los 60 Km. Y alcance en términos de popularidad, pues las tasas de clave que se pueden alcanzar no son muy elevadas.

Pero es verdaderamente interesante cómo, partiendo de una red de comunicaciones tradicional de fibra óptica, se ha podido implementar un protocolo de distribución de claves que basa su seguridad en los fundamentos de la mecánica cuántica. Gracias a técnicas sofisticadas como el método de los estados señuelo y otras más simples como el control adaptativo de potencia o la elección adecuada de rutas y longitudes de onda, los protocolos QKD pueden abarcar distancias cada vez mayores. Y sobra decir que la criptografía cuántica tiene mucho potencial por explorar todavía.

4 REFERENCIAS

[1] C. E. Shannon. "*Communication theory of secrecy systems*" in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[2] Charles H. Bennett, Gilles Brassard (1984). "*Quantum cryptography: Public key distribution and coin tossing.*" `https://doi.org/10.1016/j.tcs.2014.05.025`

[3] Michael A. Nielsen y Isaac L. Chuang. "*Quantum Computation and Quantum Information*", 10th Anniversary Edition, Cambridge University Press, 2000, pp. 13-16.

[4] W. K. Wootters and W. H. Zurek, "*A single quantum cannot be cloned*", Nature, vol. 299, no. 5886, pp. 802–803, 1982, doi: 10.1038/299802a0.

[5] Michael A. Nielsen y Isaac L. Chuang. "*Quantum Computation and Quantum Information*", 10th Anniversary Edition, Cambridge University Press, 2000, pp. 584-586.

[6] A. Niederberger, V. Scarani, and N. Gisin, "*Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography*", Phys. Rev. A, vol. 71, no. 4, p. 042316, Apr. 2005.

[7] Ma, Xiongfeng. "*Quantum Cryptography: Theory and Practice.*" arXiv:0808.1385 [quant-ph], pp. 31–35, 2008. `https://arxiv.org/abs/0808.1385`

[8] H.-K. Lo, X. Ma, and K. Chen, "*Decoy State Quantum Key Distribution*", Physical Review Letters, vol. 94, no. 23, p. 230504, Jun. 2005. `http://dx.doi.org/10.1103/PhysRevLett.94.230504`

[9] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, "*Quantum cloning*", Reviews of Modern Physics, vol. 77, no. 4, pp. 1225–1256, Nov. 2005, `http://dx.doi.org/10.1103/RevModPhys.77.1225`

[10] John Wiley and Sons, "*Solitons and optical fibers, in Electromagnetic Wave Propagation, Radiation, and Scattering*", Ltd, 2017, ch. 25, pp. 797–806, `https://doi.org/10.1002/9781119079699.ch25`

[11] G. P. Agrawal, "*Fiber-Optic Communication Systems*", 5th ed. Rochester, NY, USA: The Institute of Optics, University of Rochester, 2021, pp. 212-213.

[12] G. P. Agrawal, "*Fiber-Optic Communication Systems*", 5th ed. Rochester, NY, USA: The Institute of Optics, University of Rochester, 2021, pp. 51-52.

[13] B. Mukherjee, "*Optical WDM Networks (Optical Networks)*". Berlin, Heidelberg: Springer-Verlag, 2006, pp. 54–55.

[14] N A Peters, P Toliver, T E Chapuran, R J Runser, S R McNown, C G Peterson, D Rosenberg, N Dallmann, R J Hughes, K P McCabe, J E Nordholt y K T Tyagi, "*Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments*", New Journal of Physics, vol. 11, p. 045012, Apr. 2009, doi: 10.1088/1367-2630/11/4/045012.

[15] H. Zang, J. P. Jue y B. Mukherjee, "*A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks*", SPIE/Baltzer Science Publishers, Mar. 18, 2000.

[16] L. Ruiz y J. C. García-Escartín, "*Routing and wavelength assignment in quantum key distribution networks: Power control heuristics for quantum-classical multiplexing*", arXiv preprint, arXiv:2407.19024, 2024. https://doi.org/10.48550/arXiv.2407.19024

[17] B. C. Chatterjee, N. Sarma, P. P. Sahu, and E. Oki, "*Routing and Wavelength Assignment for WDM-based Optical Networks: Quality-of-Service and Fault Resilience*", Cham: Springer, 2017, pp. 26-14.

[18] UIT-T, "Recomendación G.694.2: Planes espectrales para las aplicaciones de multiplexación por división de longitud de onda: Plan de multiplexación por división aproximada de longitud de onda", Unión Internacional de Telecomunicaciones, Ginebra, Suiza, Dec. 2003.

[19] ITU-T, "*Recommendation G.694.1: Spectral Grids for WDM Applications: DWDM Frequency Grid, International Telecommunication Union*", Telecommunication Standardization Sector, Geneva, Switzerland, Oct. 2020.

[20] J. C. Garcia-Escartin, S. Sajeed, and V. Makarov, "*Attacking quantum key distribution by light injection via ventilation openings*", PLOS ONE, vol. 15, no. 8, p. e0236630, Aug. 2020, doi: 10.1371/journal.pone.0236630.

[21] S. Kawakami, A. Taniguchi, Y. Tonomura, K. Takasugi, and K. Azuma, "*Security of the BB84 protocol with receiver's passive biased basis choice*", arXiv:2507.04248 [quant-ph], 2025. `https://arxiv.org/abs/2507.04248`