UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DEPARTAMENTO DE COMUNICACIONES

Sistemas de Distribución de Clave Cuántica Basados en Codificación en Frecuencia

TESIS DOCTORAL

Presentada por:

Antonio Ruiz-Alba Gayá

Dirigida por:

Dr. José Mora Almerich

Dr. José Capmany Francoy

Valencia, Junio 2012

Tesis Doctoral

Sistemas de Distribución de Clave Cuántica Basados en Codificación en Frecuencia

Antonio Ruiz-Alba Gayá

Directores:
Dr. José Mora Almerich
Dr. José Capmany Francoy

Departamento de Comunicaciones

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Valencia, Junio 2012

A Pilar,
por creer siempre en mí.

“*In theory, there is no difference between theory and practice. But, in practice, there is*”

“*En teoría no hay diferencia entre teoría y práctica. Pero en la práctica, sí que la hay*”

Jan L. A. van de Snepscheut

Agradecimientos

En primer lugar, me gustaría agradecer a mis directores de tesis José Mora y José Capmany la oportunidad de trabajar con ellos en el proyecto nacional *QOIT-Quantum Optical Information Technology* (CSD2006-00019) enmarcado en el programa de excelencia CONSOLIDER-INGENIO 2010. Esta oportunidad me ha permitido realizarme como investigador y adquirir de mis directores las dotes de perseverancia en el trabajo, así como la generación de nuevas ideas y soluciones ante los problemas. Quisiera destacar sinceramente la valiosa ayuda de José Mora en su labor de orientación, su inmejorable dedicación, disposición y consejos en el desarrollo de esta tesis.

Debo agradecer especialmente a Waldimar Amaya la ayuda prestada a la hora de revisar este trabajo y por todos sus valiosos consejos. A Víctor García, Alfonso García, David Calvo y Juan Guillermo Rozo la ayuda prestada como compañeros de proyecto. También, agradezco a Arturo Ortigosa la oportunidad que me brindó inicialmente para formar parte de su equipo.

Al Ministerio de Ciencia y Tecnología por la concesión de la beca de formación de personal investigador (FPI) que me fue otorgada para la realización de esta tesis doctoral.

También quiero agradecer a mis compañeros del grupo de Comunicaciones Ópticas y Cuánticas todo el apoyo recibido, no sólo por haber formado con ellos un grupo de trabajo excepcional, también por crear un ambiente ideal, donde el compañerismo ha sido fundamental a la hora de afrontar toda clase de dificultades.

A los investigadores Hugo Zbiden y Nino Walente por brindarme la oportunidad de trabajar con ellos en el grupo GAP durante una estancia de tres meses en Suiza.

Agradezco especialmente a Pilar Laguía no sólo por su ayuda con el valenciano, también por su apoyo incondicional, su paciencia y su amor. Además quiero agradecer a mi familia, especialmente a mis padres, Antonio y María Fernanda el gran esfuerzo realizado para proporcionarme las oportunidades que me han permitido realizar este trabajo. A Miguel Ángel Laguía y Pilar Malo por su cariño durante estos años. Y a todos mis amigos de Madrid por el empuje esencial que me han mostrado en todo momento.

Resumen

Esta tesis se centra en el estudio de la aplicabilidad que dos disciplinas, la fotónica de microondas (MWP) y las comunicaciones cuánticas, pueden aportar en el desarrollo de nuevos sistemas de distribución de clave cuántica (QKD). El objetivo principal es el análisis y la validación experimental de sistemas QKD en la técnica de codificación en frecuencia (FC-QKD), por medio de distintas configuraciones de moduladores. Los sistemas FC-QKD permiten la incorporación de técnicas de multiplexación empleadas en MWP, por ello, se presenta un sistema basado en multiplexación de la subportadora (SCM) y multiplexación en longitud de onda (WDM) que permite la correcta distribución de claves mediante el protocolo BB84. Los sistemas SCM-QKD presentan algunas ventajas como su alta eficiencia espectral y la posibilidad de compartir una única fuente para todos los canales. Esto reduce considerablemente la complejidad del sistema y permite incorporar la técnica WDM aumentando el número de claves que se trasmiten paralelamente y trasmitiendo la información de estas junto a canales clásicos sobre la misma fibra óptica.

Para entender las funcionalidades de los sistemas FC-QKD se ha realizado un análisis teórico, que permite obtener expresiones para la tasa de error de bit (QBER) y la tasa de trasmisión de clave, teniendo en cuenta los diferentes factores limitantes de los sistemas SCM-QKD, incluyendo la dispersión de la fibra y los efectos de intermodulación. Complementando este análisis teórico, se desarrollan diferentes esquemas experimentales en el laboratorio para evaluar la viabilidad experimental de este tipo de estructuras y tecnologías para su uso en sistemas QKD. Finalmente, se presenta un sistema con cuatro canales independientes consiguiéndose una tasa de bit en crudo de 10 kb/s por canal, con un QBER por debajo del 2% y un enlace de 11 km. Estos resultados abren el camino para el uso de estos sistemas QKD en redes ópticas.

Abstract

This thesis brings into close connection two scientific disciplines, Microwave Photonics (MWP) and Quantum Communications (QC). The main objective is the proposal, analysis and experimental validation of quantum key distribution (QKD) systems based on the frequency coded (FC) technique by means of tandem modulator configurations. FC-QKD systems are compatible with the incorporation of multiplexing techniques used in MWP to QKD systems. The thesis presents a successful operation of a wavelength division multiplexing (WDM) optical network based on a subcarrier multiplexing (SCM) QKD system with BB84 protocol. SCM-QKD systems brings several advantages such as high spectral efficiency and the sharing of the optical source by all the multiplexed channels, which reduce the complexity of the system and permit the possibility of upgrading with WDM to increase the number of parallel keys and to coexists with other classical information channels over the same fiber infrastructure.

A theoretical analysis has been developed in order to understand the functionalities of the QKD systems based on FC technique. Expressions for the quantum key error rate (QBER) and the transmission key rate have been found taking into account several limiting factors of the SCM-QKD systems, including the dispersion of the fiber and intermodulation effects. Complementing this theoretical analysis, different schemes have been experimentally implemented in the laboratory in order to evaluate the experimental viability of this type of structures and technologies for its employment in QKD systems. Finally, a four independent channel QKD system featuring a sifted key rate of 10 kb/s/channel over an 11 km link with a QBER lower than 2 % is demonstrated. These results open the way for multi-quantum key distribution over optical fiber networks.

Resum

Aquesta tesi es centra en l'estudi de l'aplicabilitat que dos disciplines, la fotònica de microones (MWP) i les comunicacions quàntiques, poden aportar en el desenvolupament de nous sistemes de distribució de clau quàntica (QKD). L'objectiu principal és l'anàlisi i la validació experimental de sistemes QKD en la tècnica de codificació en freqüència (FC-QKD), per mitjà de distintes configuracions de moduladors. Els sistemes FC-QKD permeten la incorporació de tècniques de multiplexació empleades en MWP, per això, es presenta un sistema basat en multiplexació de la subportadora (SCM) i multiplexació en longitud d'ona (WDM) que permet la correcta distribució de claus mitjançant el protocol BB84. Els sistemes SCM-QKD presenten alguns avantatges com la seua alta eficiència espectral i la possibilitat de compartir una única font per a tots els canals. Açò reduïx considerablement la complexitat del sistema i permet incorporar la tècnica WDM augmentant el nombre de claus que es transmeten paral•lelament i transmetre la informació d'estes junt amb canals clàssics sobre la mateixa fibra òptica.

Per a entendre les funcionalitats dels sistemes FC-QKD s'ha realitzat un anàlisi teòric, que permet obtindre expressions per a la taxa d'error de bit (QBER) i la taxa de transmissió de clau, tenint en compte els diferents factors limitants dels sistemes SCM-QKD, incloent la dispersió de la fibra i els efectes d'intermodulació. Complementant aquest anàlisi teòric, es desenvolupen diferents esquemes experimentals en el laboratori per a avaluar la viabilitat experimental d'este tipus d'estructures i tecnologies per al seu ús en sistemes QKD. Finalment, es presenta un sistema amb quatre canals independents aconseguint-se una taxa de bit en cru de 10 kb/s per canal, amb un QBER per davall del 2 % i un enllaç d'11 km. Aquests resultats obrin el camí per a l'ús d'estos sistemes QKD en xarxes òptiques.

Contenido

1. Introducción.....1

1.1. Fotónica de Microondas y Comunicaciones Cuánticas.....1

1.2. Distribución de clave cuántica 2

1.2.1. Criptografía clásica 2

1.2.2. Fundamentos básicos de la distribución de clave cuántica.....4

1.2.3. La Fotónica en la distribución de claves cuánticas.....5

1.3. Objetivos y estructura.....6

Referencias.....9

2. Estado del Arte de los Sistemas de Distribución de Clave Cuántica 11

2.1. Introducción 11

2.2. Características principales y definiciones en QKD 12

2.3. Seguridad en QKD 14

2.3.1. Definición de seguridad 14

2.3.2. Ataques en los sistemas QKD 15

2.4. Protocolos 16

2.4.1. El protocolo BB84 17

2.4.2. El protocolo B92 19

2.5. Tasa de error de trasmisión y de clave secreta 20

2.5.1. Tasa de clave en crudo 21

2.5.2. Fracción secreta 21

2.5.3. Tasa de clave secreta y tasa de error para el protocolo BB84 22

2.6. Sistemas de distribución de clave cuántica basados en fibra óptica 27

2.6.1. Sistemas con codificación en polarización 27

2.6.2. Sistemas con codificación en fase 29

2.6.3. Sistemas “Plug and Play” 31

2.6.4. Sistemas con codificación en frecuencia 33

2.7. Conclusiones 35

Referencias 36

3. Implementación de BB84 mediante Codificación en Frecuencia 39

3.1. Introducción y justificación del estudio teórico 39

3.2. Estudio de la concatenación de moduladores para la implementación de BB84 mediante codificación en frecuencia....40

3.2.1. Desarrollo teórico....40

3.2.2. Configuraciones con y sin dispersión....47

3.2.3. Impacto de la dispersión en esquemas AM-PM y PM-PM....50

3.3. Distribución de clave cuántica con multiplexación por división de subportadora....54

3.3.1. Señal e intermodulación en sistemas SCM....55

3.3.2. Análisis de interferencia....62

3.3.3. QBER....64

3.3.4. Análisis del QBER....67

3.3.5. Tasa secreta de bit....69

3.4. Fuentes de degradación de la señal....70

3.4.1. Efecto Raman....71

3.4.2. Ruido de fase y ensanchamiento por modulación de la portadora óptica....72

3.4.3 Impacto de las fuentes de degradación en el QBER....74

3.5. Conclusiones....76

Referencias....78

4. Demostrador y Resultados Experimentales de Sistemas FC-QKD y WDM/SCM-QKD....81

4.1. Introducción....81

4.2. Estudio experimental de las configuraciones de moduladores AM-UM y PM-PM para la implementación del protocolo BB84....83

4.2.1. Configuración AM-UM....83

4.2.2. Configuración PM-PM 88

4.3. Demostrador experimental SCM-QKD 92

4.3.1. Esquema experimental 92

4.3.2. Factores limitantes 96

4.3.3. Tasa de trasmisión y de error de bit cuántico para sistemas experimentales SCM-QKD 102

4.4. Demostrador experimental para WDM/SCM-QKD 103

4.5. Conclusiones 105

Referencias 107

5. Conclusiones y Líneas Futuras 111

5.1. Conclusiones 111

5.2. Líneas futuras 114

Anexo A. Publicaciones Científicas del Autor 117

Capítulo 1

Introducción

1.1. Fotónica de Microondas y Comunicaciones Cuánticas

El objetivo principal de esta Tesis se centra en el estudio y análisis de la aplicabilidad que dos disciplinas, la fotónica de microondas y las comunicaciones cuánticas, pueden aportar en el desarrollo de nuevos sistemas de distribución de clave.

Ambas disciplinas, la fotónica de microondas [1, 2] y las comunicaciones cuánticas [3, 4], se han desarrollado paralelamente en los últimos 25 años. En concreto, la fotónica de microondas (MWP) ha despertado un gran interés en el contexto de la

ingeniería de comunicaciones a través del estudio de los dispositivos y sistemas fotónicos, que operan sobre señales de microondas y facilitan su procesado directamente en el dominio óptico, habilitando prestaciones imposibles de obtener en sistemas tradicionales de radiofrecuencia [1]. Por otro lado, la teoría cuántica de la información (QIT) [5, 6] concierne a la ciencia de la información que depende de los efectos cuánticos de la física. Al contrario que la fotónica de microondas, QIT ha atraído el interés de físicos, matemáticos y especialistas en teoría de la información. QIT está dividida en dos grandes áreas: computación cuántica y comunicaciones cuánticas. Dentro de este último campo es donde se ha desarrollado la primera aplicación comercial, que consiste en los sistemas de distribución de clave cuántica (QKD).

Este capítulo proporciona una breve descripción de los objetivos, estructura y principales contribuciones de esta Tesis. La sección 1.2 resume las características más importantes de MWP y QKD relacionadas con el cometido de esta Tesis. Los objetivos principales de este trabajo quedan descritos en la sección 1.3 donde también se proporciona la estructura del documento.

1.2. Distribución de clave cuántica

1.2.1. Criptografía clásica

La criptografía es una disciplina que permite generar un mensaje que no puede ser descifrado por personas no autorizadas. Dentro del amplio campo de la criptografía, se encuentra el estudio de la ruptura de códigos [7] llamado *criptoanálisis* que consiste en el estudio de métodos para recuperar el significado de un mensaje cifrado sin tener acceso a la información secreta requerida normalmente para poder recuperar la información. Para generar este mensaje secreto, se debe utilizar un algoritmo para combinar el mensaje original a transmitir con una *clave* adicional y así producir el denominado *criptograma*. Esta técnica es conocida como *encriptación*. Para que un *criptosistema* sea seguro debe ser imposible obtener el mensaje del *criptograma* sin la clave. El requerimiento de imposible, en ocasiones, es suavizado de manera que el criptograma sea extremadamente complicado de romper.

Existen dos tipos de *criptosistemas*, dependiendo de si el emisor y el receptor usan la misma clave. En sistemas *asimétricos* o de *clave pública*, se utilizan diferentes claves en los procesos de encriptación y desencriptación. Este algoritmo fue primeramente propuesto por Diffie y Hellman [8], y su primera implementación

práctica fue desarrollada por Tivest, Shamir y Adleman, conocida como el algoritmo RSA [9]. Si el receptor quiere recibir mensajes encriptados con clave pública, debe primero escoger la clave privada, la cual permanece en secreto. A continuación, crea una clave pública que no es secreta y es accesible para todos los usuarios. El emisor utiliza la clave pública para encriptar el mensaje. Trasmite el mensaje encriptado al receptor, quien desencripta el mensaje con su clave privada. El proceso se muestra esquemáticamente en la figura 1.1 donde la clave pública se muestra como un candado que se trasmite desde el receptor hacia el emisor, mientras que la clave privada se representa como la llave del candado.

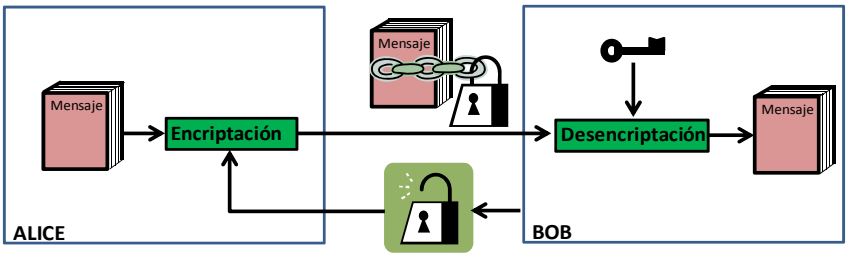

Figura 1.1. Esquema de un sistema con clave pública.

La seguridad de los algoritmos de clave privada está basada en la complejidad del cálculo. Más concretamente en funciones *f(x)* de una sola dirección, que son fáciles de obtener si se conoce *x*, pero donde es muy complejo el proceso inverso, es decir, el obtener *x* conociendo *f(x)*. Normalmente estas funciones están basadas en la factorización de números primos, que requieren un tiempo computacional del orden de la edad del universo en una computadora clásica. Aunque es aparentemente seguro, hasta la fecha no ha sido posible demostrar si la factorización de números primos es un problema complicado o no, ya que siempre está abierta la posibilidad de que exista algún algoritmo que minimice este tiempo de resolución. De hecho, en 1994 Peter Shor [10] desarrolló un método basado en un algoritmo polinómico capaz de factorizar números enteros rápidamente, usando computación cuántica, mostrando la potencial ineficiencia de los algoritmos clásicos de factorización de números y dejando patente la existencia de una brecha en la seguridad en los sistemas futuros basados en computación cuántica.

Los sistemas *simétricos o de clave privada*, por otro lado requieren el uso de una única clave para la encriptación y desencriptación. Podemos visualizar este algoritmo como si el mensaje fuera trasmitido en una caja fuerte, de la cual el emisor y el receptor tienen clave (la misma para los dos). En la figura 1.2 se muestra una ilustración del procedimiento.

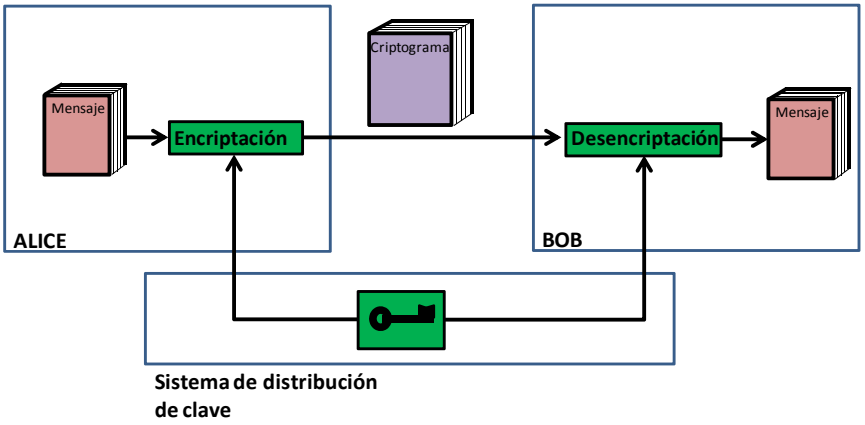

Figura 1.2. Esquema de un sistema con clave privada.

El algoritmo más utilizado que utiliza una clave simétrica es el algoritmo "*One Time Pad*" (OTP) [11]. Aunque este algoritmo es totalmente seguro, el sistema requiere que el emisor y receptor posean la misma clave, que debe ser de la misma longitud que el mensaje y de un único uso. El punto débil de los sistemas simétricos es que la clave debe ser trasmitida entre el emisor y receptor, abriéndose un bucle en la seguridad del sistema. Es en este contexto, donde los sistemas de distribución de clave cuántica juegan un papel importante, ya que son la única solución que puede proporcionar el grado de seguridad deseada. El sistema opera bajo los principios de la criptografía clásica, pero la distribución de la clave se basa en los principios de la mecánica cuántica. Por tanto, es más exacto hablar de distribución de clave cuántica (QKD) que de criptografía cuántica.

1.2.2. Fundamentos básicos de la distribución de clave cuántica

En los sistemas QKD, las dos personas autorizadas que quieren establecer una clave secreta a distancia, tradicionalmente llamados Alice y Bob, necesitan estar conectados a través de dos canales: uno cuántico, que les permite compartir señales cuánticas, y otro clásico, donde pueden enviar mensajes clásicos en ambas direcciones [3, 4]. El canal clásico ha de estar autentificado, lo que implica que Alice y Bob se identifiquen entre sí. Por otro lado, se suele considerar una espía en los sistemas QKD, normalmente llamada Eve, que puede escuchar la conversación en el canal clásico pero no intervenir en ella. El canal cuántico está abierto a cualquier manipulación por parte del espía al que se le supone una capacidad ilimitada en términos de recursos disponibles para acceder a éste. La tarea del sistema QKD consiste en garantizar la denominada *seguridad incondicional* ante un

posible ataque realizado por Eve, capaz de escuchar el canal clásico e interaccionar sin restricciones con el cuántico. La seguridad incondicional implica entonces que con independencia de los recursos ilimitados con los que cuenta Eve, cualquier manipulación que ejerza sobre el canal cuántico debe ser detectada. En la figura 1.3 se muestra un sistema QKD típico.

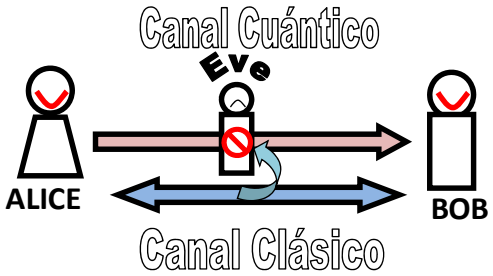

Figura 1.3. Esquema de un sistema de distribución de clave cuántica.

El origen de la seguridad incondicional de los sistemas QKD está fundamentado en los principios de la física cuántica, principalmente en (a) el principio que afirma que un sistema cambia su estado cuántico cuando se realiza una medida sobre él, (b) el teorema de la no clonación, que asegura que no se puede clonar un estado cuántico desconocido manteniendo el original sin modificaciones, y (c) que las correlaciones cuánticas obtenidas de medidas separadas de estados entrelazados violan la desigualdad de Bell y por tanto impiden crear un acuerdo antes de la medida [4]. El hecho de que la seguridad esté basada en los principios de la física sugiere la posibilidad de seguridad incondicional, que como se ha comentado con anterioridad implica la posibilidad de garantizar la seguridad sin ninguna restricción en el potencial del espía.

1.2.3. La Fotónica en la distribución de claves cuánticas

En general, el procesado cuántico de la información, y en particular los sistemas QKD pueden ser implementados de maneras diferentes [4]. Un ejemplo es la computación cuántica, donde se pueden ensamblar puertas lógicas usando iones, átomos, luz, el espín de las partículas, etc. En el caso de los sistemas QKD la luz es la elección más práctica. Los sistemas QKD solo tienen sentido si la distancia ente Alice y Bob es macroscópica (a diferencia de las puertas lógicas, por ejemplo).

La luz, compuesta por fotones, no interacciona fácilmente con la materia, y en consecuencia, los estados cuánticos de la luz pueden ser transmitidos a diferentes lugares sin prácticamente sufrir degradación. La limitación principal es la

dispersión sufrida por los fotones debido a su interacción con el medio de trasmisión, lo que conlleva pérdidas y, por consiguiente, que no todos los fotones trasmitidos por Alice llegan hasta Bob. La manera en cómo las pérdidas afectan al sistema depende del protocolo y su estudio es un aspecto común de todos los sistemas QKD. Las pérdidas limitan la tasa de bit y la distancia de trasmisión, ya que estas pueden reducir la señal hasta los niveles del ruido. Estas pérdidas pueden ser utilizadas por Eve para obtener información de la clave, lo que depende de la naturaleza de la señal cuántica, ya que, si Alice trasmite fotones individuales Eve no puede extraer información de ellos, pero en el caso de estados coherentes existe la posibilidad de que haya más de un fotón, dando la oportunidad a Eve de almacenarlo y obtener información de la clave.

Como consecuencia de ello, los sistemas QKD de hoy en día trabajan con luz, y no existe ninguna razón de que vayan a cambiar las cosas en un futuro próximo. Por tanto, el canal cuántico es cualquier medio capaz de propagar la luz con pérdidas razonables, que son típicamente el espacio libre y la fibra óptica. En este contexto, las tecnologías clásicas usadas en estos entornos también pueden ser útiles en los sistemas QKD y resulta interesante analizar cómo se pueden trasladar a los sistemas cuánticos.

1.3. Objetivos y estructura

El objetivo de esta Tesis es el estudio teórico y experimental de las técnicas de fotónica de microondas, principalmente la técnica basada en la multiplexación por subportadoras eléctricas (SCM), dentro de los sistemas de distribución de clave cuántica (SCM-QKD). Para conseguir este objetivo, ha sido necesario desarrollar un estudio teórico para analizar las características que deben cumplir los dispositivos de estos sistemas y un prototipo capaz de demostrar la eficiencia de esta técnica. Estos conceptos han sido organizados de la siguiente manera:

- En el capítulo 2 se presentan los conceptos fundamentales de los sistemas de distribución de clave cuántica, como la seguridad, protocolos y las relaciones más importantes que deben existir entre los parámetros de estos sistemas. Estos conceptos son utilizados a lo largo de toda la Tesis. El capítulo también proporciona una descripción del estado del arte de las diferentes técnicas desarrolladas para los sistemas QKD basados en fibra óptica para el protocolo BB84.

- El capítulo 3 presenta inicialmente un estudio teórico de sistemas basados en codificación en frecuencia (FC-QKD). Concretamente, se muestra el análisis general de la concatenación de distintos moduladores con el fin de analizar las diferencias desde el punto de vista cuántico entre las distintas estructuras propuestas. También se introducen los sistemas SCM-QKD, que son una evolución de los sistemas con codificación en frecuencia. Se derivan sus expresiones para los parámetros más característicos del sistema, como son la tasa de error de bit (QBER) y la tasa de trasmisión de clave. En la derivación se tiene en cuenta todos los posibles factores de degradación de los sistemas SCM-QKD, incluyendo la dispersión de la fibra y los efectos de segundo orden debidos a la multiplexación. La influencia de estos parámetros en la seguridad ha sido analizada, dejando como conclusiones los aspectos más importantes en el diseño de estos sistemas.

- En el capítulo 4 se presentan las medidas experimentales correspondientes a la concatenación de moduladores controlando la dispersión del medio de transmisión. También, se presenta el primer estudio experimental de los sistemas SCM-QKD a través de un prototipo desarrollado en el laboratorio. Este prototipo es una de las contribuciones más importantes de la Tesis ya que permite, por primera vez, demostrar experimentalmente el incremento de la tasa de trasmisión en sistemas basados en modulación en frecuencia. Los resultados obtenidos a partir del prototipo experimental dejan como conclusiones principales las características que tienen que cumplir los sistemas SCM-QKD para funcionar en entornos reales.

- En el capítulo 5 se resume el trabajo realizado en la Tesis a través de las conclusiones principales relacionadas con el estudio teórico del capítulo 3 y los resultados experimentales obtenidos en el capítulo 4. Se señala las limitaciones principales de los sistemas SCM-QKD y se describen los pasos a seguir para solventarlas. También, se proponen distintas líneas de trabajo que se derivan de la Tesis realizada.

Finalmente, destacar que el trabajo de esta Tesis se ha realizado dentro del proyecto nacional *QOIT-Quantum Optical Information Technology* (CSD2006-00019) enmarcado en el programa nacional de excelencia CONSOLIDER-INGENIO 2010. Este proyecto está dedicado al desarrollo de métodos y dispositivos para la tecnología futura de la información basados en sistemas ópticos y cuánticos. El proyecto combina una parte experimental y otra teórica dividiéndose en 12 paquetes

de trabajo. Concretamente, el trabajo de esta tesis se enmarca en el subproyecto titulado *"Practical quantum key distribution"*.

Referencias

[1] J. Capmany y D. Novak, "*Microwave photonics combines two worlds*," Nature Photon. 1, 319-330 (2007).

[2] Jianping Yao, "*Microwave Photonics*," J. Lightwave Technol. 27, 314-335 (2009).

[3] N. Gisin, G. Ribordy, W. Tittel y H. Zbiden, "*Quantum cryptography*," Rev. Mod. Phys. 74, 145-195 (2002).

[4] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus y M. Peev, "*The security of practical quantum key distribution*," Rev. Mod. Phys. 81, 1301-1350 (2009).

[5] M. Le Bellac, "*A Short Introduction to Quantum Information and Quantum Computation"* (Cambridge University Press, 2006).

[6] M. Fox, "*Quantum Optics"* (Oxford University Press, 2006).

[7] S. Singh, "*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography Fourth Estate*" (London, 1999).

[8] W. Diffie y M. E. Hellman, "*New directions in cryptography*," IEEE Trans. Inf. Theory IT-22, 644-654 (1976).

[9] R.L. Rivest, A. Shamir y L. M. Adleman, "*A method of obtaining digital signatures and public-key cryptosystems*," Commun. ACM 21, 120-126 (1978).

[10] P.W. Shor, "*Algorithms for quantum computation: discrete logarithms and factoring*," en Proc. of the Symposium on Foundations of Computer Science, 124-134 (1994).

[11] G. Vernam, "*Cipher printing telegraph systems for secret wire y radio telegraphic communications*," J. Am. Inst. Electr. Eng. 45, 109-115 (1926).

[12] R. Hui, B. Zhu, R. Huang, C. T. Allen, Kenneth R. Demarest y D. Richards, "*Subcarrier Multiplexing for High-Speed Optical Transmission*," J. Lightwave Technol. 20, 417-427 (2002).

Capítulo 2

Estado del Arte de los Sistemas de Distribución de Clave Cuántica

2.1. Introducción

Este capítulo proporciona una introducción de los conceptos, técnicas y características básicas que son importantes a la hora de entender y evaluar los sistemas QKD. Está dividido en dos bloques principales. El primero cubre desde la sección 2.2 hasta la 2.5 y consiste en una revisión de las características básicas de los sistemas QKD. El segundo bloque cubre la sección 2.6 y proporciona una descripción del estado del arte de los sistemas QKD basados en fibra óptica. Debido a las limitaciones en el tamaño del capítulo, existen algunos puntos que no se tratarán. No obstante, existen excelentes artículos de revisión en la literatura [1-3]

que dan una descripción completa de todos los aspectos relevantes de los sistemas QKD actuales.

Se proporciona una descripción general de los sistemas QKD punto a punto en la sección 2.2 que se complementa con algunas definiciones, que se aplicarán a lo largo de toda la tesis. Los aspectos de seguridad se presentan en la sección 2.3, incluyendo las definiciones básicas en 2.3.1 y un breve resumen de los ataques más importantes en 2.3.2.

Los protocolos para la implementación de los sistemas QKD son expuestos en la sección 2.4. La lista de opciones es muy extensa, así que nos hemos concentrado en los protocolos más comunes en los sistemas reales. Se presta especial atención al protocolo BB84, ya que es el que más relación guarda con el trabajo de esta Tesis.

Los parámetros principales que permiten evaluar estos sistemas son la tasa de error de bit (QBER) y la tasa de trasmisión. Ambos son introducidas en la sección 2.5.

El capítulo concluye con un repaso general del estado del arte de los sistemas QKD basados en fibra óptica, en el apartado 2.6. Para cada uno de estos sistemas se proporcionan los mejores resultados alcanzados hasta la fecha.

2.2. Características principales y definiciones en QKD

En el capítulo 1 se ha mencionado que Alice y Bob necesitan estar conectados por dos canales [1-3]. En el canal clásico, Alice y Bob intercambian señales convencionales. El posible espía (Eve) puede escuchar esta comunicación, pero no puede modificarla, es decir, el canal debe estar autentificado. En caso de no autentificar el canal se puede producir una situación donde Eve puede suplantar una de las partes, comprometiendo la seguridad. La seguridad incondicional requiere la autentificación del canal clásico, para ello Alice y Bob deben compartir una clave inicial [3]. En este sentido, es importante remarcar que los sistemas QKD no crean una clave secreta a partir de la nada, sino que expanden una clave secreta a otra de mayor longitud, por tanto, estrictamente, es un método de aumentar la clave. Por otro lado, en el canal cuántico, donde Alice puede enviar señales cuánticas a Bob, Eve puede interaccionar con estas señales, pero si lo hace, la señal será modificada de acuerdo a leyes de la física cuántica y su presencia detectada.

El primer paso de un protocolo QKD es el intercambio y medida de señales en el canal cuántico. La función principal que realiza Alice es codificar: el protocolo que utiliza debe especificar el estado cuántico $|\psi(S_n)\rangle$ que codifica la secuencia de n símbolos $S_n=\{s_1,s_2...s_n\}$. La situación más común es cuando se puede expresar

como un producto tensorial de la forma $|\psi(S_n)\rangle = |\psi(s_1)\rangle|\psi(s_2)\rangle \cdot\cdot |\psi(s_n)\rangle$. Es esencial que el protocolo use un grupo de estados no ortogonales [2], si no se hace así, Eve podría decodificar la secuencia sin introducir ningún error midiendo en la base adecuada o, en otras palabras, un conjunto de estados ortogonales puede ser clonado. Por otra parte, Bob realiza dos funciones en los sistemas de distribución de clave cuántica. Por un lado, sus medidas permiten decodificar la señal y por otro lado, ha de estimar la pérdida de coherencia en la señal y por tanto la información adquirida por Eve.

Una vez que se han intercambiado y medido *N* señales sobre el canal cuántico, Alice y Bob comienzan el procesado de sus datos comunicándose por medio del canal clásico. En todos los protocolos, Alice y Bob estiman la estadística de sus datos. En particular, pueden extraer los parámetros principales del canal cuántico tales como la tasa de error, la pérdida de la coherencia, la tasa de trasmisión, la tasa de detección, etc. Este paso es conocido como *estimación de parámetros* [4], y puede preceder, en algunos protocolos, a algún proceso que implique el descarte de alguno de los símbolos que no han sido decodificados por Bob correctamente. Después de estos dos procesos, Alice y Bob tienen una lista de $n \leq N$ símbolos, que forman la llamada *clave en crudo*, que es solo parcialmente segura. Por medio de un procesamiento clásico conocido como *corrección de errores* y *amplificación de la privacidad* [5], Alice y Bob pueden formar una clave totalmente segura de longitud $l \leq n$. La longitud *l* dependerá de la información que Eve haya adquirido de la clave cruda.

En el caso asintótico que se considere una clave de longitud infinita ($N \to \infty$), la cantidad de clave relevante es la llamada *fracción secreta* dada por:

$$r = \lim_{N\to\infty}\left(\frac{l}{n}\right) \tag{2.1}$$

La fracción secreta es uno de los parámetros más significativos en los sistemas QKD. En la las demostraciones de seguridad se debe proporcionar un expresión explícita de esta fracción para evaluar la eficiencia de un protocolo dado. También, la *tasa de clave en crudo* R_{sift} es un parámetro interesante, viniendo definida como el número de bits de clave en crudo por unidad de tiempo. Esta tasa depende parcialmente del protocolo que se esté llevando a cabo, ya que está afectada por un factor que solo tiene en cuenta los símbolos que han sido detectados correctamente por Bob. También depende de las características de los dispositivos utilizados en el

sistema como la tasa de repetición de la fuente de fotones, las pérdidas del canal, eficiencia y los tiempos característicos de los detectores, etc.

Para evaluar el rendimiento de los sistemas QKD prácticos, es costumbre definir la *tasa secreta de bit* R_{net} como el producto de la fracción secreta y la clave en crudo:

$$R_{net} = r \cdot R_{sift} \tag{2.2}$$

Las ecuaciones (2.1) y (2.2) son obtenidas bajo el régimen de claves infinitas. Cuando la clave es finita hay que tener en cuenta algunas correcciones, y una posible reducción en la fracción secreta. En primer lugar, esto es debido a que la estimación de los parámetros se realiza sobre una muestra finita, por tanto, se debe considerar el peor caso compatible con las fluctuaciones estadísticas. En segundo lugar, el rendimiento del post-procesado contiene términos que solo se anulan en el límite asintótico.

2.3. Seguridad en QKD

2.3.1. Definición de seguridad

Los sistemas QKD han suscitado un considerable interés en la comunidad científica ya que, en principio, proporcionan seguridad incondicional. Como se ha definido en el capítulo 1, esto significa que se puede demostrar que el sistema es seguro sin ninguna restricción en las capacidades que tenga Eve como espía, salvo los límites fijados por la física [6].

La posibilidad de alcanzar seguridad incondicional está estrechamente relacionada con los principios de la física cuántica. Para obtener información de la clave, Eve debe interaccionar con la clave, resultando en una trasformación del estado que Alice y Bob pueden medir. Esta acción implica que los ataques realizados al sistema inducen en el propio sistema un número determinado de errores que permiten al receptor, estimar la cantidad de información que ha podido adquirir el espía Eve. Con los algoritmos adecuados, Alice y Bob pueden determinar si la transmisión de la clave ha sido segura en función de la estimación de clave que Eve ha podido recuperar [4].

En este punto, conviene remarcar que el significado de la seguridad incondicional está definido estrictamente en el anterior párrafo, y no se debe confundir con el término de seguridad absoluta [3]. No obstante, hay otras condiciones necesarias para garantizar la seguridad incondicional. En primer lugar, Eve no puede tener acceso a los dispositivos que Alice y Bob utilizan en el sistema QKD. En segundo

lugar, los generadores de números aleatorios, con los que se selecciona el estado que se envía y las medidas que se realizan en Bob, tienen que ser de confianza. Por último, el canal clásico debe estar autentificado y los ataques de Eve tienen que cumplir las leyes de la física cuántica.

En todos los estudios y análisis de seguridad, se parte de los principios mencionados anteriormente [7]. Además, hay otros aspectos que deben ser tenidos en cuenta para garantizar seguridad incondicional. Es decir, la descripción teórica de los estados debe corresponderse con las señales que realmente se intercambian, por ejemplo, no se debe describir un sistema real de QKD como "ideal", sino que hay que tener en cuenta las posibles desviaciones que pueda sufrir, y se debe asegurar que no existen más canales por donde la información de la clave fluya de manera incontrolada, como por ejemplo un trasmisor en Bob que le comunique a Eve los números obtenidos por su generador de números aleatorios.

2.3.2. Ataques en los sistemas QKD

Antes de presentar los protocolos específicos de los sistemas QKD conviene describir los tipos de ataques que Eve puede realizar sobre el canal cuántico para obtener información. En principio hay tres tipos de ataques [2-3]:

- Ataques individuales o incoherentes. En este caso, Eve obtiene muestras individuales de cada bit cuántico (qubit) y mide sus muestras una tras otra.

- Ataques coherentes. Eve procesa varios qubits coherentemente. Los ataques coherentes más generales son llamados *ataques mutuos*.

- Ataques colectivos. Es un caso intermedio donde Eve obtiene muestras individuales de cada qubit, como en el caso de ataques individuales, pero puede medir las muestras coherentemente.

En los ataques coherentes y colectivos, se asume que Eve mide sus muestras después de que Alice y Bob han completado la discusión pública que comprende la reconciliación de bases, la corrección de errores y la amplificación de la privacidad. Para ataques individuales, se asume que Eve espera solamente hasta que la reconciliación de bases haya finalizado. Esta asunción está basada en el hecho de que Eve no puede extraer más información esperando hasta después de la discusión pública porque va a medir todas sus muestras independientemente.

Una propiedad interesante de los ataques individuales es que se pueden trasladar totalmente a un problema clásico: Alice, Bob y Eve tienen información clásica de la

clave en forma de variables aleatorias α, β y γ respectivamente, y las leyes de la física cuántica imponen ligaduras en la distribución de probabilidad $P(\alpha, \beta, \gamma)$. Estos escenarios ya han sido estudiados en profundidad, y los resultados clásicos obtenidos pueden ser aplicados directamente en este campo [8].

A continuación se describen los ataques más relevantes y conocidos:

- Ataque de interceptación y reenvío *(Intercept and resend attack)*. Es el ataque más simple, donde Eve intercepta los fotones individuales, los mide en una base que el escoge aleatoriamente entre dos bases usadas por Alice y envía nuevos fotones a Bob preparados acorde con los resultados obtenidos [6].

- Ataque del divisor de haz *(Beam splitting attack)*. Este es probablemente el ataque más apropiado que se puede realizar en los sistemas ópticos de distribución cuántica de clave. Esto es debido a que las pérdidas asociadas al medio de transmisión óptico que conecta a Alice y Bob pueden ser descritas de forma equivalente como la combinación de un medio ideal sin pérdidas y un divisor de haz óptico. Este hecho permite siempre a Eve introducir un acoplador óptico en el canal cuántico y conseguir extraer parte de la clave midiendo a través de una de las salidas del acoplador mientras que Bob mide a partir de la señal procedente de la otra salida, sin notar la presencia del espía.

- Ataque de la división del número de fotones *(Photon Number Splitting Attackn, PNS)*. En este ataque Eve realiza una medida no destructiva del número de fotones de cada pulso. Cada vez que detecta la presencia de más de un fotón en un pulso, almacena uno para medirlo, y el resto es enviado a Bob. En el caso de que mida un fotón individual bloquea el pulso [7].

2.4. Protocolos

Existe una amplia variedad de protocolos, que se pueden clasificar en tres grandes grupos: protocolos de variable discreta, protocolos de variable continua y protocolos de referencia de fase distribuida [3]. La diferencia principal de estas tres familias radica en cómo se realiza la detección. En los protocolos de variable discreta y de referencia distribuida es necesario un detector de fotones. En el caso de protocolos de variable continua son necesarias técnicas de detección heterodinas u homodinas.

Una completa descripción de todos los protocolos QKD se sale del objetivo de este capítulo, no obstante se proporcionará una breve descripción de algunos de ellos. En concreto, se describen los protocolos BB84 y B92, que son los de mayor interés ya que son los protocolos que se implementan en los sistemas de codificación en frecuencia, objetivo de estudio en esta Tesis.

2.4.1. El protocolo BB84

El protocolo BB84 pertenece al grupo de variable discreta, y su nombre proviene de sus inventores, Charles Bennet y Gilles Brassard y el año de su primera publicación (1984) [6]. En la figura 2.1, se muestra un esquema del protocolo.

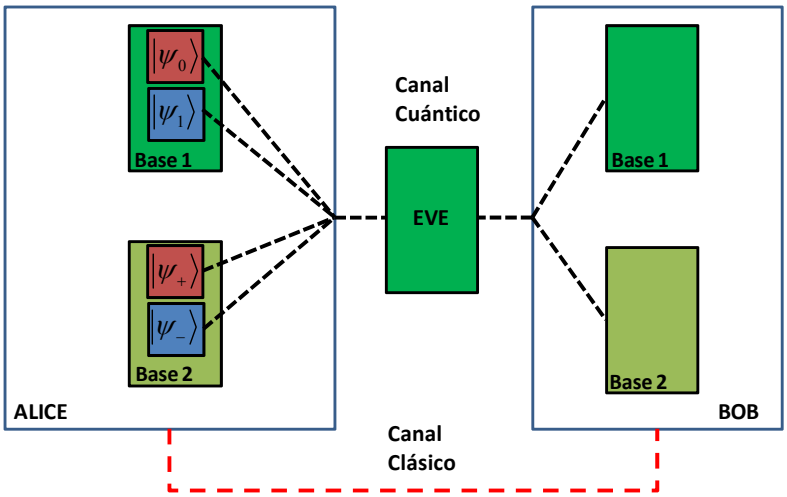

Figura 2.1. Esquema del procedimiento para implementar el protocolo BB84.

En este protocolo, Alice prepara y envía a Bob una serie de qubits aleatorios, que son seleccionados del siguiente grupo de cuatro estados:

$$Base_1 = \begin{cases} |\psi_0\rangle = |+,x\rangle = |0\rangle \\ |\psi_1\rangle = |-,x\rangle = |1\rangle \end{cases}$$

$$Base_2 = \begin{cases} |\psi_+\rangle = |+,y\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \\ |\psi_-\rangle = |-,y\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right] \end{cases} \tag{2.3}$$

donde los dos primeros estados de la expresión (2.3) forman una primera base y los otras dos forman una segunda, de forma que las condiciones $\langle \psi_0 | \psi_1 \rangle = 0$ y $\langle \psi_+ | \psi_- \rangle = 0$ correspondientes al producto escalar entre estados deben ser satisfechas. Al mismo tiempo, los estados de diferentes bases de la expresión (2.3) no son ortogonales, ya que $\langle \psi_{0,1} | \psi_{+,-} \rangle \neq 0$. Como consecuencia, no existe un procedimiento de medida que pueda determinar al 100 % qué estado está trasmitiendo Alice a Bob.

El procedimiento de medida empleado por Bob para determinar el estado que Alice envía es el siguiente: Bob escoge aleatoriamente una de las dos posibles bases de medida ($Base_1$ o $Base_2$), realiza la medida y almacena el resultado. Repite el resultado con todos los estados enviados por Alice. Una vez que el proceso finaliza Alice comunica a Bob, a través del canal público, las bases que ella ha seleccionado para codificar cada uno de los qubits, pero sin revelar en ningún momento el estado seleccionado. A continuación Bob hace público que bases ha empleado para realizar las medias en cada uno de los qubits que ha recibido, sin indicar el resultado de la medida. Alice y Bob retienen los qubits donde la base elegida por ambos coincide y descartan el resto. Como resultado obtienen una cadena de bits de longitud aproximada la mitad de la original. Esta cadena se denomina, como ya se ha mencionado anteriormente, clave en crudo.

Mientras Alice trasmite a Bob sus estados, Eve puede interaccionar con ellos e interferir en la comunicación. Eve no sabe cuál de los cuatro estados de la expresión (2.3) ha seleccionado Alice. Lo único que puede hacer es escoger una de las dos bases para realizar sus medidas. En el caso que acierte y escoja la misma base de Alice, Eve podrá trasmitir el estado correcto a Bob. En el caso que seleccione una base distinta, Eve trasmitirá a Bob un estado incorrecto y este podrá detectar la presencia del espía. Es importante remarcar que Eve no sabrá si ha elegido la base correcta hasta que se lleva a cabo la comunicación en el canal público. Por tanto, existe el 50 % de probabilidad de que Eve haya usado la base incorrecta en sus medidas, y como consecuencia existan errores entre Alice y Bob.

Alice y Bob tienen una forma sencilla de detectar la presencia de Eve. Pueden seleccionar un subconjunto de los bits transmitidos, hacerlos públicos y compararlos. Con este procedimiento se obtendría un 25 % de errores en la muestra, lo cual delata la presencia de Eve. Si el error es más pequeño, entonces Alice y Bob pueden llevar a cabo otro proceso, conocido como amplificación de la privacidad con el resto de bits que no han sido hechos públicos.

La amplificación de la privacidad se lleva a cabo tomando pares de bits de la clave y realizando con ellos una operación lógica *OR* exclusive. Si Alice y Bob obtienen el mismo resultado retienen el par de bits, y si no, los descartan. La seguridad incondicional ha sido probada para este protocolo mediante diferentes técnicas [9, 10].

2.4.2. El protocolo B92

El protocolo B92 es una versión simplificada del BB84. En 1992, Bennet propuso el uso de dos estados no ortogonales para codificar los qubits en vez de los cuatro usados en el protocolo BB84 [11]. La figura 2.2 resume el procedimiento básico del protocolo.

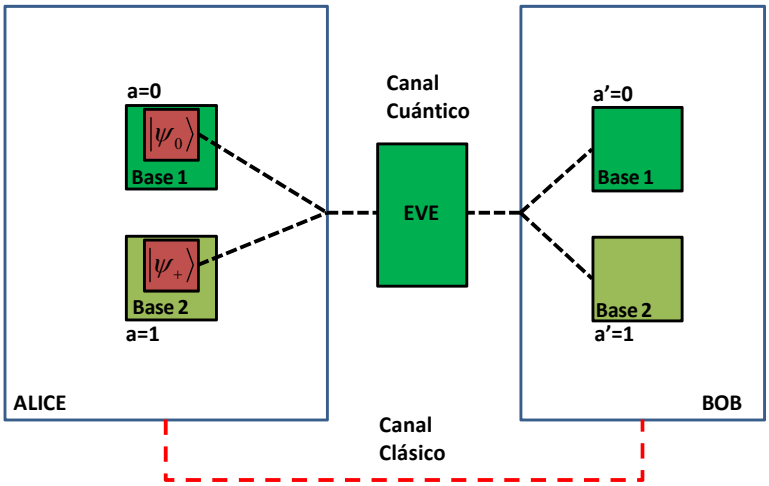

Figura 2.2. Esquema del procedimiento para implementar el protocolo B92.

La operación del protocolo se puede describir de la siguiente manera. En primer lugar, Alice genera un bit aleatorio *a* y trasmite a Bob el qubit:

$$|\psi\rangle = \begin{cases} |0\rangle & si\ a = 0 \\ |+\rangle & si\ a = 1 \end{cases} \tag{2.4}$$

Bob también genera un bit aleatorio *a'*. Si este bit es un 0, él emplea la base $\{|\psi_0\rangle, |\psi_1\rangle\}$ para realizar sus medidas. Si, por lo contrario, el valor del bit es un 1, emplea la base $\{|\psi_+\rangle, |\psi_-\rangle\}$ para medir el fotón enviado. El resultado de las medidas de Bob es otro bit *b* que comunica a Alice usando el canal público. Lo más

importante del protocolo es que Alice y Bob guardan en secreto sus secuencias de bits, *a* y *a'* respectivamente. La clave en crudo está formada por un subconjunto de bits donde el resultado de la medida de Bob es *b=1*, lo cual solo puede ocurrir en dos casos, cuando Alice escoge *a=0* y Bob *a'=1*, o también cuando el bit de Alice es *a=1* y el de Bob es *a'=0*. La probabilidad de escoger correctamente las bases es ½.

Como en el caso del protocolo BB84, Alice y Bob emplean un procedimiento para analizar los errores y de esta manera poder detectar la presencia de un posible espía. Si el número de errores es lo suficientemente bajo, se lleva a cabo el procedimiento de la amplificación de la privacidad para reducir la posible información que tenga Eve de la clave.

2.5. Tasa de error de trasmisión y de clave secreta

Ya hemos comentado en la sección anterior, que la ecuación (2.2) establece la tasa de secreta de bit R_{net} para un sistema QKD a partir del producto de dos términos: la tasa en crudo R_{sift} y la fracción secreta r. Es útil entrar más en profundidad dentro de estos dos factores, ya que serán claves para evaluar la eficiencia de los sistemas QKD en general, y más concretamente en los sistemas basados en la codificación en frecuencia, que son el objeto de estudio de esta Tesis. Mientras la tasa en crudo R_{sift} es sencilla de obtener, la fracción segura puede ser mucho más compleja, y depende de las distintas consideraciones de seguridad que se hagan, incluyendo el tipo de ataque que realice Eve [2, 3]. En este trabajo solo se va a analizar la tasa de bit y de error para el protocolo BB84, que es el protocolo con el que se va a trabajar a lo largo de la Tesis. Para el resto de protocolos se pueden encontrar resultados en [3].

2.5.1. Tasa de clave en crudo

La tasa de clave en crudo viene dada en general por [3]:

$$R_{sift} = f_{rep} \cdot p_{BOB} \tag{2.5}$$

El parámetro f_{rep} representa la tasa de repetición de la fuente y p_{BOB} es la probabilidad de detección de Bob que depende del protocolo que se use y del sistema físico que se utilice en base a las pérdidas de los componentes, la eficiencia de los detectores, etc. En el caso de detectar en el intervalo de tiempo de detección, se obtiene, para el protocolo BB84 que:

$$p_{BOB} = \frac{1}{2}\rho\mu T T_B \tag{2.6}$$

con un número promedio de fotones por pulso $\mu \leq 1$. La eficiencia de detección viene dada por el parámetro ρ y las pérdidas ópticas del canal y el proceso de detección vienen dadas por T y T_B, respectivamente.

El parámetro f_{rep} está limitado por el máximo valor que puede alcanzar la fuente f_{rep}^{max} y otros factores como:

$$f_{rep} = \min\left\{ f_{rep}^{\max}, \frac{1}{\tau_d \rho\mu T T_B}, \frac{1}{T_{dc}} \right\} \tag{2.7}$$

donde el factor $1/\tau_d\rho\mu T T_B$ representan la limitación impuesta por el tiempo muerto del detector τ_d. El factor $1/T_{dc}$ representa la limitación debida al ciclo útil, que significa que dos pulsos consecutivos no pueden ser enviados con un tiempo de separación mayor que T_{dc}, como ocurre en los sistemas "*plug and play*".

2.5.2. Fracción secreta

El post-procesado es necesario para extraer la clave secreta final [4]. Las cotas de la fracción secreta dependerán de cómo se lleve a cabo este paso. Existen dos formas de implementar este post-procesado. Como primera opción, Alice o Bob pueden enviar la información clásica a través del canal público hacia el otro, el cual actúa acorde al procedimiento establecido, pero sin contestación. El segundo procedimiento consiste en que Alice y Bob se envían información mutuamente y por tanto, en ambas direcciones.

Mientras que para el post-procesado en dos direcciones no se conoce un procedimiento óptimo para conseguir la clave final, para el caso de una única dirección de transmisión el procedimiento óptimo consta de dos pasos. El primero es la corrección de errores. Al final de este proceso la clave de Alice y Bob es menor, pero están perfectamente correlacionadas. La fracción de símbolos que pueden ser extraídos de una lista de símbolos parcialmente correlacionados está acotada por la información mutua [8]:

$$I(A:B) = H(A) + H(B) - H(A \cap B) = H(A) - H\left(\frac{A}{B}\right) \tag{2.8}$$

donde *H* representa la entropía de la distribución de probabilidad. El segundo paso es el de la amplificación de la privacidad (PA) [5]. Este proceso elimina la información mutua que pueda haber extraído Eve de la clave. Como resultado de la PA, una parte de la clave en crudo es eliminada. Esta parte viene descrita por $min(I_{EA}, I_{EB})$ donde I_{EA} y I_{EB} representan la información que Eve tiene de la clave en crudo de Alice y Bob, respectivamente.

Con estas aclaraciones, la expresión para la fracción de clave segura que puede ser extraída usando post-procesado viene dada por:

$$r = I\left(A:B\right) - \min\left(I_{EA}, I_{EB}\right) = I\left(A:B\right) - I_E \tag{2.9}$$

2.5.3. Tasa de clave secreta y tasa de error para el protocolo BB84

En estos protocolos se asume que no existe una referencia de fase. De esta manera, los estados emitidos por la fuente de Alice pueden ser descritos como pulsos que contienen n fotones con una probabilidad $p_A(n)$. Los parámetros estadísticos que describen el intercambio de clave son básicamente la tasa de detección y de error.

Si R_{sift} representa la tasa en crudo de detección total, usaremos R_n para designar la tasa de detección cuando Alice trasmite n fotones por pulso [3]:

$$R_{sift} = \sum_n R_n \tag{2.10}$$

Es también útil definir la fracción:

$$Y_n = \frac{R_n}{R_{sift}} \Rightarrow \sum_n Y_n = 1 \tag{2.11}$$

Las cuentas erróneas correspondientes a R_n serán etiquetadas como R_n^w de tal manera que la tasa de error para los pulsos con *n* fotones viene dada por:

$$\varepsilon_n = \frac{R_n^w}{R_n} \tag{2.12}$$

Y la tasa de error de bit (*QBER*) será:

$$QBER = \sum_n Y_n \varepsilon_n \tag{2.13}$$

En el caso de los protocolos estudiados, las condiciones sobre la función entropía $H(A)=H(B)=1$ y $H(A/B)=H(B/A)=h(QBER)$ se satisfacen, donde h es la entropía binaria [3]. Por tanto, sustituyendo éstas condiciones en la ecuación (2.8), podemos llegar a la siguiente relación $I(A:B)=1-h(QBER)$. Por razones prácticas, es realista proporcionar formulas que tengan en cuenta imperfecciones en la corrección de errores. A partir de las expresiones (2.2) y (2.9), se puede obtener la siguiente expresión:

$$R_{net} = R_{sift}\left[1 - leak_{EC}\left(QBER\right) - I_E\right] \tag{2.14}$$

donde $leak_{EC}\left(QBER\right) \leq h\left(QBER\right)$.

El último término de la ecuación (2.14) se va a desarrollar a continuación para comprobar que Eve solamente gana información de los pulsos no vacios y siempre que Bob detecte los fotones que ella envía. También, se puede comprobar que el ataque colectivo óptimo incluye la medida del número de fotones. En tal caso, la información de Eve viene dada por:

$$I_E = \max_{Eve}\left(\sum_n Y_n I_{E,n}\right) \tag{2.15}$$

Y el valor máximo viene dado por todos los posibles ataques de Eve compatibles con los parámetros de medida.

En el caso particular del protocolo BB84, la probabilidad de que Bob acepte el bit solo depende de si ha usado la misma base de Alice, lo cual ocurre con probabilidad p_{sift}. Por tanto, si denotamos por $\overline{f}_{rep} = p_{sift} f_{rep}$ obtenemos [3]:

$$R_n = \overline{f}_{rep} p_A\left(n\right) f_n \tag{2.16}$$

En esta expresión $p_A(n)$ es la probabilidad de que la fuente de Alice genere un pulso con n fotones y f_n es la probabilidad de que Eve envíe alguna señal, para un pulso de n fotones recibidos, a Bob. En el contexto del protocolo BB84, $I_{AE}= I_{BE}$. Si Alice envía un pulso sin fotones ($n=0$) pero Bob tiene una detección, se tiene que $I_{E,0}=0$. Para pulsos de un fotón, Eve puede ganar información a expensas de introducir un error ε_1, de tal manera que la información que puede ganar es $I_{E,1}=h(\varepsilon_1)$. En el caso de fotones múltiples, el mejor ataque es el PNS [7], en donde, como se explico en la sección 2.3.2, Eve reenvía un fotón a Bob y guarda el otro. De esta manera, para

$n \geq 2$ se obtiene $I_{E,n}=1$. Sustituyendo estos valores en la expresión (2.15) obtenemos:

$$\begin{aligned} I_E &= \max_{Eve}\left(Y_1 h\left(\varepsilon_1\right) + \sum_{n\geq 2} Y_n \right) = \max_{Eve}\left(Y_1 h\left(\varepsilon_1\right) + 1 - Y_0 - Y_1 \right) = \\ &= 1 - \min_{Eve}\left(Y_0 - Y_1\left(1 - h\left(\varepsilon_1\right)\right)\right) \end{aligned} \tag{2.17}$$

Los únicos parámetros que podemos medir con el protocolo BB84 son R_{sift} y la tasa de error de bit *QBER*. Sin ninguna consideración adicional, si asumimos como primera aproximación que $\varepsilon_{n\geq 2} = 0$, a partir la expresión (2.13) se obtiene que $\varepsilon_1 = QBER/Y_1$. Por tanto, la expresión anterior (2.17) puede expresarse como:

$$I_E = 1 - \min_{Eve}\left(Y_0 - Y_1\left(1 - h\left(\frac{QBER}{Y_1}\right)\right)\right) \tag{2.18}$$

A partir de la expresión (2.18) vemos que el ataque óptimo de Eve es el que minimiza el factor Y_1. Para ello, es necesario que $f_0 = 0$ y $f_{n\geq 2} = 1$ en cuyo caso, a partir de las expresiones (2.11) y (2.16), obtenemos:

$$\begin{aligned} Y_1 &= 1 - \sum_{n\geq 2} Y_n = \frac{R_{sift} - \sum_{n\geq 2} R_n}{R_{sift}} = 1 - \frac{1}{R_{sift}} \sum_{n\geq 2} f_{rep}\, p_A\left(n\right) = \\ &= 1 - \frac{\overline{f}_{rep}}{R_{sift}} \sum_{n\geq 2} p_A\left(n\right) = 1 - \frac{\overline{f}_{rep}}{R_{sift}}\, p_A\left(n \geq 2\right) \end{aligned} \tag{2.19}$$

Finalmente, para el caso del protocolo BB84 se obtiene [7]:

$$\begin{aligned} I_E &= 1 - Y_1\left[1 - h\left(\frac{QBER}{Y_1}\right)\right] \\ R_{net} &= R_{sift}\left\{ Y_1\left[1 - h\left(\frac{QBER}{Y_1}\right)\right] - leak_{EC}\left(QBER\right)\right\} \end{aligned} \tag{2.20}$$

A partir de la expresión anterior, podemos comprobar cómo el tipo de fuente que se utilice determina la cantidad de clave secreta que va a poder recuperarse en función del QBER existente. Para el caso de considerar fuentes de un solo fotón se tiene que

$p_A(1)=1$, y por tanto, a partir de la expresión (2.19) tenemos que $Y_1=1$. Siendo la tasa de detección total esperada $R_{sift} = \overline{f}_{rep} tt_B \rho$ y asumiendo por simplicidad un proceso de corrección de errores óptimo, es decir, $leak_{EC}(QBER)=h(QBER)$, la tasa secreta de bit a partir de la expresión anterior queda como:

$$R_{net} = \overline{f}_{rep} tt_B \rho \left[1 - 2 \cdot h\left(QBER\right)\right] \tag{2.21}$$

Como era de esperar, R_{net} es lineal con respecto a las pérdidas y a la eficiencia del detector.

Para el caso de utilizar estados coherentes donde las probabilidades vienen dadas por la distribución de Poisson, la probabilidad de emitir n fotones viene dada por $P_A\left(n\right) = \frac{\mu^n e^{-\mu}}{n!}$ [3] y la probabilidad de detección total esperada será $R_{sift} = \overline{f}_{rep} \mu tt_B \rho$. El objetivo es encontrar cuál es número de fotones μ que optimiza la tasa secreta R_{net} para este tipo de fuentes.

Para optimizar el número de fotones μ se debe encontrar un compromiso entre una alta probabilidad de detección R_{sift} y una baja probabilidad de emitir varios fotones $p_A(n>1)$. Para alcanzar este valor óptimo aproximamos $p_A(n=1)\approx\mu$, $p_A(n=2)\approx\mu^2/2$, $p_A(n>2)\approx 0$ y el caso límite dado por $QBER=0$. En este caso la ecuación (2.20) se convierte en $R_{net} \approx \overline{f}_{rep} \mu tt_B \rho - {\mu^2}/{2}$ donde el valor de μ que maximiza la expresión es $\mu_0=tt_B \rho$. Para obtener una estimación de R_{net} para $QBER>0$ podemos hacer la aproximación de usar μ_0 para calcular Y_1, es decir, tomar $Y_1=1/2$. Con ello, es inmediato encontrar el máximo valor alcanzable para R_{net}. Escribiendo $F\left(QBER\right) = 1 - h\left(2QBER\right) - h\left(QBER\right)$, el valor más alto alcanzable es

$$R_{net} = \overline{f}_{rep} tt_B \rho \frac{1}{2} \mu_{opt} F\left(QBER\right) \tag{2.22}$$

que se obtiene para un número de fotones óptimo dado por

$$\mu_{opt} = \frac{tt_B \rho F\left(QBER\right)}{1 - h\left(2QBER\right)} \tag{2.23}$$

Otro tipo de fuentes, usadas en los sistemas de distribución de clave cuántica, son aquellas que emiten pulsos con distintas intensidades, la idea que hay detrás de esto es detectar ataques PNS, los protocolos que usan este tipos de fuentes son llamados

protocolos con *decoy states* [12]. Para llevar a cabo estos protocolos Alice cambia el número de fotones μ entre distintos valores de los pulsos aleatoriamente durante el protocolo. Al final del intercambio de señales cuánticas, ella publica una lista de valores y los resultados son almacenados para estimar los parámetros independientemente para cada valor de μ. Con este método sencillo, Alice y Bob miden 2χ parámetros, que son principalmente R_{sift}^{μ} y $QBER^{\mu}$.

Aunque el conjunto χ es públicamente conocido como parte del protocolo, el hecho de que χ >1 no permite a Eve adaptar una estrategia para los pulsos trasmitidos, ya que Eve desconoce el μ de cada uno. Esto implica que tanto f_n como ε_n son independientes de μ, por tanto:

$$R_n^{\mu} = \overline{f}_{rep}\, p_A\left(n\middle|\mu\right) f_n \tag{2.24}$$

Y los parámetros de medida son en este caso:

$$\begin{aligned} R_{sift}^{\mu} &= \sum_{n\geq 0} R_n^{\mu} \\ QBER^{\mu} &= \sum_{n\geq 0}\left(\frac{R_n^{\mu}}{R_{sift}^{\mu}}\right)\varepsilon_n \end{aligned} \tag{2.25}$$

La expresión (2.25) define un sistema de $2|\chi|$ ecuaciones, donde las incógnitas son f_n y ε_n. En este caso, la optimización de (2.18) se suele llevar a cabo usando la cota mínima de Y_1^{μ} y la cota máxima de ε_1 de las obtenidas del conjunto $\left\{R_{sift}^{\mu}, QBER^{\mu}\right\}_{\mu\in\chi}$. Las contribuciones más relevantes vienen de los términos con *n=0,1, 2,* por tanto, un protocolo con decoy states con $|\chi|=3$ se aproximan muy bien a la cantidad óptima. Si consideramos que f_n y ε_n están exactamente determinados y que la etapa de post-procesado se realiza separadamente para cada valor de μ, entonces para cada uno de los posibles valores de μ se tiene

$$I_E^{\mu} = 1 - Y_0^{\mu} - Y_1^{\mu}\left[1 - h\left(\varepsilon_1\right)\right] \tag{2.26}$$

Por tanto, la tasa de trasmisión secreta para cada μ y la total vienen dadas por

$$R_{net}^{\mu} = R_{sift}^{\mu}\left\{Y_0^{\mu} + Y_1^{\mu}\left[1 - h\left(\varepsilon_1\right)\right] - leak_{EC}\left(QBER^{\mu}\right)\right\}$$
$$R_{net} = \sum_{\mu\in\chi} R_{net}^{\mu} \tag{2.27}$$

Si suponemos que se usa el mismo valor de μ en casi todos los pulsos (y esté es el parámetro que queremos optimizar), y que se emplea un número de *decoys* suficientes para realizar una correcta estimación de los parámetros entonces los valores esperados estarán dados por $R^{\mu} = \overline{f}_{rep}\mu t t_B \rho$, $R_1^{\mu} = \overline{f}_{rep}\mu e^{-\mu} t t_B \rho$ y $\varepsilon_1 = QBER$. Introduciendo estos valores en la ecuación (2.27) obtenemos un valor para la tasa secreta de $R_{net} \approx \overline{f}_{rep}\mu t t_B \rho\left\{e^{-\mu}\left[1 - 2h\left(QBER\right)\right] - h\left(QBER\right)\right\}$ usando $e^{-\mu} \approx 1 - \mu$ esta expresión alcanza su máximo valor de

$$R_{net} \approx \frac{1}{2}\overline{f}_{rep} t t_B \rho \mu_{opt}\left[1 - 2h\left(QBER\right)\right] \tag{2.28}$$

que se obtiene con un número de fotones óptimos de

$$\mu_{opt} \approx \frac{1}{2}\left(1 - \frac{h\left(QBER\right)}{1 - h\left(QBER\right)}\right) \tag{2.29}$$

Con estos resultados se puede concluir que para sistemas sin *decoy states* $\mu_{opt} \sim t$ y como consecuencia $R_{net} \propto t^2$: cuando mas pérdidas hay, mas atenuada debe estar la fuente. Esto es debido al ataque PNS: Alice debe asegurar que Eve no puede reproducir la tasa de trasmisión de Bob usando solamente fotones que provienen de pulsos con dos fotones. Con *decoy states*, se puede determinar la fracción de detecciones que provienen de pulsos con más de dos fotones. Si esta fracción es tan baja como la esperada, se puede descartar el ataque PNS, consiguiendo una tasa de trasmisión $R_{net} \propto t$ que presenta la misma tendencia que la fuente de un solo fotón.

2.6. Sistemas de distribución de clave cuántica basados en fibra óptica

2.6.1. Sistemas con codificación en polarización

Usar la polarización para codificar los qubits en los fotones es una de las soluciones más naturales. La primera demostración de un sistema real QKD se realizó por este

procedimiento por Bennett y su grupo [13]. Implementaron un sistema en donde Alice y Bob intercambiaban pulsos débiles de luz, producidos por un diodo láser y que contenían menos de un fotón por pulso, una distancia de 30 cm en el aire. Aunque la distancia era apenas de decenas de centímetros, este experimento supuso un gran impacto en la comunidad científica, ya que se mostraba, por primera vez, la posibilidad de codificar los bits en estados cuánticos de luz en vez de los pulsos ópticos clásicos.

En la figura 2.3, se muestra un sistema típico QKD con codificación en polarización y funcionando con el protocolo BB84 [2]. El trasmisor (Alice) consiste en cuatro diodos láser, los cuales emiten pulsos clásicos estrechos (alrededor de 1ns) con ángulos de polarización de -45º, 0º, 45º y 90º. Cada qubit es codificado seleccionando aleatoriamente la emisión de uno de los cuatro láseres. Los pulsos son atenuados por una serie de filtros hasta reducir el número medio de fotones por debajo de 1. Posteriormente, los qubits son transmitidos a Bob por el canal cuántico. En estos sistemas es esencial que la polarización se mantenga para que Bob pueda ser capaz de extraer la información que codifica Alice.

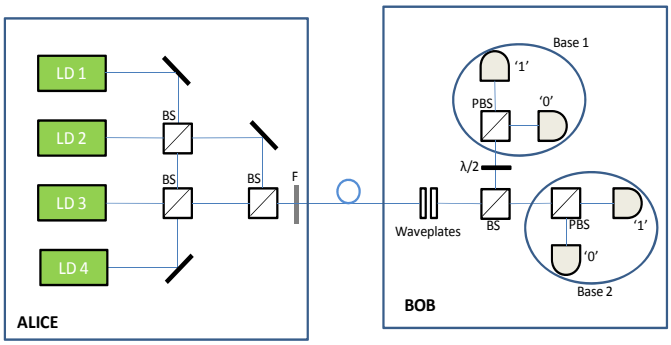

Figura 2.3. Esquema de un sistema con codificación basado en polarización.

La dispersión por polarización que sufren los fotones en el canal puede ocasionar que se modifique el estado de polarización a lo largo de la propagación, pasando a un estado de luz no polarizada. Para evitar esto, el retardo entre los modos de polarización debe ser menor que el tiempo de coherencia. Lo cual es una ligadura sobre el tipo de láser que debe usar Alice.

En Bob los pulsos son trasmitidos desde la fibra a una serie de láminas de onda para recuperar el estado inicial de polarización que se pierde durante la trasmisión en la fibra. Después, los pulsos llegan a un divisor de polarización, que implementa la elección de Base. Los fotones trasmitidos son analizados en la base vertical-horizontal con un divisor de polarización y dos contadores de fotones. El estado de

polarización de los fotones reflejados es primeramente rotado 45º con una lámina de onda (es decir 45º→0º). A la salida de la lámina los fotones son analizados con otro divisor de polarización y detectados con otros dos contadores de fotones.

Muller y su grupo de trabajo han usado este tipo de sistemas QKD. En un primer paso, llegaron a distribuir la clave con una distancia de enlace de fibra de 1100 metros y con fotones de longitud de onda de 800 nm [14]. Más tarde, usando fotones de longitud de onda en segunda ventana (1300 nm) alcanzaron longitudes de 23 km [15]. Lo interesante de este experimento es que, por primera vez, se llevó a cabo usando una instalación de fibra fuera del laboratorio.

El problema de estos sistemas es que, debido a las fluctuaciones de la fibra, los estados de polarización solo se mantienen durante un periodo breve de tiempo lo que conlleva a un aumento crítico del QBER [2]. Por tanto, los sistemas deben incorporar elementos activos que compensen estas desviaciones, complicando el sistema.

La tasa de bit más elevada que se han conseguido con codificación en polarización es de 1 MHz [16] y la máxima distancia asciende a 200 km con una tasa de bit de 15 bit/s [17].

2.6.2. Sistemas con codificación en fase

Aunque la propuesta inicial de los sistemas QKD se basaba en estados de polarización, también es posible codificar la clave en la fase de los fotones [1]. Estos esquemas están basados en las propiedades de los interferómetros y la codificación se lleva a cabo cambiando el camino óptico de los brazos del interferómetro. En la figura 2.4(a), se puede observar un esquema típico de estos sistemas para implementar el protocolo BB84. Tanto Alice como Bob controlan un modulador de fase en cada uno de los brazos del interferómetro. Si Alice envía un fotón a Bob, debido a la interferencia, este solo detectará el fotón en el detector *0* ó en el *1*, dependiendo de la diferencia de fase $\Delta\phi=\phi_A-\phi_B$ entre los dos caminos, de la misma manera que en el caso clásico.

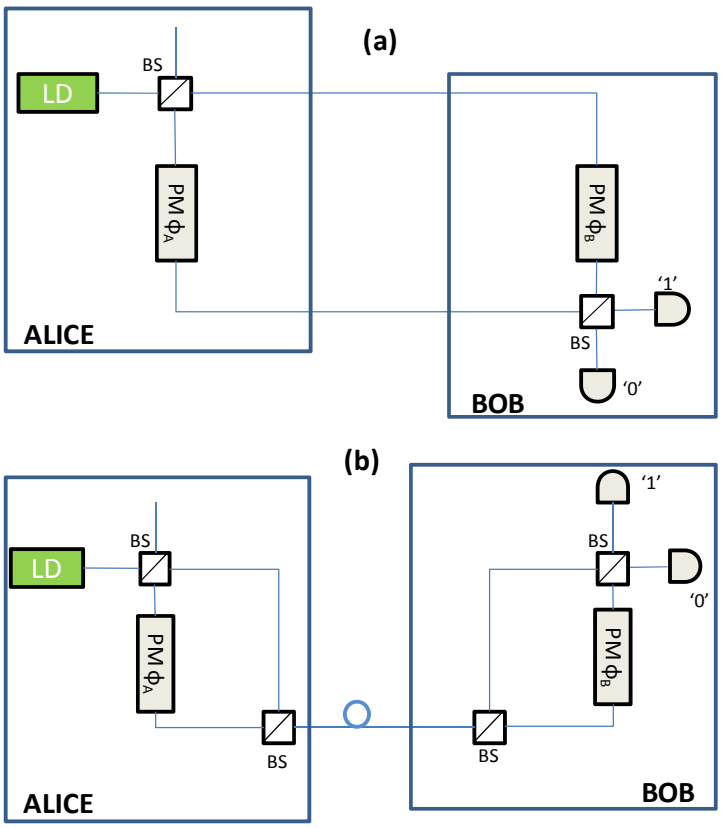

Figura 2.4. Esquemas de dos sistemas basados en codificación en fase mediante la utilización de (a) una configuración Mach-Zehnder o (b) una configuración doble Mach-Zehnder.

Si, por ejemplo, la diferencia de fase es nula ($\Delta\phi=0$) el fotón llegará al detector *0*, si por el contrario, $\Delta\phi=\pi$ el fotón llegará al detector *1*. Para valores intermedios el fotón podrá llegar a uno de los dos detectores, por ejemplo, si $\Delta\phi=\pi/2$ el fotón tendrá la misma probabilidad de llegar a uno de los dos detectores. Si se aplica alguna medida al fotón en uno de los brazos, para determinar en qué brazo está el fotón, no se producirá interferencia y la información será destruida. Aunque el sistema mostrado en la figura 2.4(a) funciona bien en condiciones de laboratorio controladas, es prácticamente imposible mantener la diferencia de fase estable cuando Alice y Bob están separados más de unos pocos metros.

En 1992, Bennett propuso una modificación de este esquema para resolver el problema de la estabilidad [11]. El esquema se basa en el uso de dos interferómetros Mach-Zehnder desbalanceados, uno para Alice y otra para Bob, conectados en serie por una fibra óptica, como se muestra en la figura 2.4 (b). La ventaja de este

esquema es que los dos *pulsos* del fotón obtenidos a la salida del interferómetro de Alice sufren los mismos efectos a través de la fibra.

Para obtener una buena visibilidad, y por tanto una tasa de error baja, la diferencia de tiempos entre los brazos de los interferómetros debe ser menor que el tiempo de coherencia de los fotones. Esto implica que la diferencia de caminos debe ser de unos pocos milímetros.

La dificultad principal de este tipo de sistemas QKD es que la diferencia de caminos, en los brazos de los interferómetros de Alice y Bob debe mantenerse constante. Fluctuaciones del orden de una fracción de la longitud de onda del fotón produce errores en la distribución de la clave. Esto implica que los interferómetros deben ser estabilizados en temperatura, y además, para intercambios de clave en un periodo de tiempo largo, es necesario incorporar elementos activos para compensar las derivas.

Townsend y su grupo fueron los primeros en probar estos sistemas sobre un rollo de fibra óptica de 10 km [18, 19] que más tarde fue mejorada gracias a la inserción de un divisor de polarización en Bob [20] y con otras técnicas que permitieron aumentar la tasa de trasmisión [21]. Hughes y su equipo también han realizado estudios de esta configuración hasta alcanzar una distancia de 48 km en canales de fibra óptica [22]. Los records obtenidos hasta la fecha con esta configuración para la tasa de bit son de 1 Mbit/s para una distancia de 20 km y de 10 kbit/s para una distancia de 100 km [23].

2.6.3. Sistemas "Plug and Play"

La evolución de los dos sistemas vistos hasta ahora son los llamados "*Plug and Play*" [24]. Su nombre es debido a que no es necesario un ajuste óptico como en los sistemas con codificación en fase y en polarización. En la figura 2.5 se muestra un esquema de este tipo de sistemas.

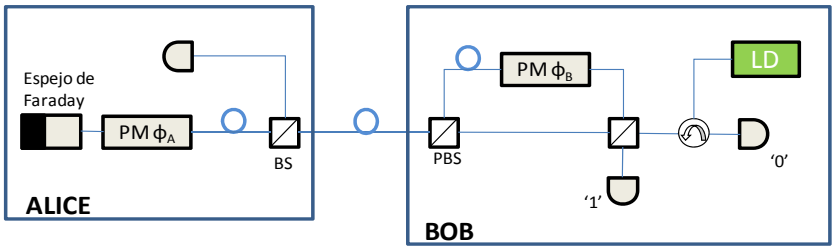

Figura 2.5. Esquema de un sistema *Plug and Play*.

En ellos se combinan los elementos de los sistemas basados en polarización y fase trabajando con un formato de multiplexación por división en el tiempo. Un pulso clásico estrecho es introducido en el sistema por medio de un circulador óptico y se divide posteriormente mediante un acoplador. Uno de los pulsos resultantes, etiquetado como P_1, se propaga por el brazo corto de Bob hasta llegar a un divisor de polarización. La polarización de este pulso se ajusta para que se trasmita en su totalidad en el divisor de polarización, de tal manera que P_1 es trasmitido por el canal de fibra óptica. El segundo pulso, etiquetado como P_2, sigue el brazo largo de Bob hasta el divisor de polarización, nuevamente se ajusta la polarización de este pulso para que sea totalmente reflejado. Un modulador de fase colocado en este brazo permanece inactivo para todos los pulsos salientes. P_2 es entonces transmitido por la fibra con un retardo de 200 ns. En Alice, P_1 llega a un acoplador, donde parte de él se dirige a un detector que genera una señal de control, y el resto se dirige a un atenuador y una línea de retardo cuya misión es que no se propaguen a la vez en el canal de fibra los pulsos que van hacia Alice y los que van hacia Bob. De esta forma, se evita que el ruido proveniente de la dispersión hacia atrás de los pulsos clásicos afecte a los pulsos cuánticos. Por último, el pulso pasa a través de un modulador de fase tras haber sido reflejado por un espejo de Faraday. P_2 sigue el mismo camino que P_1. El modulador de fase solo se activa para aplicar una fase en P_1 que servirá para codificar el bit de la misma forma que en los sistemas con codificación en frecuencia.

La función del atenuador es que los pulsos, a la salida de Alice, no contengan más de una fracción de un fotón. Cuando estos llegan de nuevo al divisor de polarización de Bob, el estado de polarización es exactamente el ortogonal al original, gracias al efecto de los espejos de Faraday en Alice. P_1 es entonces reflejado en vez de ser trasmitido, toma el camino largo y, cuando pasa a través del modulador de fase, Bob activa su modulador para aplicar la elección de base. P_2 es trasmitido y sigue el camino corto. Los dos pulsos llegan al mismo tiempo al acoplador e interfieren. A la salida del acoplador se colocan dos detectores de fotones para conocer el camino seguido por el fotón.

Gisin y su grupo fueron los primeros en usar este sistema para llevar a cabo el protocolo BB84, con una longitud de onda de 1300 nm, a lo largo de un canal de fibra de 23 km que conectaba la ciudad de Ginebra con Nyon [25]. El mismo tipo de experimento se desarrollo independientemente por Bethune y Risk con un enlace de 10 km [26]. Por último Karlsson y su equipo demostraron la viabilidad de estos sistemas a 1550 nm [27]. El record actual con este tipo de sistemas asciende a 67 km [28].

2.6.4. Sistemas con codificación en frecuencia

Los sistemas que codifican los bits en la fase de los fotones requieren una sincronización y estabilización. Debido a la longitud de onda utilizada (aproximadamente 1550 nm), esta condición no es fácil de cumplir. Para solucionar este problema, Goedgebauer y su equipo [29-31] propusieron un esquema alternativo donde el bit es codificado en la diferencia de fase que existe entre las bandas y una portadora óptica sujetas a una modulación de radiofrecuencia. En la figura 2.6, se puede observar un sistema que funciona con esta codificación.

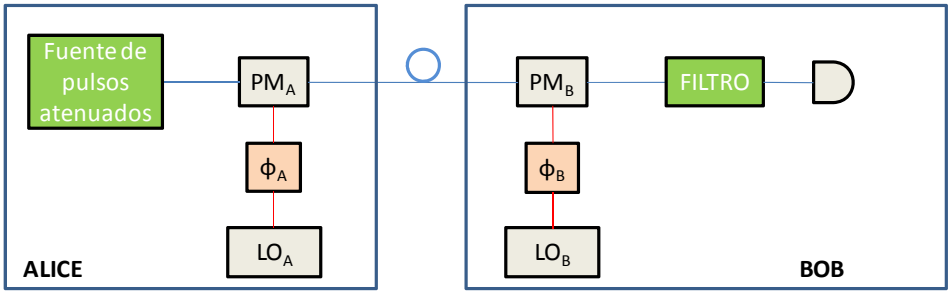

Figura 2.6. Esquema de un sistema con codificación en frecuencia.

La técnica funciona de la siguiente manera: Una fuente óptica emite pulsos monocromáticos estrechos con una frecuencia angular ω_0. Un modulador de fase PM_A modula la fase de este haz con una frecuencia de $\Omega << \omega_0$ y un índice de modulación bajo. Dos bandas son generadas a frecuencias $\omega_0 \pm \Omega$. El modulador de fase es alimentado, por medio de una de sus entradas eléctricas, por un oscilador de radiofrecuencia RFO_A cuya fase es ϕ_A. El pulso es atenuado hasta que las bandas contengan menos de una fracción de un fotón mientras que la portadora permanece clásica. En Bob el pulso sufre una segunda modulación con otro modulador de fase PM_B. El cual es alimentado por un segundo oscilador de radiofrecuencia RFO_B con la misma frecuencia Ω y una fase ϕ_B. Estos osciladores deben estar sincronizados. Tras pasar este segundo modulador el pulso contiene las dos bandas producidas por Alice y las dos producidas por Bob, las cuales interfieren. Bob puede medir el patrón de interferencia en las bandas con un detector, tras eliminar la portadora óptica con un filtro.

La ventaja de este tipo de sistemas es que ahora la interferencia se controla con la fase de los osciladores de radiofrecuencia. Su frecuencia es varios órdenes de magnitud menor que las frecuencias ópticas, y por tanto resulta más fácil de estabilizar y sincronizar. Originalmente estos sistemas se han utilizado para llevar a cabo el protocolo B92 donde Alice selecciona aleatoriamente la fase ϕ_A de cada

pulso asociando el bit *0* con la fase *0* y el bit *1* con la fase π. Bob también selecciona aleatoriamente la fase ϕ_B ente *0* y π. Si $|\phi_A - \phi_B|=0$, la interferencia es constructiva y el detector de fotones tiene una probabilidad distinta de 0 de contar un fotón. Esta probabilidad depende del número de fotones que tienen inicialmente las bandas y de las perdidas del canal. Si, por otro lado, se tiene $|\phi_A - \phi_B|=\pi$, la interferencia es destructiva, y la probabilidad de detección es 0. Por tanto, Bob puede deducir, cada vez que detecta un fotón, que ha aplicado la misma fase que Alice. Cuando un pulso no lleva consigo una detección, el motivo puede ser que se haya producido interferencia destructiva o que la diferencia de fases sea 0 y el fotón no haya llegado. En principio Bob no puede distinguir entre estos dos casos hasta que se lleva a cabo el post-procesado de la clave.

Durante estos últimos años, el trabajo realizado por Merolla y su equipo se ha traducido en una mejora considerable en este tipo se sistemas, consiguiendo implementar el protocolo BB84 [32-34]. En concreto, se han analizado los efectos del ataque PNS sobre estos sistemas que utilizan pulsos débiles coherentes con la técnica de *strong reference* [17] siendo más apropiada que la de *decoy states*, vista anteriormente. Con esta técnica Eve no puede realizar el ataque PNS porque no puede bloquear ni la señal ni la referencia sin producir errores. Lo mejor que puede hacer es extraer la información de los pulsos con más de un fotón. La información que Eve puede extraer de pulsos con más de un fotón es

$$I_E = \frac{p_\mu(k \geq 2)}{p_\mu(k \geq 1)} = \frac{1-(1+\mu)e^{-\mu}}{1-e^{-\mu}} \tag{2.30}$$

donde $P_\mu(k)=\mu^k e^{-\mu}/k!$ es la probabilidad de que un pulso contenga k fotones. Esta expresión presenta un mínimo cuando $\mu=1$, donde $I_E=0.42$, por tanto, la fracción segura en ausencia de errores y pérdidas es $r=\Delta=1-I_E=0.58$. Cuando las pérdidas y los errores son tenidos en cuenta, la tasa de trasmisión segura R_{net} puede ser estimada con los resultados obtenidos en (2.20). Bob estima el QBER, realiza la corrección de errores y la amplificación de la privacidad, asumiendo que la fracción segura de los bits que permanecen es al menos Δ y que Eve ataca estos bits aumentando el QBER, por tanto, la tasa de trasmisión segura queda:

$$R_{net} = R_{sift} \cdot \left\{ \Delta \left[1 - h\left(\frac{QBER}{\Delta} \right) \right] - h(QBER) \right\} \tag{2.31}$$

2.7. Conclusiones

Este capítulo ha proporcionado un resumen de los conceptos básicos, técnicas y propiedades que son importantes para entender y evaluar los sistemas QKD. Para alcanzar este objetivo, primero se han introducido los conceptos generales relativos a los sistemas QKD, incluyendo definiciones de tasas de clave, aspectos de seguridad, protocolos y expresiones para la evaluación de la capacidad del sistema a través de la clave secreta final y la calidad de la transmisión a través de la tasa de error de bit, que también refleja el grado de seguridad del sistema. También, se ha resumido el estado del arte de los sistemas QKD basados en fibra óptica. Las técnicas principales usadas hasta la fecha han sido descritas junto con los mejores resultados conseguidos para cada una. Al final del último apartado, se han descrito los sistemas con codificación en frecuencia, cuyo análisis es el objetivo de esta tesis.

Referencias

[1] P. D. Townsend, "*Quantum Cryptography on Optical Fiber Networks,*" Opt. Fib. Technol. 4, 345-370 (1998).

[2] N. Gisin, G. Ribordy, W. Tittel y H. Zbinden, "*Quantum Cryptography,*" Rev. Mod. Phys. 74, 145-195 (2002).

[3] V. Scarani, H.Bechmann-Pasquinucci, N.J. Cerf, M.Dusek, N. Lutkenhaus y M. Peev, "*The security of practical quantum key distribution,*" Rev. Mod. Phys. 81, 1302-1350 (2009).

[4] G. Van Assche, "*Quantum Cryptography and Secret-Key Distillation,*" (Cambridge University Press, Cambridge, 2006).

[5] C.H. Bennett, G. Brassard, C. Crépeau y U. Maurer, "*Generalized privacy amplification,*" IEEE Trans. Inf. Theory 41, 1915-1923 (1995).

[6] C. H. Bennett y G. Brassard, "*Quantum cryptography: Public key distribution and coin tossing*" en Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, 175-179 (1984).

[7] D. Gottesman, H.-K. Lo, N. Lütkenhaus, y J. Preskill, "*Security of Quantum Key Distribution with Imperfect Devices,*" Quantum Inf. Comput. 4, 325-360 (2004).

[8] T.M. Cover y J.A. Thomas, "*Elements of Information Theory"* (John Wiley, New York, 2006).

[9] P.W. Shor y J. Preskill, "*Simple Proof of Security of the BB84 Quantum Key Distribution,*" Phys. Rev. Lett. 85, 441-444 (2000).

[10] B. Kraus, N. Gisin y R. Renner, "*Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication,*" Phys. Rev. Lett. 95, 080501 (2005).

[11] C.H. Bennett, "*Quantum cryptography using any two nonorthogonal states,*" Phys. Rev. Lett. 68, 3121-3124 (1992).

[12] W.Y. Hwang, "*Quantum Key Distribution with High Loss: Toward Global Secure Communication,*" Phys. Rev. Lett. 91, 057901 (2003).

[13] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail y J. Smolin, "*Experimental quantum cryptography,*" J. Cryptology 5, 3-28 (1992).

[14] A. Muller, J. Breguet y N. Gisin, "*Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km,*" Europhys. Lett. 23, 383-388 (1993).

[15] A. Muller, H. Zbinden y N. Gisin, "*Quantum cryptography over 23 km in installed under-lake telecom fibre,*" Europhys. Lett. 33, 335-339 (1996).

[16] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. C. Bienfang, D. Su, R. F. Boisvert, C. W. Clark y C. J. Williams, "*Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s,*" Opt. Express 14, 2062-2070 (2006).

[17] Y. Liu, T.Y. Chen, J. Wang, W.Q. Cai, X. W., L.K Chen, J.H. Wang, S.B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. C., Z.-B. Chen y J.-W. Pan, "*Decoy-state quantum key distribution with polarized photons over 200 km,*" Opt. Express 18, 8587-8594 (2010).

[18] P.D.Townsend, J. G. Rarity y P. R. Tapster, "*Single photon interference in a 10 km long optical fiber interferometer,*" Electron. Lett. 29, 634 -639 (1993).

[19] P. Townsend, J. Rarity y P. Tapster, "*Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel,*" Electron. Lett. 29, 1291-1293 (1993).

[20] P. Townsend, "*Secure key distribution system based on quantum cryptography,*" Electron. Lett. 30, 809-811 (1994).

[21] C. Marand y P. D. Townsend, 1995, "*Quantum key distribution over distances as long as 30 km,*" Opt. Lett. 20, 1695-1697 (1995).

[22] R. Hughes, G. Morgan y C. Peterson, 2000, "*Quantum key distribution over a 48-km optical fiber network,*" J. Mod. Opt. 47, 533-547 (2000).

[23] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe y A. J. Shields, "*Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate,*" Opt. Express 16, 18790-18979 (2008).

[24] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden y N. Gisin, "*Plug and play systems for quantum cryptography,*" Appl. Phys. Lett. 70, 793-795 (1997).

[25] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard y H. Zbinden, "*Fast and user-friendly quantum key distribution,*" J. Mod. Opt. 47, 517-531 (2000).

[26] D. Bethune y W. Risk, 2000, "*An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light,*" J. Quantum Electron. 36, 340-347 (2000).

[27] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren y E. Sundberg, 1999, "*Experiments on long wavelength (1550 nm) 'plug and play' quantum cryptography system,*" Opt. Express 4, 383-387 (1999).

[28] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy y H. Zbinden, "*Quantum key distribution over 67 km with a plug and play system,*" New J. Phys. 4, 1-8 (2002).

[29] P.C. Sun, Y. Mazurenko y Y. Fainman, "*Long distance frequency-division interferometer for communication and quantum cryptography,*" Opt. Lett. 20, 1062- 1063 (1995).

[30] J.M. Merolla, Y. Mazurenko, J. P. Goedgebuer y W. T. Rhodes, "*Single-photon interference in sidebands of phase-modulated light for quantum cryptography,*" Phys. Rev. Lett. 82, 1656-1659 (1999).

[31] J. M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, H. Porte y W. T. Rhodes, "*Phase-modulation transmission system for quantum cryptography,*" Opt. Lett. 24, 104-106 (1999).

[32] O. Guerreau, J-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer y F. J. Malassenet, "*Long distance QKD transmission using single-sideband detection detection scheme with WDM synchronization,*" J. Sel. Top. Quantum Electron. 9, 1533-1540 (2003).

[33] O. L. Guerreau, F. J. Malassenet, S. W. McLaughlin y J. M. Merolla, "*Quantum key distribution without a single photon source using a strong reference*," Phot. Tech. Lett. 17, 1755-1757 (2005).

[34] M. Bloch, S. McLaughlin, J.M. Merolla y F. Patois, "*Frequency-coded quantum key distribution,*" Opt. Lett., 32, 301-303, (2007).

Capítulo 3

Implementación del Protocolo BB84 mediante Codificación en Frecuencia

3.1. Introducción y justificación del estudio teórico

Como se ha visto en el capítulo 2, una de las técnicas más robustas para la implementación de sistemas de distribución de clave (QKD) consiste en la utilización de la codificación en frecuencia a partir de la concatenación de distintas estructuras de moduladores [1]. El trabajo que se presenta en esta tesis se centra en los esquemas que utilizan codificación en frecuencia (FC) [2] debido a las posibilidades que la Fotónica de Microondas puede ofrecer a este tipo de estructuras.

Este capítulo se divide en tres apartados. En el primero se realiza un estudio en profundidad teniendo en cuenta los distintos moduladores más comunes existentes

en el mercado. Con este estudio se pretende analizar un conjunto de configuraciones que permitan desarrollar el protocolo BB84 y evaluar cuál de ellas resulta ser más ventajosa en términos de tasa de bit y alcance del enlace. En el segundo apartado, se realiza un estudio que permite la incorporación de la técnica de multiplexación por subportadora eléctrica (SCM) a los sistemas de distribución de clave cuántica. Esta técnica SCM es ampliamente utilizada en el mundo de las telecomunicaciones convencionales donde su finalidad es aumentar la tasa secreta de bit y poder distribuir información desde un trasmisor a múltiples usuarios. Por último, en el tercer apartado se consideran otros posibles factores de degradación como la interferencia de la portadora óptica, el efecto Raman y la eficiencia del sistema de filtrado que experimentalmente condicionan la viabilidad de este tipo de sistemas cuánticos.

3.2. Estudio de la concatenación de moduladores para la implementación del protocolo BB84 mediante codificación en frecuencia

En los sistemas QKD basados en codificación en frecuencia se requiere el uso de un par de moduladores, uno para Alice y otro para Bob. En principio, existen tres tipos de moduladores disponibles comercialmente [3], que son el modulador de amplitud (AM), el modulador de fase (PM) y el modulador desbalanceado (UM). El primero modifica la amplitud de la señal, el segundo sólo la fase y el desbalanceado tanto la amplitud como la fase de la señal óptica de entrada.

Varias configuraciones ya han sido publicadas en la literatura para la implementación de sistemas FC-QKD, por ejemplo, las PM-PM [2] y AM-AM [4] ya han sido utilizadas para implementar el protocolo B92, mientras que las UM-UM [5] y AM-PM [6] han sido publicadas para desarrollar el protocolo BB84. Sin embargo, hay otras que no han sido tratadas en la literatura y cuyo uso puede considerarse para implementar estos dos protocolos. En este apartado se va a llevar a cabo un análisis general de los sistemas FC-QKD teniendo en cuenta todas las posibles combinaciones, analizando qué condiciones tienen que cumplir para desarrollar los protocolos BB84 o B92 y cuáles resultan más eficientes.

3.2.1. Desarrollo teórico

Cualquier sistema FC-QKD se puede describir atendiendo a la configuración general mostrada en la figura 3.1, donde los dispositivos principales son los mismos que se describieron en la sección 2.6.4, pero ahora el modulador electroóptico de

Alice y Bob (EOM_A y EOM_B) va a ser uno de los tres anteriormente presentados (AM, PM, UM).

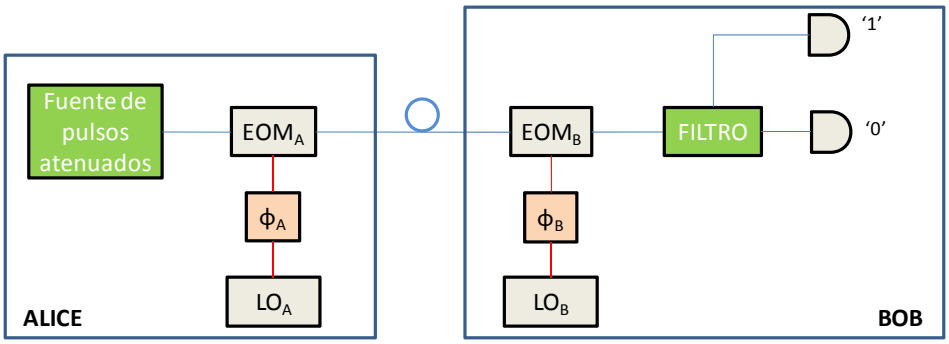

Figura 3.1. Esquema de un sistema FC-QKD.

Uno de los parámetros más críticos de los moduladores de fase al utilizarse en los sistemas QKD son las pérdidas asociadas al dispositivo. Estas pérdidas se definen en función de la transmitancia intrínseca del modulador T que tiene en cuenta las pérdidas en el acoplo entre la fibra y las guías de onda del modulador, y las propias pérdidas que sufre el campo cuando se trasmite por dichas guías. En concreto, el campo óptico a la salida del modulador de fase (PM) se describe como:

$$E_{PM}(t) = E_0(t)\sqrt{T}\cdot e^{j\frac{\pi V(t)}{V_\pi}} \tag{3.1}$$

donde $E_0(t)$ representa el campo a la salida de la fuente óptica empleada, que podemos asociar al campo a la entrada del modulador. La señal moduladora de radiofrecuencia viene definida por $V(t)$ y V_π es el voltaje característico del modulador que permite generar una diferencia de fase de π en la línea de transmisión correspondiente del modulador.

Para el caso del modulador de amplitud (AM), el campo óptico a la salida de éste se describe como:

$$E_{AM}(t) = E_0(t)\frac{\sqrt{T}}{2}\left[e^{j\frac{\pi V(t)}{V_\pi}} + e^{-j\frac{\pi V(t)}{V_\pi}}\right] = E_0(t)\sqrt{T}\cos\left(\frac{\pi V(t)}{V_\pi}\right) \tag{3.2}$$

donde se observa que el campo de salida varía sólo en amplitud de acuerdo con la señal de RF de entrada.

Por último, el modulador desbalanceado (UM) se puede describir como:

$$E_{UM}(t) = E_0(t)\frac{\sqrt{T}}{2}\left[e^{j\frac{\pi V(t)}{V_\pi}} + 1\right] \tag{3.3}$$

Estos tres moduladores pueden ser escritos por una sola expresión, que describe la salida del modulador de Alice de forma compacta y se detalla a continuación,

$$E_{ALICE}(t) = E_0(t)\frac{\sqrt{T_A}}{2}\left[e^{j\frac{\pi V^A(t)}{V_\pi}} + e^{-j\varepsilon\frac{\pi V^A(t)}{V_\pi}}\right] \tag{3.4}$$

donde el parámetro ε que aparece en la exponencial define los diferentes moduladores de acuerdo con la tabla 3.1. Realmente, la expresión anterior no tiene un significado físico pero resulta interesante disponer de una expresión compacta que permita trabajar simultáneamente con los tres tipos de moduladores más relevantes.

	ε
AM	$\varepsilon=1$
PM	$\varepsilon=-1$
UM	$\varepsilon=0$

Tabla 3.1. Valores del parámetro ε para los moduladores AM, PM y UM.

La señal de RF generada por un oscilador localizado en Alice LO_A y que alimenta al puerto de entrada eléctrico de su modulador correspondiente, viene dada por:

$$V^A(t) = V_{DC}^A + V_{AC}^A\cos\left(\Omega t + \Phi_A\right) \tag{3.5}$$

donde V_{DC}^A y V_{AC}^A son las componentes continua y alterna de la señal de RF, respectivamente, mientras que Ω y Φ_A son la frecuencia y la fase de dicha señal eléctrica.

Sustituyendo en la ecuación (3.4) obtenemos:

$$E_{ALICE}(t) = E_0(t)\frac{\sqrt{T_A}}{2}\left[e^{j\Psi_A}e^{jm_A\cos(\Omega t+\Phi_A)} + e^{-j\varepsilon\Psi_A}e^{-j\varepsilon m_A\cos(\Omega t+\Phi_A)}\right] \tag{3.6}$$

donde m_A representa el índice de modulación y Ψ_A la fase introducida en los brazos del modulador:

$$m_A = \frac{\pi V_{AC}^A}{V_\pi}, \quad \Psi_A = \frac{\pi V_{DC}^A}{V_\pi} \tag{3.7}$$

Desde el punto de vista práctico, el valor de los índices de modulación es pequeño puesto que la potencia de RF para cada subportadora eléctrica a la entrada del modulador no es muy elevada. Por tanto, asumimos inicialmente que el sistema opera bajo un régimen de pequeña señal (m_A<<1) de forma que, el campo a la salida del modulador de Alice se puede expresar como:

$$E_{ALICE}(t) = E_0(t) t_{eff,A} \cdot \left\{ 1 + 2m_{eff,A} \cdot \cos(\Omega t + \Phi_A) \right\} \tag{3.8}$$

donde los nuevos parámetros vienen definidos por:

$$\begin{aligned} t_{eff,A} &= \left(e^{j\psi_A} + e^{-j\varepsilon\psi_A}\right)\frac{\sqrt{T_A}}{2} \\ m_{eff,A} &= \frac{1}{2}\frac{\left(e^{j\psi_A} - e^{-j\varepsilon\psi_A}\varepsilon\right)}{\left(e^{j\psi_A} + e^{-j\varepsilon\psi_A}\right)} jm_A \end{aligned} \tag{3.9}$$

El parámetro $t_{eff,A}$ representa la transmitancia efectiva del modulador de Alice que tiene en cuentas las pérdidas ópticas totales que sufre la señal óptica de entrada debido a las pérdidas intrínsecas del modulador y a la tensión de polarización del mismo. Por otro lado, el término $m_{eff,A}$ representa el índice de modulación efectivo que relaciona el nivel de potencia de las subportadoras eléctricas con la portadora óptica en el dominio espectral.

El campo a la salida del modulador de Alice es transmitido por el canal de fibra óptica, sufriendo la atenuación y dispersión del canal de forma que a su salida el campo óptico puede expresarse como:

$$E(t) = t_{eff,A} \cdot e^{-\frac{\alpha L}{2}} e^{j\beta_0 L} E_0(t) \left\{ \begin{array}{l} 1 + m_{eff,A} \cdot e^{-j(\Omega t + \Phi_A)} e^{-j\beta_1 L\Omega} e^{j\frac{1}{2}\beta_2 L\Omega^2} + \\ + m_{eff,A} \cdot e^{+j(\Omega t + \Phi_A)} e^{j\beta_1 L\Omega} e^{j\frac{1}{2}\beta_2 L\Omega^2} \end{array} \right\} \tag{3.10}$$

donde β_0, β_1, β_2 son los términos de orden cero, primer y segundo orden de la constante de propagación $\beta(\omega)$ [7] de la fibra óptica. El término β_1 está relacionado con el retardo que sufre la señal óptica lo largo de un canal de fibra óptica de

longitud L, dado por $\tau=\beta_1 L$. El término β_2 es la dispersión de primer orden y está relacionada con la diferencia de tiempos entre distintas componente espectrales de una señal óptica que existe al propagarse la misma distancia L. Por último, el parámetro α representa las pérdidas del canal óptico por unidad de longitud.

Este campo será nuevamente modulado por el modulador de Bob, por una señal de RF dada por:

$$V^B(t) = V_{DC}^B + V_{AC}^B \cos\left(\Omega t + \Phi_B\right) \tag{3.11}$$

donde V_{DC}^B y V_{AC}^B son las componentes continua y alterna de la señal de RF respectivamente mientras que Ω y Φ_B son la frecuencia y la fase de dicha señal.

A la salida del modulador el campo se puede escribir como:

$$E\ (t) = E\left(\omega_o\right)e^{j\omega_0 t} + E\left(\omega_o - \Omega\right)e^{j(\omega_0-\Omega)t} + E\left(\omega_o + \Omega\right)e^{j(\omega_0+\Omega)t} \tag{3.12}$$

donde las tres componentes espectrales del campo vienen dadas respectivamente por:

$$\begin{aligned}
&E(\omega_o) = e^{-\frac{\alpha L}{2}} t_{eff,A} t_{eff,B} \cdot e^{j\beta_0 L} E_0 \\
&E(\omega_o - \Omega) = e^{-\frac{\alpha L}{2}} t_{eff,A} t_{eff,B} \cdot e^{j\beta_0 L} E_0 e^{-i\Phi_B} \left(m_{eff,B} + m_{eff,A} \cdot e^{-j\beta_1 L\Omega} e^{j\frac{1}{2}\beta_2 L\Omega^2} e^{j(\Phi_B - \Phi_A)} \right) \\
&E(\omega_o + \Omega) = e^{-\frac{\alpha L}{2}} t_{eff,A} t_{eff,B} \cdot e^{j\beta_0 L} E_0 e^{i\Phi_B} \left(m_{eff,B} + m_{eff,A} \cdot e^{j\beta_1 L\Omega} e^{j\frac{1}{2}\beta_2 L\Omega^2} e^{j(\Phi_A - \Phi_B)} \right)
\end{aligned} \tag{3.13}$$

En la expresión anterior $m_{eff,B}$ y $t_{eff,B}$ representan el índice de modulación efectivo y la transmitancia efectiva del modulador de Bob respectivamente.

A la salida del modulador de Bob se inserta un filtro óptico cuya función es separar las tres componentes espectrales del campo ω_0, $\omega_0+\Omega$, $\omega_0-\Omega$ que corresponden a la portadora, banda lateral superior e inferior, respectivamente. La potencia óptica de cada una de estas tres componentes espectrales al hacer incidir cada una de ellas sobre un detector óptico diferente viene dada por el promedio del modulo al cuadrado de la expresión (3.13):

$$
\begin{aligned}
P(\omega_o) &= e^{-\alpha L}\left|t_{eff,A}\right|^2\left|t_{eff,B}\right|^2 \\
P(\omega_o - \Omega) &= P_{\max}\left[1+V\cdot\cos\left(\Phi_B - \Phi_A - \Omega\beta_1 L - \Theta\right)\right] \\
P(\omega_o + \Omega) &= P_{\max}\left[1+V\cdot\cos\left(\Phi_B - \Phi_A - \Omega\beta_1 L + \Theta\right)\right]
\end{aligned}
\tag{3.14}
$$

En la ecuación (3.14) se han definido los parámetros de visibilidad V, potencia máxima P_{max} y fase Θ como:

$$
\begin{aligned}
V &= \frac{2\left|m_{eff,A}\right|\left|m_{eff,B}\right|}{\left|m_{eff,A}\right|^2+\left|m_{eff,B}\right|^2} \\
P_{\max} &= e^{-\alpha L}\left|t_{eff,A}\right|^2\left|t_{eff,B}\right|^2\left(\left|m_{eff,A}\right|^2+\left|m_{eff,B}\right|^2\right) \\
\Theta &= \arg\left(m_{eff,B}\right) - \arg\left(m_{eff,A}\right) - \frac{1}{2}\beta_2 L\Omega^2
\end{aligned}
\tag{3.15}
$$

La visibilidad V es un parámetro que se utiliza para caracterizar cualquier fenómeno de interferencia [8]. En este caso, según la ecuación (3.15), la visibilidad V está relacionada con los índices de modulación efectivos de Alice y Bob. Cuando ambos índices son iguales se tiene un valor máximo de visibilidad (V=1) y a medida que la diferencia entre ambos aumenta, la visibilidad se reduce hasta un valor mínimo (V=0). La potencia P_{max} está relacionada con la máxima potencia que se puede obtener para cada una de las bandas, lo cual es clave para evaluar la tasa de bit como se verá más adelante. Por último, el término de fase Θ está relacionado con la diferencia de fase que aparece entre las bandas debido a los índices de modulación efectivo entre Alice y Bob y la propia dispersión acumulada en la propagación.

La adaptación del protocolo BB84 [9] a sistemas basados en codificación en frecuencia implica que la probabilidad de detección de un fotón es máxima en la banda superior o inferior, cuando Bob selecciona la base correcta. El hecho de que sea una u otra banda lateral estará determinado por el bit transmitido. Por el contrario, si existe la misma probabilidad de que el fotón se detecte en ambas bandas implicaría que la base seleccionada no ha sido correcta. Teniendo esto en cuenta, el protocolo BB84 se puede implementar fácilmente considerando que las probabilidades de detección en las bandas superior e inferior deben ser complementarias en función de la diferencia de fase entre Alice y Bob. A partir de la expresión (3.14), la potencia óptica asociada a cada banda debería tener la forma siguiente:

$$P(\omega_o + \Omega) = P_{\max} \cdot \cos^2\left(\frac{\Phi_B - \Phi_A}{2}\right)$$
$$P(\omega_o - \Omega) = P_{\max} \cdot \sin^2\left(\frac{\Phi_B - \Phi_A}{2}\right) \tag{3.16}$$

Para que se cumpla la condición de complementariedad expresada en la ecuación (3.16), a partir de los parámetros mostrados en la (3.15) podemos establecer las siguientes condiciones:

$$\left|m_{eff,A}\right|^2 = \left|m_{eff,B}\right|^2$$
$$\Theta = (2n+1)\frac{\pi}{2} \qquad n = 0, \pm 1, \pm 2... \tag{3.17}$$

Cuando el sistema verifica las condiciones (3.17) estará optimizado para llevar a cabo la implementación del protocolo BB84 con visibilidad máxima (V=1). Sin embargo, los sistemas reales sufren ciertas perturbaciones ambientales o simplemente los dispositivos presentan ciertas tolerancias en sus especificaciones de forma que las condiciones derivadas de (3.17) no pueden satisfacerse completamente, es decir, $|m_{eff,A}|^2/|m_{eff,B}|^2 \approx 1$ y $\Theta \approx (2n+1)\pi/2$. Debido a este desajuste en el sistema se producen errores en la clave detectada, de forma que es necesaria una descripción más completa del impacto de estos errores cuando los efectos de la dispersión son considerados. En este caso, definimos la probabilidad de detectar un error debido a este desajuste en la interferencia como P_{opt}^{error}, la probabilidad de detectar correctamente P_{opt}^{ok} y la probabilidad de que Bob detecte un fotón en las bandas $P_{\exp}^{sig}$. La relación existente entre ellas nos permite definir una visibilidad efectiva V_{eff} que tenga en cuenta los efectos de la dispersión:

$$P_{opt}^{error} = \frac{(1 - V_{eff})}{2} P_{\exp}^{sig}$$
$$P_{opt}^{ok} = \frac{(1 + V_{eff})}{2} P_{\exp}^{sig} \tag{3.18}$$
$$P_{\exp}^{sig} = P_{opt}^{ok} + P_{opt}^{error}$$

A partir de la ecuación anterior, se puede observar que cuando la visibilidad toma el valor máximo (V_{eff}=1), la probabilidad de error debida al desajuste es nulo y la

probabilidad de medir en el detector correcto es máxima. Despejando y sustituyendo en estas expresiones, la visibilidad efectiva V_{eff} puede escribirse como:

$$V_{eff} = \frac{P_{opt}^{ok} - P_{opt}^{error}}{P_{opt}^{ok} + P_{opt}^{error}} = \frac{V \sin^2 \Theta}{1 + V \cos^2 \Theta} \tag{3.19}$$

donde se ha tenido en cuenta que P_{opt}^{ok} es proporcional a $P(\omega_o+\Omega)$ cuando se transmite un bit midiendo con la base correcta y que P_{opt}^{error} es proporcional a $P(\omega_o-\Omega)$ cuando se detecta con la base correcta. Ahora este parámetro está relacionado con las dos condiciones previas de la ecuación (3.17).

La nueva definición de la probabilidad de error debido al desajuste en la interferencia implica realizar una modificación en la expresión del QBER presentada en los sistemas de codificación en frecuencia que no consideran la dispersión [9]. Con todo esto, el QBER vendría dado por la siguiente expresión:

$$QBER = \frac{(1 - V_{eff})\rho\mu_{\max} + d_B}{2\left(\rho\mu_{\max} + d_B\right)} \tag{3.20}$$

Las expresiones obtenidas en este apartado van a permitir evaluar todas las posibles configuraciones de moduladores con las que se puede llevar a cabo el protocolo BB84, que se pasa a hacer en el siguiente apartado.

3.2.2. Configuraciones con y sin dispersión

Como se puede observar en las expresiones (3.15) y (3.19), la dispersión de la fibra afecta a la visibilidad efectiva V_{eff}, por ello su efecto se compensa en las configuraciones FC-QKD implementadas hasta el momento (β_2=0) [9]. Como primer paso, se tomará β_2=0 para todas las configuraciones y se determinarán aquellas que se pueden llevar a cabo y cuáles no.

Sustituyendo los valores de t_{eff} y m_{eff} para todas las posibles configuraciones atendiendo al tipo de modulador que se utiliza en Alice y Bob, se puede analizar en la tabla 3.2 como quedan las condiciones (3.17) para cada una de ellas.

A	B	Θ	V=1	BB84
UM	UM	$\psi_B - \psi_A$	$\frac{m_A}{m_B} = \left\|\frac{\cos(\psi_A)}{\cos(\psi_B)}\right\|$	OK $\psi_B =$ $\psi_A + (2n+1)\frac{\pi}{2}$
AM	AM	0	$\frac{m_A}{m_B} = \left\|\frac{\tan(\psi_B)}{\tan(\psi_A)}\right\|$	NO
PM	PM	0	$\frac{m_A}{m_B} = 1$	NO
PM	AM	$\pi/2$	$\frac{m_A}{m_B} = \left\|\tan(\psi_B)\right\|$	OK
AM	PM	$-\pi/2$	$\frac{m_A}{m_B} = \frac{1}{\tan(\psi_A)}$	OK
UM	PM	$-\psi_A$	$\frac{m_A}{m_B} = 2\left\|\cos(\psi_A)\right\|$	NO V=0 si $\psi_A = (2n+1)\frac{\pi}{2}$
PM	UM	$-\psi_B$	$\frac{m_A}{m_B} = \frac{1}{2\left\|\cos(\psi_B)\right\|}$	NO V=0 si $\psi_B = (2n+1)\frac{\pi}{2}$
UM	AM	$\frac{\pi}{2} - \psi_A$	$\frac{m_A}{m_B} = 2\left\|\cos(\psi_A)\tan(\psi_B)\right\|$	OK $\psi_A = n\,\pi$
AM	UM	$\frac{\pi}{2} + \psi_B$	$\frac{m_A}{m_B} = 2\left\|\frac{\cos(\psi_B)}{\tan(\psi_A)}\right\|$	OK $\psi_B = n\,\pi$

Tabla 3.2. Requerimientos de los parámetros en las diferentes configuraciones de moduladores para implementar el protocolo BB84 con FC-QKD compensando la dispersión.

En la tabla 3.2, se puede observar como algunas configuraciones son factibles y otras no. De las que son posibles cabe destacar dos nuevas que no han sido evaluadas hasta la fecha, que son las configuraciones UM-AM y AM-UM. El objetivo de este apartado es evaluar cuales son las más eficientes y estables.

Con el fin de comparar todas las configuraciones, tomamos como punto de partida que todas las estructuras tienen la misma visibilidad efectiva y por tanto el mismo QBER, considerando que la fuente óptica atenuada, el sistema de filtrado de bandas laterales y los detectores utilizados tienen características idénticas. Con todo esto, la eficiencia se puede evaluar directamente a través de la clave en crudo R_{sift} del sistema, que se puede expresar de la siguiente forma a partir de nuestra nomenclatura:

$$R_{sift} = \frac{1}{2} f_s p_{\exp}^{sig} = \frac{1}{2} f_s \frac{P_{\max}}{h\nu} \tau \tag{3.21}$$

donde f_s es la frecuencia de repetición de la fuente y $P_{\exp}^{sig}$ la probabilidad de detectar un fotón en una de las bandas laterales. Esta probabilidad de detección de señal $P_{\exp}^{sig}$ viene dada por el número de fotones que pueden detectarse en un pulso de duración τ y potencia promedio P_{max}. La constante de proporcionalidad viene dada por la constante de Plank h, la frecuencia óptica del fotón v y la duración del pulso τ.

A partir de la expresión (3.15), la potencia P_{max} se puede reescribir en función de las pérdidas ópticas asociadas al enlace, el número de fotones a la salida de Alice μ_A procedente de la subportadora eléctrica y las pérdidas efectivas asociadas a Bob:

$$P_{\max} = e^{-\alpha L} \mu_A \left| t_{eff,B} \right|^2 \cdot \left(1 + \frac{1}{V} - \sqrt{\frac{1}{V^2} - 1} \right) \tag{3.22}$$

El último término en la expresión anterior sólo depende de la visibilidad que se ha asumido idéntica para todas las configuraciones. El número medio de fotones a la salida de Alice μ_A también se considera constante para todas las configuraciones, ya que es impuesto por la seguridad del sistema. Por tanto, el parámetro que permite comparar la eficiencia de todas las configuraciones viene asociado a las pérdidas efectivas de Bob a través de la transmitancia $|t_{eff,B}|^2$, y en este contexto, las configuraciones más eficientes serán las que maximicen la transmitancia del receptor de Bob. Estas resultan ser AM-PM y AM-UM, ya que el valor de $|t_{eff,B}|^2$ es el doble que el resto de las configuraciones. Además resulta que para los moduladores existentes en la literatura el que presenta menos pérdidas intrínsecas (T_B) es el PM [10] quedando como configuración más eficiente la AM-PM.

Como hemos visto en el apartado anterior la dispersión juega un papel negativo en todas las configuraciones posibles estudiadas. No obstante, se puede observar que si

no se compensa la dispersión aparecen algunas configuraciones novedosas en las que la dispersión juega un papel positivo, ya que permite la implementación del protocolo BB84 para unos valores determinados de longitud del canal y frecuencia del tono. Dichas configuraciones se pueden observar en la siguiente tabla:

A	B	Θ	V=1	BB84
AM	AM	$\frac{1}{2}\beta_2 L\Omega^2$	$\frac{m_A}{m_B}=\left\lvert\frac{\tan(\psi_B)}{\tan(\psi_A)}\right\rvert$	Si $\frac{1}{2}\beta_2 L\Omega^2=(2n+1)\frac{\pi}{2}$
PM	PM	$\frac{1}{2}\beta_2 L\Omega^2$	$\frac{m_A}{m_B}=1$	Si $\frac{1}{2}\beta_2 L\Omega^2=(2n+1)\frac{\pi}{2}$
UM	PM	$\frac{1}{2}\beta_2 L\Omega^2-\psi_A$	$\frac{m_A}{m_B}=2\lvert\cos(\psi_A)\rvert$	Si $\frac{1}{2}\beta_2 L\Omega^2-\psi_A=(2n+1)\frac{\pi}{2}$
PM	UM	$\frac{1}{2}\beta_2 L\Omega^2-\psi_B$	$\frac{m_A}{m_B}=\frac{1}{2\lvert\cos(\psi_B)\rvert}$	Si $\frac{1}{2}\beta_2 L\Omega^2-\psi_A=(2n+1)\frac{\pi}{2}$

Tabla 3.3. Requerimientos de los parámetros para las diferentes configuraciones de moduladores para implementar el protocolo BB84 con FC-QKD sin compensar la dispersión.

En este caso, las configuraciones más eficientes que maximizan $t_{eff,B}$ son PM-PM, UM-PM y PM-UM. Como se ha comentado, en la actualidad los valores más bajos de pérdidas se han conseguido para los moduladores de fase, por lo que resultan más eficientes las configuraciones PM-PM y UM-PM.

También cabe destacar que en la configuración PM-PM la visibilidad no depende del punto de cuadratura (m_A/m_B=1) y por tanto, las fluctuaciones experimentales del modulador en torno a este punto no llevaran consigo una pérdida en la visibilidad, a diferencia del resto de configuraciones.

3.2.3. Impacto de la dispersión en esquemas AM-PM y PM-PM

Como hemos visto en el apartado anterior, las configuraciones más eficientes y estables son AM-PM y PM-PM. En la configuración AM-PM es importante recalcar la importancia de compensar la dispersión para conseguir un valor de V_{eff} próximo a uno y, de esta manera, un valor bajo del QBER. Por otro lado, la

dispersión en la configuración PM-PM requiere que se cumpla el requisito de la tabla 3.3 para poder satisfacer las condiciones de complementariedad de bandas laterales.

En la figura 3.2(a), se representa la evolución del QBER y en la figura 3.2(b) la expresión de la tasa secreta de bit a partir de las ecuaciones (3.20) y (2.31), respectivamente. En ambos casos, en función de la distancia para la configuración AM-PM y empleando una subportadora de 20 GHz. Se han representado las curvas en función de los parámetros usuales de los sistemas reales (Δ=0.58, μ=1, α=0.2, ρ=0.1 y V=0.99) a los cuales se hará mención a lo largo del capítulo. La línea negra muestra los resultados para un valor de $\beta_2=2\cdot10^{-23}$ s^2/km mientras que la línea roja compensando la dispersión (β_2=0). Se puede observar cómo se obtienen mejores valores compensando la dispersión que sin compensar, excepto para las longitudes que cumplen $1/2\beta_2 L\Omega^2=n\pi/2$ donde coinciden. En la figura 3.2(b) vemos como la tasa secreta de bit compensando la dispersión decrece de tal manera que no se puede trasmitir más de 105 km, mientras que sin compensar apenas se puede trasmitir 10 km.

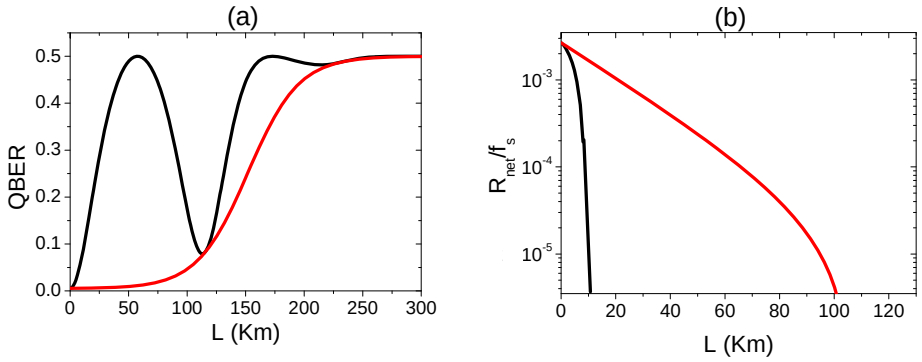

Figura 3.2. Evolución del QBER (a) y tasa secreta de bit (b) para la configuración AM-PM en función de la longitud para una frecuencia de RF de 20 GHz compensando la dispersión (—) y sin compensar (—).

En la figura 3.3(a), se muestra la evolución del *QBER* y en la figura 3.3(b) la tasa secreta de bit, en ambos casos en función de la frecuencia de la portadora eléctrica para una longitud de 20 km para $\beta_2=2\cdot10^{-23}$ s^2/km y compensando la dispersión con β_2=0. Se puede observar como compensando la dispersión se puede transmitir correctamente con todas las frecuencias de subportadora, donde la tasa secreta de bit es constante, mientras que sin compensar solamente se puede en las frecuencias

que están cercanas a la condición $1/2\beta_2 L\Omega^2=n\pi/2$. De hecho, para el caso que estamos analizando de L=20 Km, tan solo las frecuencias que tienen un QBER menor que el 6% contribuyen a la tasa secreta de bit, lo que es equivalente a decir que solo las frecuencias que están en el rango $n\pi/2-\pi/8 < 1/2\beta_2 L\Omega^2 < n\pi/2+ \pi/8$ presentan tasas secretas de bit significativas. Por tanto, se puede concluir que el sistema con compensación no fija ninguna relación entre la distancia de trasmisión y frecuencia de subportadora para conseguir un *QBER* óptimo, mientras que compensando la dispersión se debe guardar la relación $1/2\beta_2 L\Omega^2=n\pi/2$ para trasmitir de forma óptima.

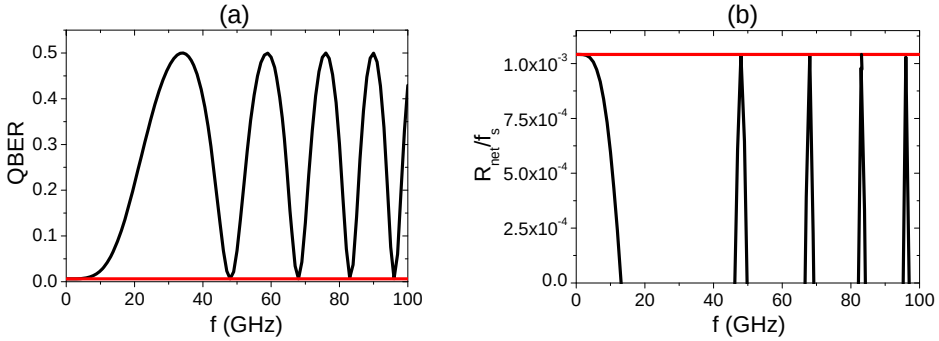

Figura 3.3. Evolución del QBER (a) y tasa secreta de bit (b) para la configuración AM-PM en función de la frecuencia $f=\Omega/2\pi$ para una longitud L=20 km compensando la dispersión (—) y sin compensar (—).

A continuación vamos a analizar el caso PM-PM. Como ya se ha comentado esta configuración necesita la dispersión para implementar el protocolo BB84 a diferencia de la configuración AM-PM. En la figura 3.4(a), se muestra el QBER y en la figura 3.4(b) la tasa secreta de bit, en ambos casos en función de la longitud del canal, para la configuración PM-PM. Se compara con la configuración AM-PM compensando la dispersión, ambas con una frecuencia de subportadora de 20 GHz. El resto de parámetros se han valorado de igual forma que para calcular los resultados mostrados en la figura 3.2. Se puede ver, como para una determinada frecuencia de RF, solamente es posible trasmitir para unos determinados valores de la longitud del canal.

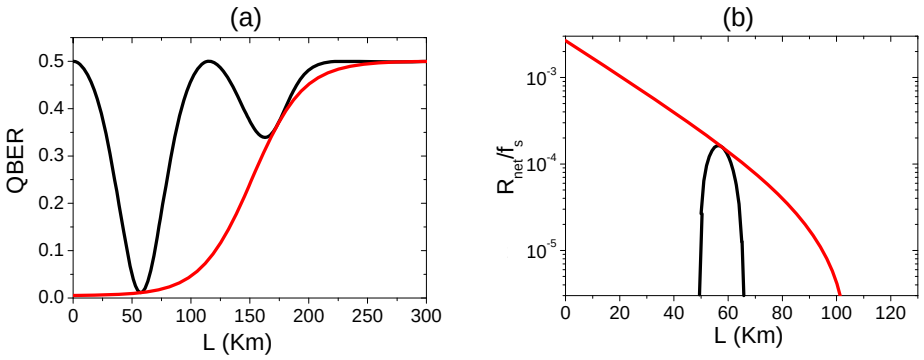

Figura 3.4. Evolución del QBER (a) y tasa secreta de bit (b) en función de la longitud para una frecuencia de RF de 20 GHz para la configuración AM-PM compensando la dispersión (—) y para la configuración PM-PM sin compensar (—).

En la figura 3.5(a) se muestra el QBER y en la figura 3.5(b) la tasa secreta de bit, en ambos casos en función de la frecuencia, para una longitud del canal de 20 km. Nuevamente, las frecuencias que cumplen $1/2\beta_2 L\Omega^2=(2n+1)\pi/2$ son las que se pueden trasmitir de forma óptima.

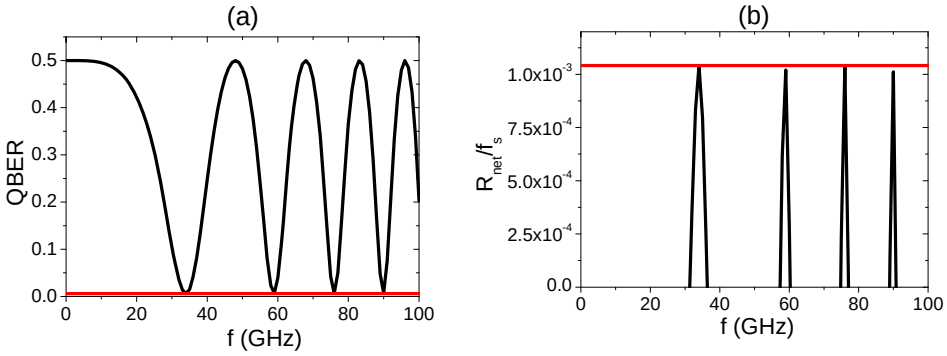

Figura 3.5. Evolución del QBER (a) y tasa secreta de bit (b) en función de la frecuencia $f=\Omega/2\pi$ para una longitud L=20 km para la configuración AM-PM compensando la dispersión (—) y para la configuración PM-PM sin compensar (—).

Con la estructura PM-PM no se puede compensar la dispersión, por tanto, a diferencia de la configuración AM-PM con la dispersión compensada, se tiene que

guardar una relación entre la frecuencia de RF y la longitud del canal como ya se ha comentado.

3.3. Distribución de clave cuántica con multiplexación por división de subportadora

Una limitación principal de los sistemas QKD, es el hecho de que las tasas de bits transmitidos son muy bajas en comparación con los utilizados en las telecomunicaciones clásicas [11]. Una de las principales restricciones reside en la calidad de las fuentes de fotones individuales así como la velocidad de los detectores cuánticos. Una alternativa y un enfoque complementario para aumentar la velocidad de transmisión de bits es hacer que los sistemas de QKD trabajen en paralelo. Este enfoque de ingeniería simple se convierte en un reto cuando se trabaja con sistemas cuánticos: el sistema debe funcionar en paralelo, pero todavía dependen de una sola fuente y la seguridad aún debe ser garantizada por los principios de la mecánica cuántica.

En este contexto, los recientes avances en la fotónica de microondas [12] señalan que ésta es una tecnología que puede ser clave para la aplicación de los sistemas comerciales de distribución de clave cuántica para convertirse en una tecnología competitiva. Para que esto ocurra a un coste razonable, es fundamental tomar disposición de los componentes fotónicos que actualmente están disponibles para aplicaciones en el campo de las telecomunicaciones clásicas. Concretamente, la técnica de multiplexación por subportadora eléctrica (SCM) ha tomado un especial interés ya que tiene como características una alta eficiencia espectral y solamente es necesaria una fuente que comparten los diferentes canales reduciendo la complejidad del sistema.

La adaptación de la técnica SCM a la distribución cuántica de claves la denominaremos SCM-QKD [13, 14]. En este caso, la señal de radiofrecuencia que alimenta la entrada eléctrica de los moduladores de Alice y Bob, ahora está compuesta por la suma de N subportadoras eléctricas de diferentes frecuencias y fases. Esta adaptación permite el envío de múltiples claves en paralelo entre una estación central proporcionando tasas de distribución más altas en configuraciones punto a punto o multipunto, ya que la mecánica cuántica permite medir simultáneamente diferentes frecuencias de forma independiente, sin comprometer los principios de seguridad en los que se basan los sistemas QKD.

En este apartado se va a llevar a cabo un análisis clásico, similar al del apartado anterior, donde se estudiará cómo afecta la dispersión del canal al campo óptico, el cual ahora estará formado por la suma de N términos iguales a los obtenidos en el apartado anterior y un nuevo término no deseado que denotaremos como término de intermodulación, consecuencia de la multiplexación en frecuencia eléctrica. También se obtendrán las expresiones del QBER y la tasa secreta de bit para esta nueva adaptación, y se estudiarán las condiciones que se tienen que cumplir para obtener los resultados más eficientes.

3.3.1. Señal e intermodulación en sistemas SCM

En la figura 3.6 se muestra el esquema de un sistema SCM-QKD. Este es similar al correspondiente a FC-QKD en su configuración, pero ahora la señal de radiofrecuencia está formada por la suma de N subportadoras, cada una con una frecuencia (Ω_i, i=1,..,N) un desfase (Φ_{Ai}, i=1,..,N) de 0, π y $\pi/2$, $3\pi/2$ para Alice y 0 y $\pi/2$ para el caso de Bob (Φ_{Bi}, i=1,..,N). Esta señal de radiofrecuencia se puede representar con la siguiente expresión para Alice:

$$V(t) = V_{DC} + \sum_{i=1}^{N} V_{AC} \cos\left(\Omega_i t + \Phi_i\right) \tag{3.23}$$

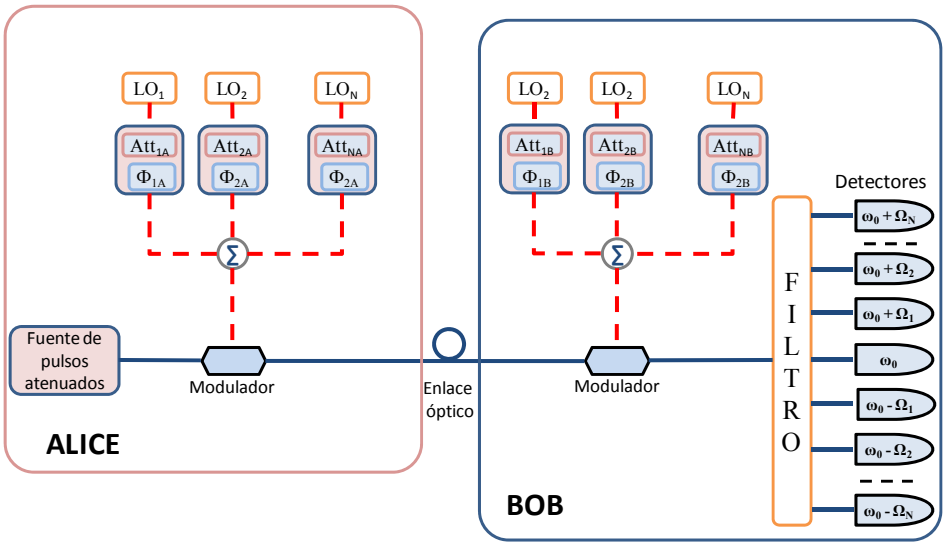

Figura 3.6. Esquema de un sistema con N canales para la distribución de clave con multiplexación de la subportadora.

Teniendo en cuenta la descripción de los moduladores del apartado anterior, la salida del modulador de Alice se puede escribir en campo óptico como:

$$E_{ALICE}(t) = E_0(t)\frac{\sqrt{T_A}}{2}\left[e^{j\Psi_A} e^{\sum_{i=1}^{N} jm_A \cos(\Omega_i t+\Phi_{Ai})} + e^{-j\varepsilon\Psi_A} e^{-\sum_{i=n}^{N} j\varepsilon m_A \cos(\Omega_i t+\Phi_{Ai})} \right] \quad (3.24)$$

En este caso, al igual que en el caso FC-QKD, consideramos que las potencias de las subportadoras de radiofrecuencia son bajas, por tanto, se puede expresar el campo en la aproximación de pequeña señal como:

$$E_{ALICE}(t) = E_0(t) t_{eff,A} \cdot \left\{ 1 + 2\sum_{n=1}^{N} m_{eff,A} \cdot \cos\left(\Omega_i t + \Phi_{A,n}\right) \right\} \quad (3.25)$$

donde $m_{eff,A}$ y $t_{eff,A}$ se definen de igual manera que en el caso de FC-QKD. Este campo es trasmitido a través de un canal de fibra, sufriendo la atenuación y dispersión, de tal manera que a su salida queda:

$$E(t) = \\ = E_0(t) t_{eff,A} \cdot e^{-\frac{\alpha L}{2}} e^{j\beta_0 L} \left\{ 1 + \sum_{n=1}^{N} \left(\begin{array}{l} m_{eff,A} \cdot e^{-j(\Omega_n t+\Phi_{A,n})} e^{-j\beta_1 L\Omega_n} e^{j\frac{1}{2}\beta_2 L\Omega_n^2} \\ +m_{eff,A} \cdot e^{+j(\Omega_n t+\Phi_{A,n})} e^{j\beta_1 L\Omega_n} e^{j\frac{1}{2}\beta_2 L\Omega_n^2} \end{array} \right) \right\} \quad (3.26)$$

A la salida del modulador de Bob el campo se trasforma en:

$$E(t) = t_{eff,A} t_{eff,B} e^{-\frac{\alpha L}{2}} \cdot e^{j\beta_0 L} \cdot E_0(t) \\ \cdot \left\{ \begin{array}{l} 1 + \sum_{n=1}^{N} \left(\begin{array}{l} \left(m_{eff,B} e^{-j\Phi_{B,n}} + m_{eff,A} \cdot e^{-j\beta_1 L\Omega} e^{j\frac{1}{2}\beta_2 L\Omega^2} e^{-j\Phi_{A,n}} \right) e^{-j\Omega_n t} + \\ + \left(m_{eff,B} e^{j\Phi_{B,n}} + m_{eff,A} \cdot e^{j\beta_1 L\Omega} e^{j\frac{1}{2}\beta_2 L\Omega^2} e^{j\Phi_{A,n}} \right) e^{j\Omega_n t} \end{array} \right) \\ + \sum_{n=1}^{N}\sum_{m=1}^{N} m_{eff,B} m_{eff,A} \cdot e^{j\frac{1}{2}\beta_2 L\Omega_n^2} \left(e^{-j\beta_1 L\Omega_n} e^{-j(\Omega_n+\Phi_{A,n})t} + e^{j\beta_1 L\Omega_n} e^{j(\Omega_n+\Phi_{A,n})t} \right) \left(e^{-j(\Omega_m+\Phi_{B,m})t} + e^{j(\Omega_m+\Phi_{B,m})t} \right) \end{array} \right\} \quad (3.27)$$

donde también se ha tenido en cuenta la aproximación de baja señal. En esta expresión, se puede ver como los primeros términos son iguales a los de FC-QKD de la ecuación (3.10) para cada una de las subportadoras mientras que el último se corresponde con la intermodulación.

El sistema de filtrado ubicado a la salida del modulador de Bob tiene como misión separar las diferentes bandas de radiofrecuencia, de tal manera que cada par de detectores centrados en ω_0-Ω_n y ω_0+Ω_n servirán para obtener una clave transmitida en paralelo. La salida del filtro que corresponde a la frecuencia Ω_i será:

$$E\left(\omega_o+\Omega_i\right)= t_{eff,A}t_{eff,B}\cdot e^{-\frac{\alpha L}{2}}e^{j\beta_0 L} \cdot\left[\left(m_{eff,B}e^{j\Phi_{B,i}}+m_{eff,A}\cdot e^{j\beta_1 L\Omega_i}e^{j\frac{1}{2}\beta_2 L\Omega_i^2}e^{j\Phi_{A,i}}\right)+ +e^{j\frac{1}{2}\beta_2 L\Omega_i^2}\sum_{n=-N}^{N}\sum_{m=-N}^{N}m_{eff,B}m_{eff,A}e^{j\beta_1 L\Omega_n}\cdot e^{j\left(\Phi_{A,n}+\Phi_{B,m}\right)}\delta_{\Omega_i,\Omega_n+\Omega_m}\right] \tag{3.28}$$

El primer término de esta expresión es equivalente al de la (3.13) de FC-QKD y el último son las contribuciones no deseadas del término de intermodulación, donde se emplea la siguiente notación:

$$\begin{aligned}\Omega_{-n}&=-\Omega_n\\ \Phi_{A,-n}&=-\Phi_{A,n}\\ \Phi_{B,-n}&=-\Phi_{B,n}\end{aligned} \tag{3.29}$$

La potencia asociada a este campo se puede dividir en dos contribuciones:

$$P_{\Omega_i}=P_{\Omega_i}^{S}+P_{\Omega_i}^{IM} \tag{3.30}$$

La potencia asociada al primer término $P_{\Omega_i}^{S}$ es igual a la suma de N términos iguales a la expresión (3.14) de FC-QKD y el segundo término $P_{\Omega_i}^{IM}$ es la potencia debido a la intermodulación.

Se comenzará analizando el primer término $P_{\Omega_i}^{S}$, que no está afectado por la intermodulación, para cada una de las subportadoras considerando un plan de

frecuencias con 50 subportadoras de radiofrecuencia separadas 1 GHz con f_n=n GHz. Este análisis es válido también cuando el sistema esté trabajando en un régimen donde el término de intermodulación $P_{\Omega_i}^{IMD}$ no sea relevante. Cada una de estas subportadoras tendrá su propia visibilidad efectiva si no se compensa la dispersión como vimos en la expresión (3.19) donde el *QBER* venía dado por la ecuación (3.20). En consecuencia, su propia tasa secreta de bit R_{net}^{i} vendrá dada por:

$$R_{net}^{i} = R_{sift}^{i}\left\{\Delta\left[1-h\left(\frac{QBER(\Omega_i)}{\Delta}\right)\right]-h\left(QBER(\Omega_i)\right)\right\} \qquad (3.31)$$

En la figura 3.7 se muestra las tasas secretas de bit para cada uno de los tonos compensando la dispersión $R_{net}^{C_i}$ (●) y sin compensar $R_{net}^{D_i}$ (■) con la configuración AM-PM para cuatro longitudes del canal (0 km, 20 km, 40 km y 60 km).

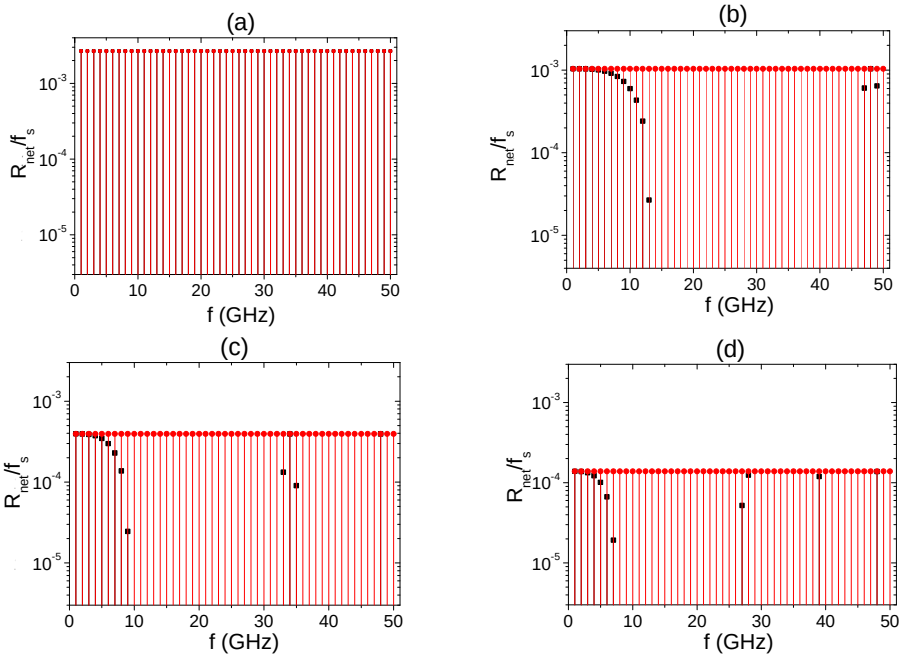

Figura 3.7. Tasa secreta de bit para 50 subportadoras eléctricas en una configuración AM-PM compensando la dispersión (●) y sin compensar (■) para distintas longitudes del canal óptico: (a) 0 km, (b), 20 km, (c) 40 km y (d) 60 km.

Para el caso en el que la intermodulación no sea relevante y la dispersión se compense, todas las subportadoras tienen el mismo QBER dado por la expresión (3.20) puesto que la visibilidad efectiva es la misma para todas. Por tanto, como muestra en la figura 3.7, la tasa secreta $R_{net}^{C_i}$ resulta ser la misma para cada una de la subportadoras, es decir, $R_{net}^{C_i} = R_{net}^{C}$. También, en la figura 3.7 se puede observar cómo la tasa secreta $R_{net}^{D_i}$ sin compensar la dispersión resulta ser diferente para cada subportadora. Esto se debe a que la visibilidad efectiva depende de la frecuencia de la subportadora debido a la dispersión del canal y por tanto, las subportadoras tienen diferente *QBER*. Estos resultados se han calculado con los parámetros usuales de los sistemas reales mencionados en la sección anterior (Δ=0.58, μ=1, α=0.2, ρ=0.1 y V=0.99).

Podemos observar que si no se compensa la dispersión tan solo algunas frecuencias contribuyen a la tasa secreta de bit total, que son las que se aproximan a la condición (3.17). De hecho, al igual que vimos en el apartado anterior, solo las frecuencias que cumplen $n\pi/2-\pi/8 < 1/2\beta_2 L\Omega^2 < n\pi/2+\pi/8$ tiene un $R_{net}^{D_i}$ diferente de cero mientras que compensando la dispersión todas las frecuencias contribuyen de la misma forma.

La tasa secreta de bit total considerando fibra compensada (R_{net}^{TC}) y fibra dispersiva (R_{net}^{TD}), es decir, compensando y sin compensar la dispersión del canal óptico, vienen dadas por:

$$R_{net}^{TC} = \sum_{i=1}^{N} R_{net}^{C_i}, \quad R_{net}^{TD} = \sum_{i=1}^{N} R_{net}^{D_i} \tag{3.32}$$

Como hemos visto anteriormente, para el caso en que la intermodulación no sea relevante compensado la dispersión, todas las subportadoras tienen la misma tasa de bit. Por tanto, la tasa de bit total será $R_{net}^{TC} \cong N \cdot R_{net}^{C}$.

Mientras que el cociente entre la suma de todas las tasas secretas de bit individuales con la tasa secreta de bit de un solo canal con la dispersión compensada viene dado por:

$$\mathrm{M}_D = \frac{R_{net}^{TD}}{R_{net}^{C}} \tag{3.33}$$

donde R_{net}^{C} es la tasa correspondiente a cada uno de los canales teniendo en cuentas las pérdidas de canal óptico pero con la dispersión compensada.

Así pues, el parámetro M_D representa la ganancia efectiva de la multiplexación de las distintas claves. En la figura 3.8(a) se representan las tasas secretas de bit totales en función de la longitud del canal considerando un plan de frecuencias con 50 subportadoras eléctricas separadas 1 GHz. Para obtener tasas secretas de bit más eficientes con SCM-QKD es necesario compensar la dispersión, ya que para todas las posibles longitudes del canal, la tasa secreta de bit compensando la dispersión es superior a sin compensar, excepto para L=0 que son iguales.

En la figura 3.8(b) se muestran el cociente M para planes de frecuencia diferentes, en negro se tiene $\Omega_i=i$ GHz para i=1,2,..,50. Para L=0, el cociente M es igual al número de canales (50) y, según va aumentando L, más subportadoras dejan de aproximarse a la condición $1/2\beta_2 L\Omega^2=n\pi/2$. De hecho las frecuencias que no cumplen $n\pi/2-\pi/8 < 1/2\beta_2 L\Omega^2 < n\pi/2+\pi/8$ presentan una tasa secreta de bit $R_{net}^{D_i}=0$. Para L en torno a 1 km tan solo las frecuencias en torno a 50 GHz dejan de cumplir esta condición, pero a medida que aumenta L, frecuencias más bajas también dejan de cumplirla, no contribuyendo en la tasa secreta de bit total, resultando en un descenso en el cociente M_D. En torno a 20 km la tasa aumenta ligeramente, esto es debido a que las subportadoras con frecuencias próximas a 50GHz empiezan de nuevo a contribuir a la tasa secreta de bit total de forma significativa ya que vuelven a cumplir la condición $n\pi/2-\pi/8 < 1/2\beta_2 L\Omega^2 < n\pi/2+\pi/8$ que es periódica, como veíamos en la figura 3.7.

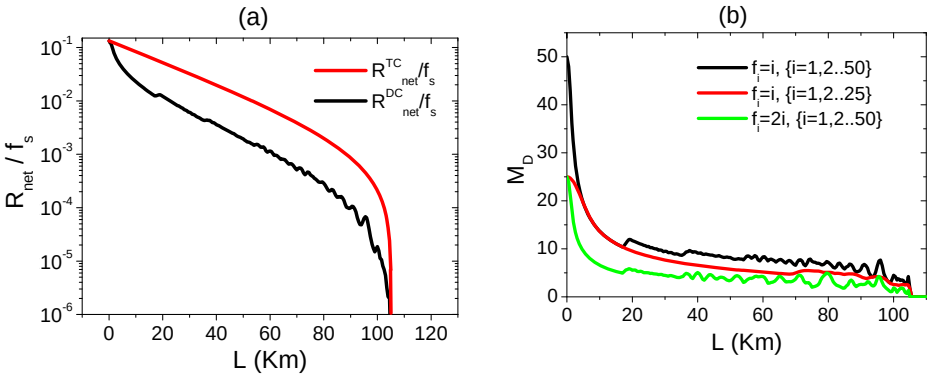

Figura 3.8. (a) Tasa secreta de bit multiplexada compensando la dispersión (—) y sin compensar (—) para el plan de frecuencia f_i=1, 2,…50 GHz y (b) cociente M_D para tres planes de frecuencia diferentes.

También, en la figura 3.8(b) se representa el cociente para dos planes de frecuencia de 25 subportadoras, para el caso de estar equiespaciadas 1 GHz (rojo) y 2 GHz (verde) siendo la frecuencia máxima 25 y 50 GHz, respectivamente. Tanto en el primer caso como en el segundo caso, para una longitud L=0 km la tasa secreta de bit es igual al número de tonos. Conforme vamos aumentando L, el segundo caso decae más rápidamente, ya que hay menos frecuencias bajas que cumplan $n\pi/2-\pi/8 < 1/2\beta_2 L\Omega^2 < n\pi/2+\pi/8$ y por tanto puedan contribuir a la tasa secreta de bit total. En este caso, al igual que el de 50 subportadoras, cuando la longitud del enlace es próxima a 20 km las frecuencias próximas a 50 GHz vuelven a cumplir esta condición que, como antes hemos comentado, es periódica.

Como hemos visto la dispersión es un parámetro que afecta considerablemente a la tasa secreta de bit obteniéndose valores más altos cuando se compensa. Por tanto, conviene evaluar la tolerancia del sistema frente a pequeñas desviaciones en la compensación de la dispersión y estudiar la tolerancia que deben tener los componentes a la hora de compensar este efecto.

Existen varios métodos para compensar la dispersión de las fibras [15]. El análisis que se realiza en este trabajo se basa en el empleo de fibra compensadora [8]. En dichas fibras la dispersión es de signo contrario a la fibra estándar monomodo del canal. En este caso, se debe cumplir la siguiente condición para la compensación total de la dispersión en un enlace determinado:

$$\left(\beta_2 L\right)_T = \beta_2^{SMF} L_{SMF} + \beta_2^{DCF} L_{DCF} = 0 \tag{3.34}$$

donde β_2^{SMF} y L_{SMF} representan la dispersión y la longitud del canal de fibra estándar monomodo respectivamente y β_2^{DCF} y L_{DCF} lo mismo para el canal de fibra compensadora de dispersión. Los valores típicos de estas fibras verifican aproximadamente $\beta_2^{DCF} \approx -10\beta_2^{SMF}$. En la figura 3.9, se muestra la tasa secreta de bit para un tono de 1 GHz, 25 GHz y 50 GHz en función de la longitud de la fibra compensadora, para un plan de frecuencias de $\Omega_i=i$ GHz para i=1,2,..,50 con los parámetros anteriores. Se observa como el máximo de la tasa secreta de bit para todos los tonos se produce cuando la longitud de la fibra compensadora es de 2 km y como, a medida que la frecuencia del tono aumenta, es necesaria más precisión en la longitud para mantener la tasa secreta máxima. En esta misma figura se muestra la suma de todas las tasas secretas de bit de todas las subportadoras con frecuencias desde 1 GHz hasta 50 GHz ($\Omega_i=i$ GHz, i=1,2,..,50). La máxima contribución se produce a una longitud de 2 km, la contribución de los diferentes tonos, en otras longitudes, produce que la suma de todas las tasas secretas de bit no sea cero. De

hecho, cuando se tiene una desviación de 200 m en la fibra compensadora, la tasa secreta decrece 2 dB, y cuando es de 1.5 km la reducción es de 7 dB.

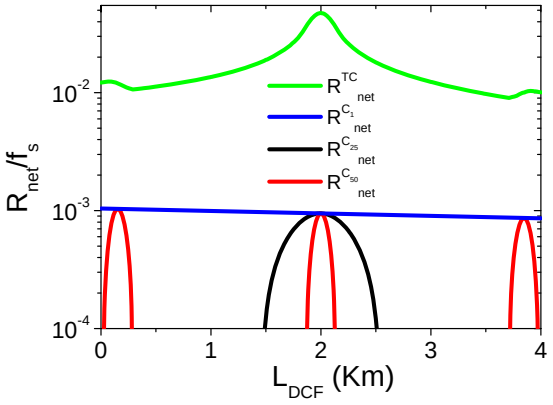

Figura 3.9. Impacto de las desviaciones en la compensación de la dispersión en la tasa secreta de bit para una subportadora de 1 GHz (—), 25 GHz (—), 50 GHz (—) y tasa multiplexada (—) de 50 subportadoras (1, 2…50 GHz) con 20 km de longitud del canal.

Con los resultados de este apartado se puede concluir que para obtener la tasa secreta de bit lo más elevada posible en sistemas SCM-QKD es necesario compensar la dispersión del enlace de fibra. En el caso anteriormente analizado, dicha compensación requiere una precisión de decenas de metros, ya que una desviación de 100 m conlleva pérdidas en la tasa secreta de las subportadoras con frecuencias cercanas a 50 GHz, resultando en 1dB de pérdidas totales con respecto a la tasa máxima.

3.3.2. Análisis de interferencia

En este apartado, vamos a analizar el segundo término de la expresión (3.30). En el régimen de trabajo de baja señal. Este es un orden de magnitud menor que el primero, por tanto, la mejor opción es iniciar el análisis del segundo término con los parámetros que maximizan la tasa secreta de bit del primero, es decir compensando la dispersión (β_2=0), con esta premisa la potencia en la frecuencia Ω_i debida a la intermodulación queda como:

$$P_{\Omega_i}^{IM} =$$

$$= t_{eff,A}^2 t_{eff,B}^2 \cdot e^{-\alpha L} \left[\begin{array}{l} \sum_{n=-N}^{N} \sum_{m=-N}^{N} 2m_{eff,B}^2 \left| m_{eff,A} \right| \cos\left(\Phi_{A,n} + \Phi_{B,m} - \Phi_{B,i} + \arg\left(m_{eff,A} \right) \right) \delta_{\Omega_i, \Omega_n + \Omega_m} \\ + \sum_{n=-N}^{N} \sum_{m=-N}^{N} 2 \left| m_{eff,B} \right| m_{eff,A}^2 \cos\left(\Phi_{A,n} + \Phi_{B,m} - \Phi_{A,i} + \arg\left(m_{eff,B} \right) \right) \delta_{\Omega_i, \Omega_n + \Omega_m} \\ + m_{eff,A}^2 m_{eff,B}^2 \left| \sum_{n=-N}^{N} \sum_{m=-N}^{N} \cdot e^{i\left(\Phi_{A,n} + \Phi_{B,m} \right)} \delta_{\Omega_i, \Omega_n + \Omega_m} \right|^2 \end{array} \right] \quad (3.35)$$

donde aparecen las diferentes fases $\Phi_{A,n}$ y $\Phi_{B,m}$ de las subportadoras eléctricas. Todas estas fases son aleatorias y $\Phi_{A,n} + \Phi_{B,m}$ pueden tomar los valores (0,π,- π/2, π/2), cada uno de ellos con probabilidad ¼ (para $m,n=\{-N....N\}$) [13]. Por tanto, el parámetro de interés que se puede estimar y medir en un sistema real es su valor medio. Para los tres términos que aparecen en la expresión (3.35) se obtienen los siguientes valores medios.

$$\begin{aligned} E\left[\cos\left(\Phi_{A,n} + \Phi_{B,m} - \Phi_{B,i} + \arg\left(m_{eff,A} \right) \right) \right] &= 0 \\ E\left[\cos\left(\Phi_{A,n} + \Phi_{B,m} - \Phi_{B,i} + \arg\left(m_{eff,B} \right) \right) \right] &= 0 \\ E\left[\left| \sum_{n=-N}^{N} \sum_{m=-N}^{N} e^{j\left(\Phi_{A,n} + \Phi_{B,m} \right)} \delta_{\Omega_i, \Omega_n + \Omega_m} \right|^2 \right] &= NCSO\left(\Omega_i \right) \end{aligned} \quad (3.36)$$

Por lo que el valor medio de la potencia de intermodulación queda definido a partir del parámetro $NCSO(\Omega_i)$, que es el número de términos de segundo orden, parámetro clave en otras tecnologías como televisión por cable [16], y depende del plan de frecuencias que se utilice, con esto, el valor medio de la expresión (3.35) queda como:

$$E\left[P_{\Omega_i}^{IM} \right] = t_{eff,A}^2 t_{eff,B}^2 \cdot e^{-\alpha L} \; m_{eff,A}^2 m_{eff,B}^2 \; NCSO\left(\Omega_i \right) \quad (3.37)$$

Para tener en cuenta la relación entre la señal deseada y la de intermodulación se define el parámetro de relación cuántica entre la portadora y el ruido (*Quantum Carrier to Noise Ratio QCNR* [17]) como:

$$QCNR = \frac{P_{\max}}{E\left[P_{\Omega_i}^{IM} \right]} = \frac{16}{NCSO\left(\Omega_i \right) \cdot m^2} \quad (3.38)$$

Esta definición de *QCNR* expresa el cociente entre la probabilidad de detectar un fotón de la señal en la banda Ω_i cuando la visibilidad es 1 (los índices de modulación de Alice y Bob son iguales a m) y la probabilidad de detectar un fotón en la banda $-\Omega_i$ debido a la intermodulación.

En la figura 3.10 se muestra la evolución de *QCNR* en función del índice de modulación para tres planes de frecuencias de 15 subportadoras separadas 2 GHz, 30 subportadoras separadas 1 GHz y 50 subportadoras separadas 1 GHz. Se ha considerado que N_{CSO} tiene el valor más alto posible, el de la frecuencia más baja (Ω_1=1 GHz, Ω_{-1}=-1 GHz), para cada plan de frecuencias. Podemos observar que a medida que el índice de modulación aumenta la relación *QCNR* disminuye, esto es debido a que la potencia de intermodulación aumenta con el índice de modulación. Cuando tenemos más tonos la relación también disminuye debido a que el término *NCSO(Ω_i)* aumenta, lo que conlleva un aumento en la potencia de intermodulación.

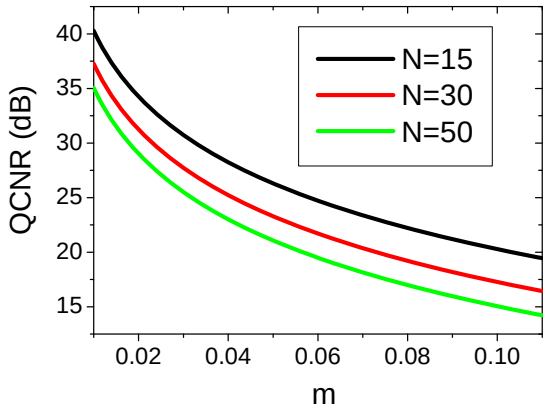

Figura 3.10. *QCNR* en función del índice de modulación para tres planes de frecuencia.

3.3.3. QBER

El rendimiento de un sistema QKD viene dado por el *QBER*. Después de la discusión de bases entre Alice y Bob, este último formará una clave que contendrá errores. En esta sección se obtiene una expresión del *QBER* cuando la dispersión está compensada y teniendo en cuenta la intermodulación.

Para obtener una expresión del *QBER* para nuestro sistema SCM-QKD se usa el método descrito en la referencia [18] pero adaptándolo a N subportadoras. La

probabilidad de que un detector, situado después de un filtro ideal centrado en $\omega_0+\Omega_i$, detecte un fotón tiene tres contribuciones diferentes. La primera proviene de la propia señal detectada que denotaremos por $P_{\exp}^{signal}(\Omega_i) = P_{\max}\tau / h\nu$. Otra es debida a la intermodulación y la expresaremos por $P_{\exp}^{imd}(\Omega_i) = P_{\Omega_i}^{IM}\tau / h\nu$ y por último la contribución debida a las cuentas oscuras $P_{\exp}^{d}(\Omega_i)$. La combinación de las tres nos dará la probabilidad total de detectar un fotón que la expresamos como:

$$\begin{aligned} & p_{\exp}(\Omega_i) = p_{\exp}^{signal}(\Omega_i) + p_{\exp}^{imd}(\Omega_i) + p_{\exp}^{d}(\Omega_i) \\ & - p_{\exp}^{signal}(\Omega_i)\, p_{\exp}^{imd}(\Omega_i) - p_{\exp}^{signal}(\Omega_i)\, p_{\exp}^{d}(\Omega_i) \\ & - p_{\exp}^{imd}(\Omega_i)\, p_{\exp}^{d}(\Omega_i) + p_{\exp}^{imd}(\Omega_i)\, p_{\exp}^{d}(\Omega_i)\, p_{\exp}^{signal}(\Omega_i) \end{aligned} \tag{3.39}$$

donde se ha asumido que todas las contribuciones son independientes. La probabilidad de que la fuente emita k fotones en la banda Ω_i la vamos a representar por $R_i(k)$ por lo que la probabilidad de que un fotón en esta banda sea detectado vendrá dada en términos de la eficiencia del detector ρ de la siguiente manera:

$$p_{\exp}^{signal}(\Omega_i) = \sum_{k=0}^{\infty} R_i(k) \left[\sum_{l=1}^{k} \binom{k}{l} \left(\rho T_L(\Omega_i)\right)^l \left(1 - \rho T_L(\Omega_i)\right)^{l\text{-}1} \right] \tag{3.40}$$

donde $T_L(\Omega_i)$ es la transmitancia de la fibra, el modulador de Bob y el sistema de filtrado que se pueden expresar como:

$$T_L(\Omega_i) = e^{-\alpha L} \cdot \left| t_{eff,B} \right|^2 \cdot T_F(\Omega_i) \tag{3.41}$$

siendo $T_F(\Omega_i)$ la transmitancia de los filtros ópticos empleados para seleccionar el canal.

Por otra parte $I_i(k)$ representa la probabilidad de que se produzca un fotón en la banda Ω_i por intermodulación. La probabilidad de que este sea detectado es:

$$p_{\exp}^{imd}(\Omega_i) = \sum_{k=0}^{\infty} I_i(k) \left[\sum_{l=1}^{k} \binom{k}{l} \left(\rho T_L(\Omega_i)\right)^l \left(1 - \rho T_L(\Omega_i)\right)^{l\text{-}1} \right] \tag{3.42}$$

Por último, la distribución de cuentas oscuras viene dada por:

$$p_{\exp}^{d}(\Omega_i) = d_B \tag{3.43}$$

La fuente óptica pulsada se atenúa fuertemente, por lo que el número de fotones por bit puede considerarse que viene representado por medio de una distribución de Poisson con media μ_i, que representa el número medio de fotones por bit:

$$R_i(k) = \frac{e^{-\mu_i}\left(\mu_i\right)^k}{k!} \tag{3.44}$$

Introduciendo la expresión (3.44) en (3.40), la probabilidad de detección de señal viene dada por:

$$p_{\exp}^{signal}\left(\Omega_i\right) = 1 - e^{-\rho T_L(\Omega_i)\mu_i} \approx \rho T_L\left(\Omega_i\right)\mu_i \tag{3.45}$$

de forma similar, los fotones generados por intermodulación también siguen una distribución de Poisson con media μ_i^{imd}.

$$I_i(k) = \frac{e^{-\mu_i^{imd}}\left(\mu_i^{imd}\right)^k}{k!} \tag{3.46}$$

De acuerdo con los resultados de [19] se obtiene:

$$\mu_i^{imd} = \mu_i \frac{m^2 NCSO\left(\Omega_i\right)}{16} = \frac{\mu_i}{QCNR} \tag{3.47}$$

por lo que:

$$\begin{aligned} p_{\exp}^{imd\_i} &= 1 - e^{-\rho T_L \mu_i^{imd}} \approx \rho T_L\left(\Omega_i\right)\mu_i^{imd} = \\ &= \left(\frac{NCSO\left(\Omega_i\right)m^2}{16}\right)\rho T_L\left(\Omega_i\right)\mu_i = \rho T_L\left(\Omega_i\right)\frac{\mu_i}{QCNR} \end{aligned} \tag{3.48}$$

La probabilidad de error viene dada nuevamente por tres términos, el primero es debido a los errores en la alineación del sistema, los cuales afectan a la visibilidad del sistema. Esto se puede expresar como vimos en (3.18) mediante:

$$p_{visibility}^{error}\left(\Omega_i\right) = \frac{(1 - V_{eff})}{2} p_{\exp}^{signal}\left(\Omega_i\right) \tag{3.49}$$

Solamente la mitad de las cuentas oscuras contribuirán al error, por tanto:

$$p_{dark}^{error\_i} = \frac{d_B}{2} \tag{3.50}$$

Finalmente la contribución de la intermodulación al error es:

$$p_{imd}^{error\_i} = \frac{p_{\exp}^{imd\_i}}{2} \tag{3.51}$$

Teniendo en cuenta (3.45)-(3.51) se llega a la siguiente expresión para el *QBER*:

$$QBER(\Omega_i) = \frac{\frac{(1-V)}{2} p_{\exp}^{signal}(\Omega_i) + \frac{d_B}{2} + \frac{p_{\exp}^{imd}(\Omega_i)}{2}}{p_{\exp}^{signal}(\Omega_i)} \tag{3.52}$$

Esta expresión se puede simplificar si tenemos en cuenta que d_B<<1 y también $\rho T_L \mu_i$<<1 llegando a:

$$QBER(\Omega_i) = \frac{\left\{(1-V) + \left(\frac{1}{QCNR_{CSO}^i}\right)\right\} \rho T_L(\Omega_i) \mu_i + d_B}{2\left[\left\{1 + \left(\frac{1}{QCNR_{CSO}^i}\right)\right\} \rho T_L(\Omega_i) \mu_i + d_B\right]} \tag{3.53}$$

3.3.4. Análisis del QBER

En este subapartado, se va a hacer uso de la expresión (3.53) para realizar un análisis del QBER para diferentes configuraciones del sistema SCM-QKD. Se considera que los moduladores poseen un ancho de banda de modulación suficiente, de tal forma que las pérdidas sean independientes de la frecuencia de la subportadora. Las figuras 3.11(a), (b) y (c) muestran los valores del *QBER* para distintas longitudes, obtenidas para unos planes de frecuencias con un número de subportadoras de N = 1, 15, 30 y 50 respectivamente, con un espaciado de 1 GHz entre ellas. Para realizar estas simulaciones se ha tomado los siguientes valores típicos de los parámetros: V = 98 % eficiencia del detector ρ = 0.13, α = 0.2 dB/km y T_B = 9.6 dB. Se ha considerado que N_{CSO} tiene el valor más alto posible para cada plan de frecuencias y el número medio de fotones para cada banda es μ = 0.05. El QBER aumenta cuando la longitud del enlace aumenta, ya que, debido a las

pérdidas de este, Bob presenta menos probabilidad de detectar correctamente. También aumenta cuando hay más tonos, debido a la intermodulación, pero este efecto es despreciable para valores de *m* pequeños como se puede observar en la figura 3.11(a), mientras que para índices de modulación más grandes (figuras 3.11 (b) y 3.11 (c)) el efecto comienza a ser apreciable.

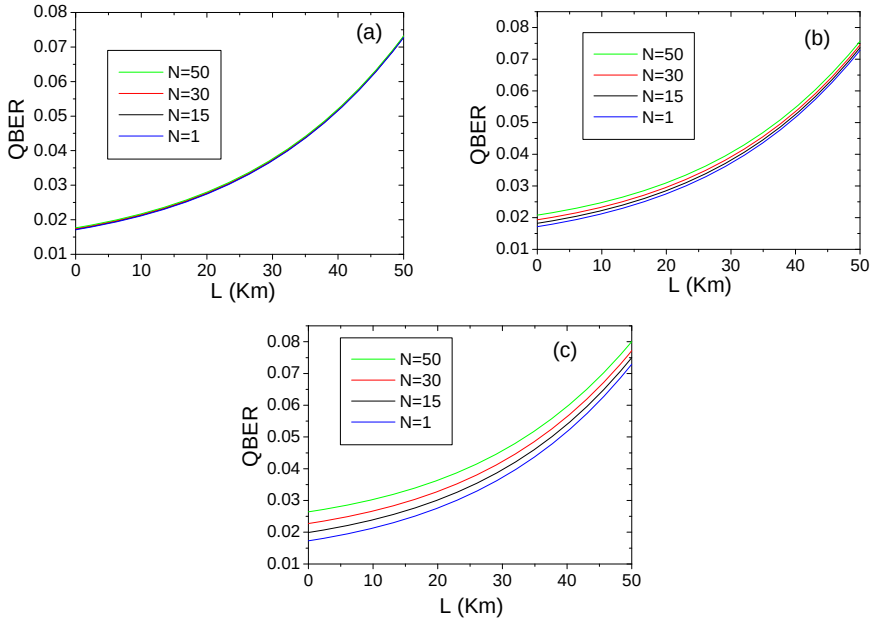

Figura 3.11. Impacto de la intermodulación en el QBER para distintos planes de frecuencia (N = 1, 15, 30, 50) en función de la longitud del canal con un índice de modulación de (a) $m = 0.02$, (b) $m = 0.04$ y (c) $m = 0.08$.

En la figura 3.12(a) se muestran la evolución del *QBER*, en función de la distancia del canal, para distintas visibilidades, con *N*=15 y el resto de parámetros del sistema iguales a los de la gráfica 3.11. Se puede observar que, de las cuatro curvas que se muestran, las que tienen valores más altos de visibilidad, debido a un mal ajuste en la interferencia, son las que registran valores más altos en el *QBER*. En la figura 3.12(b) se muestra la evolución del *QBER*, en función en este caso de la longitud del enlace que separa Alice y Bob, para distintos valores de μ. Las curvas que tienen el número medio de fotones más alto tienen una probabilidad más alta de que Bob detecte correctamente, dando lugar a un *QBER* más bajo.

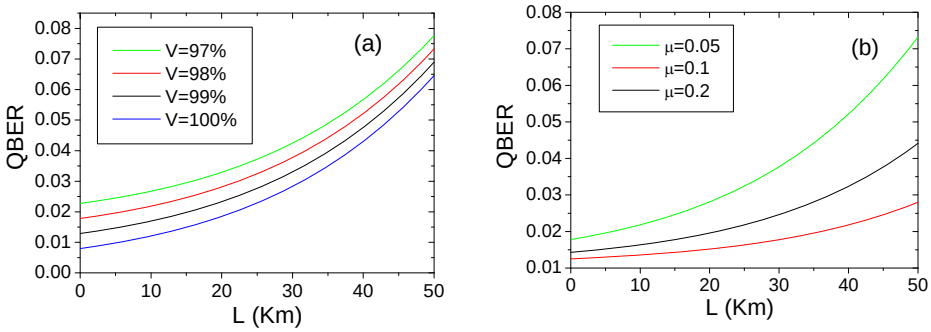

Figura 3.12. Impacto de la visibilidad (a) y el número promedio de fotones (b) en el QBER en función de la longitud del canal.

Tras este análisis podemos concluir que el *QBER* de una única subportadora se aproxima al de FC-QKD para índices de modulación bajos.

3.3.5. Tasa secreta de bit

Ya se ha comentado que uno de los usos de la técnica de SCM es para incrementar la tasa secreta de bit. En este apartado se va a evaluar bajo qué condiciones se puede conseguir este objetivo. Para ello, comenzamos con la tasa secreta de bit para cada una de las subportadoras que viene dada por la expresión (3.31) [1].

La tasa secreta de bit total R_{net}^{IMD} teniendo la intermodulación debido a la multiplexación de las distintas subportadoras eléctricas, será la suma de las tasas secretas de cada una de las suportadoras R_{net}^{i} de forma que:

$$R_{net}^{IMD} = \sum_{i=1}^{N} R_{net}^{i} \tag{3.54}$$

Para evaluar el incremento en la tasa secreta de SCM-QKD con respecto a FC-QKD se define la ganancia de trasmisión como:

$$M_{IMD} = \frac{R_{net}^{IMD}}{R_{net}^{C}} \tag{3.55}$$

donde R_{net}^{C} se corresponde con la tasa secreta de bit de una subportadora eléctrica compensando la dispersión. En la figura 3.13(a), se representa la tasa secreta total para distintos índices de modulación y con un plan de frecuencias de 15 tonos

separados 1GHz, y con unos parámetros del sistema dados por $V = 99$ %, $\rho = 0.13$, $\mu = 1$, $\alpha = 0.2$ dB/km y $T_B = 9.6$ dB. Como cabía esperar, para curvas con índices de modulación altos, la tasa secreta disminuye debido a la intermodulación. En la figura 3.13(b), se observa lo que ocurre con la ganancia de trasmisión, en función del índice de modulación, para distintos planes de frecuencias, donde las subportadoras están separadas 1 GHz, una longitud del canal de $L = 30$ km y con el resto de parámetros iguales a los de la figura 3.11. Para índices de modulación pequeños se consigue que la ganancia sea igual al número de tonos, pero a medida que aumenta el índice de modulación se produce más intermodulación dando lugar a una caída en la ganancia.

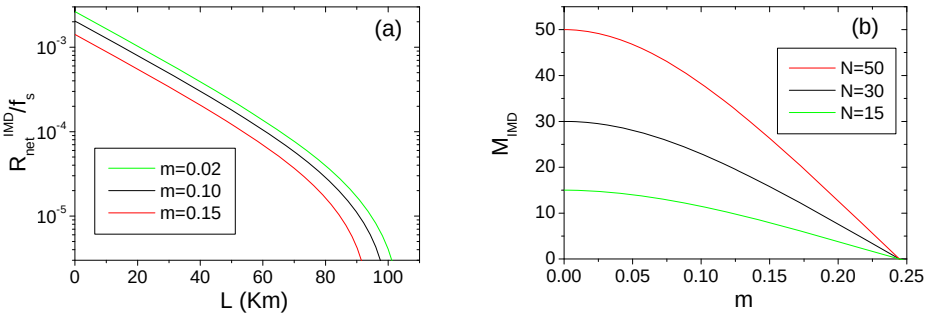

Figura 3.13. (a) Tasa secreta de bit total para distintos índices de modulación (m = 0.02, 0.10, 0.15) en función de la longitud y (b) ganancia de trasmisión en función del índice de modulación para distintos planes de frecuencia (N = 15, 30, 50).

Con estos resultados se puede concluir que con la técnica SCM se puede conseguir aumentar la tasa secreta de bit un factor igual al número de tonos siempre y cuando se trabaje en el régimen de baja señal, es decir, con índices de modulación bajos.

3.4. Fuentes de degradación de la señal

Aparte de la intermodulación existen otro tipo de efectos que producen errores en la clave, como el efecto Raman y la interferencia producida por fotones de otras bandas y la portadora óptica debido al ensanchamiento producido al modular la fuente y por el ruido de fase, respectivamente. En este apartado, se realiza una descripción general de cada uno de ellos por separado, y en el último apartado se obtiene el *QBER* teniendo en cuenta todos estos efectos conjuntamente.

3.4.1. Efecto Raman

Cuando la señal cuántica es trasmitida a través de un canal, acompañado de otras señales clásicas en otras longitudes de onda, aparecen efectos como la dispersión Raman [20], mezcla de cuatro ondas (FWM), en el caso de más de una señal clásica [19], y emisión espontanea (en el caso de amplificación de la señal clásica) [8] degradando el sistema QKD. Por eso, hasta recientemente, era necesario trasmitir la señal cuántica y la señal clásica (empleada para la destilación de clave y la encriptación de la comunicación) por fibras diferentes.

Las primeras investigaciones para trasmitir ambas señales a través de una misma fibra fueron llevadas a cabo por Townsend en los 90 [21], más tarde, en el 2005, Lee y Wellbrock demostraron un sistema QKD capaz de trasmitir una señal clásica y otra cuántica por la mima fibra óptica, ambos en la banda C con una separación entre ellas por debajo de 400 GHz [18]. Pero en ambos casos la señal clásica no tenía otra finalidad más que el estudio del efecto de la diafonía. Estudios más recientes [21, 23] investigan estos efectos cuando se trasmite más de un canal clásico junto a la señal cuántica, dichos canales clásicos interaccionan entre sí afectando al canal cuántico a través del FWM.

En los sistemas FC-QKD y SCM-QKD, es necesario trasmitir, por medio de un canal clásico, las subportadoras de radiofrecuencia entre Alice y Bob para compensar las fluctuaciones de los retardos de las fibra, debido a condiciones ambientales que se traducen en una variación en las diferencias de fase entre las subportadoras de Alice y Bob [9]. El canal clásico se trasmite junto a la señal cuántica en diferentes longitudes de onda mediante CWDM con una separación típica de alrededor de 20 nm [24]. Por tanto, el canal clásico, puede afectar a la señal cuántica debido al efecto Raman, en la figura 3.14 se muestra un esquema de este efecto.

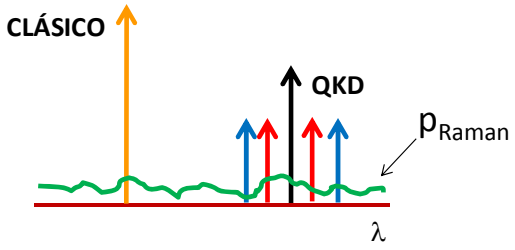

Figura 3.14. Descripción del efecto Raman en sistemas FC-QKD debido a la coexistencia de canales clásicos y cuánticos.

El efecto Raman es debido a la interacción fotón-fotón, los fotones pueden cambiar su longitud de onda y por tanto comprometer otros canales. Dependiendo de si el fotón es excitado o desexcitado se producen fotones de longitudes de onda superiores (Stokes) o longitudes de onda inferiores (anti-Stokes) a la inicial. El scattering de fotones acústicos (Brillouin scattering) no es crucial, ya que el ancho de banda de este efecto está por debajo de 10 GHz y no afectaría a la señal cuántica. Sin embargo, el scattering de fotones ópticos (efecto Raman) tiene un ancho de banda que cubre toda la banda C.

La potencia Raman (dP_{ram}) a una longitud de onda λ producida por un elemento diferencial dx en la posición x cuando una potencia P_{in} es introducida en la fibra viene gobernada por la ecuación [20]:

$$dP_{ram}(\lambda, x) = P_{in} e^{-\alpha x} \rho(\lambda) \Delta\lambda dx \tag{3.56}$$

Donde $\rho(\lambda)$ es la sección eficaz de Raman . La dispersión Raman es igual para todas las direcciones (isotrópica), por tanto, la potencia Raman propagada hacia adelante (en el mismo sentido que lleva la señal de bombeo) para una longitud L, teniendo en cuenta las pérdidas de la fibra para esa longitud, es:

$$dP_{ram,f} = dP_{ram}(\lambda, x) e^{-\alpha(L-x)} \tag{3.57}$$

Integrando sobre toda la fibra obtenemos

$$P_{ram} = P_{in} e^{-\alpha L} \rho(\lambda) L \Delta\lambda \tag{3.58}$$

de esta manera la señal detectada por los detectores en Bob será, teniendo en cuenta que el único factor de degradación es la dispersión Raman:

$$P_{\Omega_i}^{\det} = P_{\Omega_i} + P_{ram} \tag{3.59}$$

donde $P_{\Omega i}$ representa la potencia de la señal deseada en la frecuencia Ω_i.

3.4.2. Ruido de fase y ensanchamiento por modulación de la portadora óptica

Otro factor a tener en cuenta en los sistemas QKD basados en modulación en frecuencia es el ruido de fase de la portadora óptica que puede afectar a las bandas laterales que se generan por la modulación. También, la portadora óptica tiene cierta anchura espectral asociada a la pulsación de la fuente que en caso de trabajar

con pulsos estrechos del orden de nanosegundos podrían afectar a las bandas laterales situadas a frecuencias de GHz respecto de la portadora. Mientras que el ruido de fase de la portadora óptica está espectralmente caracterizado por una función lorentziana cuyos parámetros dependen de la fuente láser [8], el espectro óptico asociado a la modulación de la portadora óptica viene dado por el tipo de pulso utilizado cuya anchura es T_s.

En la figura 3.15 se muestra un esquema de estos efectos donde puede observarse que las bandas más cercanas a la portadora óptica son las más afectadas. Este efecto debe ser tenido en cuenta a la hora de diseñar un sistema FC-QKD, considerando la mínima distancia en frecuencia que debe existir entre portadora y bandas, para obtener valores del QBER aceptables. Los fotones procedentes de la portadora óptica son los que más pueden afectar a las bandas laterales de interés ya que, en general, la relación en potencia entre la portadora óptica y las bandas suele ser de unos 30 dB. No obstante, en ciertas circunstancias las bandas laterales más próximas también pueden afectar a las bandas de interés con el correspondiente aumento del QBER.

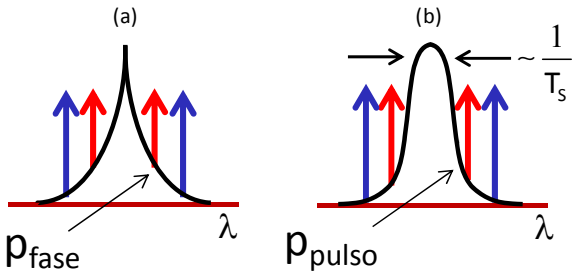

Figura 3.15. Descripción del ensanchamiento de la portadora óptica debido (a) al ruido de fase y (b) la modulación pulsada de la fuente óptica.

Por tanto, la potencia detectada en cada una de las bandas, teniendo en cuenta que el único factor de degradación procede de la portadora óptica, se puede expresar como:

$$P_{\Omega_i}^{\det} = P_{\Omega_i} + P_{\Omega_i}^{fase} + P_{\Omega_i}^{pulso} = P_{\Omega_i} + P_{\Omega_i}^{port} \tag{3.60}$$

donde $P_{\Omega_i}^{fase}$ y $P_{\Omega_i}^{pulso}$ son la potencia debida al ruido de fase y a la modulación de la portadora óptica en la frecuencia Ω_i, y que se engloban ambas en $P_{\Omega_i}^{port}$.

3.4.3. Impacto de las fuentes de degradación en el QBER

A la hora de tener en cuenta los efectos limitantes de los apartados anteriores en el *QBER,* hay que calcular la probabilidad de detectar un fotón por algunos de estos efectos. Para el efecto Raman, la probabilidad de detección viene dada por la siguiente expresión:

$$p_{ram} = \frac{\lambda}{hc} \cdot \eta \cdot \Delta t_{gate} \cdot \left| t_{eff,B} \right|^2 \cdot T_F\left(\Omega_i\right) \cdot P_{ram} \cdot \Delta f_{filtro} \qquad (3.61)$$

donde η es la eficiencia del detector, Δt_{gate} es la duración de la ventana de detección y Δf_{filtro} es el ancho de banda del filtro. En esta expresión, también se tienen en cuenta las pérdidas en el modulador de Bob y en el sistema de filtrado a través de $t_{eff,B}$ y T_F , respectivamente.

La probabilidad de detectar un fotón en una de las bandas debido a la portadora es:

$$p_{port} = \frac{\lambda}{hc} \cdot \eta \cdot \Delta t_{gate} \cdot \int_{-\infty}^{\infty} P_{port}\left(\omega\right) \cdot T_L\left(\Omega_i\right) d\omega \qquad (3.62)$$

donde se ha tenido en cuenta las pérdidas del canal, del modulador de Bob y del filtrado óptico que están todas incluidas en $T_L(\Omega_i)$ de la expresión (3.41). En este caso, la densidad espectral de potencia P_{port} no es constante a lo largo del ancho de banda del filtro a diferencia del efecto Raman, siendo necesario realizar la integral.

Con estas probabilidades y teniendo en cuenta la expresión (3.52), obtenemos la expresión general para el QBER que contiene todas las contribuciones analizadas:

$$\begin{aligned} &QBER\left(\Omega_i\right) = QBER\left(\Omega_i\right)_v + QBER\left(\Omega_i\right)_d + \\ &QBER\left(\Omega_i\right)_{imd} + QBER\left(\Omega_i\right)_{raman} + QBER\left(\Omega_i\right)_{port} = \\ &\frac{1}{2}\frac{(1-V_{eff}) \cdot p_{signal} + d_B + p_X}{p_{signal} + d_B + p_X} \end{aligned} \qquad (3.63)$$

donde $QBER(\Omega_i)_v$ y $QBER(\Omega_i)_d$ son el QBER producido por el desajuste en el sistema reflejado en la visibilidad efectiva y las cuentas oscuras, respectivamente. El resto de parámetros $QBER(\Omega_i)_{imd}$, $QBER(\Omega_i)_{raman}$ y $QBER(\Omega_i)_{port}$ son el QBER producido por la intermodulación, el efecto Raman y la portadora óptica, respectivamente. Todos estos efectos son incluidos en p_x, que viene dado por:

$$p_X = p_{imd} + p_{port} + p_{raman} \tag{3.64}$$

que es la expresión final que tiene en cuenta todas las fuentes de errores de los sistemas SCM-QKD.

Con el fin de evaluar cada una de las contribuciones, se ha considerado un sistema SCM-QKD con un plan de frecuencias formado por 50 subportadoras con una separación espectral Δf de forma que la frecuencia, $\Omega_i = i2\pi\Delta f$ *con* i=1,2,…,50). En la figura 3.16 se muestra cómo afecta cada uno de los términos descritos en el QBER en función del índice de modulación y del ancho de banda del filtro utilizado. La visibilidad del sistema es de V = 98 % y la potencia de bombeo debido a la trasmisión de los tonos es P_{in} = -20 dBm. La fuente óptica asociada a la portadora óptica se considera espectralmente como una lorentziana de 10 MHz de ancho de banda. La modulación de la fuente se corresponde con un espectro gaussiano cuya anchura es de 1GHz. La probabilidad de cuentas oscuras es de d=10^{-4}, el sistema de filtrado con un ancho de banda de Δf_{filtro} para cada banda y una longitud del canal de L=20 km. Se toma el *QBER* del peor caso de todos dado por la subportadora más cercana a la portadora.

En la figura 3.16(a), se puede observar que al considerar índices de modulación pequeños, el ruido asociado a la portadora óptica predomina. A medida que el índice de modulación aumenta, el factor asociado a la intermodulación es el que más afecta al QBER. En este caso, se ha tomado el valor $\Delta f_{filtro}/\Delta f$=0.5.

El ancho de banda del filtro también juega un papel importante puesto que determina la relación señal-ruido del sistema. Para minimizar el impacto de las fuentes degradantes, el ancho de banda del filtro debería ajustarse al ancho de banda la modulación de la fuente óptica. De esta forma, se reduce el número de fotones debidos al efecto Raman y al ruido asociado a la portadora óptica. La figura 3.16(b) muestra que la intermodulación es el efecto predominante para anchos de banda de filtrado pequeños, mientras que para anchos de banda más altos son el efecto Raman y el ruido de la portadora los más importantes. En este caso, el índice de modulación es m=0.12.

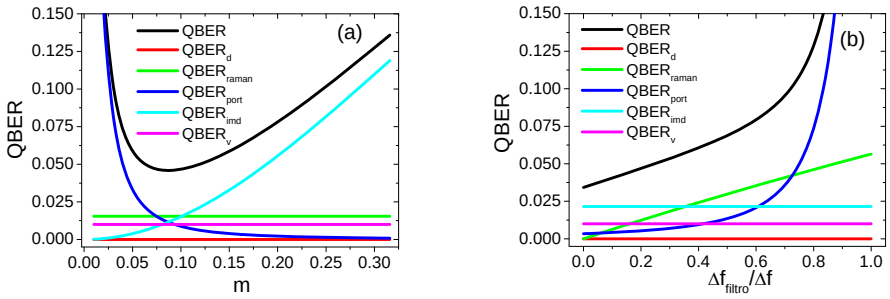

Figura 3.16. QBER producido por diferentes efectos de degradación en función del (a) índice de modulación y del (b) ancho de banda del filtro normalizado por la separación espectral entre subportadoras.

3.5. Conclusiones

En el segundo apartado de este capítulo, se han analizado los sistemas FC-QKD, teniendo en cuenta todas las posibles configuraciones que se pueden hacer con los moduladores que existen en el mercado. Para ello se ha desarrollado una notación que ha permitido trabajar con todas las configuraciones de forma general y se han obtenido las condiciones que deben cumplir para implementar el protocolo BB84. Como resultado han aparecido configuraciones nuevas como la PM-PM, capaces de aprovechar la dispersión del canal y funcionar con este protocolo, que no se habían tenido en cuenta hasta la fecha. También se ha estudiado la eficiencia de todas las configuraciones en términos de su tasa secreta de bit, resultando como más eficientes la PM-PM y AM-PM. Se ha analizado el impacto de la dispersión en las diferentes configuraciones. Esta impone una ligadura entre la distancia del canal y la frecuencia de la subportadora eléctrica en la configuración PM-PM que no se puede eliminar compensando la dispersión, pero si en la configuración AM-PM.

En el tercer apartado se han estudiado los sistemas de distribución de clave con multiplexación de la subportadora. Se ha obtenido que la condición necesaria para obtener un tasa secreta de bit lo más efectiva posible es compensar la dispersión del canal de fibra. De este modo todas las frecuencias contribuyen en la tasa secreta. También se ha obtenido como condición trabajar con índices de modulación bajos, minimizándose la intermodulación, encontrado una expresión que ha permitido evaluarla. Con estas condiciones se ha encontrado que la ganancia en la tasa secreta de bit, usando esta técnica, es igual al número de subportadoras eléctricas en el sistema.

Por último en el cuarto apartado se ha obtenido una expresión para el *QBER* que tiene en cuenta todos los efectos de degradación que presentan los sistemas SCM-QKD. Se han evaluado cada uno de ellos en función de los parámetros del sistema y se han encontrado las condiciones que tienen que guardar para minimizar estos efectos.

Referencias

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing" en Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, 175-179 (1984).

[2] J-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer y W. T. Rhodes, "Single-photon interference in Sidebands of Phase-Modulated Light for Quantum Cryptography," Phys. Rev. Lett. 82, 1656-1659 (1999).

[3] G. E. Betts, "LiNbO3 external modulators and their use in high performance analog links", en RF Photonic Technology in Optical Fiber Links (Cambridge Univ. Press, 2002), cap. 4.

[4] O. Guerreau, J-M. Mérolla, J. Malassenet y J. P. Goedgebuer, "60 km QKD Transmission with Polarization Control, using 4+2 Protocol with Strong Reference," J. Sel. Top. Quantum Electron. 11, 15633-1640 (2004).

[5] M. Mérolla, L. Duraffourg, J. P. Goedgebuer, A. Soujaeff, F. Patois y W. T. Rhodes, "Integrated quantum key distribution system using single sideband detection," Eur. Phys. J. D 18, 141-146 (2002).

[6] J. Cussey, F. Patois, N. Pelloquin y J-M Merolla, "High Frequency Spectral Domain QKD Architecture with Dispersion Management for WDM Network," en Proc. Optical Fiber Communication Conference, paper OWJ3 (2008).

[7] G. P. Agrawal, "Fiber-Optics Communications Systems" (John Wiley & Sons, New York, 2002).

[8] B. E. A. Saleh and M. C. Teich," Fundamentals of Photonics" (John Wiley & Sons, New York, 1991).

[9] O. Guerreau, J-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer y F. J. Malassenet, "Long distance QKD transmission using single-sideband detection detection scheme with WDM synchronization", J. Sel. Top. Quantum Electron. 9, 1533-1540 (2003).

[10] M. Howerton, and W. K. Burns, "Broadband traveling wave modulators in LiNbO3", en RF Photonic Technology in Optical Fiber Links, W.S. Chang, (Cambridge Univ. Press, 2002), cap. 5.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N.Lütkenhaus y M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. 81, 1301-1350 (2009).

[12] J. Capmany y D. Novak, "Microwave photonics combines two worlds", Nature Photon. 1, 319-330 (2007).

[13] J. Capmany, A. Ortigosa- Blanch, J. Mora, A. Ruiz-Alba, W. Amaya y A. Martinez "Analysis of Subcarrier Multiplexed Quantum Key distribution systems: Signal, Intermodulation and Quantum Bit Error rate", J Sel. Topics Quantum. Electron. 15, 1607-1620 (2009).

[14] A. Ortigosa-Blanch y J. Capmany, "Subcarrier multiplexing optical quantum key distribution," Phys. Rev. A 73, 024305 (2006).

[15] C. H. Cox III, "Analog Optical Links: Theory and Practice" (Cambridge Univ. Press, 2004).

[16] N. J. Frigo, M. R. Phillips y G. E. Bodeep, "Clipping distortion in lightwave CATV systems: Models, simulations, and measurements", J. Lightwave Technol. 11, 138-146 (1993).

[17] W. I. Way, "Broadband Hybrid Fiber/Coax Access System Technologies", (San Diego, CA Academic, 1998).

[18] T. J. Xia, D. Z. Chen, G. A. Wellbrock, A. Zavriyev, A. C. Beal y K. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels", en Proc. Optical Fiber Communication Conference, paper OTuJ7 (2006).

[19] R. W. Tkach, A. R. Chraplyvy, F. Forghieri, A. H. Gnauck y Derosier, "Four-photon mixing and high-speed WDM systems", J. Lightwave Technol. 13, 841–849 (1995).

[20] Q. Lin, F. Yaman y G. P. Agrawal, "Photon-pair generation in optical fibers through four-wave mixing: role of Raman scattering and pump polarization", Phys. Rev. A, 75, 023803 (2007).

[21] P.D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing", Electron. Lett. 33, 188-190 (1997).

[22] N. A. Peters, “Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments”, New J. Phys. 11, 045012 (2009).

[23] R. J. Runser, T. Chapuran, P. Toliver, A. Nicolas, M.S. Goodman, J. Kosloski, N. Nweke, S.R. McNown, R.J. Hughes, D. Rosenberg, C.G. Peterson, K.P.McCabe, J.E. Nordholt, K. Tyagi, P. A. Hiskett y N. Dallman, “Progress toward quantum communications networks: opportunities and challenges,” en Proc. Optoelectronic Integrated Circuits 6476, 647601 (2007).

[24] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer y H. Dardy “Optical networking for quantum key distribution and quantum communications,” New J. Phys. 11, 105001 (2009).

Capítulo 4

Demostrador y Resultados Experimentales de Sistemas FC-QKD y WDM/SCM-QKD

4.1. Introducción

Con carácter general, la viabilidad de transferir una nueva tecnología al mercado actual reside en su capacidad para ser integrada de manera eficiente manteniendo un coste razonable. Por ello, en esta Tesis se ha puesto en práctica un sistema de distribución cuántica de clave con componentes de telecomunicación estándar. En este contexto, debido al interés de la seguridad en las comunicaciones, las redes ópticas para sistemas de distribución de clave cuántica se están desarrollando rápidamente, y es de vital interés que lo hagan de una manera eficiente [1]. Por ello, en estas redes se está empezando a implementar técnicas de multiplexación WDM,

con el fin trasmitir diferentes canales QKD por la misma fibra [2-4], reduciéndose el número de fibras y resultando en una menor complejidad y un menor coste de la red.

En estos momentos ya se ha demostrado el funcionamiento de distintas redes y demostradores piloto de distribución de clave cuántica, como son la red SECOQC [5] inaugurada en el 2008 en Viena y la red Tokio QKD [6] implementada en la capital japonesa en 2010. En todas ellas están involucradas un gran número de empresas como id Quantique (Ginebra) [7], MagiQ Technologies (New York), SmartQuantum (Francia) y Quintessence Labs (Australia). Otras compañías también tienen programas activos de investigación en este campo como son Toshiba, HP, IBM, Mitsubishi, NEC y NTT.

Es en este tipo de escenarios donde las técnicas combinadas de SCM y WDM juegan un papel importante, ya que permiten la trasmisión de datos entre diferentes usuarios a una mayor velocidad y eficiencia espectral, compartiendo el mismo enlace.

Los primeros resultados publicados basados en WDM han servido para estudiar el impacto de uno o múltiples canales clásicos de información sobre un canal cuántico aislado [8]. Normalmente, los canales clásicos y cuánticos se ubican en distintas bandas espectrales con el fin de minimizar el efecto Raman que resulta ser el factor más negativo sobre el canal QKD. Recientemente, un primer sistema QKD con tres canales WDM, con frecuencias dentro de la banda C, ha sido demostrado de forma experimental [9, 10]. En este caso, se han alcanzado tasas de generación de clave de 200 kb/s, unas pérdidas de trasmisión de 14.5 dB y una tasa de generación de pulsos de 1.22 GHz. La técnica WDM, por si sola, tiene la desventaja de consumir un canal entero para cada longitud de onda por lo que es, espectralmente, muy ineficiente. Una alternativa interesante es distribuir más de un canal por cada longitud de onda y, de esta manera, conseguir una mayor eficiencia espectral usando sistemas SCM-QKD [11]. Esta técnica a su vez puede ser combinada con WDM (WDM/SCM-QKD).

En este capítulo se va a continuar con el estudio de las estructuras de sistemas FC-QKD y SCM-QKD desarrollado en el capítulo 3. En este caso el estudio es experimental, y se lleva a cabo a través de diferentes prototipos.

En el apartado 4.2, se realiza un estudio experimental de dos configuraciones de moduladores: la AM-UM y la PM-PM. Como se vio en el capítulo 3, estas configuraciones resultan ser las más ventajosas en términos de tasa de trasmisión de clave junto con la configuración AM-PM. En ambos casos, usando una fuente que

proporciona pulsos ópticos con frecuencia de repetición de 1 MHz, Alice modula la portadora óptica con una subportadora eléctrica de 15 GHz. En el apartado 4.3, se presenta un demostrador experimental que se ha ensamblado en el laboratorio del grupo de Comunicaciones Ópticas y Cuánticas del iTEAM-UPV y que ha permitido verificar la viabilidad de la técnica SCM-QKD. La señal de Alice está compuesta, en este caso, por dos subportadoras eléctricas de 10 GHz y 15 GHz que modulan la portadora óptica. Dicha señal es trasmitida por un canal de 10 km de fibra óptica, tras el cual se encuentra Bob que selecciona su base volviendo a modular la señal. En el apartado 4.4, se demuestra experimentalmente la viabilidad de la combinación de las dos técnicas de multiplexación SCM y WDM (WDM/SCM-QKD). Por último, en el apartado 4.5, se discuten las conclusiones más importantes del capítulo.

4.2. Estudio experimental de las configuraciones de moduladores AM-UM y PM-PM para la implementación del protocolo BB84

En este apartado, se continúa con el estudio realizado en el apartado 3.2. En este caso, se realiza un estudio experimental de dos configuraciones de moduladores, AM-UM y PM-PM, para implementar el protocolo BB84 [12].

4.2.1. Configuración AM-UM

La figura 4.1 muestra el montaje experimental del sistema FC-QKD con la configuración AM-UM. Alice produce pulsos débiles coherentes atenuando una fuente láser cuya longitud de onda es 1548.78 nm (figura 4.2(a)). Los pulsos son atenuados, por medio de un atenuador óptico (At), hasta un valor promedio de fotones μ=1, que es el valor óptimo para implementar el protocolo BB84 con *strong reference* [13]. Estos pulsos son generados a partir de un modulador de amplitud alimentado a través de su entrada eléctrica por un tren de pulsos generados a partir del sistema de control. Como se observa en la figura 4.2(b), a la salida de la fuente los pulsos ópticos presentan una tasa de repetición de 1 MHz con anchura FWHM (del inglés *full width at half maximum*) de 1.5 ns.

El sistema de control que aparece en la figura 4.1 está formado por una FPGA (del inglés *Field Programmable Gate Array*) conectada al ordenador mediante el protocolo RS-232. Las señales eléctricas generadas por la FPGA son distribuidas al sistema por medio de una PCB (del inglés *Printed Circuit Boards*). Todas las

señales de control son sincronizadas con una frecuencia de operación de 1 MHz y el retardo de cada una de ellas se controla independientemente.

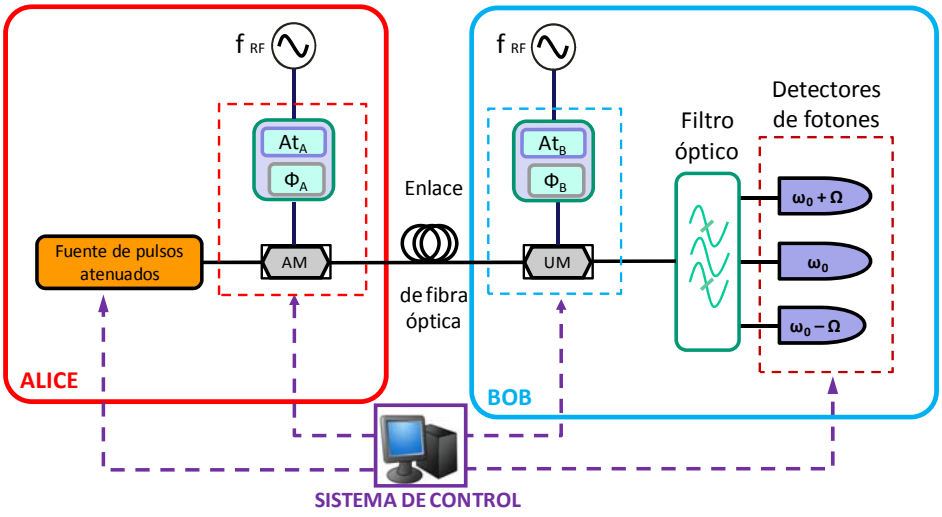

Figura 4.1. Esquema de el sistema experimental FC-QKD con la configuración AM-UM.

Los bits de la clave secreta se codificaron modulando los pulsos por medio de otro modulador de amplitud (AM_A) de 20 GHz de ancho de banda con una tensión de polarización de forma que se encuentra en el punto de cuadratura ($\Psi_A=\pi/4$). En principio, no hay una condición preestablecida para Ψ_A en esta configuración como se vio en la tabla 3.2. Sin embargo, este valor resulta conveniente porque el modulador se encuentra en régimen lineal, resultando más estable y minimizándose los armónicos de segundo orden.

La subportadora eléctrica consistió en un tono de 15 GHz generado por un oscilador local (LO_A). La fase correspondiente (Φ_A) se aplicó por medio de un desfasador de radiofrecuencia de 8 bits, que permitía sintonizar la fase digitalmente entre 0º y 360º con pasos de 1.4º y con un tiempo de conmutación de 500 ns. Dicho desfasador se sincronizó por medio del sistema de control que también generaba las señales de 8 bits para éste, proporcionando la fase correspondiente para implementar el protocolo BB84. A la entrada del desfasador se situó un atenuador de radiofrecuencia (At_A), que permitía controlar la amplitud de la señal eléctrica. El objetivo de este atenuador era ajustar, al nivel deseado, el índice de modulación de Alice, y así, optimizar la visibilidad del sistema.

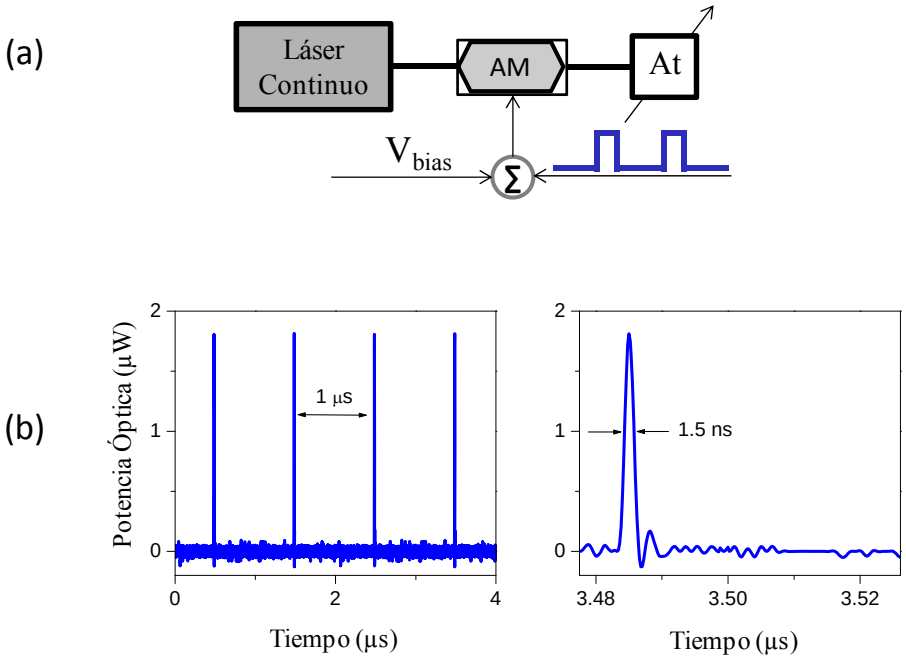

Figura 4.2. (a) Esquema de componentes de la fuente óptica pulsada y (b) tren de pulsos ópticos de la fuente a la salida del modulador de amplitud.

En Bob se situó un modulador desbalanceado (UM_B) de 20 GHz de ancho de banda. Al igual que en el caso de Alice, la fase de la subportadora eléctrica de 15 GHz se controló mediante un desfasador (Φ_B), sincronizado con el sistema de control, y se atenuó la amplitud del tono con un atenuador (At_B), con las mismas propiedades que el de Alice. También se le aplicó una tensión de alimentación continua al modulador tal que $\Psi_A = \pi$, condición necesaria para implementar el protocolo BB84 como se vio en la sección 3.2.2 (tabla 3.2). El índice de modulación del modulador de Alice (m_A) y el del modulador de Bob (m_B) se escogieron para obtener una relación entre la potencia de las bandas y la portadora de 30 dB, cumpliendo con la condición dada por la tabla 3.2. El canal óptico consistió en la combinación de 10 km de fibra monomodo convencional con unas pérdidas de 0.2 dB/km y 1 km de fibra compensadora con pérdidas de 0.3 dB/km, consiguiéndose de esta forma un enlace total de 11 km con la dispersión compensada (ecuación 3.34).

Para comprobar el correcto funcionamiento del esquema experimental, se realizó, en primer lugar, una caracterización en régimen clásico utilizando una fuente láser continua y un analizador de espectros ópticos. En la figura 4.3, se muestran los resultados de la caracterización, donde se observa como la amplitud de las bandas

laterales de 15 GHz aumentan o disminuyen debido a la interferencia en función de la diferencia de fase $\Delta\Phi = \Phi_B - \Phi_A$. Se puede comprobar como para una diferencia de fase $\Delta\Phi = 0$ se elimina la banda inferior en frecuencia mientras que para $\Delta\Phi = \pi$ se elimina la banda superior. En esta figura también se puede apreciar la concordancia entre los resultados experimentales (línea en negro) y teóricos (línea en rojo), obtenidos con las ecuaciones (3.14).

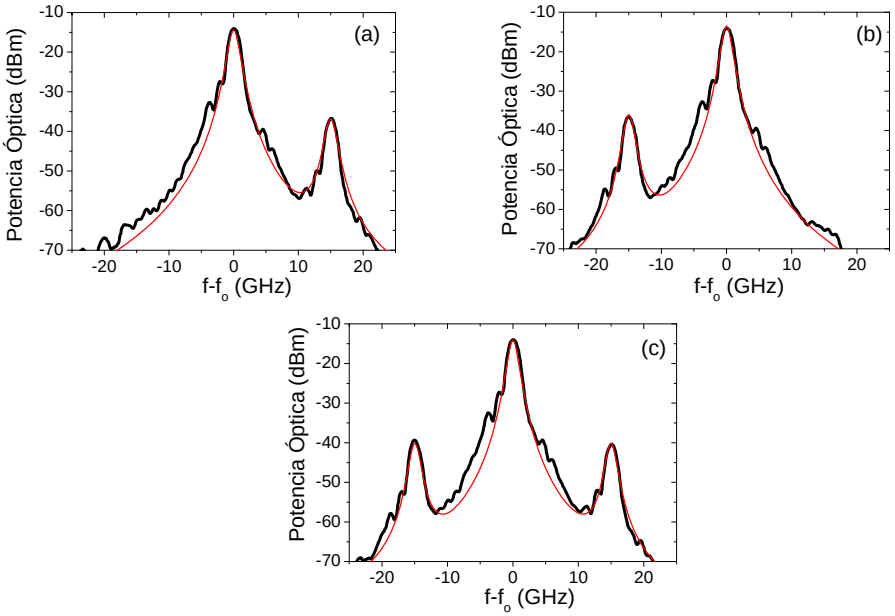

Figura 4.3. Espectros ópticos experimentales (—) y teóricos (—) para la configuración AM-UM para distintas diferencias de fase: (a) $\Delta\Phi=0$, (b) $\Delta\Phi=\pi$ y (c) $\Delta\Phi=\pi/2$.

Con el fin de trabajar en régimen cuántico, cada una de las bandas ópticas se filtraron por medio de un sistema de filtrado basado en redes de difracción de Bragg apodizadas (AFBG). En la figura 4.4(a), se muestra un esquema de dicho sistema de filtrado que consta de tres etapas. La primera etapa proporcionaba la *strong reference* reflejando la portadora óptica por medio de una AFBG con un coeficiente de reflexión cercano al 99.9 %. La segunda etapa separaba la banda lateral superior de la inferior y la tercera etapa eliminaba el residuo de portadora óptica que todavía persistía. Finalmente, se colocó un aislador en cada brazo para eliminar las reflexiones de las AFBGs. Por tanto, el filtro tenía tres puertos de salida, uno para cada banda lateral y otro para la portadora óptica. Cada AFBG estaba centrada a una longitud de onda determinada con una precisión de 1 pm mediante un sistema de control de temperatura. En la figura 4.4(b) se muestra la función de transferencia

experimental del filtro. Se puede observar que la anchura de banda lateral superior (+15 GHz) es 0.060 nm y para la banda inferior (-15 GHz) es 0.056 nm, ambos medidos a 3 dB (FWHM). Las pérdidas para cada canal son de 1 dB y la relación de extinción entre las bandas y la portadora óptica a la salida del filtro es de alrededor de 30 dB.

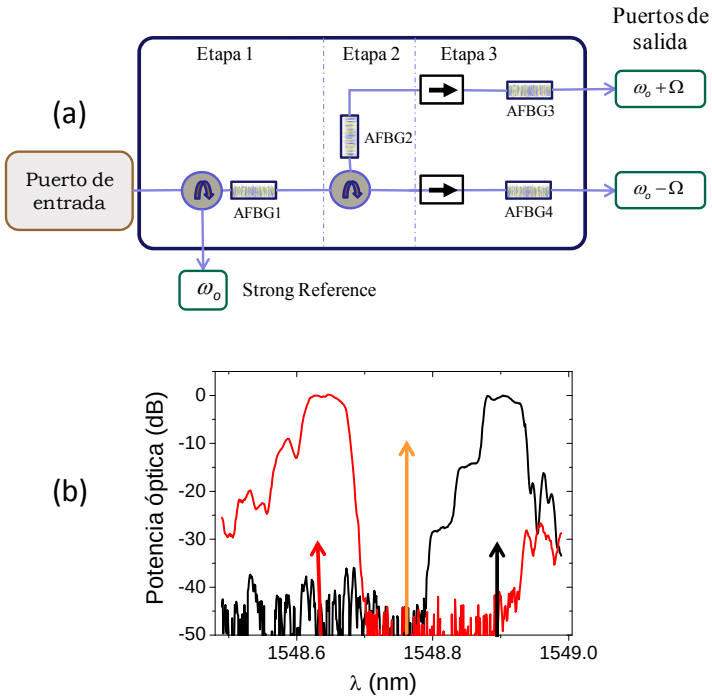

Figura 4.4. (a) Esquema del sistema de filtrado basado en FBGs y (b) correspondiente función de transferencia del filtro. Las flechas indican la posición de la portadora óptica y las bandas laterales que se desean filtrar.

A la salida del filtro se colocó un detector de fotones para cada una de las bandas. Las características principales de estos detectores venían dadas por una eficiencia cuántica del 10 %, una probabilidad de detectar una cuenta oscura de 10^{-5} y una ventana de detección de 2.5 ns. Los detectores se sincronizaron con la fuente por medio del sistema de control. Éste generaba señales TTL que servían de disparo para los detectores de fotones y se sincronizaban con la llegada de los pulsos ópticos generados por Alice. Cada vez que se producía una cuenta, el sistema de control detectaba y almacenaba la posición en la cadena de bits de la señal eléctrica producida por el detector. La FPGA en Alice, almacenaba y generaba a través de un generador pseudo-aleatorio las tramas de bits que codificaba y trasmitía. En Bob, se generaba la elección de base y se almacenaban las cuentas para la banda superior, la

banda inferior y la portadora óptica. Con esta información se obtuvo la clave en crudo tras llevar a cabo la reconciliación de bases y el correspondiente QBER.

En la figura 4.5 se muestra el número normalizado de cuentas detectadas, a la salida del detector, para cada una de las bandas. Se puede observar que la evolución de la banda superior es de la forma coseno al cuadrado y la de la banda inferior de tipo seno al cuadrado, como se vio en la ecuación (3.16). Con estos resultados se obtiene una visibilidad efectiva de V_{eff} = 98. 5%, un QBER del 2 %, que es ligeramente superior al esperado teniendo en cuenta la visibilidad del sistema, debido a efectos adicionales de degradación estudiados en el apartado 3.4, y una tasa de clave en crudo de 10 kbit/s.

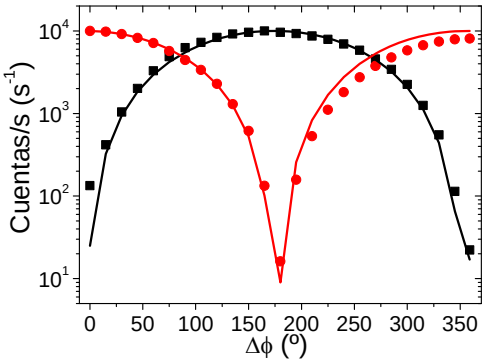

Figura 4.5. Evolución del número de cuentas en función de la diferencia de fase ΔΦ para la banda inferior (■) y banda superior (●). Las líneas continuas representan los resultados teóricos.

4.2.2. Configuración PM-PM

La figura 4.6 muestra el montaje experimental del sistema FC-QKD con la configuración PM-PM. Los componentes del sistema fueron los mismos que en el caso AM-UM, vistos y descritos en la sección anterior exceptuando los moduladores de Alice y Bob. En este caso, se utilizaron dos moduladores de fase (PM_A y PM_B) con un ancho de banda de 20 GHz.

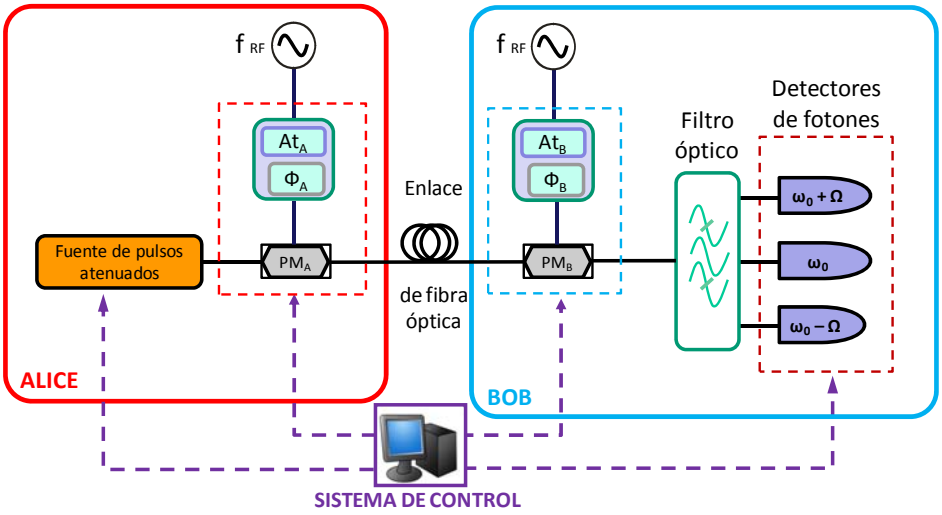

Figura 4.6. Esquema de un sistema FC-QKD con la configuración PM-PM.

Nuevamente se realizó una caracterización en régimen clásico utilizando un láser continuo y un analizador de espectros ópticos. En la figura 4.7(a) se observa que el protocolo BB84 puede ser implementado cuando se cumple $\beta_2 L\Omega^2=\pi$. Como se mostró en la tabla 3.3, esta condición era necesaria para obtener una respuesta complementaria entre las bandas laterales y en este caso se produce para una longitud del canal de L = 10 km. En la parte izquierda de la figura 4.7 se muestran los espectro para un desfase $\Delta\Phi = 0$ y en la derecha para $\Delta\Phi = \pi$. Se puede observar claramente como el bit 0 y el bit 1 se pueden discernir asociándolos a la detección realizada en la banda lateral superior e inferior, respectivamente. En la figura 4.7(b), se muestra el espectro cuando la longitud del canal es de 5 km, con lo que se obtiene $\beta_2 L\Omega^2 = \pi/2$. En la figura 4.7(c) se muestra el caso de una longitud del canal de 0 km o de forma equivalente, con la dispersión compensada, de forma que $\beta_2 L\Omega^2 = 0$. En estos dos casos la banda superior y la banda inferior no permiten la codificación del bit 1 y bit 0, ya que, como se puede observar en la figura, ambos estados no son distinguibles claramente. En todos los casos se puede observar la concordancia entre los resultados experimentales (en negro) y los teóricos (en rojo), obtenidos con la ecuación (3.14).

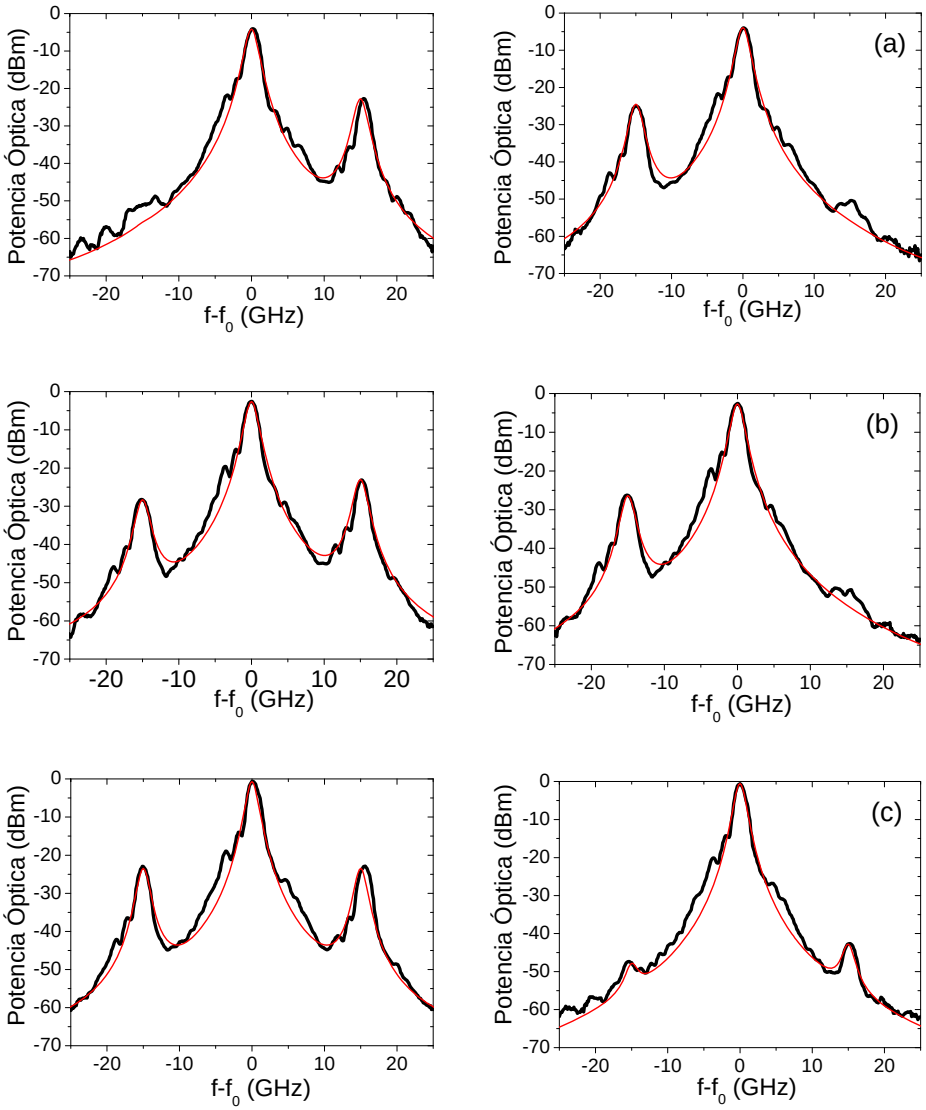

Figura 4.7. Espectros ópticos experimentales (—) y teóricos (—) para una longitud del canal de (a) 10 km, (b) 5 km y (c) 0 km donde el término $\beta_2 L\Omega^2$ tiene los valores π, $\pi/2$ and 0, respectivamente. La parte izquierda de la gráfica corresponde con la trasmisión del bit "0" con $\Delta\Phi = 0$ y la parte derecha corresponde al bit "1" con $\Delta\Phi = \pi$. Resultados experimentales se muestran en negro y teóricos en rojo.

Los resultados teóricos y experimentales de las amplitudes de las bandas detectadas se muestran en la figura 4.8(a) y 4.8(b) que se corresponden con la banda inferior y

superior, respectivamente. Ambas se representan en función de la diferencia de fase de las señales de radiofrecuencia de Alice y Bob (ΔΦ). Los resultados se han obtenido para las tres longitudes del canal óptico previamente consideradas. Se observa una buena concordancia entre los resultados teóricos y experimentales. Solamente en el caso donde la longitud del canal cumple la condición $\beta_2 L\Omega^2 = \pi$ se aprecia la complementariedad de las bandas permitiendo implementar el protocolo BB84 y satisfaciendo la ecuación 3.16.

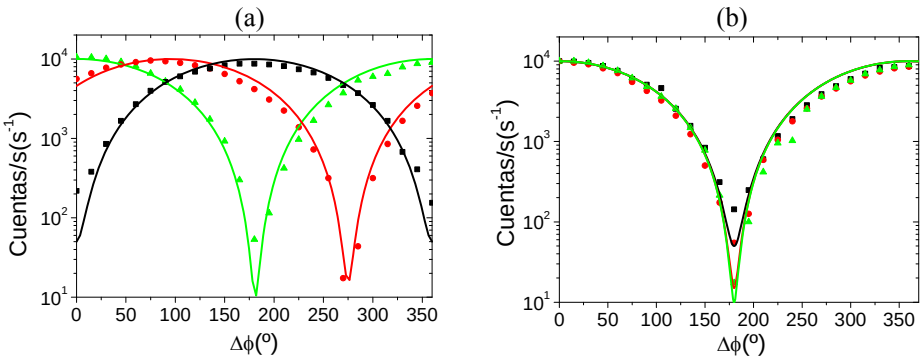

Figura 4.8. Número de cuentas en función de la diferencia de fase (Δϕ) correspondientes a la banda lateral (a) inferior y (b) superior para longitudes del canal de 10 km (■), 5 km (●), and 0 km (▲). Las líneas continuas representan los resultados teóricos.

En la figura 4.9 se muestra la visibilidad efectiva en función de la longitud del canal (z) normalizada por la longitud del canal L = 10 km. En esta figura, se observa cómo se alcanza una visibilidad efectiva de V_{eff} = 0.99 para z = 1. También se muestran los resultados teóricos dados por la ecuación 3.19, ajustándose correctamente a los resultados experimentales. El QBER obtenido presenta un valor del 2 %, que es ligeramente superior al esperado, y la tasa de clave en crudo es de 10 kbit/s al igual que en el caso AM-UM.

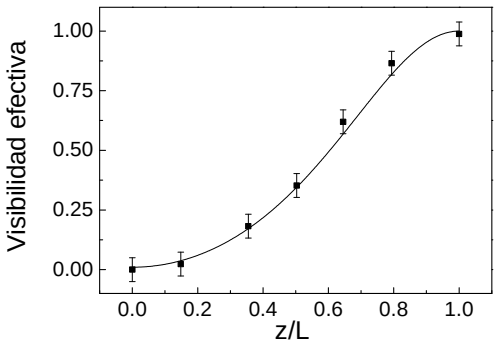

Figura 4.9. Visibilidad efectiva en función de la longitud del canal (z) normalizada por la longitud del canal L=10 km.

4.3. Demostrador experimental SCM-QKD

4.3.1. Esquema experimental

La figura 4.10 muestra el primer montaje experimental desarrollado para demostrar la viabilidad de los sistemas SCM-QKD mediante la generación de dos claves independientes. Se pueden distinguir cuatro bloques principales que corresponden con el trasmisor (Alice), el receptor (Bob), el canal de referencia y el sistema de control. La configuración de moduladores es AM y PM para Alice y Bob, respectivamente, ambos conectados por medio de un canal de 10 km de fibra óptica.

La fuente presentaba las mismas características que las configuraciones AM-UM y PM-PM de las secciones anteriores. Alice produjo sus estados con un modulador de amplitud de 20 GHz de ancho de banda con una tensión de polarización para trabajar en la zona lineal del modulador ($\Psi_A=\pi/4$). Las dos claves independientes se multiplexaron eléctricamente a partir de dos osciladores de radiofrecuencia de f_1=10 GHz y f_2=15 GHz. Las fases de las señales de RF para cada subportadora eléctrica (Φ_{A1} y Φ_{A2}) se seleccionaron aleatoriamente por medio de dos desfasadores controlados independientemente por el sistema de control. Dos atenuadores de radiofrecuencia (At_{A1} y At_{A2}) se ubicaron a la entrada de los desfasadores para controlar independientemente la amplitud de las subportadoras eléctricas. La atenuación de la fuente fue tal que el número medio de fotones por pulso era nuevamente μ=1.

En Bob, los estados trasmitidos por Alice se modularon por medio de un modulador de fase (PM) de 20 GHz de ancho de banda. Bob seleccionaba aleatoria y

sincronizadamente sus bases mediante las fases Φ_{B1} y Φ_{B2} para cada subportadora por medio de dos desfasadores. Después del filtrado de cada una de las bandas laterales de cada subportadora se llevó a cabo la detección, por medio de un contador de fotones, así como para la portadora óptica. Las características de estos detectores eran las mismas que para las configuraciones FC-QKD de la sección anterior.

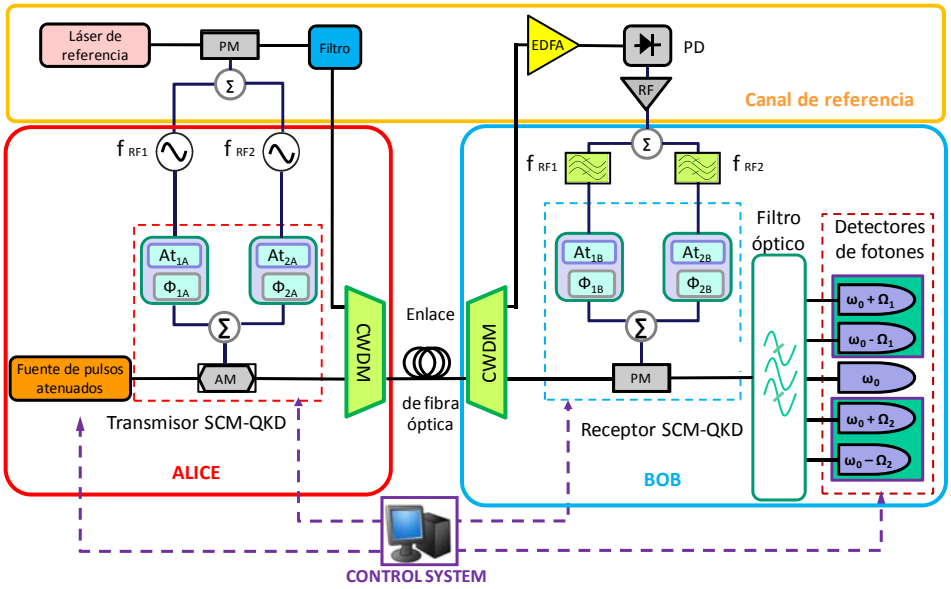

Figura 4.10. Sistema experimental implementado en el laboratorio para estudiar la viabilidad de la transmisión de dos claves multiplexadas por medio de un sistema SCM-QKD.

El canal de referencia mostrado en la figura 4.10 fue necesario para establecer cierta sincronización entre el transmisor y el receptor así como para compensar las fluctuaciones del canal de fibra que conllevaban a una degradación del sistema [14]. Por tanto, el esquema experimental debía ser capaz de permitir la coexistencia de las señales cuánticas que contenían las claves y las señales clásicas que permitían el control del sistema óptico. Así pues, el canal de referencia y el cuántico son multiplexados mediante la técnica CWDM [15], con el fin de compartir el mismo canal. El multiplexor CWDM discernía dos canales ópticos con una separación en longitud de onda entre ellos de 20 nm y unas pérdidas de inserción de 0.5 dB. Como se muestra en la figura 4.11, la banda óptica centrada en 1551 nm se utilizó para trasmitir el canal cuántico mientras que la banda óptica en 1531 nm se utilizó para el canal de referencia. En Bob, otro demultiplexador CWDM separaba el canal clásico y el cuántico.

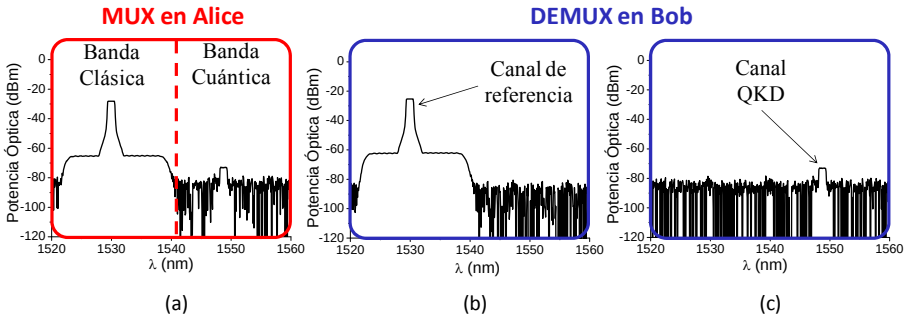

Figura 4.11. (a) Espectro óptico correspondiente a la multiplexación en Alice de los canales clásicos y cuánticos cuando son multiplexados en Alice. Espectros ópticos demultiplexados en Bob de (b) la banda clásica y (c) cuántica. El canal cuántico se ha amplificado para poder ubicarlo en la banda correspondiente del espectro óptico.

Nuevamente se realizó una caracterización en régimen clásico utilizando un analizador de espectro óptico. En la figura 4.12, se muestran los espectros ópticos correspondientes a distintas combinaciones de diferencias de fase $\Delta\Phi_1 = \Phi_{B1} - \Phi_{A1}$ y $\Delta\Phi_2 = \Phi_{B2} - \Phi_{A2}$ para cada una de las subportadoras eléctricas de 10 y 15 GHz, respectivamente. Debido a la interferencia producida por la concatenación de los moduladores de Alice y Bob, se observa como las bandas laterales de 10 y 15 GHz aparecen o desaparecen, en función de si se ha transmitido un bit 0 o un bit 1 y la elección de bases tomada por Bob. A título de ejemplo, en el caso de transmitir el bit 0 en ambas subportadoras y Bob seleccionar la base correcta, se obtendría el espectro mostrado en la figura 4.12(a). La amplitud de las bandas laterales superiores en frecuencia sería máxima para ambas subportadoras. Si se transmite el bit 0 para la subportadora de 10 GHz y el bit 1 para la de 15 GHz seleccionando Bob la base correcta, el espectro obtenido sería el que se muestra en la figura 4.12(d). En este caso, la banda superior de 10 GHz y la banda inferior de 15 GHz aparecerían con amplitud máxima. Por último, en el caso de que Bob seleccione la base incorrecta en ambas subportadoras obtendríamos la figura 4.12(c) independientemente de los bits transmitidos con la misma amplitud para las bandas inferiores y superiores. En esta figura, también se puede apreciar la concordancia entre los resultados experimentales (línea en negro) y teóricos (línea en rojo), obtenidos con las ecuaciones (3.28) y (3.30).

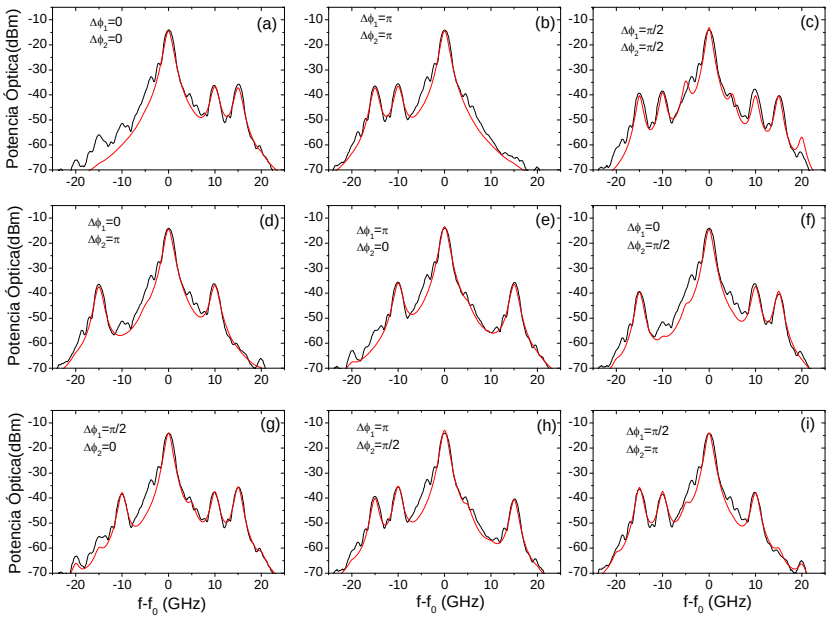

Figura 4.12. Espectros ópticos experimentales (—) y teóricos (—) a la salida del modulador de Bob para distintas diferencias de fase $\Delta\Phi_1$ y $\Delta\Phi_2$.

En la figura 4.13 se muestra un conjunto de fotografías del demostrador así como algunos de sus componentes principales.

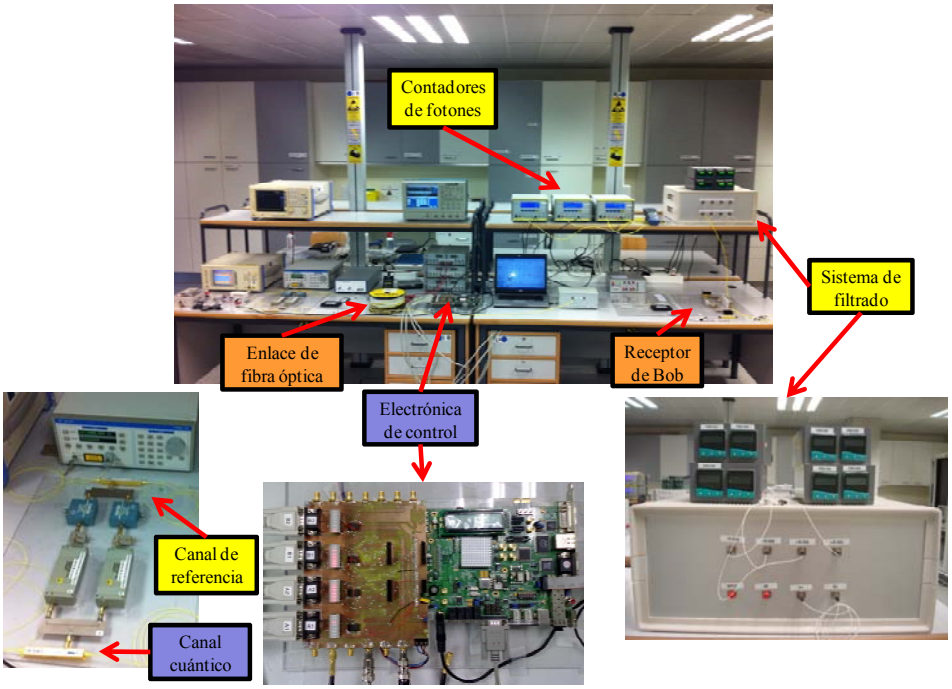

Figura 4.13. Fotografía del prototipo experimental desarrollado en el laboratorio para demostrar la viabilidad de la trasmisión de dos claves multiplexadas por medio de un sistema SCM-QKD (parte superior) y algunos de sus componentes principales (parte inferior).

4.3.2. Factores limitantes

El diseño del prototipo SCM-QKD implicó la solución de varias limitaciones que podían reducir drásticamente la tasa de trasmisión segura del sistema QKD. Entre ellas cabe destacar el diseño e implementación de un filtro óptico capaz de separar las bandas con elevadas relaciones de extinción, la reducción del efecto Raman producido por el canal de referencia sobre el canal cuántico, el control de las fluctuaciones ambientales en el camino óptico y la compensación de la dispersión.

(a) Filtrado óptico

Para filtrar cada una de las bandas con una buena relación de extinción a la salida del modulador de Bob, se diseñó un filtro fotónico compuesto por diferentes etapas de FBGs (del inglés *Fiber Bragg Grating*) como se muestra en la figura 4.14(a). Al igual que en el caso de una subportadora eléctrica, la primera etapa del filtro permite separar la portadora óptica, que se utiliza como *strong reference* para garantizar la seguridad incondicional. Las diferentes etapas del filtro fueron diseñadas para reducir la diafonía debida a las subportadoras adyacentes y a los

productos de intermodulación (localizados fuera de las bandas laterales) con un nivel de amplitud por debajo de 23 dB respecto a la probabilidad de detectar un fotón en la banda de interés.

La primera etapa proporciona la strong reference, reflejando la portadora óptica por medio de una FBG con un coeficiente de reflexión cercano al 99.9 %. La segunda etapa separa las bandas laterales superiores de las inferiores y la tercera etapa filtra cada una de las bandas de RF con una relación de extinción de 20 dB. Por tanto, el filtro tiene 5 puertos de salida, uno para cada banda y otro para la portadora óptica. Cada FBG está centrada a una longitud de onda determinada con un sistema de control de temperatura igual al del caso anterior.

El funcionamiento del filtro se comprobó en el régimen clásico con un analizador de espectros, situado a la salida de esté. La figura 4.14(b) muestra el espectro medido para las bandas de ±10 GHz y ±15 GHz con respecto a la portadora óptica. Todas las bandas presentan la misma potencia óptica (probabilidad) con una relación de extinción de 25 dB y unas pérdidas de inserción de 1.5dB.

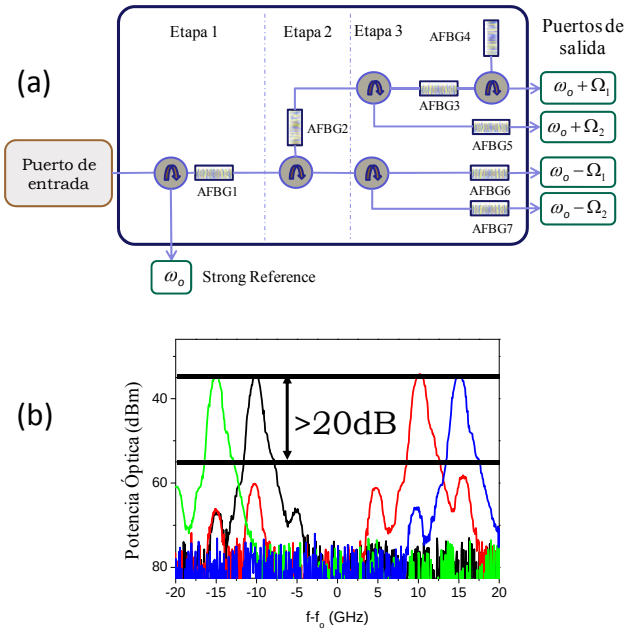

Figura 4.14. (a) Estructura del filtro empleado para separar las bandas y la portadora óptica. (b) Espectro óptico de cada banda en régimen clásico después del filtrado.

(b) Efecto Raman

También se evaluó como, a través del efecto Raman, el canal de referencia interfería con cada uno de los canales multiplexados mediante SCM-QKD. La figura 4.15 muestra la probabilidad de detección para cada banda óptica en función del producto de la potencia óptica de entrada del canal de referencia P_{in} y las pérdidas del canal T_B en Bob. Para potencias ópticas elevadas, se observa una dependencia lineal entre los fotones generados dentro de cada banda por efecto Raman como se mostró en la ecuación (3.58). Para potencias menores, la probabilidad de detección viene determinada por las cuentas oscuras. El comportamiento es muy similar para todas las bandas, aunque se presentan ligeras diferencias debido a las uniformidades del filtro óptico, como ya vimos en la ecuación (3.61). Las diferencias encontradas son debidas a la anchura efectiva de cada una de las salidas del filtro. En principio, las pérdidas en Bob (alrededor de 4.5 dB) relajan el número de cuentas debidas al efecto Raman hasta el nivel de las cuentas oscuras para una potencia óptica de entrada del canal de referencia cercana a -25 dBm. Por esta razón el canal de referencia se amplifica ópticamente después del demultiplexador CWDM y eléctricamente, después de detectar con un fotodetector (PD).

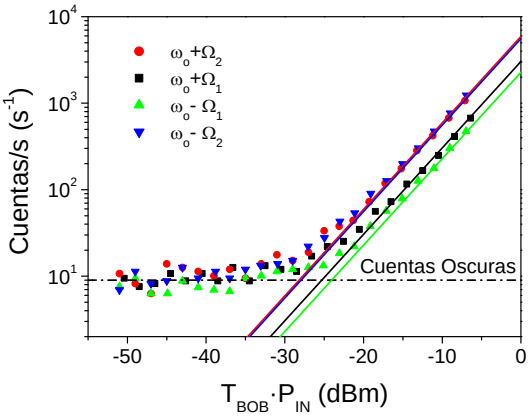

Figura 4.15. Probabilidad de detección experimental correspondiente a cada salida del filtro óptico en función de la potencia óptica del canal de referencia y las pérdidas en Bob. Las simulaciones teóricas se muestran en líneas continuas.

(c) Estabilidad del sistema: fluctuaciones y polarización

El canal de referencia era necesario para sincronizar a Alice y Bob y también para compensar las fluctuaciones de longitud del canal de fibra, que conllevaban fluctuaciones en la diferencias de fases de radiofrecuencia entre Alice y Bob [14].

Para compensar las fluctuaciones se trasmitieron los tonos de 10 GHz y 15 GHz a través del canal modulando otra portadora óptica con un modulador de fase. El espectro a la salida del modulador de fase se puede observar en la figura 4.16(a). A la salida de este modulador se situó un filtro que eliminaba las dos bandas laterales de la izquierda y parte de la portadora como se muestra en la figura 4.16(b), obteniendo una potencia total de -25 dBm. Así podíamos obtener modulación en banda lateral única [16], que era útil para el caso de enlaces sin compensación de dispersión. Con este procedimiento se consiguió maximizar la potencia de RF que obtenía Bob al fotodetectar para una potencia óptica determinada, consiguiéndose minimizar el efecto Raman.

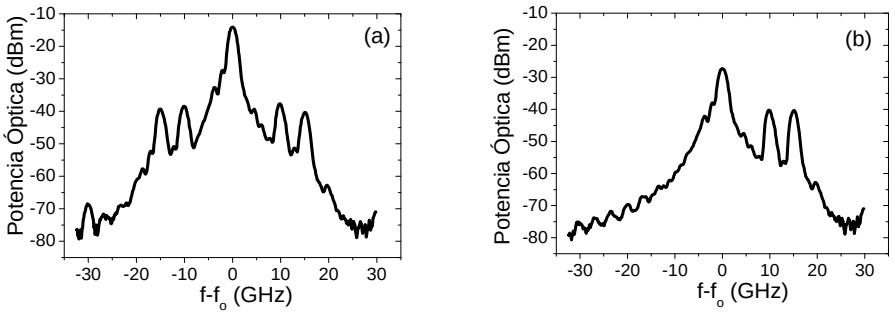

Figura 4.16. (a) Espectro a la salida del modulador de fase del canal de referencia y (b) espectro a la salida del filtro del canal de referencia.

También, se evaluó la estabilidad del canal SCM-QKD con el canal de referencia en régimen clásico. Para ello se seleccionó el estado con una diferencia de fase $\Delta\Phi_1 = \pi$ y $\Delta\Phi_2 = \pi$ y se dejó evolucionar durante una hora. En la figura 4.17(a) se muestra el espectro óptico del canal SCM-QKD en el instante inicial (t=0). En la figura 4.17(b) se muestra la evolución de las bandas de ±15 GHz y la portadora óptica durante una hora. Se puede observar cómo se mantuvo una relación de extinción entre estas bandas de alrededor de 20 dB, lo que demuestra la estabilidad del sistema frente a las fluctuaciones de longitud del canal de fibra. También se observa como la potencia de las bandas y la portadora se mantuvo estable, indicando que el estado de polarización, a la salida del canal, se mantuvo constante durante este periodo de tiempo. De hecho, el modulador de fase empleado en Bob modulaba solamente una componente de polarización del estado de entrada, la otra componente la eliminaba. Para ver este efecto en la figura 4.17(c) se muestra la potencia óptica, a la salida de este modulador de fase, de las bandas superior e inferior de la segunda subportadora (±15 GHz) y la portadora óptica, para distintos valores del ángulo de polarización

(α), formado por la componente de polarización del campo y el eje horizontal. Se puede observar como el índice de modulación se mantiene prácticamente, mientras que la eficiencia de modulación se reduce. Por tanto, en este caso un cambio de polarización en la fibra implica pérdidas adicionales y no una detección de cuentas erróneas.

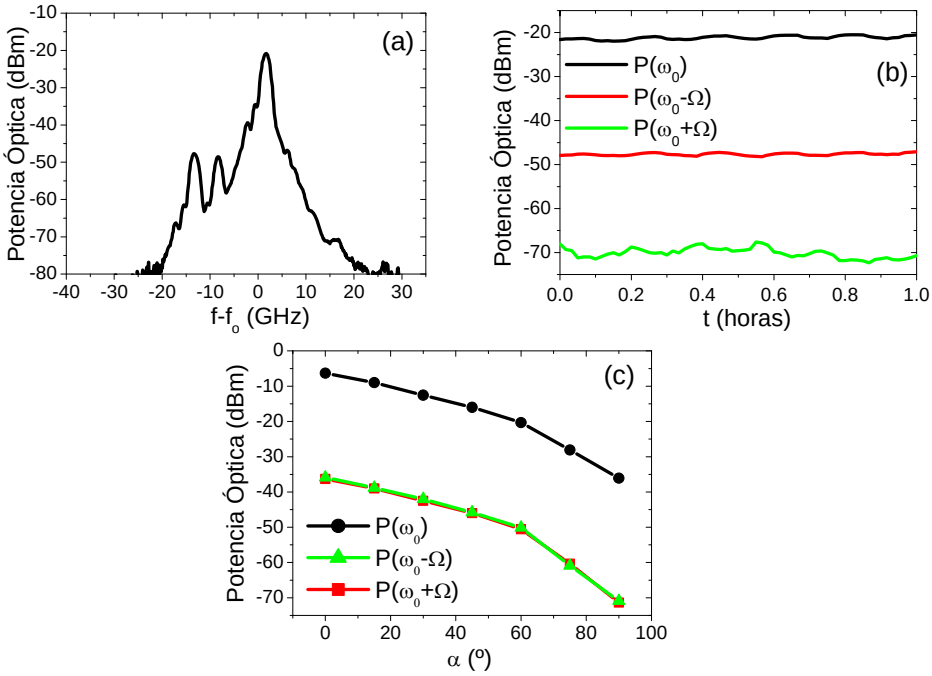

Figura 4.17. (a) Espectro de la señal SCM-QKD en t=0 a la salida del modulador de Bob con $\Delta\Phi_1 = \pi$ y $\Delta\Phi_2 = \pi$. (b) Evolución de las bandas de ±15 GHz y la portadora óptica de la señal SCM-QKD durante una hora. (c) Potencia de las bandas ±15 GHz y portadora óptica a la salida del modulador de Bob para diferentes estados de polarización.

En la figura 4.18(a), se puede observar el correcto funcionamiento del canal de referencia a partir del QBER medido durante un intervalo de una hora (tras este periodo de tiempo el sistema de control necesita ser recalibrado).

Se puede observar una clara diferencia cuando el canal de referencia está desactivado. En este caso, el valor del QBER es cercano al 50 % durante un largo periodo de tiempo en comparación a cuando está activo. Para este último caso, los valores del QBER están por debajo del 2 % y, como consecuencia, se alcanzan valores medios de visibilidad efectiva superiores al 96 % comparable con los obtenidos para el sistema con una longitud del canal de 0 km. Con el fin de analizar

la estabilidad en la tasa de trasmisión con el enlace de 11 km, se realizó una medida durante una hora y se comparó con la obtenida para un enlace de 0 km. En la figura 4.18(b) se observa que la tasa de trasmisión para 11 km permaneció prácticamente constante al igual que el caso de 0 km.

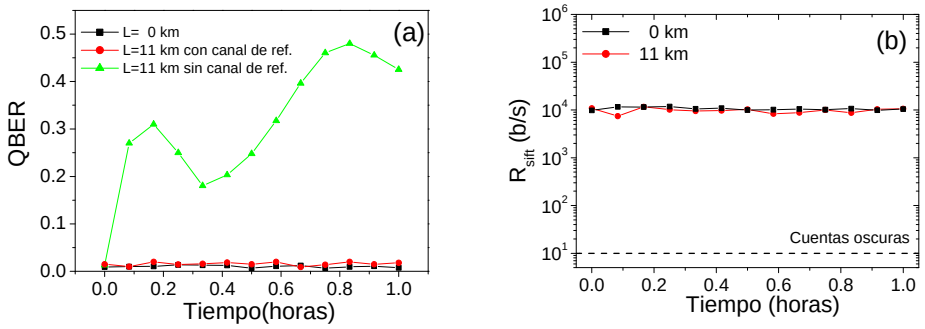

Figura 4.18. (a) QBER del canal de referencia activado (●) y desactivado (▲) durante una hora para un enlace de 11 km y de 0 km (■). (b) Tasa de transmisión en crudo del sistema con una longitud de canal de 11 km (●) y de 0 km (■).

(d) Dispersión cromática

La dispersión cromática también podía degradar la visibilidad del sistema y por tanto debía de ser compensada. En nuestro caso, se añadió 1 km de fibra compensadora de la dispersión a los 10 km del enlace de fibra óptica (ecuación 3.34).

En la figura 4.19 se ha representado la medida experimental de las cuentas detectadas para la banda lateral inferior (■) y superior (●) en función de la diferencia de fase cuando se considera un enlace con y sin dispersión. Las gráficas superiores e inferiores se corresponden con los resultados obtenidos para la subportadora eléctrica de 10 GHz y 15 GHz, respectivamente. Los puntos muestran los resultados experimentales y la línea continua representa la evaluación teórica a través de la ecuación (3.16).

Para el caso de considerar un enlace en el que no se compensa la dispersión, la figura 4.19(a) muestra como la complementariedad entre las bandas laterales (superior e inferior) se pierde. Sin embargo, en la figura 4.19(b) se recupera la complementariedad para ambas subportadoras (10 y 15 GHz) cuando la dispersión se compensa completamente. Así pues, se obtienen valores del QBER de 17 % y 35 %, para las subportadoras de 10 y 15 GHz, en el caso de no compensar la

dispersión. Estos valores son reducidos al 1.5 % para las dos subportadoras cuando la dispersión se compensa.

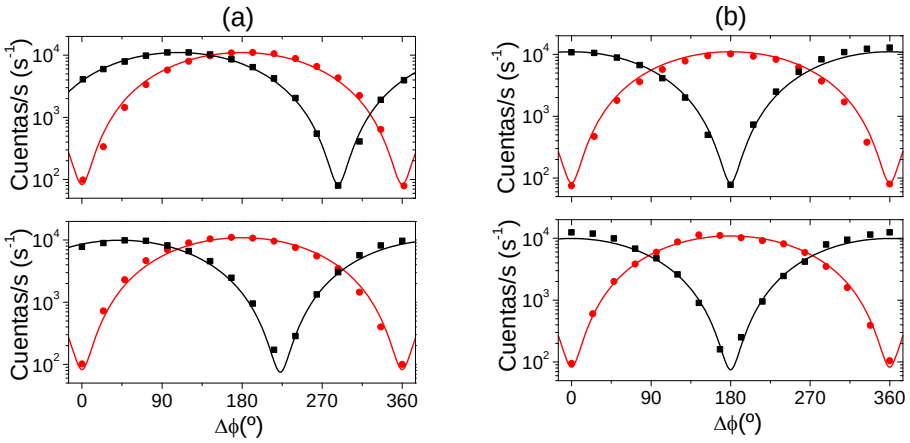

Figura 4.19. Cuentas por segundo para la banda lateral inferior (■) y superior (●) en función de la diferencia de fase cuando la dispersión (a) no está compensada y (b) cuando se compensa. Las gráficas superiores se corresponden con la subportadora de 10 GHz y las inferiores con 15 GHz. Los resultados teóricos se muestran con líneas continuas.

4.3.3. Tasa de trasmisión y de error de bit cuántico para sistemas experimentales SCM-QKD

El rendimiento del sistema SCM-QKD se analizó experimentalmente midiendo la tasa de trasmisión en crudo y el QBER individual, después de la trasmisión con el canal de fibra de 11 km. Primero se codificaron los bits en las subportadoras independientemente, es decir, una subportadora permanecía desactiva y la otra activa, con un número medio de fotones por pulso de μ=1 y una frecuencia de repetición de 1 MHz. La longitud de onda de la portadora óptica fue de 1548.7 nm. La figura 4.20(a) muestra la tasa de clave en crudo para las subportadoras individuales que resultó ser del orden de 10 kbit/s para las subportadoras de 10 y 15 GHz. En esta figura también se muestra el caso donde ambas subportadoras están activadas a la vez, donde se obtuvo una tasa de clave en crudo resultante de 20 kbit/s.

Así pues, la distribución de clave en paralelo con una separación espectral tan pequeña (5 GHz) queda demostrada por primera vez. Además, la tasa de clave en crudo en el caso de las dos subportadoras activas al mismo tiempo (N=2) presenta una ganancia máxima (3 dB) con respecto al caso de una solo portadora, como se

vio teóricamente en la ecuación (3.55). El QBER obtenido se muestra en la figura 4.20(b) donde se alcanza un valor por debajo del 2 % para todos los casos. También se puede observar como el sistema permanece estable durante un intervalo de tiempo de una hora. Esto demuestra que las derivas del canal, debidas a variaciones en la temperatura y vibraciones, son correctamente compensadas por el canal de referencia.

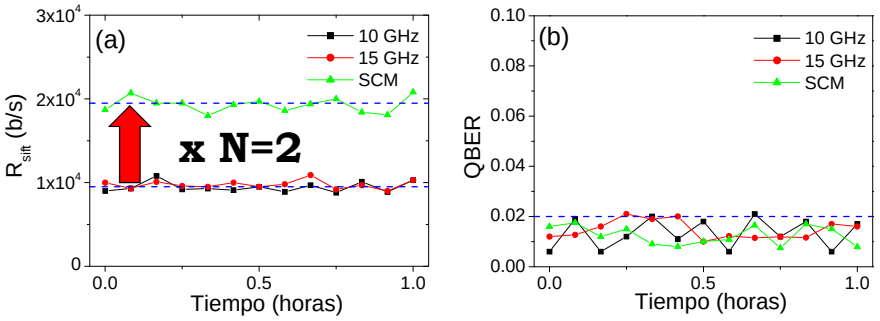

Figura 4.20. (a) Evolución de la tasa de clave en crudo y (b) medida correspondiente del QBER para cada una de las subportadoras individuales y para las dos subportadoras multiplexadas.

En esta tesis, se muestran los resultados experimentales obtenidos para la tasa de clave en crudo. La tasa de clave secreta no ha sido obtenida experimentalmente, ya que el post-procesado clásico mediante la corrección de errores y la amplificación de la privacidad no han sido desarrollados. Sin embargo, es posible estimar esta tasa mediante la ecuación (2.31) que tiene en cuenta el ataque PNS y que el máximo valor obtenido para el QBER es del 2%. En este caso, la tasa secreta es de alrededor el 31% la tasa en crudo. Por tanto, la tasa secreta de bit por canal estimada es de 3 kbit/s.

4.4. Demostrador experimental para WDM/SCM-QKD

Finalmente, para demostrar la escalabilidad y flexibilidad del sistema propuesto, se ensamblo un sistema experimental que incluía multiplexación en longitud de onda (WDM/SCM-QKD). El sistema estaba formado por dos trasmisores SCM-QKD independientes centrados en una longitud de onda de 1548.7 y 1557.3 nm (M=2). Cada uno de ellos, generaba una subportadora de 10 GHz y otra de 15 GHz multiplexadas (N=2) en Alice. Estos canales se multiplexaron en longitud de onda usando un DWDM (del inglés *Dense Wavelength Division Multiplexer*) [17]. Todos

estos canales cuánticos fueron también multiplexados mediante CWDM con el canal de referencia. En la figura 4.21 se representa un esquema de multiplexación en longitud de onda de dos canales SCM-QKD.

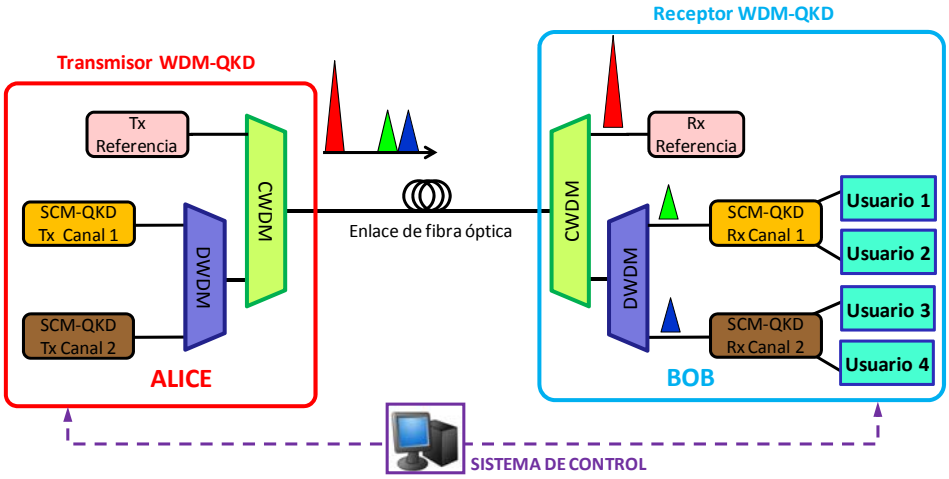

Figura 4.21. Esquema del sistema QKD para multiplexación WDM y SCM.

De forma similar al caso SCM-QKD, la señal clásica se separó de la señal cuántica mediante un demultiplexador CWDM y los distintos canales cuánticos se filtraron por medio de un demultiplexador DWDM. Por último, se filtraron las distintas bandas, con filtros basados en FBGs, en cada uno de los receptores SCM-QKD para implementar el protocolo BB84. La figura 4.22(a) muestra la tasa individual de clave en crudo obtenida para cada una de las cuatro subportadoras (10 kbit/s) y la tasa de bit de clave en crudo total. En este caso, el sistema presenta una ganancia máxima correspondiente a NxM=4 (40 kbit/s). En la figura 4.22(b), se muestra el QBER para cada uno de los canales cuando el resto están desactivados (FC-QKD) y para el caso de todos los canales activados a la vez (WDM/SCM-QKD). Para todos ellos el QBER obtenido está por debajo del 2 % y por tanto la tasa de bit secreta estimada es de 12 kbit/s

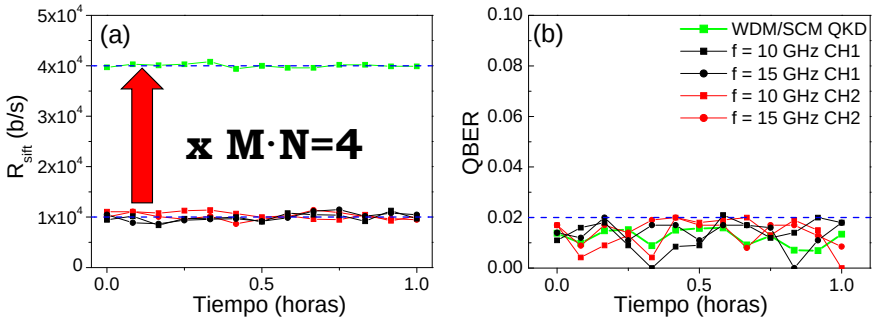

Figura 4.22. (a) Tasa de clave en crudo y (b) medida correspondiente del QBER para cada canal individual y con todos los canales multiplexados.

4.5. Conclusiones

En este capítulo, se ha mostrado experimentalmente dos de las configuraciones de moduladores (PM-PM y AM-UM) más eficientes y seguras, en términos de tasa secreta de bit y de QBER. En ambos casos, considerando el protocolo BB84, se han obtenido valores del QBER del 2 % y visibilidad efectiva superior al 98 %, teniendo en cuenta la dispersión del canal.

Los sistemas SCM-QKD están basados en una técnica que se caracteriza por su alta eficiencia espectral. Se ha visto que la técnica SCM puede ser utilizada en los sistemas QKD para conseguir la distribución simultánea de claves ocupando un ancho de banda espectral muy reducido. Las tasas de trasmisión de clave alcanzadas actualmente por los sistemas QKD son muy modestas en comparación con los sistemas de comunicaciones clásicos. El uso de una técnica de multiplexación que reduce el ancho espectral entre canales adyacentes parece ser una solución natural y sostenible para la distribución de múltiples claves. Por tanto, debido a que la separación entre canales con DWDM es alrededor de 100 GHz, la eficiencia espectral intra-canal está limitada entre el 2 % y el 4 %. En este sentido, el uso de la técnica SCM puede incrementar esta eficiencia hasta valores más altos del 50 %, usando moduladores con un ancho de banda en torno a 50 GHz y filtros ópticos con un espacio entre canales muy estrecho (~1-2 GHz). Esta estimación muestra que la técnica SCM-QKD podría incrementar en un orden de magnitud la tasa de transmisión final.

Una ventaja adicional de estos sistema SCM-QKD, reside en que la fuente óptica es compartida por todos los canales multiplexados, reduciéndose la complejidad, el

mantenimiento y el coste del sistema ya que todos los canales son trasmitidos con la misma portadora óptica. También, esta técnica puede ser combinada con WDM, para incrementar el número de claves que se distribuyen de forma paralela y combinar los canales cuánticos con los clásicos a través del mismo enlace de fibra.

Aunque demostramos experimentalmente tasas de bit en crudo modestas, la capacidad del sistema podría ser mejorada al menos en dos órdenes de magnitud por medio de componentes que ya están comercialmente disponibles. Por ejemplo, podría utilizarse desfasadores con un tiempo de conmutación de 25 ns, detectores de fotones con frecuencias de ventana superiores a 100 MHz y filtros ópticos con 32 salidas con un espaciado entre canales de aproximadamente 5 GHz.

En resumen, se ha demostrado la viabilidad de los sistemas de distribución de clave basados en las técnicas de multiplexación WDM y SCM, para mejorar aun más la capacidad de trasmisión sobre redes de fibra óptica. La propuesta permite incrementar la tasa de clave final o la distribución de clave entre usuarios diferentes. La ventaja de la técnica SCM respecto a WDM en un sistema de distribución de clave es que la misma fuente de fotones es compartida y en consecuencia, la complejidad de la sincronización y el control del sistema se reducen drásticamente cuando el sistema QKD trabaja en una red óptica.

Los resultados obtenidos confirman que la fotónica de microondas es una tecnología prometedora para mejorar la viabilidad de los sistemas cuánticos.

Referencias

[1] R. J. Runser, T. Chapuran, P. Toliver, A. Nicolas, M.S. Goodman, J. Kosloski, N. Nweke, S.R. McNown, R.J. Hughes, D. Rosenberg, C.G. Peterson, K.P.McCabe, J.E. Nordholt, K. Tyagi, P. A. Hiskett y N. Dallman, "Progress toward quantum communications networks: opportunities and challenges," en Proc. Optoelectronic Integrated Circuits 6476, 647601 (2007).

[2] P.D. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature 385, 47-49 (1997).

[3] P.D. Townsend, "Quantum Cryptography on Optical fiber networks", Opt. Fiber Technol. 4, 345-370 (1998).

[4] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer y H. Dardy "Optical networking for quantum key distribution and quantum communications," New J. Phys. 11, 105001 (2009).

[5] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. 11, 075001 (2009).

[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe,A. Allacher, O. Maurhart, T. Länger, M. Peev y A. Zeilinger "Field test of quantum key

distribution in the Tokyo QKD Network," Optics Express 19, 10387-10409 (2011).

[7] http://www.idquantiqe.com

[8] P. Eraerds, N. Walenta, M. Legré, N. Gisin y H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New J. Phys. 12, 063027 (2010).

[9] A. Tanaka, A. Tajima y A. Tomita, "Colourless interferometric technique for large capacity quantum key distribution systems by use of wavelength division multiplexing," en Proc. 35th European Conference on Optical Communication, paper 1.4.2 (2009).

[10] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki y A. Tajima, "A Scalable Full Quantum Key Distribution System based on Colourless Interferometric Technique and Hardware Key Distillation", en Proc. 37th European Conference on Optical Communications, paper Mo.1.B.3 (2011).

[11] J. Capmany, A. Ortigosa- Blanch, J. Mora, A. Ruiz-Alba, W. Amaya and A. Martinez "Analysis of Subcarrier Multiplexed Quantum Key distribution systems: Signal, Intermodulation and Quantum Bit Error rate", IEEE J. Sel. Topics Quantum. Electron. 15, 1607-1621 (2009).

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N.Lütkenhaus y M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. 81, 1301-1350 (2009).

[13] O. L. Guerreau, F. J. Malassenet, S. W. McLaughlin y J. M. Merolla, "Quantum key distribution without a single photon source using a strong reference," IEEE Phot. Tech. Lett. 17, 1755-1757 (2005).

[14] O. Guerreau, J-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer y F. J. Malassenet, "Long distance QKD transmission using single-sideband detection detection scheme with WDM synchronization," IEEE J. Sel. Top. Quantum Electron. 9, 1533-1540 (2003).

[15] H. Ishio, J. Minowa y K. Nosu, "Review and status of wavelength-division-multiplexing technology and its application," J. Lightwave Technol. 2, 448-463 (1984).

[16] G.H. Smith, D. Novak, Z. Ahmed, "Technique for optical SSB generation to overcome dispersion penalties in fibre-radio systems," Electronics Letters 33, 74-75 (1997).

[17] C.A. Brackett, “Dense wavelength division multiplexing networks: principles and applications,” IEEE Journal on Selected Areas in Communications 8, 948-964 (1990).

Capítulo 5

Conclusiones y Líneas Futuras

5.1. Conclusiones

El objetivo de esta tesis se ha centrado en los sistemas de distribución de clave cuántica con el fin de aumentar la capacidad de transmisión y evaluar los aspectos relevantes de seguridad mediante la utilización de dispositivos ópticos de telecomunicación y tecnología fotónica disponibles actualmente. En concreto, el trabajo realizado ha sido la adaptación de los sistemas con codificación en frecuencia, conocidos ampliamente en el campo de la Fotónica de Microondas, a sistemas de distribución de clave cuántica basados en el protocolo BB84.

El desarrollo de la tesis ha requerido la puesta a punto de diversos análisis teóricos y esquemas experimentales. Entre ellos, cabe destacar el estudio teórico de sistemas basados en codificación en frecuencia (FC-QKD). Concretamente, se ha mostrado un análisis general para la concatenación de distintos moduladores, con el fin de analizar las diferencias desde el punto de vista cuántico entre las distintas

estructuras propuestas. En este análisis, la dispersión del canal cuántico ha jugado un papel relevante. También se han introducido los sistemas SCM-QKD, que pueden considerarse una evolución de los sistemas con codificación en frecuencia. Se han derivado las expresiones para los parámetros más característicos del sistema, como son la tasa de error de bit (QBER) y la tasa de trasmisión de clave. En la derivación se ha tenido en cuenta todos los posibles factores de degradación de los sistemas SCM-QKD, incluyendo la dispersión de la fibra y los efectos de segundo orden debidos a la multiplexación. La influencia de estos parámetros en la seguridad ha sido analizada teniendo en cuenta los aspectos más importantes en el diseño de estos sistemas.

A continuación, se detallan las conclusiones más importantes de esta parte teórica:

- Entre todas las configuraciones de moduladores posibles para implementar el protocolo BB84, se han identificado aquellas que son más eficientes en términos de tasa secreta de bit y seguras en términos de QBER. Estas configuraciones son AM-PM, PM-PM y AM-UM.

- Para mantener un QBER aceptable es necesario mantener una ligadura entre la distancia del canal y la frecuencia de la subportadora eléctrica, debido a la restricción impuesta por la dispersión del canal, que se puede eliminar compensando su efecto en algunas configuraciones.

- Se puede aumentar la capacidad de los sistemas que implementan el protocolo BB84 mediante la técnica SCM. Esta técnica permite trasmitir diversas claves paralelamente de forma eficiente ya que todas se envían empleando la misma portadora óptica. Esto se consigue usando una subportadora eléctrica para cada clave.

- La técnica SCM-QKD podría incrementar en un orden de magnitud la tasa de transmisión final en los sistemas actuales. Teniendo en cuenta que la separación entre canales DWDM es alrededor de 100 GHz y las tasas de transmisión actuales, la eficiencia espectral intra-canal está limitada entre el 2 % y el 4 %. En este sentido, el uso de la técnica SCM podría incrementar esta eficiencia hasta valores más altos del 50 %. Para ello, se utilizarían moduladores con un ancho de banda en torno a 50 GHz y filtros ópticos con un espacio entre canales muy estrecho (~1-2 GHz).

- Para conseguir la máxima eficiencia en los sistemas SCM-QKD es necesario compensar la dispersión.

- Los efectos de segundo orden, son despreciables en los sistemas SCM-QKD para índices de modulación por debajo del 5%.

- Los efectos de degradación debidos al efecto Raman y la interferencia con la portadora óptica conllevan una cota para el valor de los parámetros de la potencia del canal de referencia, ancho de banda del filtro, índice de modulación y la separación entre las bandas y la portadora para mantener niveles de QBER aceptables.

Complementando este análisis teórico, se han implementado distintos esquemas en el laboratorio con el fin de evaluar la viabilidad experimental de este tipo de estructuras y técnicas para su empleo en QKD. Para ello, ha sido necesario el desarrollo experimental de:

- Una fuente pulsada y atenuada que cumple con las exigencias de seguridad, ya que es capaz de producir pulsos de 1.3 ns de ancho, con distintos valores de número medio de fotones por pulso.

- Un sistema de codificación y multiplexación en frecuencia, mediante moduladores electroópticos y dispositivos de radiofrecuencia (desfasadores, atenuadores y osciladores).

- Un sistema de filtrado óptico mediante FBGs, que permite obtener la portadora óptica como *strong reference* y cada una de las bandas utilizadas para la codificación en frecuencia de la clave cuántica.

- Un canal de referencia, que permite estabilizar el sistema frente a fluctuaciones de la longitud del canal de fibra. Para ello se trasmite un canal clásico multiplexado en longitud de onda con el cuántico, siendo necesario un estudio para evaluar el nivel de potencia de esta canal y, de esta manera, evitar el efecto Raman. Esta exigencia conlleva el diseño de una doble etapa de amplificación (mediante amplificadores ópticos y eléctricos), que es desarrollada en el receptor.

Con los distintos esquemas de laboratorio, en primer lugar se han mostrado las medidas experimentales correspondientes a la concatenación de moduladores controlando la dispersión del medio de transmisión. En segundo lugar, se ha presentado el primer estudio experimental de los sistemas SCM-QKD a través de un prototipo desarrollado en el laboratorio. Este prototipo es una de las contribuciones más importantes de la Tesis ya que permite, por primera vez, demostrar experimentalmente el incremento de la tasa de trasmisión en sistemas basados en modulación en frecuencia.

Las principales conclusiones que se derivan de la parte experimental son detalladas a continuación:

- Los nuevos sistemas FC-QKD con las configuraciones más eficientes y seguras (PM-PM y AM-UM) son experimentalmente viables. En ambos casos, en la demostración experimental se han obtenido valores del QBER del 2 % y de visibilidad efectiva superiores al 98 %, teniendo en cuenta la dispersión del canal. En este caso, la tasa de transmisión de clave en crudo es del orden de 10 kb/s.

- La técnica SCM-QKD es experimentalmente viable. Esto se ha corroborado mediante un prototipo que sustenta la transmisión de dos subportadoras independientes donde la tasa de clave presenta una ganancia máxima de 3 dB con respecto al caso FC-QKD. El QBER obtenido alcanza un valor por debajo del 2 % para las dos subportadoras, lo que implica una visibilidad efectiva mínima del 96 %.

- El prototipo permanece estable durante un intervalo de tiempo de una hora tras la incorporación del sistema de referencia diseñado. Esto demuestra que las derivas del canal, debidas a variaciones en la temperatura y vibraciones, son suficientemente compensadas.

- Los sistemas de distribución de clave cuántica basados en la combinación de las técnicas SCM y WDM son experimentalmente viables. Esto se ha demostrado mediante un sistema formado por dos trasmisores SCM-QKD independientes centrados en longitudes de onda de 1549.78 y 1557.30 nm. La tasa de bit de clave en crudo total presenta una ganancia de 4. El QBER obtenido para cada uno de los canales está por debajo del 2 %.

- La ventaja de SCM frente a WDM en un sistema de distribución de clave es que se usa la misma fuente de fotones para las distintas claves. Así pues, la complejidad del sistema de control se reduce considerablemente cuando el sistema QKD se introduce en una red óptica.

- Los sistemas SCM-QKD cumplen las condiciones de seguridad incondicional y es resistente al ataque PNS ya que pueden implementar el protocolo BB84 con *strong reference y* con estados *decoy* para cada subportadora.

5.2. Líneas futuras

El trabajo realizado en esta tesis apunta una serie de posibles líneas de investigación futuras que se detallan a continuación.

- Mejorar la capacidad actual del sistema en dos órdenes de magnitud por medio de componentes que ya están comercialmente disponibles. Por

ejemplo, desfasadores con un tiempo de conmutación de 25 ns, detectores de fotones con frecuencias de ventana superiores a 100 MHz y un mayor número de subportadoras incorporando filtros ópticos de 32 salidas con un espaciado entre canales de aproximadamente 5 GHz.

- Adaptación experimental del protocolo BB84 con estados *decoys* en los sistemas SCM-QKD. Con esta adaptación se puede aumentar la tasa de trasmisión segura y la máxima longitud de trasmisión. La adaptación de este protocolo implica el uso de una nueva fuente, la cual debe emitir, aleatoriamente, pulsos con más de un fotón de media. También se debe realizar cambios en el sistema de control, para tener en cuenta estos pulsos y llevar a cabo la estimación de parámetros, que permita detectar el ataque PNS.

- Completar el estudio de FC-QKD teniendo en cuenta otro tipo de moduladores diferentes a los electroópticos, como son los de electro-absorción.

- Aumentar la estabilidad del sistema SCM-QKD mediante la adaptación de un receptor independiente del estado de polarización a la salida del canal. Ya se han propuesto distintos receptores de este tipo para los sistemas FC-QKD, que han permitido que el sistema permaneciese estable, sin ningún sistema de control activo, durante varios días.

- Estudio de la seguridad de los sistemas FC-QKD teniendo en cuenta el canal de referencia. Este canal estaría sujeto a las manipulaciones de un espía, el cual podría desactivar los osciladores de Bob, sin ser detectada su presencia, inutilizando el sistema de *strong reference*.

- Estudio de la seguridad de los sistemas FC-QKD teniendo en cuenta el sistema de filtrado. Este sistema elimina todas las señales que no estén dentro del ancho de banda del filtro. Por tanto, Eve podría utilizar estas señales para manipular el sistema y obtener información sin ser detectada.

- Adaptación de los sistemas SCM-QKD a la nueva generación de protocolos con la referencia de fase distribuida (COW y DPS). Este tipo de protocolos permiten simplificar tanto el trasmisor y el receptor, y proporcionan seguridad frente al ataque PNS sin necesidad de *strong reference* ni estados *decoy*.

Anexo A

Publicaciones Científicas del Autor

A.1. Publicaciones en revistas internacionales

J. Mora, **A. Ruiz-Alba**, W. Amaya y J. Capmany, "*Dispersion supported BB84 quantum key distribution using phase modulated light",* IEEE Photonics Journal 3, 433-440 (2011).

A. Ruiz-Alba, D. Calvo, V. García-Muñoz, A. Martinez, W. Amaya, J. G. Rozo, J. Mora y J. Capmany, "*Practical Quantum Key Distribution based on the BB84 protocol*," Waves 2, 4-14 (2011).

J. Capmany, A. Ortigosa-Blanch, J. Mora, **A. Ruiz-Alba**, W. Amaya y A. Martinez, *"Analysis of subcarrier multiplexed quantum key distribution systems: signal, intermodulation, and quantum bit error rate*," IEEE Journal of Selected Topics in Quantum Electronics, 15, 1607-1621 (2009).

J. Mora, **A. Ruiz-Alba**, W. Amaya, A. Martinez, V. García-Muñoz, D. Calvo y J. Capmany, "*Experimental demonstration of subcarrier multiplexed quantum key distribution system*," Optics Letters, 37, 2031–2033 (2012).

A. Ruiz-Alba, J. Mora, W. Amaya, A. Martinez, V. García-Muñoz, D. Calvo y J. Capmany, "*Microwave Photonics Parallel Quantum Key Distribution*," Photonics Journal, 4, 931-942 (2012).

J. Mora, W. Amaya, **A. Ruiz-Alba**, A. Martinez, D. Calvo, V. García-Muñoz y J. Capmany, "*Simultaneous Transmission of 20x2 WDM/SCM-QKD and 4 Bidirectional Classical Channels Over a PON*," (enviado a Optics Express).

A. Ruíz-Alba, J. Mora, W. Amaya y J. Capmany, "*Experimental evaluation of intermodulation for subcarrier multiplexed quantum key distribution*" (enviado a Optics Letters).

J. Mora, **A. Ruiz-Alba**, V. García-Muñoz, W. Amaya, J. Capmany, *"Novel modulator configuration for BB84 Frequency Coded Quantum Key Distribution"* (enviado a Photonics Technology Letters).

J. Mora, **A. Ruíz-Alba** y J. Capmany, "*Theoretical investigation on tandem modulator configurations for Frequency Coded Quantum Key Distribution systems*" (enviado a Photonics Journal).

J. Mora, **A. Ruíz-Alba** y J. Capmany, *"Impact of first-order dispersion on the performance of subcarrier multiplexed quantum key distribution"* (enviado a Optics Express).

A. Ruiz-Alba, N. Walenta, R. Houlmann, J. Mora, H. Zbinden, "*Multi-Protocol Emitter for QKD using a Dual-drive Modulator"* (enviado a Applied Physics Letters).

A.2. Publicaciones en congresos nacionales e internacionales

A. Ruiz-Alba, D. Calvo, V. García-Muñoz, A. Martinez, W. Amaya, J. G. Rozo, J. Mora and J. Capmany, "*Experimental Demonstration of Subcarrier Multiplexed Quantum Key Distribution System Feasibility*", 13th International Conference on Transparent Optical Networks ICTON 1-4 (2011).

J. Mora, V. García-Muñoz, **A. Ruiz-Alba**, W. Amaya, A. Martinez and J. Capmany."*Experimental demonstration of a novel configuration for BB84 frequency coded QKD*", International Conference on Information Photonics (IP) 1-2 (2011).

J. Mora, **A. Ruiz-Alba**, W. Amaya, V. García-Muñoz and J. Capmany. "*Microwave photonic filtering scheme for BB84 Subcarrier Multiplixed Quantum Key Distribution*" International Topical Meeting on Microwave Photonics 286-289 (2010).

A. Ruiz-Alba, J. Mora, V. García-Muñoz, W. Amaya, J. Juan-Colás and J. Capmany. "*Demostración Experimental de la Viabilidad de Sistemas Fotónicos de Distribución Cuántica de Clave con Multiplexación de Subportadora*" Simposium Nacional de la Unión Científica Internacional de Radio URSI 154-158 (2010).

A. Ruiz-Alba, J. Mora, J. Capmany, W. Amaya and A. Ortigosa-Blanch. "*Experimental Demonstration of Subcarrier Multiplexed*" International Topical Meeting on Microwave Photonics 1-4 (2009).

A.3. Patentes

A. Ruiz-Alba, J. Mora and J. Capmany. "*Técnica y Protocolo de Distribución de Clave Cuántica Basado en Modulación de Frecuencia y Fase Diferencial*", (solicitud del 14 de Marzo con referencia P201230385).