Multiplexación de Subportadora para Sistemas de Distribución Cuántica de Clave

Autor: Antonio Ruiz-Alba Gayá
Director1: José Capmany Francoy
Director2: José Mora Almerich

Resumen — Este trabajo presenta un sistema de distribución de clave cuántica con codificación en frecuencia (FC-QKD) usando la técnica de multiplexado de subportadora (SCM). La finalidad de este trabajo consiste en aumentar la tasa de bit de transmisión de estos sistemas cuánticos que se ve drásticamente reducida por las pérdidas de transmisión. En primer lugar, se presenta un modelo teórico teniendo en cuenta el impacto de la intermodulación en el error cuántico de bit (QBER) y en la tasa de bit efectiva. En segundo lugar, se muestra la implementación experimental desarrollada con dos subportadoras de radiofrecuencia. La viabilidad del sistema experimental queda demostrada.

Abstract —This work presents a frequency coded quantum key distribution system (FC-QKD) using the subcarrier multiplexing technique (SCM). The goal of this work is to improve the rate of quantum key distribution rate which is reducing for the system loses. To do this, first we develop a theoretical analysis taking into account the influence of nonlinear photon mixed on the quantum bit error rate and the useful key rate. Second, we provide a first experimental approach using two radiofrequency subcarriers. The feasibility of the system is demonstrated.

Autor: Antonio Ruiz-Alba Gayá, email: anruiz@iteam.upv.es
Director 1: José Capmany, email: jcapmany@iteam.upv.es
Director 2: José Mora, email: jmalmer@iteam.upv.es
Fecha de entrega: 22-03-10

ÍNDICE

I. Introducción.

En la actualidad existen dos campos en continuo desarrollo en el mundo de las comunicaciones, el aumento de la capacidad de transmisión de la información y el de su seguridad. Este segundo campo ha suscitado un gran interés debido a que existen aplicaciones en la que es necesario garantizar máxima seguridad como puede ser el caso de operaciones bancarias, aplicaciones militares y aplicaciones aeroespaciales.

En los últimos años están emergiendo nuevos sistemas que utilizan los principios de la física cuántica para garantizar al 100% la seguridad a través de la distribución cuántica de clave (Quantum Key Distribution, QKD). En estos sistemas, las dos partes autorizadas que quieren compartir una clave secreta a distancia, son tradicionalmente llamadas Alice (transmisor) y Bob (receptor). Ellos necesitan estar conectados por dos canales, uno cuántico, que les permitirá compartir señales cuánticas, y un canal clásico, en el cual pueden enviar mensajes clásicos [1].

El canal clásico necesita ser autentificado, esto significa que Alice y Bob se identifican entre ellos. Una tercera persona puede escuchar la conversación, pero no participar en ella. El canal cuántico, sin embargo, está abierto a cualquier manipulación de una tercera persona. La tarea de Alice y Bob es garantizar la seguridad aunque un adversario espía, usualmente llamado Eve, manipule el canal cuántico y escuche los mensajes del canal clásico. La figura 1.1 muestra un esquema general de esta técnica.

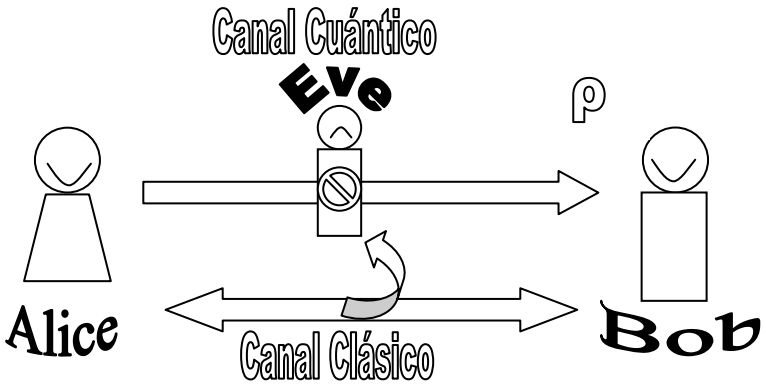


Figura 1.1. Esquema de un sistema QKD. Alice y Bob están conectados a través de un canal cuántico, donde Eve puede intervenir sin ninguna restricción excepto las leyes de la física cuántica, y un canal clásico donde Eve solo puede escuchar.

Por garantizar la seguridad entendemos que una clave no segura nunca es usada, es decir, las partes autorizadas crean una clave secreta o se descarta la clave. Por tanto, después de la transmisión de la secuencia de símbolos, Alice y Bob deben estimar cuanta información se ha vertido sobre Eve. Esta estimación es imposible en comunicaciones clásicas, ya que pueden

permanecer inalteradas si Eve hace una escucha. Es aquí donde la física cuántica entra en juego; en un canal cuántico, una fuga de información es cuantificable por medio de la degradación de la comunicación [1].

Los fotones son los mejores candidatos para trasmitir los estados cuánticos, ya que son partículas que no interactúan fácilmente con la materia y pueden ser transmitidos a grandes distancias. Los canales de transmisión que se utilizan son la fibra óptica y el aire libre.

El uso de dispositivos de fotónica de para desarrollar estos sistemas con un enlace de fibra óptica abre la posibilidad de usar diferentes configuraciones. La primera fue descrita en 1992 por Bennett y sus colegas [2], que consiste en codificar los bits en los vectores de polarización de la función de onda del fotón. El problema que presenta este método es mantener constante la polarización a lo largo del enlace. No obstante, los sistemas *"plug and play"* resuelven en gran parte estas limitaciones [3]. Una segunda configuración fue descrita por Townsend y sus colegas [4] y [5], la cual se basa en retardos ópticos e interferómetros balanceados en el trasmisor y receptor. El problema de esta configuración es mantener constante el comportamiento de los interferómetros frente a las variaciones mecánicas y ambientales. En la tercera configuración, la función de onda del fotón es repartida en tres pulsos donde la información de los bits es llevada en la diferencia de fase de dos pulsos consecutivos (distribución de clave cuántica por desplazamiento de fase) [6], [7] y [8]. La cuarta configuración fue propuesta por Merolla y sus colegas [9], también llamada codificación en frecuencia (Frequency Coded QKD, FC-QKD), consiste en codificar la información en las bandas laterales producidas al modular en fase o en amplitud. Originalmente este sistema se utilizó para implementar el protocolo B92 (protocolo de Bennett 1992) [9],[10]; pero más tarde se mejoró para poder implementar el protocolo BB84 (protocolo de Bennett- Bassard 1884) [11], [12] y [13].

Existen varias configuraciones propuestas en la bibliografía para la implementación de sistemas basados en FC-QKD. Éstos dependen del tipo de moduladores electroópticos que utilizan Alice y Bob, como los moduladores de fase PM-PM [9] y los moduladores de amplitud AM-AM [13] que desarrollan el protocolo B92 así como los moduladores desbalanceados UM-UM [14] o una combinación de moduladores de amplitud y fase como AM-PM [13] para desarrollar el protocolo BB84.

Con la cuarta configuración que acabamos de mencionar se han conseguido tasas de bit del orden de 1Mbit/s para distancias de 20km de fibra y 10kb/s para distancias de 100km de fibra [21]. El récord se ha conseguido para la configuración de desplazamiento de fase, que es de 17Kb/s en 105km de fibra [17] y 12b/s para 200km [22]. Estas tasas se consideran todavía modestas, existiendo un gran interés en el desarrollo de técnicas para aumentar estos valores.

El trabajo presentado en este documento está enmarcado dentro del proyecto financiado por el gobierno de España a través del llamado Consolider Quantum Optical Information Technology

(QOIT), donde participan un total de 11 grupos de investigación. Los principales objetivos que se persiguen con este trabajo de investigación son los siguientes:

- Presentar un sistema de multiplexación de subportadora para la distribución de clave cuántica (SCM-QKD) que alcance una tasa de bit más elevada que los propuestos hasta ahora.
- Estudio teórico de los parámetros más relevantes, como son el QBER y la tasa de bit.
- Desarrollo experimental y análisis de resultados de un sistema SCM-QKD.

Este escrito está estructurado en 6 apartados. El primero corresponde a esta introducción, donde se ha comentado la terminología de QKD, el estado del arte y en qué va a consistir este trabajo. En el segundo y el tercero se describe el comportamiento general de este tipo de sistemas, tanto en transmisión como en recepción, analizando el campo electromagnético en los puntos de interés del sistema y deduciendo la visibilidad y los términos que causarán interferencias. A continuación, en el capitulo 4, se estudia la tasa de error de bit cuántico (QBER), y se muestran diferentes simulaciones de esta magnitud para diferentes parámetros del sistema. En el capítulo 5, se muestra los resultados experimentales de un sistema con dos subportadoras, y se contrastan con los teóricos obtenidos en la sección anterior. En esta sección, también evaluaremos las dificultades experimentales que existen a la hora de implementar estos sistemas. Por último, para concluir este trabajo de investigación se hace una recopilación de los principales resultados obtenidos y se plantean líneas futuras de investigación con las que se pretende realizar un futuro trabajo de investigación con carácter de tesis doctoral.

II. Análisis téorico del sistema SCM-QKD.

II. 1. Análisis del sistema QKD con una subportadora: Visibilidad.

En este capítulo se presentan los conceptos generales de un sistema FC-QKD, mostrando sus componentes fundamentales, y las consideraciones a tener en cuenta para su correcto funcionamiento. En primer lugar, se estudia el sistema FC-QKD con una subportadora desarrollado previamente por Merolla que utiliza el protocolo BB84 [12] con el fin de conocer la estructura básica del sistema sobre el que se va a implementar la multiplexación cuántica.

En la introducción se ha comentado que estos sistemas funcionan con señales cuánticas, es decir, con fotones. Por tanto, formalmente sería necesario un estudio teórico bajo una descripción asociada a la física cuántica. Sin embargo, la viabilidad del sistema puede ser demostrada trabajando bajo un régimen clásico utilizando la potencia óptica como densidades de probabilidad asociadas a la naturaleza probabilística de la física cuántica [15]. Matemáticamente, la expresión del número de fotones calculada con el formalismo de la mecánica cuántica coincide con la potencia óptica del formalismo clásico. En este contexto, mostraremos el procedimiento cuántico, pero sin entrar en detalle, desarrollando las expresiones clásicas.

La figura 2.1 muestra un esquema del sistema FC-QKD con una única portadora [12], que pasamos a describir.

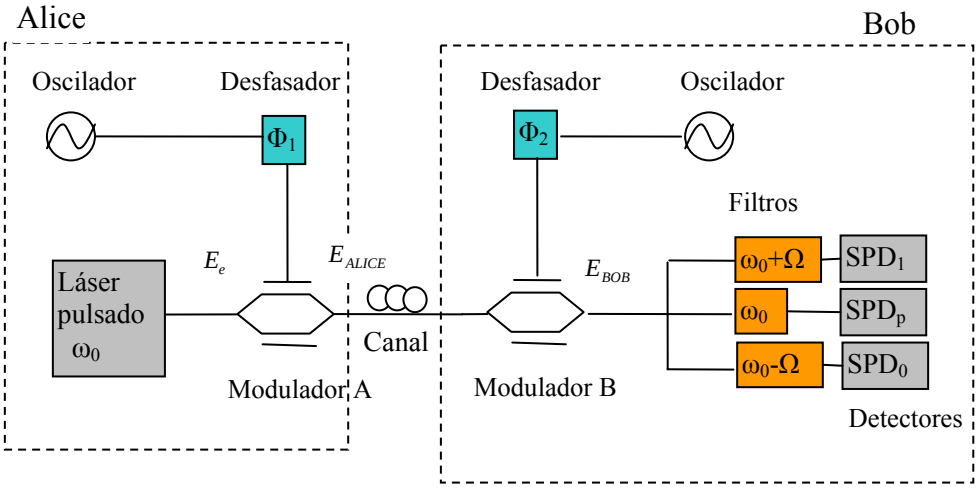


Figura 2.1. Diagrama del sistema FC-QKD de una subportadora.

Llevando a cabo la descripción teórica clásica, el sistema genera un campo $E_e(z,t)$, descrito por una onda plana monocromática de frecuencia ω_0, con un láser continuo. La descripción clásica de este campo a la salida de la fuente se realiza mediante

$$E_e(z,t) = E_0 e^{j(\beta z - \omega_o t)} \hat{x}\,. \tag{2.1}$$

Donde $\hat{x}$ denota la polarización del campo, β la constante de propagación y E_0 la amplitud del campo

Este campo tiene como equivalente cuántico a un estado coherente $|\alpha\rangle$, que representa un vector perteneciente a un espacio vectorial C (complejo de una dimensión).

El campo eléctrico es externamente modulado, con un modulador desbalanceado, por una subportadora de radiofrecuencia generado por un oscilador. La señal de radiofrecuencia generada se describe como

$$V(t) = -V_{DC} - V_{AC}\cos(\Omega t + \Phi_1), \tag{2.2}$$

donde Ω es la frecuencia angular de la subportadora eléctrica y Φ_1 la fase introducida a la subportadora mediante un desfasador eléctrico, la cual puede tomar los valores de 0, π y π /2, 3 π/2. Por tanto, el campo a la salida del modulador viene dado por

$$E_{ALICE}(t) = \hat{x}E_e\left(e^{j\frac{V(t)}{V_\pi}} + 1\right), \tag{2.3}$$

donde V_π es un parámetro intrínseco del modulador [16]. Desarrollando la expresión llegamos a

$$E_{ALICE}(t) = \hat{x}E_e\left(e^{j\psi_1}\cdot e^{jm_1\cdot\cos(\Omega t+\Phi_1)} + 1\right), \tag{2.4}$$

y se define el parámetro ψ_1, asociado a la tensión de polarización V_{DC} del modulador y el índice de modulación m_1

$$\begin{aligned} \psi_1 &= \pi\,\frac{V_{DC}}{V_\pi} \\ m_1 &= \pi\,\frac{V_{AC}}{V_\pi}\,. \end{aligned} \tag{2.5}$$

Si tenemos en cuenta que trabajamos en régimen de baja modulación (m<<1) estas expresiones pueden reducirse a [12]

$$E_{ALICE}(t) \approx \frac{\hat{x}E_e}{2}\left[\left(1 + e^{j\Psi_1}\right) + \frac{ie^{j\Psi_1}}{2}m_1\left(e^{j(\Omega t+\Phi_1)} + e^{-j(\Omega t+\Phi_1)}\right)\right]. \tag{2.6}$$

A la salida del modulador, el campo puede tomar 4 formas posibles (una para cada valor de Φ_1). El equivalente cuántico a este campo ($E_{ALICE}(t)$) es otro estado coherente $|A\rangle$ que representa un vector perteneciente a un espacio vectorial C^2 (complejo de dos dimensiones), y puede ser 1 de 4 estados diferentes, dependiendo de la fase (Φ_1) elegida. Estos estados forman

dos bases diferentes, M_+ y $M_\times$ del mismo espacio vectorial, de forma que $|A\rangle \in C^2 : |A\rangle = \{|0\rangle_+, |1\rangle_+ \in M_+ \; y \; |0\rangle_\times, |1\rangle_\times \in M_\times\}$, por tanto, Alice puede transmitir el bit 0 y el bit 1 de dos maneras diferentes. La tabla 1 muestra este procedimiento.

Bit que quiere mandar Alice	0		1	
Desfase (Φ_1) que generan los estados	0	$\pi/2$	π	$3\,\pi/2$
Estados que se transmiten	$\|0\rangle_+$	$\|0\rangle_\times$	$\|1\rangle_+$	$\|1\rangle_\times$

Tabla 1. Correspondencia entre los bits que manda Alice con el desfase (Φ_1) y el estado que se trasmite.

Esta señal se propaga por el canal de fibra óptica, y tras compensar la dispersión llega al modulador de Bob, que también es desbalanceado. Siguiendo con el formalismo clásico, a la salida de este modulador el campo presenta el siguiente aspecto [12]

$$E_{BOB}(t) \approx \frac{E_{ALICE}(t)}{2}.\left[\left(1+e^{j\Psi_2}\right)+\frac{je^{j\Psi_2}}{2}m_2\left(e^{j(\Omega_2 t+\Phi_2)}+e^{-j(\Omega_2 t+\Phi_2)}\right)\right]. \tag{2.7}$$

En esta expresión m_2, ψ_2 y Φ_2 tienen el mismo significado que en el caso de Alice, pero ahora Φ_2 toma los valores 0 y $\frac{\pi}{2}$ que representan la elección de base que hace Bob para realizar sus medidas. Desarrollando esta expresión obtenemos [15]

$$E_{BOB}(t) \approx \frac{\hat{x}E_e}{4}\left[\begin{array}{l}\left(1+e^{j\Psi_1}\right)\left(1+e^{j\Psi_1}\right)+\dfrac{i\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}}{2}m_B\left(e^{j(\Omega t+\Phi_2)}+e^{-j(\Omega t+\Phi_2)}\right)+\\ +\dfrac{j\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}}{2}m_A\left(e^{j(\Omega t+\Phi_1)}+e^{-j(\Omega t+\Phi_1)}\right)\end{array}\right]. \tag{2.8}$$

El equivalente cuántico de $E_{Bob}(t)$ es otro estado coherente $|B\rangle$ que representa otro vector en un espacio vectorial C^2 y se obtiene de $|A\rangle$ a partir un operador que se representa por una matriz S y describe la interacción entre el estado coherente $|A\rangle$ y Bob. Esta matriz puede ser de dos formas diferentes, dependiendo de la elección de base de Bob (Φ_2).

Volviendo al formalismo clásico, si el campo atraviesa un par de filtros ideales (SPD_1 y SPD_1) centrados en $\omega_o \pm \Omega$ se obtiene la información contenida en cada una de estas dos bandas, y los campos a la salida de estos filtros será

$$E_{+\Omega}(t) \approx \frac{\hat{x}E_0 e^{j(\beta z-(\omega_0-\Omega)t)}}{4}\left[\frac{j\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}e^{j\Phi_2}}{2}m_2+\frac{i\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}e^{j\Phi_1}}{2}m_1\right] \quad (2.9)$$

$$E_{-\Omega}(t) \approx \frac{\hat{x}E_0 e^{j(\beta z-(\omega_0+\Omega)t)}}{4}\left[\frac{i\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}e^{-j\Phi_1}}{2}m_2+\frac{i\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}e^{-j\Phi_1}}{2}m_1\right].$$

La intensidad óptica de los campos eléctricos a la salida de los filtros es

$$I^S_{+\Omega} \propto \left|E_\Omega\right|^2$$
$$I^S_{-\Omega} \propto \left|E_{-\Omega}\right|^2. \quad (2.10)$$

Introduciendo (2.9) en (2.10) obtenemos para la primera banda

$$I^S_{+\Omega_i} = I_{\max}(m_1,m_2,\Psi_1,\Psi_2)\left[1+V(m_1,m_2,\Psi_1,\Psi_2)\cos(\Delta\Phi+\Delta\Psi)\right]. \quad (2.11)$$

Definimos los siguientes parámetros

$$I_{\max}(m_1,m_2,\Psi_1,\Psi_2) = \frac{\left|E_e\right|^2}{16}\left[m_1^2\cos^2\left(\frac{\Psi_2}{2}\right)+m_2^2\cos^2\left(\frac{\Psi_1}{2}\right)\right]$$

$$V(m_1,m_2,\Psi_1,\Psi_2) = \left|\frac{2m_1m_2\cos\left(\frac{\Psi_1}{2}\right)\cos\left(\frac{\Psi_2}{2}\right)}{m_1^2\cos^2\left(\frac{\Psi_2}{2}\right)+m_2^2\cos^2\left(\frac{\Psi_1}{2}\right)}\right| \quad (2.12)$$

$$\Delta\Phi = \Phi_2-\Phi_1$$
$$\Delta\Psi = (\Psi_2-\Psi_1)/2.$$

donde $V(m_1,m_2,\Psi_1,\Psi_2)$ toma valores entre 0 y 1. Interesa tener los valores más altos posibles para este parámetro, más adelante se verá porqué, por tanto hay que hacer una elección adecuada de los parámetros m_1, m_2, Ψ_1 y Ψ_2.

La intensidad de la banda inferior tiene una expresión similar dada por

$$I^S_{-\Omega_i} = I_{\max}(m_1,m_2,\Psi_1,\Psi_2)\left[1+V(m_1,m_2,\Psi_1,\Psi_2)\cos(\Delta\Phi-\Delta\Psi)\right]. \quad (2.13)$$

Las expresiones (2.11)- (2.13) son equivalentes a las obtenidas en el formalismo cuántico para el número medio de fotones del estado $|B\rangle$,

Se fijan las siguientes condiciones; para los índices de modulación, $m_{1i} = m_{2i} = m$ y para los puntos de cuadratura, $\Psi_1 = \pi/2$ y $\Psi_2 = 3\pi/2$ que corresponden con los de pendiente negativa y positiva respectivamente. Por último la fase de Bob se toma como $\Phi_2+\pi/2$ en vez de Φ_2. Estas condiciones son necesarias para implementar el protocolo BB84 [12].

Cuando se cumplen estas condiciones la intensidad en las bandas se reduce a [12]

$$I^S_{+\Omega_i} = \frac{\left|E_e\right|^2m^2}{16}\left[1+\cos(\Delta\Phi)\right] = \frac{\left|E_e\right|^2m^2}{8}\cos^2\left(\frac{\Delta\Phi}{2}\right) = I_s\cos^2\left(\frac{\Delta\Phi}{2}\right)$$
$$I^S_{-\Omega_i} = \frac{\left|E_e\right|^2m^2}{16}\left[1-\cos(\Delta\Phi)\right] = \frac{\left|E_e\right|^2m^2}{8}\sin^2\left(\frac{\Delta\Phi}{2}\right) = I_s\sin^2\left(\frac{\Delta\Phi}{2}\right). \quad (2.14)$$

La elección de base correcta se produce cuando cuando $\Delta\Phi = 0$ ó $\Delta\Phi = \pi$ dependiendo si se trasmite un “0” o un “1” respectivamente. Esto implica según (2.14) que la banda inferior o

superior es eliminada debido a la interferencia. Cuando Bob escoge la base incorrecta $\Delta\Phi = \pm\frac{\pi}{2}$ ninguna de las bandas es eliminada, en este caso se elimina el bit detectado. La figura 2.2 muestra estos tres casos, donde aparece una banda central en $\nu_0 = \frac{\omega_0}{2\pi}$, correspondiente a la potencia (o número medio de fotones en formalismo cuántico) medida por el detector SPD_p y dos laterales, correspondientes a los detectores SPD_1 y SPD_0. Si la elección de base es correcta ($\Delta\Phi = 0$ ó $\Delta\Phi = \pi$) se elimina una de las bandas como se observa en la figura 2.2a y 2.2b, pero cuando la elección no es correcta ($\Delta\Phi = \pm\frac{\pi}{2}$) aparecen las dos bandas con la mitad de intensidad (ver figura 2.2c).

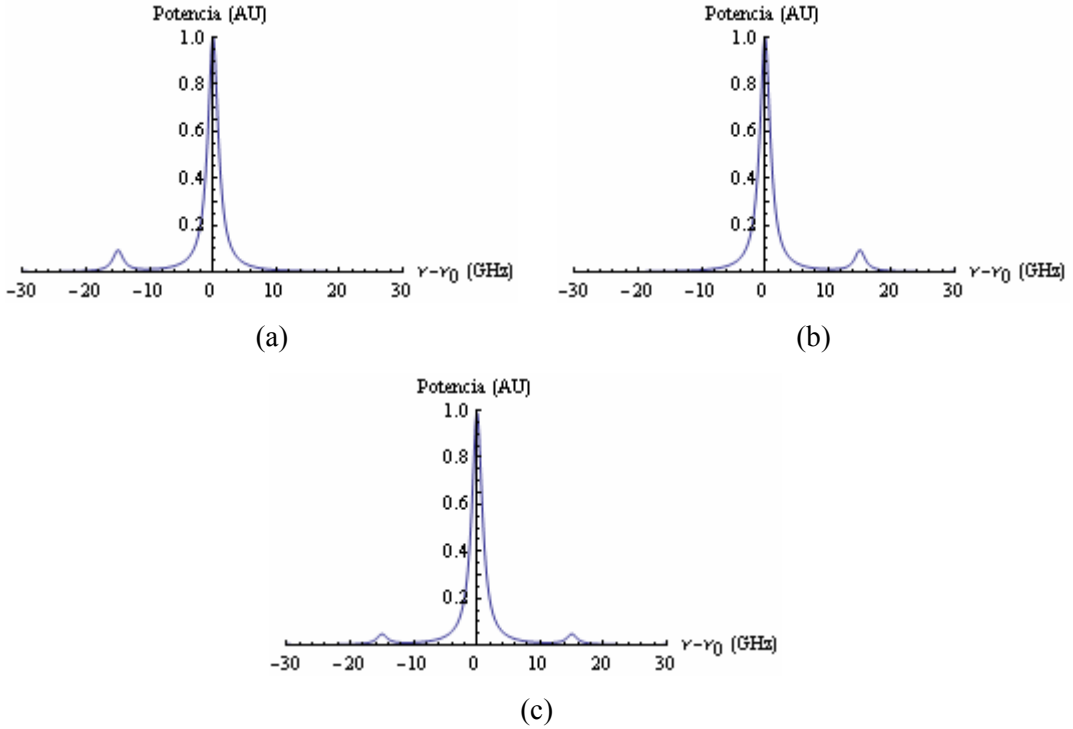


Figura 2.2. Potencia espectral, en unidades arbitrarias (AU), para diferencias de fase $\Delta\Phi$ de (a) 0 (acierto de bases y se transmite un "0") , (b) π (acierto de bases y se transmite un "1"), y (c) $\pm\frac{\pi}{2}$ (no se aciertan bases).

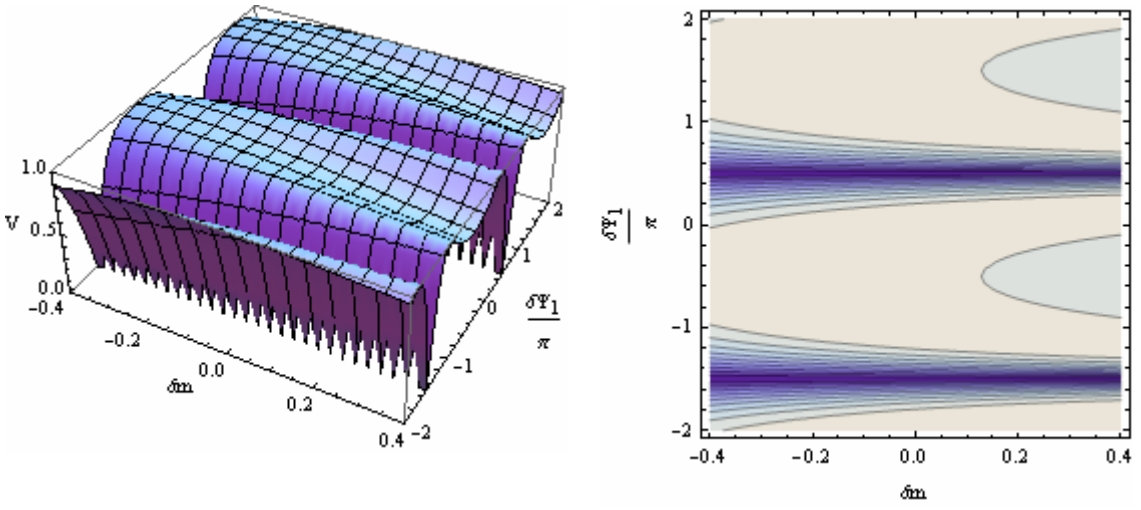
El caso anterior muestra el caso ideal donde $V(m_1, m_2, \Psi_1, \Psi_2) = 1$. Si las relaciones entre los parámetros m_1, m_2, Ψ_1 y Ψ_2 no son las adecuadas $V(m_1, m_2, \Psi_1, \Psi_2)$ es menor que 1 y el máximo de potencia en una banda no se corresponden con el mínimo de la otra, disminuyendo la calidad del sistema. Es por eso que se define la magnitud $V(m_1, m_2, \Psi_1, \Psi_2)$ como la visibilidad, al igual que en otros procesos de interferencia.

La ecuación (2.14) se obtiene bajo la consideración de máxima visibilidad (V=1). Pequeñas desviaciones de las condiciones de los índices de modulación y puntos de cuadratura necesarias

para implementar el protocolo BB84, disminuyen la visibilidad y, por tanto, a la calidad del sistema. Si el modulador de Alice fluctúa una cantidad $\delta\Psi_1 \Rightarrow \Psi_1 = \pi/2 + \delta\Psi_1$ y hay una diferencia entre los índices de modulación dada por δm de tal manera que $m_1 = m$ y $m_2 = m(1+\delta m)$, entonces la visibilidad viene dada por

$$V(\delta m, \delta\Psi_1) = \left| \frac{2(1+\delta m)\left[\cos\left(\frac{\delta\Psi_1}{2}\right) - \sin\left(\frac{\delta\Psi_1}{2}\right)\right]}{1+(1+\delta m)^2 - 2\cos\left(\frac{\delta\Psi_1}{2}\right)\sin\left(\frac{\delta\Psi_1}{2}\right)} \right| \quad . \tag{2.15}$$

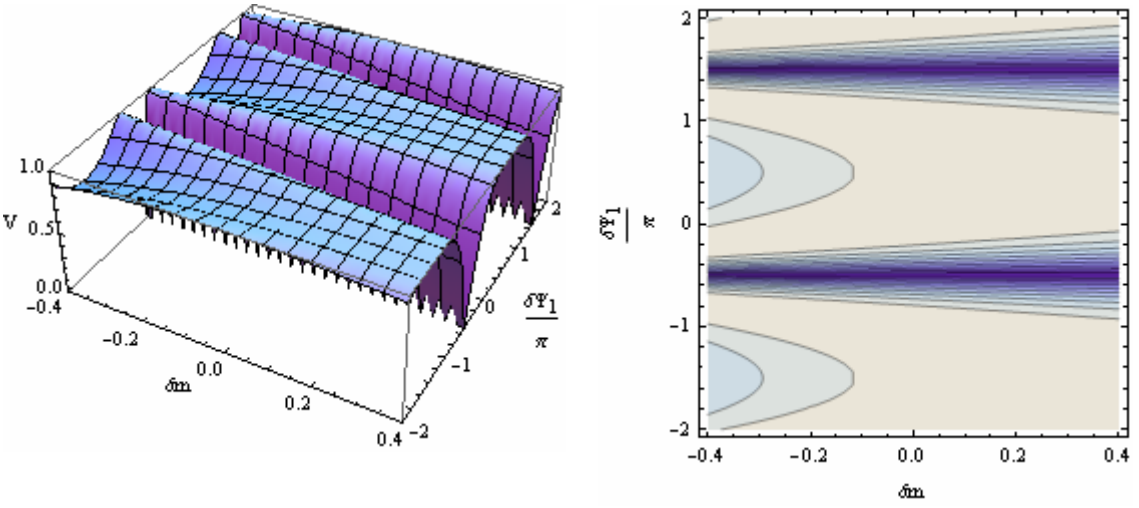
La figura 2.3 muestra la visibilidad (2.15) en función de estas dos desviaciones δm y $\delta\Psi_1$. En la parte izquierda (a) se muestra con una gráfica en tres dimensiones, mientras que en la parte derecha (b) se muestra en dos dimensiones. Se puede observar que la visibilidad es bastante robusta frente al desajuste de los índices de modulación (fluctuaciones de $\delta m = \pm 0.2$ producen variaciones despreciables en la visibilidad), pero por otro lado es más sensible a las desviaciones $\delta\Psi_1$ (especialmente positivas).



(a) (b)

Figura 2.3. Visibilidad en función de las desviaciones en el punto de cuadratura del modulador de Alice ($\delta\Psi_1$) y del desajuste del índice de modulación (δm) en (a) 3D y (b) 2D.

Un comportamiento similar ocurre cuando se producen las desviaciones en el punto de cuadratura del modulador de Bob, las cuales son descritas como $\delta\Psi_2 \Rightarrow \Psi_2 = 3\pi/2 + \delta\Psi_2$ y el desajuste en los índices de modulación como δm. Los resultados se pueden observar en la figura 2.4, el comportamiento es similar al caso anterior, donde la visibilidad es sensible a las desviaciones negativas sobre el punto de cuadratura del modulador de Bob.



(a) (b)

Figura 2.4. Visibilidad en función de las desviaciones en el punto de cuadratura del modulador de Bob ($\delta\Psi_2$) y del desajuste del índice de modulación (δm) en (a) 3D y (b) 2D.

II.2. *Análisis del sistema QKD con varias portadoras: Intermodulación.*

En esta sección se trata el caso de multiplexación de N suportadotas eléctricas (SCM-QKD). La técnica de multiplexación de subportadora es usada en fotónica de radio sobre fibra para telecomunicaciones y en televisión por cable (CATV), con el objetivo de aumentar la información trasmitida por el canal y es utilizada en QKD con la intención de generar una clave con mayor tasa de bit o generar varias multiplexadas.

La figura 2.5 muestra un esquema del sistema propuesto. Este es análogo al de una subportadora, pero esta vez se puede observar que la señal de radiofrecuencia esta formada par la suma de N subportadoras, cada uno con un desfase (Φ_{1i} , i=1,…,N) de 0 , π y $\frac{\pi}{2}, \frac{3\pi}{2}$ para el caso de Alice y de 0 y $\frac{\pi}{2}$ para el caso de Bob (Φ_{2i} , i=1,…,N) Esta señal tiene la forma

$$V(t) = -V_{DC1} - \sum_{i=1}^{N} V_{1i} \cos(\Omega_i t + \Phi_{1i}). \tag{2.16}$$

Con esta señal de radiofrecuencia, la intensidad óptica a la salida del sistema es

$$I_{\Omega_i} \propto \left|E_{\Omega_i}\right|^2 = I_{\Omega_i}^S + I_{\Omega_i}^{IM}. \tag{2.17}$$

En esta expresión $I_{\Omega_i}^S$ representa la intensidad de la señal deseada mientras que $I_{\Omega_i}^{IM}$ denota la intensidad de la señal no deseada cuya expresión es vista más adelante. Se verá en las próximas secciones como conseguir que este nuevo término sea despreciable.

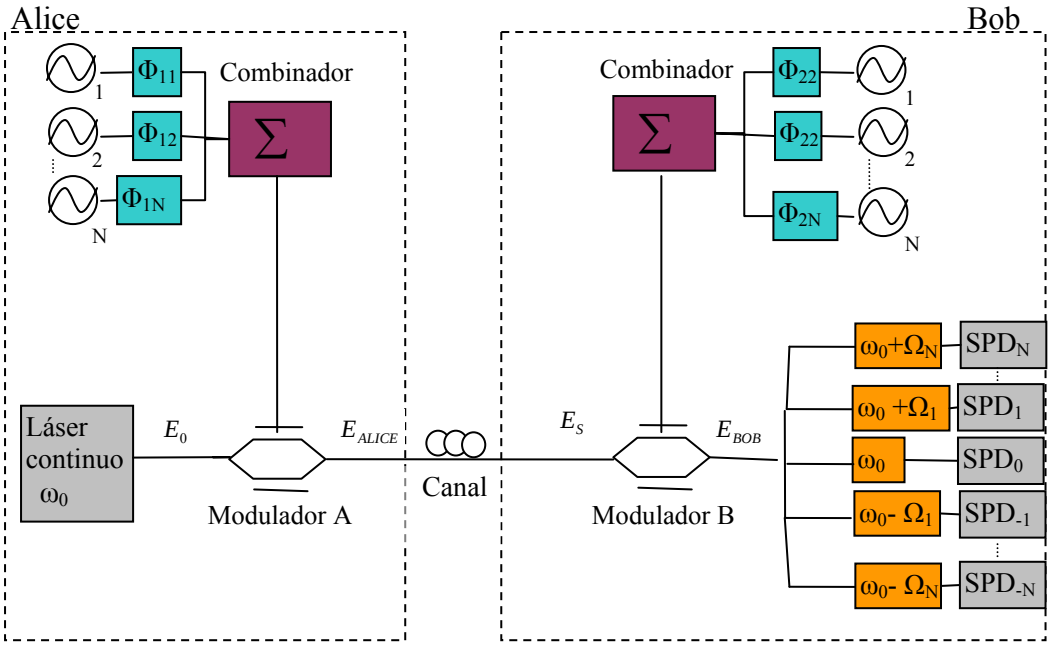


Figura 2.5. Diagrama del sistema para el análisis de N subportadoras.

El campo a la salida del modulador de Alice es

$$E_{ALICE}(t)=\frac{\hat{x}E_e}{2}\left[e^{j\Psi_1}e^{j\sum_{i=1}^{N}m_{1i}\cos(\Omega_i t+\Phi_{1i})}+1\right]. \tag{2.18}$$

Donde Ψ_1 y m_{1i} están definidos de igual manera que en el caso de una subportadora. A la salida del modulador de Bob el campo es

$$E_{BOB}(t)\approx\frac{E_{ALICE}(t)}{2}\left[\left(1+e^{j\Psi_2}\right)+\frac{je^{j\Psi_2}}{2}\sum_{i=1}m_{2i}\left(e^{j(\Omega_i t+\Phi_{2i})}+e^{-j(\Omega_i t+\Phi_{2i})}\right)\right], \tag{2.19}$$

donde se ha tomado también la aproximación de baja modulación ($m_1<<1$). Desarrollando esta expresión se llega a

$$E_{BOB}(t)\approx\frac{E_e}{4}\left[\begin{array}{l}\left(1+e^{j\Psi_1}\right)\left(1+e^{j\Psi_2}\right)+j\dfrac{\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}}{2}\sum_{i=1}m_{2i}\left(e^{j(\Omega_i t+\Phi_{2i})}+e^{-j(\Omega_i t+\Phi_{2i})}\right)+\\ j\dfrac{\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}}{2}\sum_{i=1}m_{1i}\left(e^{j(\Omega_i t+\Phi_{1i})}+e^{-j(\Omega_i t+\Phi_{1i})}\right)-\\ -\dfrac{e^{j(\Psi_1+\Psi_2)}}{4}\sum_{l,k=1}^{N}m_{1l}m_{2k}\left\{\left(e^{j(\Omega_l t+\Phi_{1l})}+e^{-j(\Omega_l t+\Phi_{1l})}\right)\left(e^{j(\Omega_k t+\Phi_{2k})}+e^{-j(\Omega_k t+\Phi_{2k})}\right)\right\}\end{array}\right]. \tag{2.20}$$

En esta expresión se puede ver los tres primeros términos son análogos a los de una portadora, mientras que el último término se corresponde con la intermodulación del sistema entre subportadoras.

Se filtra la señal de igual manera que para una subportadora, pero ahora se realiza con N pares de filtros ideales centrados en $\omega_o\pm\Omega_i$. A la salida de estos filtros el campo tiene dos contribuciones no deseadas del término de interferencia, que ocurren cuando las frecuencias Ω_l

y Ω_k cumplen $\Omega_l - \Omega_k = \Omega_i$ y también ocurren cuando las frecuencias Ω_r y Ω_s cumplen $\Omega_r + \Omega_s = \Omega_i$ como muestra la siguiente expresión:

$$E_{\Omega_i}(t) \approx \frac{E_e}{4}\cdot\left[j\frac{\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}e^{j\Phi_{2i}}m_{2i}}{2} + j\frac{\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}e^{j\Phi_{1i}}m_{1i}}{2}\right] -$$
$$-\frac{E_e}{16}e^{j(\Psi_1+\Psi_2)}\left[\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N} m_{1l}m_{2k}e^{j\Delta\Phi_{l,k}} + \sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} m_{1r}m_{2s}e^{j\Sigma\Phi_{r,s}}\right], \tag{2.21}$$

donde se emplean las siguientes definiciones

$$\begin{aligned}\Delta\Phi_{l,k} &= \Phi_{1l} - \Phi_{2k}\\ \Sigma\Phi_{r,s} &= \Phi_{1r} + \Phi_{2s}\end{aligned} \tag{2.22}$$

La intensidad óptica de este campo se puede expresar como

$$I_{\Omega_i} \propto \left|E_{\Omega_i}\right|^2 = I^S_{\Omega_i} + I^{IM}_{\Omega_i}, \tag{2.23}$$

donde el término de la intensidad deseada viene dada por

$$I^S_{\Omega_i} = I_{\max}(m_{1i}, m_{2i}, \Psi_1, \Psi_2)\left[1 + V(m_{1i}, m_{2i}, \Psi_1, \Psi_2)\cos\left(\Delta\Phi_i + \Delta\Psi\right)\right]. \tag{2.24}$$

Este término es exactamente igual al que se obtuvo para una subportadora, donde $I_{\max}(m_{1i}, m_{2i}, \Psi_1, \Psi_2)$, $V(m_{1i}, m_{2i}, \Psi_1, \Psi_2)$, $\Delta\Phi_i$ y $\Delta\Psi$ se definen igual que en el caso anterior. El estudio que se hace de la visibilidad ($V(m_{1i}, m_{2i}, \Psi_1, \Psi_2)$) frente a las fluctuaciones de los parámetros del modulador para una subportadora es perfectamente válido para el caso de N subportadoras.

El término $I^{IM}_{\Omega_i}$ de la expresión (2.23) se corresponde con el término de intermodulación, que viene dado por la expresión

$$\begin{aligned} I^{IM}_{+\Omega_i} &= I^{IM}\\ &-\frac{I_s m}{2\sqrt{2}}\cos\left(\frac{\Delta\Phi_i}{2}\right)\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N}\cos\left(\Delta\Phi_{l,k} - \Delta\Phi_{1,i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right) +\\ &+\frac{I_s m}{2\sqrt{2}}\cos\left(\frac{\Delta\Phi_i}{2}\right)\sum_{\substack{r,s=1\\ \Omega_r-\Omega_s=\Omega_i}}^{N}\cos\left(\Delta\Phi_{r,s} - \Delta\Phi_{1,i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right). \end{aligned} \tag{2.25a}$$

De forma análoga, podemos encontrar el término de intermodulación correspondiente a la banda centrada en $\omega_o - \Omega_i$

$$I_{-\Omega_i}^{IM} = I^{IM} + \frac{I_s m}{2\sqrt{2}} \sin\left(\frac{\Delta\Phi_i}{2}\right) \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \cos\left(\Delta\Phi_{l,k} - \Delta\Phi_{1,i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right) - \frac{I_s m}{2\sqrt{2}} \sin\left(\frac{\Delta\Phi_i}{2}\right) \sum_{\substack{r,s=1 \\ \Omega_r - \Omega_s = \Omega_i}}^{N} \cos\left(\Delta\Phi_{r,s} - \Delta\Phi_{1,i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right). \quad (2.25b)$$

El término común I^{IM} viene dado por

$$I^{IM} = \frac{I_s m^2}{32} \left[\left| \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} e^{j(\Delta\Phi_{l,k})} \right|^2 + \left| \sum_{\substack{r,s=1 \\ \Omega_r + \Omega_s = \Omega_i}}^{N} e^{j(\Sigma\Phi_{r,s})} \right|^2 + 2 \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \sum_{\substack{r,s=1 \\ \Omega_r + \Omega_s = \Omega_i}}^{N} \cos\left(\Delta\Phi_{lk} - \Sigma\Phi_{rs}\right) \right]. \quad (2.26)$$

Se puede observar de (2.26) que la interferencia en ambas bandas no es simétrica. La contribución más importante es proporcional m^3 para algunos valores de $\Delta\Phi_i$ y de m^4 para el resto. Aprovechando el hecho de que Φ_{1l} y Φ_{2k} son variables aleatorias se puede obtener más información acerca de estos valores de intermodulación. Teniendo en cuenta esto $\Delta\Phi_{l,k} = \Phi_{2k} - \Phi_{1l}$ es también una variable aleatoria que puede tomar los valores $\Delta\Phi_{l,k} = \left\{\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi\right\}$ con probabilidad ¼. Lo mismo ocurre con $\Sigma\Phi_{r,s} = \Phi_{2s} + \Phi_{1r}$ que puede tomar los valores $\Sigma\Phi_{r,s} = \left\{\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi\right\}$, al igual que $\Delta\Phi_{l,k} - \Sigma\Phi_{r,s}$ que toma los valores $\Delta\Phi_{l,k} - \Sigma\Phi_{r,s} = \left\{\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi\right\}$ con probabilidad ¼. Con esto se puede calcular los valores esperados de $I_{+\Omega_i}^{IM}$ y $I_{-\Omega_i}^{IM}$, los cuales están detallados en la referencia [17] y cuyo resultado son

$$E\left[I_{+\Omega_i}^{IM}\right] = E\left[I_{-\Omega_i}^{IM}\right] = E\left[I^{IM}\right] = \frac{I_s m^2 N_{CSO}(\Omega_i)}{16}, \quad (2.27)$$

donde N_{CSO} es el número de CSO (composite second order terms)[18]. Se puede observar que tanto la interferencia de la banda superior como la inferior tienen el mismo valor esperado y es independiente de la base elegida por Bob. Esto es debido a que el único término que contribuye en el valor esperado es I^{IM} el cual es definido en (2.27).

El número de CSO (N_{CSO}) depende del número de subportadoras usadas y también de su separación en frecuencia. Por tanto es importante hacer un plan de frecuencias donde se minimice su valor. Es útil definir la magnitud CNR (Carrier to Noise Ratio) [18] que es debida a la intermodulación de segundo orden, nosotros vamos a usar el nombre QCNR (Quantum Carrier to Noise Ratio) que se expresa mediante

$$QCNR_{CSO}^{i} = \frac{I_s}{E\left[I_{-\Omega_i}^{IM}\right]} = \frac{16}{m^2 N_{CSO}(\Omega_i)} \quad . \tag{2.28}$$

Esta magnitud representa el conciente entre la probabilidad de detectar un fotón en la banda positiva con una visibilidad 1 y la probabilidad de detectar un fotón de intermodulación no lineal en la banda negativa. Es importante notar que $QCNR_{CSO}^{i}$ aumenta al disminuir el índice de modulación y el número de canales.

III. BER cuántico y tasa efectiva de transmisión.

El rendimiento de un sistema QKD viene dado por el BER (tasa de error de bit) cuántico o QBER [15]. Después de la discusión de bases entre Alice y Bob, este último formará una clave que contendrá errores. El QBER informa de la cantidad de errores de la clave, ya que es el cociente entre el número de bits erróneos y el número de bits totales. También se puede definir como el cociente entre la probabilidad de fallar un bit y la probabilidad de detectarlo. En esta sección se obtiene una expresión del QBER donde se tiene en cuenta la intermodulación.

Por otra parte, la justificación de la viabilidad de un sistema SCM-QKD debe encontrarse en la tasa efectiva de transmisión de clave. Por tanto, en el último apartado de este capítulo se muestra un estudio sobre ella.

III.1. *Derivación del QBER*

Para obtener una expresión del QBER para nuestro sistema SCM-QKD se usa el método descrito en la referencia [19], adaptándolo a N subportadoras. La probabilidad de que un detector, situado después de un filtro ideal centrado en $\omega_o + \Omega_i$, detecte un fotón tiene tres contribuciones diferentes. La primera proviene de la propia señal detectada que denotaremos por $p_{\exp}^{signal}(\Omega_i)$. La segunda es debida a la intermodulación y la expresaremos como $p_{\exp}^{imd}(\Omega_i)$ y por último la contribución debida a las cuentas oscuras $p_{\exp}^{dark}(\Omega_i)$. La combinación de las tres nos dará la probabilidad total de detectar un fotón que la expresamos como

$$\begin{aligned} p_{\exp}(\Omega_i) &= p_{\exp}^{signal}(\Omega_i) + p_{\exp}^{imd}(\Omega_i) + p_{\exp}^{d}(\Omega_i) - \\ &- p_{\exp}^{signal}(\Omega_i)p_{\exp}^{imd}(\Omega_i) - p_{\exp}^{signal}(\Omega_i)p_{\exp}^{d}(\Omega_i) - p_{\exp}^{imd}(\Omega_i)p_{\exp}^{d}(\Omega_i)' \end{aligned} \tag{3.1}$$

donde se ha asumido que todas las contribuciones son independientes. La probabilidad de que la fuente emita k fotones en la banda Ω_i se representa 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 [18]

$$p_{\exp}^{signal}(\Omega_i) = \sum_{k=0}^{\infty} R_i(k)\left[\sum_{l=1}^{k}\binom{k}{l}(\rho T_L(\Omega_i))^l(1-\rho T_L(\Omega_i))^{l-1}\right] \quad , \tag{3.2}$$

donde $T_L(\Omega_i)$ es la transmitancia del canal de fibra óptica que se puede expresar por [20]

$$T_L(\Omega_i) = 10^{-\frac{\alpha L}{10}}.T_B.T_F(\Omega_i) \quad , \tag{3.3}$$

siendo α el coeficiente de perdidas de la fibra, L la longitud del canal de fibra, T_B es la trasmitancia del modulador de Bob y T_F es la trasmitancia 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

$$p_{\exp}^{imd}(\Omega_i) = \sum_{k=0}^{\infty} I_i(k) \left[\sum_{l=1}^{k} \binom{k}{l} (\rho T_L(\Omega_i))^l (1-\rho T_L(\Omega_i))^{l-1} \right] . \tag{3.4}$$

Por ultimo, la distribución de cuentas oscuras viene dada por

$$p_{\exp}^{d}(\Omega_i) = d_B . \tag{3.5}$$

Como se mencionó anteriormente la fuente pulsada es fuertemente atenuada, por tanto el número de fotones por banda puede considerarse como una distribución de Poisson con media $\overline{\mu}_i$

$$R_i(k) = \frac{e^{-\overline{\mu}_i} (\overline{\mu}_i)^k}{k!} . \tag{3.6}$$

El parámetro $\overline{\mu}_i$ representa el número promedio de fotones por bit.

Introduciendo la expresión (3.6) en (3.2), la probabilidad de detección de señal viene dada por

$$p_{\exp}^{signal}(\Omega_i) = 1 - e^{-\rho T_L(\Omega_i)\overline{\mu}_i} \approx \rho T_L(\Omega_i)\overline{\mu}_i , \tag{3.7}$$

de forma similar, los fotones generados por intermodulación también siguen una distribución de Poisson con media $\overline{\mu}_i^{imd}$

$$I_i(k) = \frac{e^{-\overline{\mu}_i^{imd}} \left(\overline{\mu}_i^{imd}\right)^k}{k!} . \tag{3.8}$$

De acuerdo con los resultados de [17] se obtiene

$$\overline{\mu}_i^{imd} = \overline{\mu}_i \frac{m^2 N_{CSO}(\Omega_i)}{16} = \frac{\overline{\mu}_i}{QCNR_{CSO}^i} , \tag{3.9}$$

por lo que

$$\begin{aligned} p_{\exp}^{imd\_i} &= 1 - e^{-\rho T_L \overline{\mu}_i^{imd}} \approx \rho T_L \overline{\mu}_i^{imd} = \\ &= \left(\frac{N_{CSO}(\Omega_i) m^2}{16} \right) \rho T_L \overline{\mu}_i = \rho T_L \frac{\overline{\mu}_i}{QCNR_{CSO}} \end{aligned} . \tag{3.10}$$

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 mediante

$$p_{visibility}^{error}(\Omega_i) = \frac{(1-V)}{2} p_{\exp}^{signal}(\Omega_i) . \tag{3.11}$$

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

$$p_{dark}^{error\_i} = \frac{d_B}{2}. \tag{3.12}$$

Finalmente la contribución de la intermodulación al error es

$$p_{imd}^{error\_i} = \frac{p_{\exp}^{imd\_i}}{2} \quad . \tag{3.13}$$

Teniendo en cuenta (3.7-3.13) se llega a la siguiente expresión para el QBER

$$QBER(\Omega_i) = \frac{\frac{(1-V)}{2} p_{\exp}^{signal}(\Omega_i) + \frac{d_B}{2} + \frac{p_{\exp}^{imd}(\Omega_i)}{2}}{p_{\exp}^{signal}(\Omega_i)} \quad . \tag{3.14}$$

Esta expresión se puede simplificar si tenemos en cuenta que $d_B<<1$ y también $\rho T_L \overline{\mu}_i << 1$ llegando a

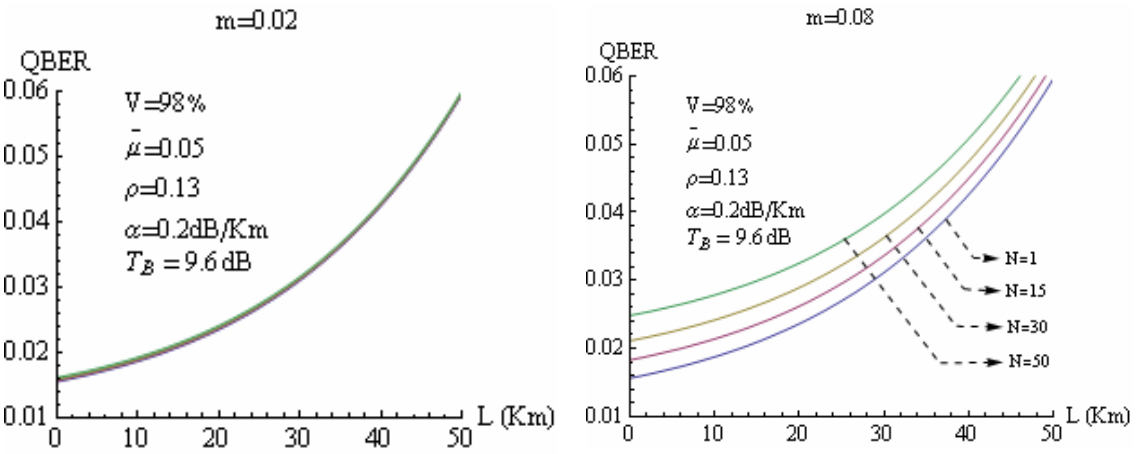
$$QBER(\Omega_i) = \frac{\left\{(1-V) + \left(\frac{1}{QCNR_{CSO}^i}\right)\right\}\rho T_L \overline{\mu}_i + d_B}{2\left[\left\{1 + \left(\frac{1}{QCNR_{CSO}^i}\right)\right\}\rho T_L \overline{\mu}_i + d_B\right]}. \tag{3.15}$$

III.2. *Análisis del QBER*

En este subapartado se va a hacer uso de la expresión (3.15) para hacer un análisis del QBER para diferentes configuraciones del sistema SCM-QKD. Se considera a los moduladores con un ancho de banda de modulación tal que las pérdidas son independientes de la frecuencia de la subportadora. Las figuras 3.1.a y 3.1.b muestran los valores del QBER para distintas longitudes en Km obtenidas para unos planes de frecuencias con un número de subportadoras de N=1, 15, 30 y 50 equiespaciados. Para N=15 las subportadoras están separadas 2GHz entre dos consecutivos y para el resto la separación será de 1GHz. Para realizar estas simulaciones se han tomado los siguientes valores de los parámetros: V=98% eficiencia del detector $\rho = 0.13$, $\alpha = 0.2 dB/Km$ y $T_B = 9.6 dB$.

Se ha cosiderado que N_{CSO} tiene el valor más alto posible para cada plan de frecuencias. El número medio de fotones para cada banda es $\overline{\mu} = 0.05$. En la figura 3.1(a) representamos el valor del QBER cuando el índice de modulación para cada banda es m=0.02. Se puede observar como el impacto de la intermodulación en este caso es despreciable para todos los planes de frecuencias. La situación cambia cuando se aumenta el índice de modulación. La figura 3.1.b representa el QBER para valores del índice de modulación de m=0.08. Podemos observar que en este caso el impacto de la intermodulación es apreciable y afecta más a los sistemas con más subportadoras.

Con estos resultados se observa que el sistema con un índices de modulación de m=0.02 es inmune a la intermodulación.



(a) (b)

Figura 3.1. Evolución del QBER frente a la longitud del canal de fibra para sistemas de N=1, 15, 30 y 50 subportadoras con (a) m=0.02 y (b) m=0.08.

III.3. *Tasa efectiva de bit*

Centraremos ahora nuestra atención en la tasa de de bit que se puede conseguir con SCM-QKD. En principio el objetivo de usar esta técnica es aumentar la tasa de bit alcanzable en un factor N (siendo N el número de subportadoras). En esta sección se describe las condiciones que se deben cumplir para conseguir dicho objetivo.

Para un único canal, la tasa de error de clave, después de que Alice y Bob hayan descartado los bits procedentes de medidas donde no coincidían sus bases, en función de la distancia viene dada por

$$R_{sift}(\Omega_i) = \frac{1}{2}\rho T_L(\Omega_i)\overline{\mu_i} f_{rep}, \tag{3.16}$$

donde f_{rep} es la frecuencia de repetición de pulso de la fuente óptica. Para calcular la tasa de error efectiva en función de la distancia es necesario saber la fracción de bits perdidos debido a la corrección de errores y a la amplificación de privacidad, la cual depende de la estrategia seguida por Eve. Se puede expresar la tasa efectiva de clave como el producto de la tasa de clave y la diferencia entre la información mutua de Alice y Bob $I(A,B,\Omega_i)$ y la información máxima de Shannon de Eve $I^{\max}(A,E,\Omega_i)$; [1]

$$R_{net} = R_{sift}(\Omega_i)\left[I(A,B,\Omega_i) - I^{\max}(A,E,\Omega_i)\right]. \tag{3.17}$$

En el caso que Eve realice ataques a estados, uno después de otro, es decir, ataques individuales, la expresión que se obtiene para la información mutua en términos del QBER es [15]:

$$I(A,B,\Omega_i) = 1 + QBER(\Omega_i)\log_2(QBER(\Omega_i)) + (1 - QBER(\Omega_i))\log_2(1 - QBER(\Omega_i)) \tag{3.18}$$

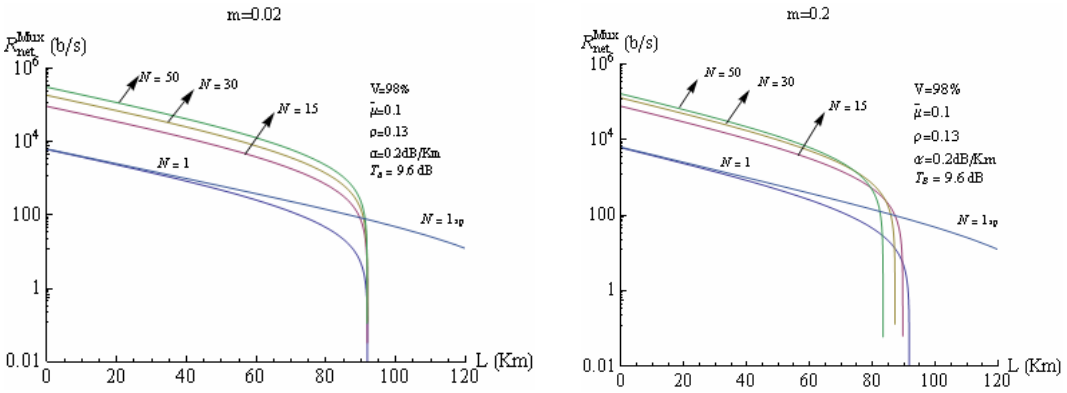
$$I^{\max}(A,E,\Omega_i) = 1 + \left(\frac{1+2\sqrt{QBER(\Omega_i)(1-QBER(\Omega_i))}}{2}\right)\log_2\left(\frac{1+2\sqrt{QBER(\Omega_i)(1-QBER(\Omega_i))}}{2}\right) \left(\frac{1-2\sqrt{QBER(\Omega_i)(1-QBER(\Omega_i))}}{2}\right)\log_2\left(\frac{1-2\sqrt{QBER(\Omega_i)(1-QBER(\Omega_i))}}{2}\right). \tag{3.19}$$

Las ecuaciones (3.16), (3.17) y (3.18) junto con la (3.19) nos permiten obtener una expresión para la tasa de bit en función de la longitud del canal. Para un sistema de multiplexación la tasa de error de bit total efectiva se puede expresar como

$$R_{net}^{MUX} = \sum_{\Omega_i} R_{net}(\Omega_i)\,. \tag{3.20}$$

Con el objetivo de comparar estos resultados con el caso de una sola subportadora, se considera un sistema con los siguientes parámetros típicos: $f_{rep} = 10MHz$, V=98%, eficiencia del detector $\rho = 0.13$, $\alpha = 0.2dB/Km$ y $T_B T_F = 9.6dB$. La evolución de la tasa de bit efectiva total en función de la longitud del canal, para dos valores diferentes del índice de modulación, es representada en las figura 3.2.a y 3.2.b, respectivamente. En cada figura se considera un número de canales de N=50, N=30, N=15, así como N=1, donde se tiene en cuenta dos modos de operación, estados coherentes y un solo fotón por pulso (en este último caso la $f_{rep} = 1MHz$). Todas las curvas tienen un comportamiento similar, con un decrecimiento exponencial al principio y a continuación, debido a la amplificación de privacidad, la tasa decae rápidamente a cero. Las curvas mostradas permanecen paralelas mientras que la longitud del canal no esté cerca del límite impuesto por la amplificación de privacidad.

La comparación entre la tasa efectiva total y la tasa para N=1 nos proporciona la ganancia de multeplexación M_G . En el caso ideal, esta ganancia es N. Los efectos principales del aumento del índice de modulación sobre esta tasa son los siguientes: por un lado la ganancia de multiplexación se reduce de tal manera que $M_G < N$ y por otro lado la longitud del canal a lo largo que M_G permanece constante se reduce.



(a) (b)

Figura 3.2. Tasa de Bit total efectiva frente a la longitud del canal en Km. Obtenida para tres planes de frecuencia (N=15, N=30, N=50) y el caso de una sola subportadora (N=1) para los modos de operación de estados coherentes y 1 fotón por pulso. Con (a) m=2% y (b) m=20%.

Para valores bajos del índice de modulación (m<10%) la tasa efectiva de multiplexación permanece constante e igual a N a lo largo de longitudes de canal de 85 km. Los efectos no lineales no empiezan a ser visibles en la tasa efectiva hasta valores del índice de modulación del 10%. En la figura 3.2.b, la tasa efectiva, así como la longitud del canal que permanece constate, se reducen con respecto al caso del 2%.

La figura 3.3 muestra la evolución de la ganancia de multiplexado en función del índice de modulación para los mismos planes de frecuencias vistos anteriormente.

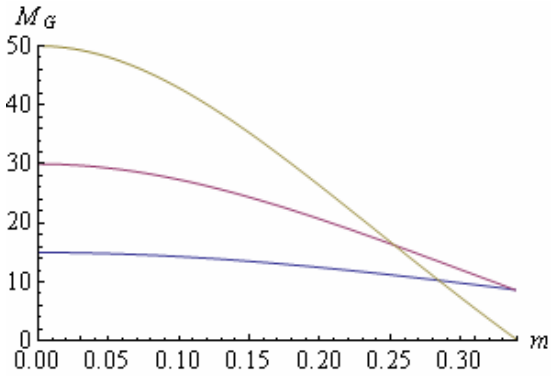


Figura 3.3. Ganancia de multiplexación, frente al índice de modulación, para una longitud del canal de 30Km y los tres planes de frecuencia de N=15 (azul), N=30 (rojo) y N=50 (marrón).

Se pude apreciar cómo la tasa permanece muy cercana al caso ideal para las regiones de baja modulación, en particular, para índices de modulación por debajo del 5%, el sistema es inmune a los efectos no lineales. Más allá de este valor la ganancia decrece más abruptamente en el caso

de N altos. Estos resultados han sido computados para una frecuencia de repetición de pulsos de $f_{rep} = 10MHz$.

En el caso de una frecuencia de repetición de $f_{rep} = 1GHz$ y con un índice de modulación de 0.02 la tasa de bit efectiva para una longitud de 30Km estaría alrededor de 2Mb/s para N=15, 4Mb/s para N=30 y de 7Mb/s para N=50. Estos valores están por encima de los existentes en el estado del arte para el protocolo BB84 (1Mb/s para 20Km [21]).

IV. Medidas experimentales.

El estudio teórico realizado en los apartados anteriores considera la multiplexación de N subportadoras eléctricas en el sistema general mostrado en la figura (2.5). Desde el punto de vista experimental, pasar de la estructura con N=1 que se corresponde con la configuración experimental de Merolla [12] al caso de más de una subportadora (N>1) implica resolver una gran cantidad de problemas asociados a la multiplexación y demultiplexación. Por tanto, la primera configuración experimental que se propone considera una multiplexación con 2 subportadoras eléctricas con una frecuencia de 10GHz y 15GHz. En primer lugar, se muestran las medidas experimentales con el sistema con una sola portadora eléctrica para dos frecuencias de 10 y 15GHz. En segundo lugar, se contrastan estos resultados con las medida de los dos subportadoras de 10 y 15 GHz multiplexados. En esta fase inicial se trabajará en régimen clásico.

IV.1. *Sistema experimental con una subportadora.*

En la figura 4.1 se muestra el esquema experimental para una subportadora eléctrica. El transmisor Alice está formado por una fuente óptica que consiste en un láser cuya longitud de onda es 1548.9 nm con un ancho de banda de 1MHz y una potencia óptica de emisión de 5 dBm. Esta fuente láser se modula externamente mediante un modulador electroópico desbalanceado (Modulador A) polarizado en el punto de cuadratura mediante un voltaje contínuo ψ_1 de 5V. También se le aplica una subportadora de radiofrecuencia generado por un oscilador de 10dBm. A la salida del modulador la señal óptica generada se propaga por un enlace de fibra mantenedora de la polarización de unos pocos metros hasta llegar al receptor Bob. El primer componente del receptor consiste en un modulador electroóptico desbalanceado (Modulador B) el cual tiene una función de transferencia similar al modulador de Alice, con un V_π de 3V pero en este caso se le aplica un voltaje continuo de 8V para polarizarlo en un punto de cuadratura de pendiente contraria ψ_2. También se le aplica una señal de RF generada por un oscilador, de igual frecuencia y potencia que el anterior.

Para controlar los desfases de RF, que generan la interferencia entre las bandas, se usan 2 desfasadores, controlados por un ordenador que permite la elección de Alice entre los cuatro posibles estados (0º, 90º,180º y 270º) así como la elección de Bob de las bases de medida (0º y 90º). Las señales de radiofrecuencia, a la salida de los desfasadores, atraviesan un atenuador que ajusta su amplitud para que los índices de modulación de los dos moduladores sean iguales, condición necesaria para conseguir máxima visibilidad a la hora de implementar el protocolo BB84 como se vio en la sección anterior.

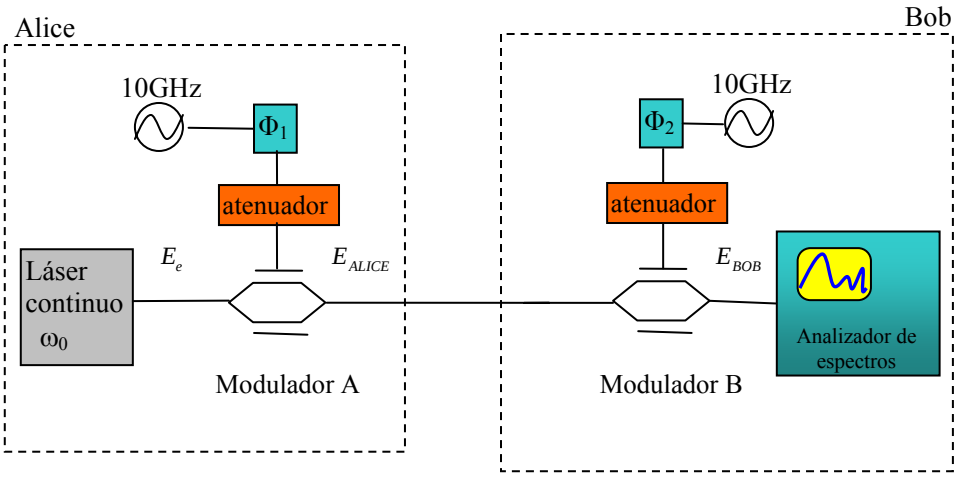


Figura 4.1. Esquema experimental para una subportadora de 10GHz.

Los resultados que se obtienen de la potencia espectral para las diferencias de fase de 0º, 180º, (se aciertan bases) y 90º y 270º (no se aciertan) entre las señales de RF a 10GHz y 15GHz de Bob y Alice se representan en la figura 4.2a y 4.2b.

Cuando las bases coinciden desaparece una de las bandas dependiendo si se transmite un "0" o un "1", pero cuando las bases no coinciden aparecen las dos bandas.

El analizador de espectros afecta considerablemente a la medida ya que tiene una resolución de 0.01nm. Para comprobar la concordancia entre resultados teóricos e experimentales teniendo en cuenta esta resolución, se convoluciona la señal teórica con una función Lorentziana de 0.01nm de ancho y se representa junto a los datos experimentales.

La concordancia es bastante estrecha, apareciendo algunas desviaciones debido al espectro del láser entre las medidas experimentales y los resultados teóricos. Estos resultados demuestran la viabilidad del sistema para implementar el protocolo BB84 [11].

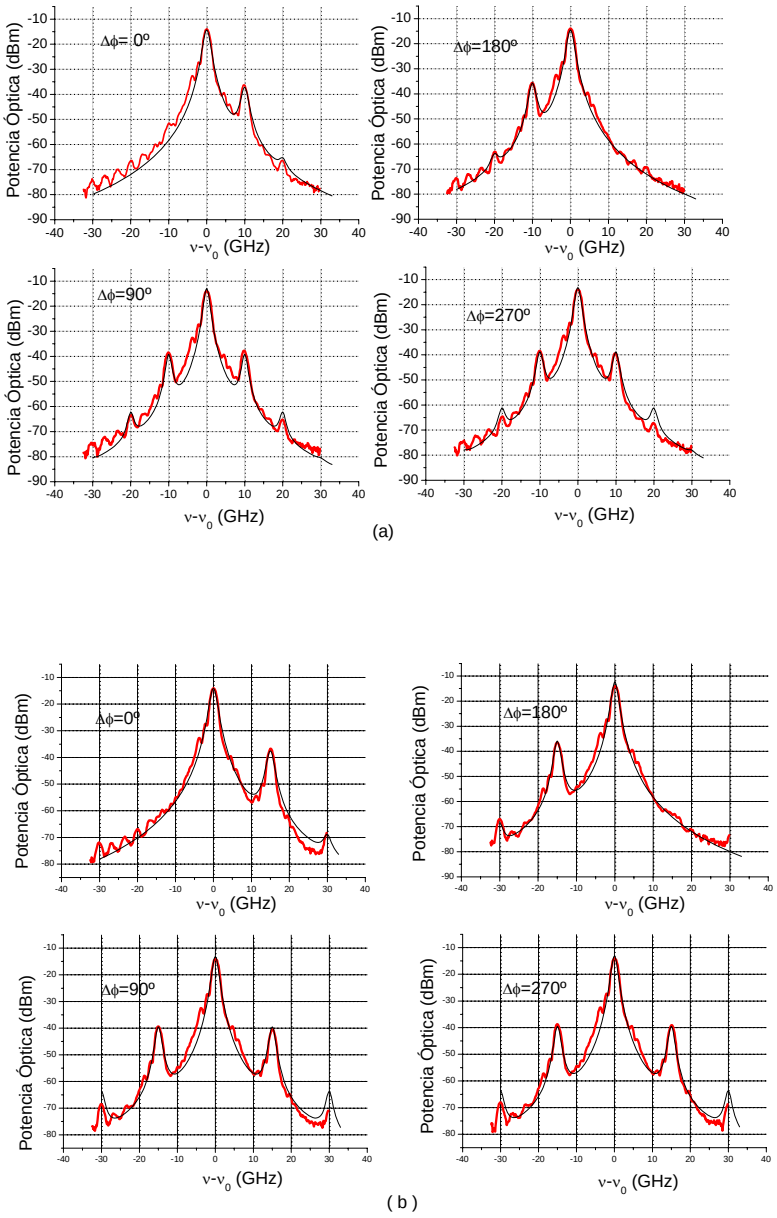


Figura 4.2. Potencia espectral del campo a la salida del modulador de Bob, teórica (en negro) y experimental (en rojo) para las diferencias de fase de las señal de RF de (a) 10GHz y (b) 15GHz de 0º (coinciden bases y Alice transmite un "0"), 90º (no coinciden bases), 180º (coinciden bases y Alice transmite un "1") y 270º(no coinciden bases).

La información de la clave se codifica en los fotones de las bandas laterales. Por lo tanto, para extraer dichos fotones es necesario filtrar estas bandas de tal manera que los procedentes de la portadora, que no llevan información, no afecten las medidas.

En la sección dos y tres se han supuesto filtros con un comportamiento ideal y que solamente dejan pasar la banda deseada. El sistema experimental de filtrado no puede alejarse mucho de

este comportamiento ideal, ya que los fotones que no provengan de la banda de interés producirán una perdida en la visibilidad, conduciendo a un aumento en el QBER.

El filtro tiene que ser capaz de eliminar totalmente la portadora, que se encuentra a unos 30dB por encima de las bandas, por tanto, se propone dos filtros en cascada capaces de conseguir una buena relación de extinción.

La figura 4.3 muestra un diagrama del proceso de filtrado, formado por un Fabry- Perot (FP) en cascada con un red de difracción de Bragg (FBG), trabajando en reflexión, para cada una de las bandas. Los filtros se sintonizan para que pase la banda deseada y para eliminar la porción de portadora que pasa a través del FP. En una primera etapa se filtra la banda inferior, que pasa el FP. El resto del espectro que no pasa el FP es reflejado hacia un circulador que lo dirige a una etapa que filtra la banda superior de la misma manera que se hizo con la inferior. A la entrada del filtro colocamos un aislador para evitar reflexiones.

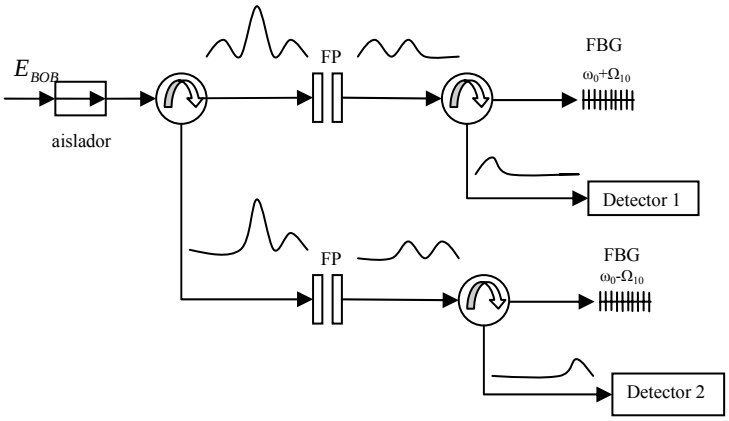
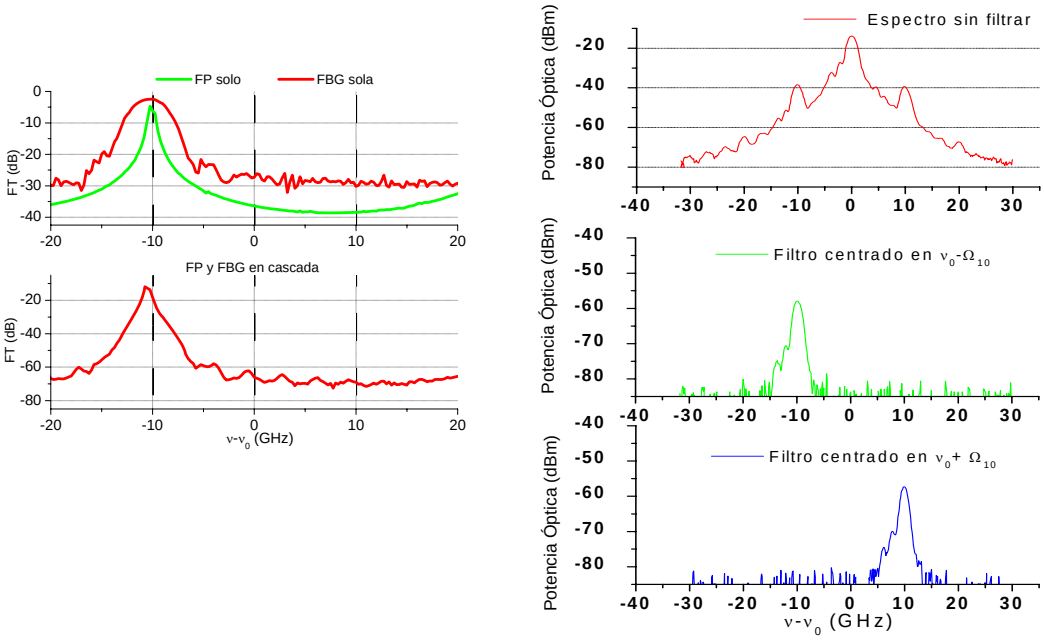


Figura 4.3. Esquema del sistema de filtrado para las dos bandas laterales cuando modulamos la luz con una portadora de RF.

La figura 4.4.a muestra la función de transferencia experimental del FP y la FBG en cascada. En este caso los filtros están preparados para filtrar la banda de -10GHz. Los puntos más interesantes están en 0GHz (portadora) y en 10GHz (banda contraria). Todos estos puntos están por debajo de los 60dB. En la figura 4.4.b se muestra cómo quedan las bandas después del filtrado, estas se encuentran a unos 30dB del nivel del ruido del analizador, nivel que no supera la portadora.

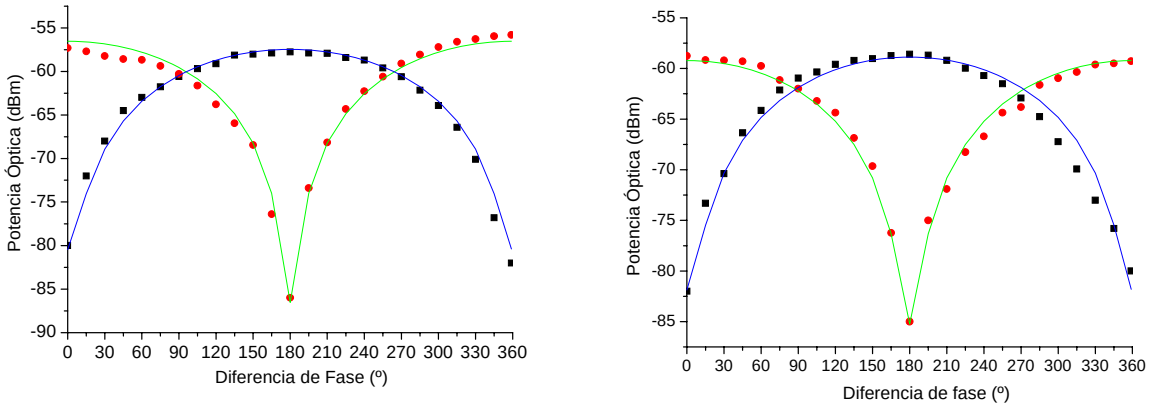


(a) (b)

Figura 4.4. (a) Función de transferencia del FP y la FBG en reflexión y (b) espectros de potencia antes y después de filtrar las bandas.

Para saber si nuestro sistema de filtrado es válido se puede medir la intensidad de cada una de las bandas en función del desfase, y de esta manera obtener una medida experimental de la visibilidad, de donde inferiremos dicha validez. La figura 4.5a muestra estos valores para cada una de las bandas a 10GHz. De esta figura, usando la ecuación (2.11), obtenemos un valor de la visibilidad de V = 0.99.

Para el caso de 15GHz, la figura 4.5b muestra los valores obtenidos de las potencias de las bandas, en este caso obtenemos para la visibilidad el valor V=0.99.



(a) (b)

Figura 4.5. Intensidad de las bandas experimentales (línea de puntos) y teórica (línea continua) cuando modulamos con una subportadora de (a) 10GHz y (b) 15GHz en función de la diferencia de fase de las señales de RF.

Ambas medidas de visibilidad superan el 98%, por tanto nuestro sistema de una subportadora se puede usar para QKD, como ya hizo Merolla [12], para señales de RF de 10GHz y 15GHz.

IV.2. *Sistema con 2 subportadoras.*

Una vez mostradas las dificultades experimentales a la hora de desarrollar un sistema con una subportadora y cómo superarlas, se está ya en disposición de desarrollar un sistema experimental con 2 subportadoras. La dificultad experimental reside en la multiplexación de estas subportadoras, ya que será necesario doblar algunos de los componentes del sistema con las consiguientes complicaciónes del esquema experimental. Por otro lado, se ha visto en la teoría como el comportamiento con varias subportadoras es similar al de dos subportadoras por separado, salvo una serie de nuevos términos de intermodulación.

En esta sección se presentan las medidas obtenidas con 2 subportadoras, así como una ampliación del sistema de filtrado para una subportadora, viendo que los resultados obtenidos de visibilidad son los mismos que con las 2 subportadoras por separado.

La figura 4.6 muestra un esquema del montaje experimental.

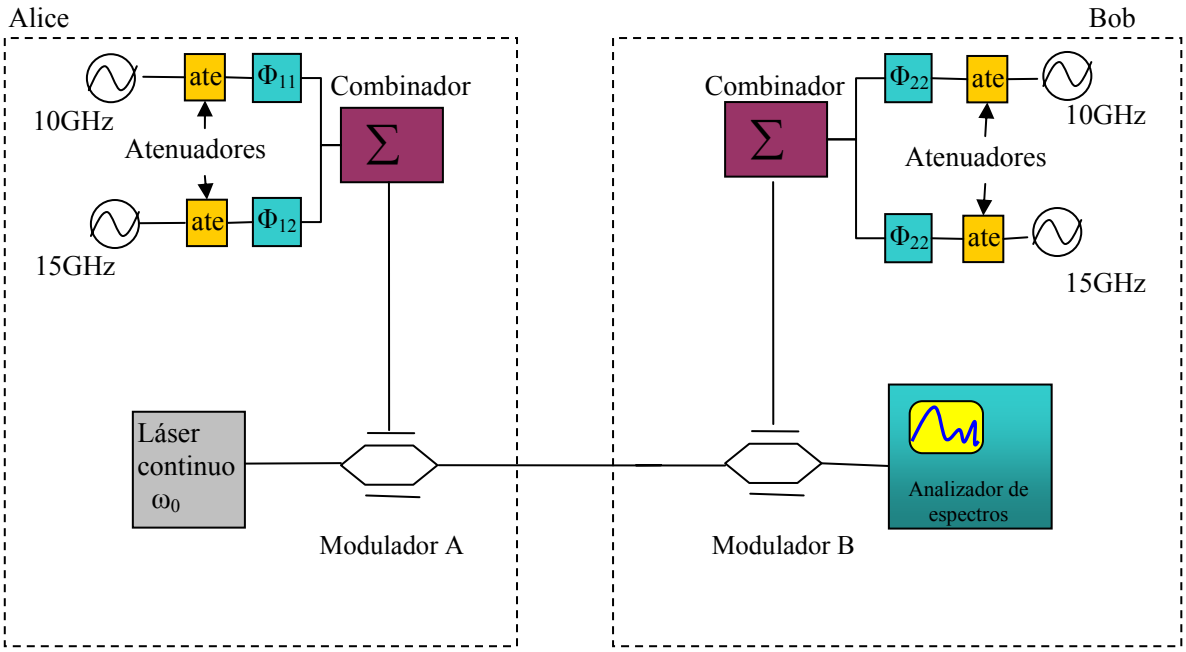


Figura 4.6. Esquema del sistema experimental con 2 subportadoras de RF.

Los espectros ópticos para las distintas diferencias de fase de las subportadoras de 10GHz y 15GHz se pueden observar en la figura 4.7. Los resultados obtenidos se corresponden con las simulaciones, donde también se han tenido en cuenta la resolución del analizador de espectros.

Vemos que es similar al de una sola subportadora, pero esta vez se usan 4 osciladores, dos para Bob y otros dos para Alice, los cuales se suman (multiplexado) para obtener un sistema SCM, que es la novedad de nuestro sistema. A si mismo se usan 4 desfasadores que desfasan la señal de 4 subportadoras de radiofrecuencia generadas por 4 osciladores, codificando los bits de la misma forma que con una subportadora.

También se usan 4 atenuadores (ate) para ajustar los índices de modulación, uno por cada oscilador. El láser sigue siendo el del caso anterior, al igual que los moduladores.

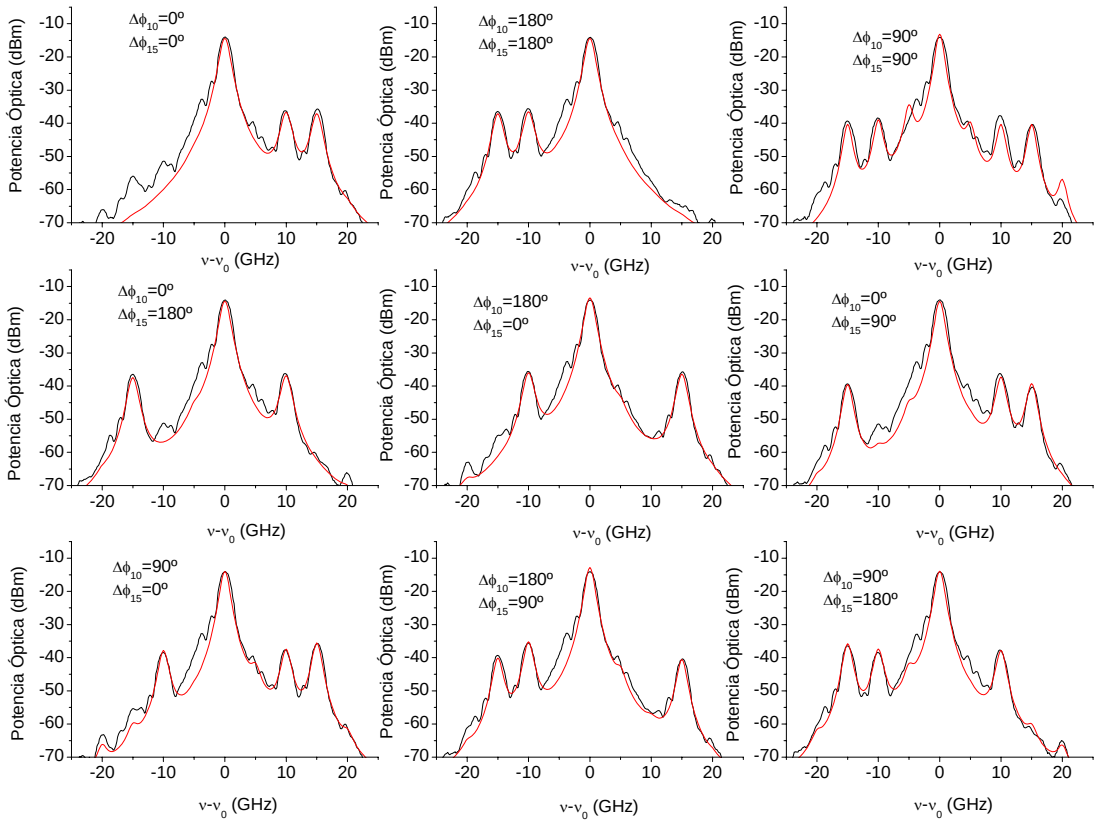
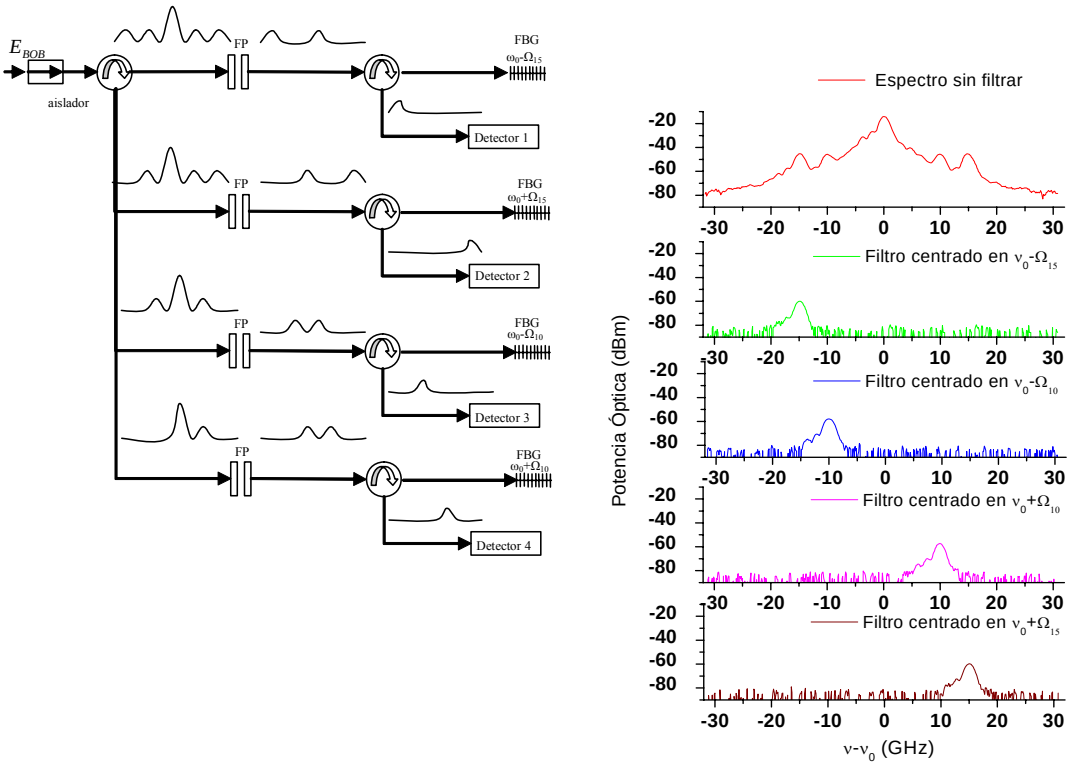


Figura 4.7. Potencia espectral a la salida del modulador de Bob, teórica (en rojo) y experimental (en negro), para el sistema SCM- QKD, para las diferencias de fase de 0º (se aciertan bases y Alice envía un "0"), 90º (no se aciertan bases), 180º (se aciertan bases y Alice envía un "1") y 270º (no se aciertan bases) de las señales de RF de 10GHz y 15GHz.

Para obtener medidas de visibilidad se tiene que desarrollar nuevamente un sistema de filtrado para las bandas de interés. La figura 4.8.a muestra el esquema de este sistema. La base de su funcionamiento es el mismo que en el caso de una subportadora, pero esta vez se necesitan 2 etapas más, ya que tenemos en total 4 bandas en vez de 2. Dos filtros Fabry-Perot, al igual que dos FBG, estarán sintonizados para las bandas de 10GHz y los otros 2 para las bandas de 15GHz.

En la figura 4.8.b se puede observar como el sistema de filtros selecciona correctamente cada una de las 4 bandas, siendo inapreciable la portadora óptica, así como las bandas contiguas. La potencia total de cada uno de los espectros que se muestran en esta figura será la que los detectores medirán, por eso es importante conseguir que la aportación de las otras bandas y la portadora sea despreciable y de esta manera el QBER no se vea afectado.

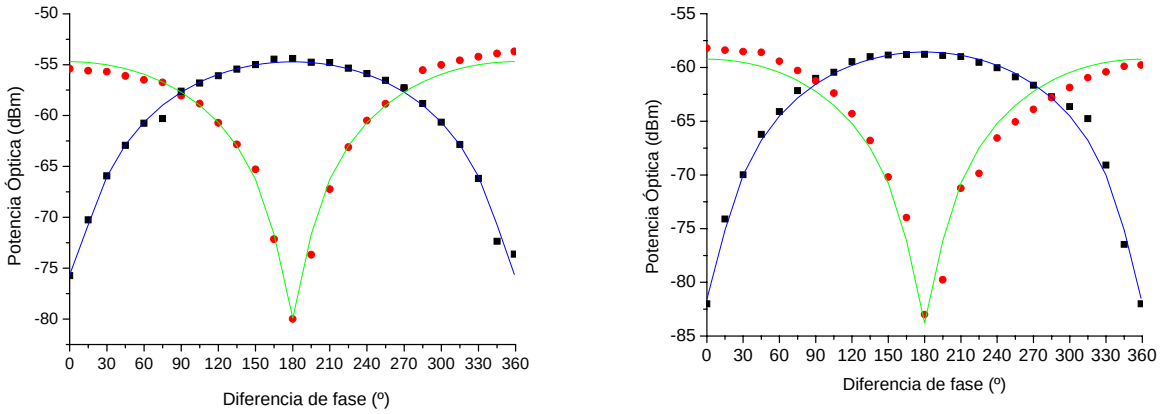


(a) (b)

Figura 4.8. (a) Esquema del sistema de filtrado de las cuatro bandas laterales y (b) espectros de potencia antes y después de filtrar las bandas.

Con este sistema de filtrado se puede medir la potencia de las bandas en función del desfase de las señales de RF. La figura 4.9.a y 4.9.b muestra dichas medidas, con las que obtenemos los valores de visibilidad de V = 0.99 para 10GHz y 15GHz, respectivamente.

Los resultados obtenidos coinciden con los anteriores, cuando se modula la luz con las subportadoras por separado. Por tanto, podemos afirmar que los términos de intermodulación y el crosstalk no afectan a nuestro sistema, consecuentemente el sistema previsto es válido para SCM- QKD.



(a) (b)

Figura 4.9. Intensidad de las bandas experimentales (línea de puntos) y teórica (línea continua) cuando modulamos con 2 subportadoras sumados de (a) 10GHz y (b) 15GHz en función de la diferencia de fase de las señales de RF.

Por último, mostramos algunos ejemplos de las bandas filtradas para las diferencias de fase de 0º y 180º de las subportadoras de 10GHz y 15GHz, es decir, el equivalente a trasmitir un "0" o un "1" cuando Alice y Bob aciertan en la elección de base. De esta manera se aprecia mejor visualmente como la potencia detectada, tras pasar los filtros correspondientes, proviene de la banda de interés.

Cuando la diferencia de fase de las señales de RF a 10GHz es de 0º (se transmite un "0") el detector 4 recibe la potencia de la banda a +10GHz mientras que el detector 3 no recibe señal (figura 4.10.a). Cuando la diferencia de fase es de 180º (se transmite un "1"), ocurre el caso inverso, es decir recibimos señal en el detector 3 y ruido en el 4 (figura 4.10.b).

Por otro lado, cuando la diferencia de fase de las señales de RF a 15GHz es de 0º (se transmite un "0") es el detector 2 el que recibe señal mientras que el 1 ruido (figura 4.10.c) y cuando la diferencia de fase es de 180º (se transmite un "0") el caso contrario (figura 4.10.d).

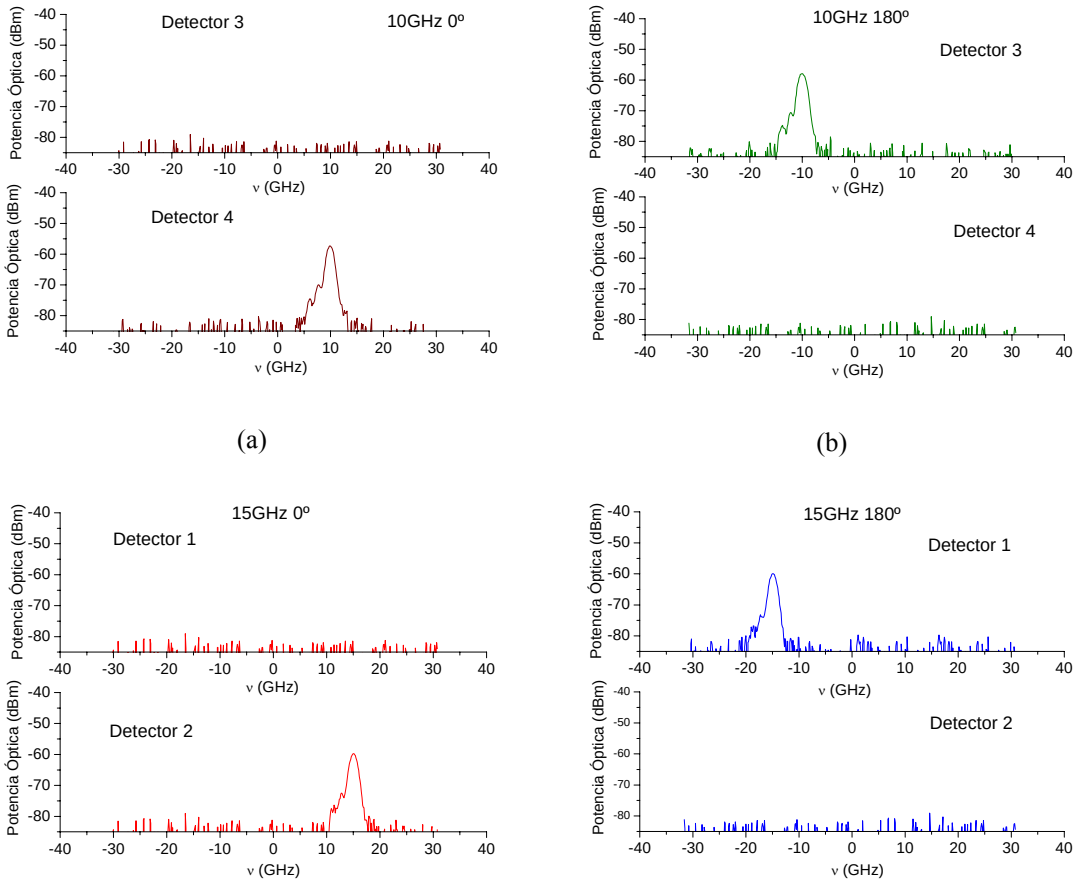


Figura 4.10. Potencia espectral que llega a los detectores para los casos de una diferencia de fase de 0º y 180º entre las señales de RF de 10GHz (a y b) y 15GHz (c y d).

V. Conclusiones y líneas futuras

V.1. *Conclusiones*

Para finalizar el trabajo procedemos a comentar las principales contribuciones que se han obtenido a lo largo de las secciones anteriores. En primer lugar, se ha contextualizado el trabajo presentado dentro del campo de la seguridad en los sistemas de comunicaciones. Se ha descrito brevemente el estado del arte de los sistemas de distribución de clave cuántica (QKD) mostrando sus limitaciones en la tasa de bit y proponiendo el uso de la tecnología SCM para mejorarla.

En el segundo apartado, se ha llevado a cabo el desarrollo teórico para una subportadora eléctrica obteniendo una expresión para la visibilidad, cuya expresión también es valida para N subportadoras, en función de los parámetros del sistema, mostrando su sensibilidad frente a desviaciones de éstos. También se han obtenido expresiones de la intensidad óptica detectada para el caso de N subportadoras, donde aparece un nuevo término equivalente de intermodulación que da cuenta de la interferencia entre los distintos canales cuánticos.

En el tercer apartado, se han derivado las expresiones para la tasa de error de bit cuántico o QBER para N subportadoras incorporando el término de intermodulación. Se ha mostrado que el QBER obtenido al transmitir N canales es igual al caso de una subportadora en condiciones de baja modulación, ya que el efecto de las interferencias en esta aproximación puede llegar a ser despreciable. También se ha derivado una expresión para la tasa de bit efectiva que demuestra que bajo condiciones de modulación pequeña la tasa de tranmisión de clave puede incrementarse un factor N.

Finalmente, en el cuarto apartado se han presentrado los primeros resultados experimentales del sistema implementado. En primer lugar, se han mostrado los resultados con una sola subportadora (10GHz ó 15GHz), a través de medidas de la potencia espectral y viendo que reproducen correctamente nuestro modelo teórico. Desarrollando un primer sistema de filtrado con un FP y una FBG, que nos ha permitido extraer las bandas de interés, alcanzando valores de visibilidad del 99% que permiten el correcto funcionamiento para distribuir la clave. También, se ha desarrollado un sistema SCM con dos subportadoras a 10GHz y 15GHz superando las dificultades experimentales de la multiplexación. Se ha ampliado el sistema de filtrado, para su funcionamiento con 2 subportadoras, que ha permitido medir valores de visibilidad del 99%. Demostrando que la intermodulación no afecta al sistema, indicando que nuestro sistema de filtrado funciona correctamente.

VI.2. *Líneas futuras*

En el trabajo presentado se ha demostrado experimentalmente la viabilidad del sistema, trabajando en régimen clásico. La línea de trabajo tiene que continuar con el fin de poder operar en régimen cuántico para permitir la transmisión real de la clave segura. Esto implica el desarrollo de una fuente pulsada fuertemente atenuada así como detectores capaces de contar fotones. También, se requerirá el desarrollo de un sistema de control que permita la generación de números aleatorios que corresponderán con la el estado cuántico de los fotones enviados por Alice, así como la base de medida de Bob. También el sistema debe ser capaz de sincronizarse correctamente, para que Bob sepa cuándo tiene que realizar las medidas y a qué bit corresponden. En segundo término, cabe la posibilidad de realizar estudios experimentales para conocer cuál es la máxima distancia de transmisión que permite el sistema SCM-QKD al tener que incorporar sistemas adicionales de control de la dispersión y polarización. Por ultimo, se plantea simular ataques al sistema y ver cómo afecta al QBER.

Los resultados que se obtengan de estos puntos, así como nuevas ideas y propuestas, se enmarcarán en un trabajo de investigación que pretende dar cómo fruto una tesis doctoral.

AGRADECIMIENTOS

Este trabajo esta enmarcado dentro del proyecto financiado por el gobierno de España a través del llamado Consolider Quantum Optical Information Technology (QOIT). Además también se quiere agradecer al programa "Ajudes per a la realització de projectes precompetitius de I+D per a equips d'investigació" GVPRE/2008/250 soportado por la Generalitat Valenciana y PROMETEO 2008/092 MICROWAVE PHOTONICS un programa de excelencia llevado a cabo también por la Generalitat Valenciana.

A título personal me gustaría agradecer la ayuda prestada por mis compañeros del Grupo de Comunicaciones Ópticas y Cuánticas del ITEAM así como a las personas que me han dirigido; Jose Capmany y José Mora sin cuya ayuda no hubiera sido posible la realización de este trabajo.

A Pilar, mi familia y amigos

BIBLIOGRAFÍA

[1] V. Scarani, H.Bechmann- Pasquinucci, N.J. Cerf, N. Lütkenhaus, M. Peev, "*The security of practical quantum key distribution",* Reviews of modern physics **81**, 1301-1310 (2009).

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

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

[4] P.D. Townsend, D.J.D. Phoenix, K.J. Blow and S. Cova, "*Design of quantum cryptography Systems for passive optical Networks"*, Electron. Lett., **30**, 1875-1876 (1994).

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

[6] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue and Y. Yamamoto, *"Differential phase shift quantum key distribution over 105 km fibre"*, New J. Phys. Vol. **7**, pp. 1-12, 2005.

[7] H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki and Y. Yamamoto, "*Quantum Key distribution over a 40-dB channel loss using superconducting single-photon detectors"*, Nature Photonics **1**, 343-348 (2007).

[8] K. Inoue, E. Waks and Y. Yamamoto, "*Differential phase shift quantum key distribution"*, Phys. Rev. Lett. **89** (037902) (2002).

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

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

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

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

[13] Xavier, G.B.; von der Weid, J.-P., "*Modulation schemes for frequency coded quantum key distribution"*, Electronics Letters **41**, 607-608 (2005).

[14] O. Guerreau, J-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer, and 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] N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, "*Quantum Cryptography"* , Rev. Mod. Phys. **74**, 145-195 (2002).

[16] A. Yariv and P. Yeh, "*Photonics: Optical Electronics in Modern Communications"*, 6th Edition, Oxford University Press, Oxford, UK (2006).

[17] J. Capmany, A. Ortigosa- Blanch, José 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).

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

[19] N. Lütkenhaus "*Security against individual attacks for realistic quantum key distribution"*, Phisical Review A **61,** (052304) (2000).

[20] J.W. Goodman, "*Statistical Optics"*, John Wiley & Sons, New York, 1985.

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

[22] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue and Y. Yamamoto, "Differential phase shift quantum key distribution over 105 km fibre", New J. Phys. **7**, 1-12 (2005).

ANEXOS

[1] 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).

[2] **A. Ruiz-Alba**, J. Mora, J. Capmany, W. Amaya, A. Ortigosa-Blanch, "*Experimental Demonstration of Subcarrier Multiplexed Quantum Key Distribution*, International Topical Meeting on Microwave Photonics", paper TH 4.42 (2009).

Analysis of Subcarrier Multiplexed Quantum Key Distribution Systems: Signal, Intermodulation, and Quantum Bit Error Rate

José Capmany, *Fellow, IEEE*, Arturo Ortigosa-Blanch, José Mora, Antonio Ruiz-Alba, Waldimar Amaya, and Alfonso Martínez

***Abstract*—This paper provides an in-depth theoretical analysis of subcarrier multiplexed quantum key distribution (SCM-QKD) systems, taking into account as many factors of impairment as possible and especially considering the influence of nonlinear signal mixing on the end-to-end quantum bit error rate (QBER) and the useful key rate. A detailed analysis of SCM-QKD is performed considering the different factors affecting the sideband visibility (drifts in the modulator bias points, modulation index mismatch between Alice and Bob subcarriers) and the impact of nonlinear signal mixing leaking into otherwise void subcarrier sidebands. In a similar way to classical photonic radio-over-fiber telecommunication and cable TV systems, the impact of this nonlinear signal mixing can be accounted in terms of a quantum carrier to noise ratio that depends on the specific frequency plan that is implemented. QBER and useful key rate results for three different frequency plans featuring $N = 15$ (low-count channel system), $N = 30$ (intermediate-count channel system), and $N = 50$ (high-count channel system) channels are provided, showing that photon nonlinear mixing can be of importance in middle- and high-count SCM-QKD systems ($N > 30$), with moderate RF modulation indexes ($m > 5\%$). In practical terms, nonlinear signal mixing can be neglected if low modulation indexes ($m < 2\%$) are employed to encode the photons in the subcarrier sidebands.**

***Index Terms*—Optical fiber communications, quantum information, quantum key distribution (QKD), subcarrier multiplexing.**

I. Introduction

QUANTUM cryptography features a unique way of sharing a random sequence of bits between users with a certifiable security not attainable with either public or secret-key classical cryptographic systems [1], [2]. This is achieved by means of quantum key distribution (QKD) techniques. In essence, QKD relies on exploiting the laws of quantum mechanics that are often viewed in other contexts of physics as limiting or negative [3].

The objective of QKD systems is to distribute a key between a transmitter (Alice) and a receiver (Bob) with complete confidentiality. To achieve this, Alice (the sender) and Bob (the receiver) encode their bits as states of a quantum system, also known as qubits. If a third party or eavesdropper (usually known as Eve) measures the qubits sent by Alice to Bob, she will modify their quantum states and produce a considerable number of errors that will be detected by Alice and Bob, allowing them to disregard the key. At the same time, the eavesdropper will not be able to make a perfect copy of the sequence (without actually measuring the key before Alice and Bob finish their public discussion) to prevent from being detected, as this is not allowed by the noncloning theorem [4].

A limitation of QKD systems, which is still under research, is the fact that the useful bit rates for key exchange are very low, ranging from a few bits per second to some tens of kilobits per second [3]. An interesting approach to increase these figures relies on exploiting the well-known multiplexing techniques employed in optical communication systems to allow the delivery of N different keys using the N available channels in the multiplex. The N keys can be either treated independently by Bob or assembled to distill a key with an effective bit rate N times larger. This simple engineering approach becomes a challenge when working with quantum systems. The system should work in parallel but its security should still be guaranteed by the principles of quantum mechanics, both when Alice prepares the photons and when Bob "measures" the incoming states. At the same time, the multiplexing technique should be safe to Eve, gaining any information that may result in a tradeoff between multiplexing and security.

Photonics has proved to be one of the principal enabling technologies for long-distance QKD using optical fiber links. Four main different photonic-based techniques have been reported in the literature for implementing QKD. In 1992, Bennett *et al.* [5] proposed to exploit the polarization of photons to implement the four required states by employing one circular polarization and one linear polarization basis. The main disadvantage of this method resides on the difficulty of preserving the polarization over long lengths of standard telecommunication fibers. Nevertheless, the elegant plug and play approach proposed in [6] overcomes most of the aforementioned limitations. Furthermore, recent results have reported the successful operation of this technique at higher data rates [7]. The second approach, initially developed by Townsend and coworkers [8]–[10], relies on the use of optical delays and balanced interferometers at the transmitter and the receiver. The main challenge of this approach resides in keeping the interferometers free from environmental

Manuscript received February 6, 2009; revised August 3, 2009 and August 18, 2009. First published November 10, 2009; current version published December 3, 2009. This work was supported in part by the Spanish Government through Quantum Optical Information Technology, a CONSOLIDER-INGENIO 2010 Project, and in part by the Generalitat Valenciana through the PROMETEO 2008/092 Research Excellency Award.

The authors are with the Optical and Quantum Communications Group, Institute of Telecommunications and Multimedia, Universidad Politécnica de Valencia, Valencia 46021, Spain (e-mail: jcapmany@iteam.upv.es; ortigosa_art@gva.es; anruiz@iteam.upv.es; walamoc@doctor.upv.es; alfonsomg@dcom.upv.es).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTQE.2009.2031065

and mechanical variations, and preserving the matching of the path difference at the transmitter and the receiver. A third approach, based on differential phase shift QKD [11], has enabled secure key generation and distribution along distances over 100 km [12], [13].

The fourth approach, proposed by Merolla and coworkers [14], also known as frequency coding, relies on encoding the information bits on the sidebands of either phase [15] or amplitude [16] RF-modulated light. The coding principles of subcarrier multiplexing are widely employed in the field of microwave photonics [17] for a variety of applications, including remote antenna beam steering and the optical processing of microwave signals [18]. Alice randomly changes the phase of the electrical signal used to drive a light modulator among four phase values $0,\ \pi$, and $\pi/2,\ 3\pi/2$, which form a pair of conjugated bases. When it arrives at Bob, he modulates the signal again using the same microwave signal frequency, and thus, his new sidebands will interfere with those created by Alice [14]. Over the past few years, the work done by Merolla *et al*. has led to substantial improvements in this kind of system. Originally used for implementing the Bennett 1992 (B92) protocol [14], [19], it was subsequently improved by adjusting the modulator characteristics that let them demonstrate the implementation of the Bennett–Bassard 1984 (BB84) protocol [2], [20], [21].

The approaches described before have yield different state-of-the-art rates and distances for key distribution. For instance, the highest bit rate system currently demonstrated for the BB84 protocol exchanges secure keys at 1 Mbit/s (over 20 km of optical fiber) and 10 kbit/s (over 100 km of fiber) [22], in combination with the technique of decoy states [23]. For the differential phase-shift keying (DPSK) approach, the current record values yield rates of 17 kbit/s over 105 km of optical fiber [12] and 12 bit/s over 200 km [13]. These rates can still be considered the modest, so there is an increasing interest and effort in the development of techniques that can increase the current state-of-the-art values.

The useful key bit rates achieved by means of frequency coding can be considerably increased by incorporating into the system a multiplexing technique widely employed in microwave photonics [17] and known as subcarrier multiplexing (SCM) to provide parallel QKD. In [24], we have proposed the extension of frequency coding to multiple subcarriers, showing that it opens the possibility of parallel quantum key distribution, and therefore, of a potential substantial improvement in the bit rate of such systems. The concept behind subcarrier multiplexed QKD (SCM-QKD) can be explained by referring to Fig. 1, where parallel and serial detection schemes are, respectively, depicted.

A faint-pulse laser source emitting at frequency ω_o is externally modulated by *N* RF subcarriers by Alice. Each subcarrier, generated by an independent voltage-controlled oscillator (VCO), is randomly phase-modulated among four possible values $0,\ \pi$ and $\pi/2,\ 3\pi/2$ which, as aforementioned, form a pair of conjugated bases. The compound signal is then sent through an optical fiber link and, on reaching Bob's location, is externally modulated by *N* identical subcarriers in a second modulator. These subcarriers are phase-modulated between two possible values, 0 and $\pi/2$, which represent the choice between

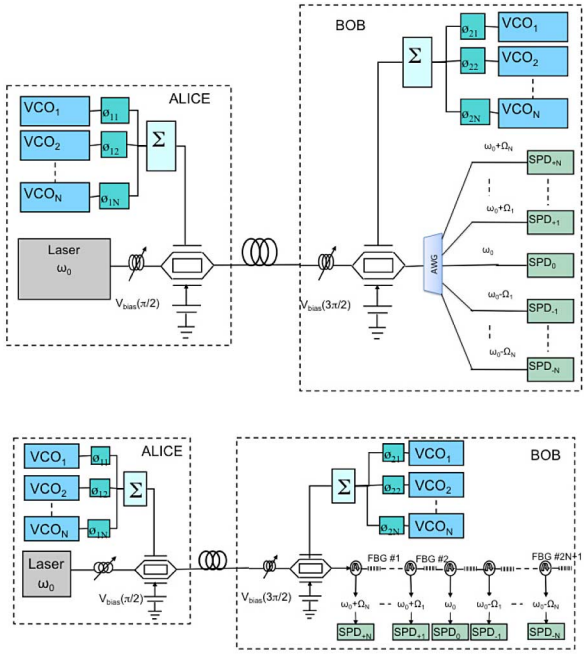


Fig. 1. System layout of an *N* channel subcarrier multiplexed quantum key distribution systems. (Top) Parallel detection/filtering scheme using an AWG device. (Bottom) Serial detection/filtering scheme using FBGs. SPD_N stands for the photon counter placed after the filter selecting the Ω_N subcarrier.

the two encoding bases. As a consequence, an interference signal is generated at each of the sidebands (upper and lower) of each subcarrier.

For a given subcarrier $\Omega_i = 2\pi f_i$, if Bob and Alice's bases match, then the photon will be detected with probability 1 by either the detector placed after the filter centered at $\omega_o + \Omega_i$ or by the detector placed after the filter centered at $\omega_o - \Omega_i$. If, on the contrary, Bob and Alice's bases do not match, there will be an equal probability of 1/2 of detecting the single photon at any of the two detectors, and this detection will be discarded in a subsequent procedure of public discussion.

The advantages of SCM-QKD, however, come at a price. System design is expected to be more demanding, and especially, the impact of nonlinear signal mixing by harmonic distortion and intermodulation needs to be thoroughly addressed. The purpose of this paper is precisely to provide an in-depth theoretical analysis of SCM-QKD systems, taking into account as many factors of impairment as possible, and especially considering the influence of nonlinear signal mixing on the end-to-end quantum bit error rate (QBER).

The paper is organized as follows. Section II provides a classical analysis of the SCM-QKD configuration, which is useful from an engineering point of view since it outlines the main basic factors of limitation. The thorough analysis of SCM-QKD systems is carried out in Section III, where we sequentially consider the different factors affecting the sideband visibility (drifts in the modulator bias points, modulation index mismatch between Alice and Bob subcarriers) and the impact of nonlinear signal mixing leaking into otherwise void subcarrier sidebands. In a similar way to classical photonic radio-over-fiber

telecommunication [25] and cable TV (CATV) systems [26], the impact of this nonlinear signal mixing can be accounted in terms of a quantum carrier to noise ratio (QCNR) that depends on the specific frequency plan that is implemented. For the purpose of illustrating the impact of this factor, we consider three different frequency plans featuring $N = 15$, 30, and 50 channels. The analysis of the impact of nonlinear signal mixing alone and in combination with visibility and average photon number on the system performance is carried out in Section IV, where we consider its impact on the system QBER. For this purpose, a new expression for the QBER is derived that takes into account the photon nonlinear mixing. The results show that this effect can be of importance in middle- and high-count SCM-QKD systems ($N > 30$) with moderate RF modulation indexes ($5\% < m$). In practical terms, nonlinear signal mixing can be neglected if low modulation indexes ($m < 2\%$) are employed to encode the photons in the subcarrier sidebands. The section concludes with a discussion on other practical issues that limit the bit rate performance of these systems, in particular, the bandwidth of the external modulators and the characteristics of the optical filters. The summary and conclusions of the paper presented in Section V. Throughout this paper, we consider the use of the BB84 protocol, although our results can be easily extended to the B92 protocol.

II. System Analysis

A. General Expressions

Referring to the configuration of the SCM-QKD system shown in Fig. 1 (top) (parallel detection) or Fig. 1 (bottom) (serial detection), we assume that Alice employs a standard monochromatic continuous wave (CW), linearly polarized (in the *x*-direction) laser providing an input intensity to the system given by $I_e = |E_e|^2$ and emitting at an optical carrier ω_o. This signal is fed to a single drive electrooptic modulator, which modulates the CW carrier according to an input voltage signal that includes the dc bias voltage to the modulator V_{dc1} and *N* different and independently phase-encoded subcarriers, each one having an RF Ω_i, an amplitude V_{1i}, and a different random phase code Φ_{1i}[1] [27]

$$V(t) = -V_{\mathrm{dc1}} - \sum_{i=1}^{N} V_{1i} \cos\left(\Omega_i t + \Phi_{1i}\right). \tag{1}$$

The output signal from Alice's modulator is given by

$$E_{\mathrm{ALICE}}(t) = \frac{\hat{x}E_e}{2}\left[e^{j\Psi_1} e^{\,j\sum_{i=1}^{N} m_1 \cos(\Omega_i t+\Phi_{1i})} + 1\right] \tag{2}$$

where $\hat{x}$ represents the direction of the electric field polarization vector and Ψ_1 represents the normalized (to the quadrature voltage V_π) bias voltage, which is given by

$$\Psi_1 = \frac{V_{\mathrm{dc1}}\pi}{V_\pi}. \tag{3}$$

In addition, we define the modulation index (assumed equal for all the subcarriers) as

$$m_1 = \frac{2V_1\pi}{V_\pi}. \tag{4}$$

Our next step is to assume that the modulation indexes of the individual subcarriers will be low enough, so we can approximate the exponential function by a first-order polynomial as follows:

$$\begin{aligned} &E_{\mathrm{ALICE}}(t) \\ &\approx \frac{\hat{x}E_e}{2}\left[1 + je^{j\Psi_1}\left(1 + \sum_{i=1}^{N} m_1 \cos\left(\Omega_i t + \Phi_{1i}\right)\right)\right] \\ &= \frac{\hat{x}E_e}{2}\left[\left(1 + e^{j\Psi_1}\right) + \frac{je^{j\Psi_1}}{2}\sum_{i=1} m_1 \left(e^{j(\Omega_i t+\Phi_{1i})}\right.\right. \\ &\qquad \left.\left. + e^{-j(\Omega_i t+\Phi_{1i})}\right)\right]. \end{aligned} \tag{5}$$

This field is also the input field to the fiber optic link. A case of interest is when the phase-shift contribution from the fiber chromatic dispersion can be neglected. In practice, this can be achieved by incorporating these values into the data or bias phase shifts to obtain optimum operation conditions (see [16], eq. (11)]) or by employing a dispersion compensation scheme. In this way, we do not include the dispersion effects.

The output field from the optical fiber link inputs Bob's electrooptic modulator, which we assume to work in the same way as Alice's. Thus,

$$\begin{aligned} E_{\mathrm{BOB}}(t) \approx \frac{E_{\mathrm{ALICE}}(t)}{2}\Bigg[&\left(1 + e^{j\Psi_2}\right) + \frac{je^{j\Psi_2}}{2} \\ &\times \sum_{i=1} m_2 \left(e^{j(\Omega_i t+\Phi_{2i})} + e^{-j(\Omega_i t+\Phi_{2i})}\right)\Bigg]. \end{aligned} \tag{6}$$

In the previous expression, Ψ_2, m_2, and Φ_{2i} have a similar meaning as their equivalents in Alice's modulator, which have been previously defined. However, in this case, the individual phase modulation parameter Φ_{2i} at each subcarrier reflects the choice of base made by Bob and can take the values 0 or $\pi/2$.

Introducing (5) into (6), we get (7), as shown at the bottom of the next page.

Upon leaving Bob's modulator, the content of each channel is measured by a pair of filters. For instance, to observe the results corresponding to the key carried by Ω_i, we place two optical filters centred at $\omega_o \pm \Omega_i$. The output of each filter is then sent to a photodetector or a photon counter.

We will now evaluate the output of each filter, taking into account that due to the nonlinear nature of the signal beating at the second modulator and the photodetector, both harmonic distortion and intermodulation products can fell within the filter bandpass altogether with the desired key information.

[1]In the BB84 protocol, Φ_{1i} can take the following values: 0, π, $-\pi/2$ and $\pi/2$ and reflects the choice of basis made by Alice to encode the |0> and |1> states.

B. Signal Detected at the Output of the Filter Centered

If an ideal optical filter centered at $\omega_o \pm \Omega_i$ at the output of Bob's modulator, the filter will select the desired information regarding the key carried by subcarrier Ω_i, but it will also select undesired contributions arising from the beating terms [fourth term in (7)]. Two undesired contributions are envisaged: those arising from frequencies Ω_l and Ω_k such that $\Omega_l - \Omega_k = \Omega_i$ and those arising from frequencies Ω_r and Ω_s such that $\Omega_r + \Omega_s = \Omega_i$. Therefore, the output optical field from the filter for the upper sideband is given by

$$E_{\Omega_i}(t) \approx \frac{E_e e^{j\Omega_i t}}{4}\left[j\frac{\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}e^{j\Phi_{2i}}m_2}{2} + j\frac{\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}e^{j\Phi_{1i}}m_1}{2}\right] - \frac{E_e e^{j\Omega_i t}}{16}e^{j(\Psi_1+\Psi_2)}\left[\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N} m_1 m_2 e^{j\Delta\Phi_{l,k}} + \sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} m_1 m_2 e^{j\Sigma\Phi_{r,s}}\right]. \quad (8)$$

In the previous expression, we have employed the following definitions:

$$\Delta\Phi_{l,k} = \Phi_{1l} - \Phi_{2k}$$
$$\Sigma\Phi_{r,s} = \Phi_{1r} + \Phi_{2s}. \quad (9)$$

The intensity detected at the (upper sideband) filter output can be expressed as follows:

$$I_{+\Omega_i} \propto |E_{+\Omega_i}|^2 = I^S_{+\Omega_i} + I^{\mathrm{IM}}_{+\Omega_i}. \quad (10)$$

In the previous expression, $I^S_{+\Omega_i}$ is the intensity corresponding to the desired (key) signal while $I^{\mathrm{IM}}_{+\Omega_i}$ denotes the undesired signal that leaks into the filter bandpass.

The desired signal is given by

$$I^S_{+\Omega_i} = I_{\max}(m_1, m_2, \Psi_1, \Psi_2) \times \left[1 + V(m_1, m_2, \Psi_1, \Psi_2)\cos\left(\Delta\Phi_i + \Delta\Psi\right)\right] \quad (11)$$

where we define the following parameters:

$$I_{\max}(m_1, m_2, \Psi_1, \Psi_2) = \frac{|E_e|^2}{16}\left[m_1^2\cos^2(\Psi_2/2) + m_2^2\cos^2\left(\frac{\Psi_1}{2}\right)\right]$$
$$V(m_1, m_2, \Psi_1, \Psi_2) = \frac{2m_1 m_2\cos(\Psi_1/2)\cos(\Psi_2/2)}{m_1^2\cos^2(\Psi_2/2) + m_2^2\cos^2(\Psi_1/2)}$$
$$\Delta\Phi_i = \Phi_{2i} - \Phi_{1i}$$
$$\Delta\Psi = \frac{(\Psi_2 - \Psi_1)}{2}. \quad (12)$$

Following a similar filtering procedure for the lower sideband, the intensity detected at the filter output can be expressed as

$$I_{-\Omega_i} \propto |E_{-\Omega_i}|^2 = I^S_{-\Omega_i} + I^{\mathrm{IM}}_{-\Omega_i}. \quad (13)$$

Again, in the previous expression, $I^S_{-\Omega_i}$ is the intensity corresponding to the desired (key) signal while $I^{\mathrm{IM}}_{-\Omega_i}$ denotes the undesired signal that leaks into the filter bandpass. The desired signal is given by

$$I^S_{-\Omega_i} = I_{\max}(m_1, m_2, \Psi_1, \Psi_2) \times \left[1 + V(m_1, m_2, \Psi_1, \Psi_2)\cos\left(\Delta\Phi_i - \Delta\Psi\right)\right]. \quad (14)$$

The undesired signal leaking into the selected sideband can be expressed as follows (15), as shown at the bottom of the next page.

Equations (10)–(15) are the central results of this general classical analysis. Although the results are quite general, we will apply them to gain insight into the system behavior for several cases of practical interest, where simplifying assumptions can be made which render simpler results.

III. Signal and Intermodulation in a Practical System

At this point, we shall assume that the modulation indexes for all the subcarriers are equal in Alice and Bob's modulators, i.e., $m_1 = m_2 = m$. As in [16], we further set the following biasing points for the modulators: $\Psi_1 = \pi/2$ (negative slope quadrature bias point) and $\Psi_2 = 3\pi/2$ (positive slope quadrature bias point). Finally, the random phase chosen by Bob for each subcarrier is given by $\Phi_{2i} + \pi/2$, rather than by Φ_{2i}, so in the earlier equations, the following replacements have to be done: $\Delta\Phi_i \to \Delta\Phi_i + \pi/2$, $\Delta\Phi_{l,k} \to \Delta\Phi_{l,k} - \pi/2$, and $\Sigma\Phi_{r,s} \to \Sigma\Phi_{rs} + \pi/2$.

A. Signal Analysis When Bob Chooses the Correct Base or the Incorrect Base

According to the previous considerations, the desired signals at each sideband are given by

$$I^S_{+\Omega_i} = \frac{|E_e|^2 m^2}{16}\left[1 + \cos\left(\Delta\Phi_i\right)\right] = I_S\cos^2\left(\frac{\Delta\Phi_i}{2}\right)$$
$$I^S_{-\Omega_i} = \frac{|E_e|^2 m^2}{16}\left[1 - \cos\left(\Delta\Phi_i\right)\right] = I_S\sin^2\left(\frac{\Delta\Phi_i}{2}\right). \quad (16)$$

$$E_{\mathrm{BOB}}(t) \approx \frac{E_e}{4}\left[\begin{array}{l}\left(1+e^{j\Psi_1}\right)\left(1+e^{j\Psi_2}\right) + j\frac{\left(1+e^{j\Psi_1}\right)e^{j\Psi_2}}{2}\sum_{i=1} m_2\left(e^{j(\Omega_i t+\Phi_{2i})} + e^{-j(\Omega_i t+\Phi_{2i})}\right)\\ \quad + j\frac{\left(1+e^{j\Psi_2}\right)e^{j\Psi_1}}{2}\sum_{i=1} m_1\left(e^{j(\Omega_i t+\Phi_{1i})} + e^{-j(\Omega_i t+\Phi_{1i})}\right)\\ \quad - \frac{e^{j(\Psi_1+\Psi_2)}}{4}\sum_{l,k=1}^{N} m_1 m_2\left(e^{j(\Omega_l t+\Phi_{1l})} + e^{-j(\Omega_l t+\Phi_{1l})}\right)\left(e^{j(\Omega_k t+\Phi_{2k})} + e^{-j(\Omega_k t+\Phi_{2k})}\right)\end{array}\right]. \quad (7)$$

The correct choice of base by Bob for subcarrier Ω_i results in either $\Delta\Phi_i = 0$ or $\Delta\Phi_i = \pi$, depending on whether a "0" or a "1" is sent by Alice. This, in turn, implies, according to (16), that the lower or upper sideband is eliminated, respectively, due to interference. When Bob chooses the incorrect basis, then $\Delta\Phi_i = \pm\pi/2$ and therefore none of the sidebands is eliminated.

B. Visibility Versus Fluctuations in the Modulator Bias Points and the Modulation Indexes

Equation (16) is obtained under the assumption of perfect visibility ($V = 1$), which results from the modulator biasing and equal modulation indexes conditions stated before. In practice, small deviations can be expected in both which can affect the visibility at a given subcarrier frequency channel. For instance, if the phase of Alice's modulator fluctuates a quantity $\delta\Psi_1 \Rightarrow \Psi_1 = \pi/2 + \delta\Psi_1$ and there is a relative subcarrier modulation index mismatch δm between Alice and Bob's modulators [for example, $m_1 = m$, $m_2 = m\,(1+\delta m)$], then the visibility is given by

$$V(\delta m, \delta\Psi_1) = \left| \frac{2\,(1+\delta m)\,[\cos(\delta\Psi_1/2) - \sin(\delta\Psi_1/2)]}{1+(1+\delta m)^2 - 2\cos(\delta\Psi_1/2)\sin(\delta\Psi_1/2)} \right|. \tag{17}$$

The Fig. 2 (top) shows the 2-D surface plot of (17) versus the fluctuations in the modulation index and the bias phase of Alice's modulator. Note that visibility is quite robust against modulation index mismatches (fluctuations of $\delta m = \pm 0.2$ form the optimum biasing point result in a negligible variation of the visibility). On the other hand, it is more sensitive to phase deviations (especially, positive phase deviations) from the optimum biasing point of Alice's modulator.

A similar behavior is observed if the phase of Bob's modulator fluctuates a quantity $\delta\Psi_2 \Rightarrow \Psi_2 = 3\pi/2 + \delta\Psi_2$ and there is a relative subcarrier modulation index mismatch δm between Alice and Bob's modulators [for example, $m_1 = m$, $m_2 = m\,(1+\delta m)$]. The results are shown in Fig. 2 (bottom), where a 2-D surface plot is again depicted. This time for the visibility versus the fluctuations in the modulation index and the bias phase of Bob's modulator. The behavior in relation to the modulation index fluctuations is similar to the previous case, while the visibility is very sensitive to negative phase deviations from Bob's modulator ideal biasing point.

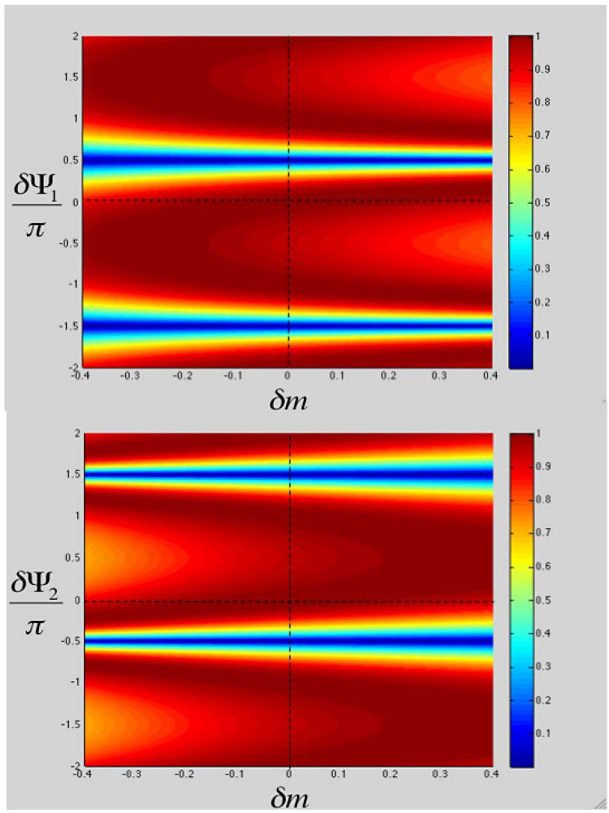


Fig. 2. (Top) 2-D surface plots of (22) versus the fluctuations in the modulation index and the bias phase of Alice's modulator. (Bottom) 2-D surface plots of the visibility versus the fluctuations in the modulation index and the bias phase of Bob's modulator.

C. Interference Analysis When Bob Chooses the Correct and Incorrect Bases

As far as interference is concerned, we will examine the signal leaking into the upper and lower sidebands. The undesired

$$\begin{aligned} I^{\mathrm{IM}}_{\pm\Omega_i} = {} & \frac{|E_e|^2}{256}\left[\left|\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N} m_1 m_2 e^{j\Delta\Phi_{l,k}}\right|^2 + \left|\sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} m_1 m_2 e^{j\Sigma\Phi_{r,s}}\right|^2\right] \\ & + \frac{|E_e|^2}{128}\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N}\ \sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} m_1 m_2 m_1 m_2 \cos(\Delta\Phi_{lk} - \Sigma\Phi_{rs}) \\ & \pm \frac{|E_e|^2}{32}\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N} m_1 m_2 \left[\begin{array}{l} m_2\cos\left(\frac{\Psi_1}{2}\right)\sin\left(\Delta\Phi_{lk} - \Phi_{2i} \pm \frac{\Psi_1}{2}\right) \\ \quad + m_1\cos\left(\frac{\Psi_2}{2}\right)\sin\left(\Delta\Phi_{lk} - \Phi_{1i} \pm \frac{\Psi_2}{2}\right) \end{array}\right] \\ & \pm \frac{|E_e|^2}{32}\sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} m_1 m_2 \left[\begin{array}{l} m_2\cos\left(\frac{\Psi_1}{2}\right)\sin\left(\Sigma\Phi_{rs} - \Phi_{2i} \pm \frac{\Psi_1}{2}\right) \\ \quad + m_1\cos\left(\frac{\Psi_2}{2}\right)\sin\left(\Sigma\Phi_{rs} - \Phi_{1i} \pm \frac{\Psi_2}{2}\right) \end{array}\right]. \end{aligned} \tag{15}$$

intermodulation signals for each subcarrier channel can be written as follows:

$$I^{\mathrm{IM}}_{+\Omega_i} = I^{\mathrm{IM}} - \frac{I_S m}{2\sqrt{2}} \cos\left(\frac{\Delta\Phi_i}{2}\right) \times \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \cos\left(\Delta\Phi_{lk} - \Phi_{1i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right) + \frac{I_S m}{2\sqrt{2}} \cos\left(\frac{\Delta\Phi_i}{2}\right) \sum_{\substack{r,s=1 \\ \Omega_r + \Omega_s = \Omega_i}}^{N} \cos\left(\Sigma\Phi_{rs} - \Phi_{1i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right) \tag{18a}$$

$$I^{\mathrm{IM}}_{-\Omega_i} = I^{\mathrm{IM}} + \frac{I_S m}{2\sqrt{2}} \sin\left(\frac{\Delta\Phi_i}{2}\right) \times \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \cos\left(\Delta\Phi_{lk} - \Phi_{1i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right) - \frac{I_S m}{2\sqrt{2}} \sin\left(\frac{\Delta\Phi_i}{2}\right) \sum_{\substack{r,s=1 \\ \Omega_r + \Omega_s = \Omega_i}}^{N} \cos\left(\Sigma\Phi_{rs} - \Phi_{1i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right) \tag{18b}$$

where the common term I^{IM} is given by

$$I^{\mathrm{IM}} = \frac{I_s m^2}{32} \left[\left| \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} e^{j\Delta\Phi_{l,k}} \right|^2 + \left| \sum_{\substack{r,s=1 \\ \Omega_r + \Omega_s = \Omega_i}}^{N} e^{j\Sigma\Phi_{r,s}} \right|^2 + 2 \sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \sum_{\substack{r,s=1 \\ \Omega_r + \Omega_s = \Omega_i}}^{N} \cos\left(\Delta\Phi_{lk} - \Sigma\Phi_{rs}\right) \right]. \tag{19}$$

We can observe from (18) that the interference in both sidebands is not symmetric. Furthermore, as the reader can observe, the term proportional to *m* can vanish, and therefore, the most important contribution here is proportional to m^2, depending of the chosen base by Bob, which is determined by the value of $\Delta\Phi_i$. Thus, interference is, in principle, expected to be one order of magnitude smaller.

To proceed further, we must have more information regarding $\Delta\Phi_{l,k}$ and $\Sigma\Phi_{r,s}$. Since Φ_{1l} is a random variable and so is Φ_{2k}, then $\Delta\Phi_{l,k} = \{-\pi/2, 0, \pi/2, \pi\}$, each value with a uniform probability of 1/4.

A similar argument applies to $\Sigma\Phi_{r,s} = \Phi_{2s} + \Phi_{1r}$, with $\Sigma\Phi_{r,s} = \{-\pi/2, 0, \pi/2, \pi\}$, each value with a uniform probability of 1/4. Finally, for $\Delta\Phi_{l,k} - \Sigma\Phi_{r,s}$, we have $\Delta\Phi_{l,k} - \Sigma\Phi_{r,s} = \{-\pi/2, 0, \pi/2, \pi\}$, again each value with a uniform probability of 1/4. These considerations are identical, regardless of Bob chooses the correct or incorrect base.

We can now compute the expected values for the interference terms corresponding to $I^{\mathrm{IM}}_{+\Omega_i}$ and $I^{\mathrm{IM}}_{-\Omega_i}$. For simplicity, we have included the theoretical development in Appendix A. We can find a simple expression of the expected value for the interference terms, which is given by

$$E\left[I^{\mathrm{IM}}_{+\Omega_i}\right] = E\left[I^{\mathrm{IM}}_{-\Omega_i}\right] = E\left[I^{\mathrm{IM}}\right] = \frac{I_e m^2 N_{\mathrm{CSO}}(\Omega_i)}{16} \tag{20}$$

where N_{CSO} is defined as the number of composite second-order terms N_{CSO}.

First, we observe that both interference terms corresponding to the lower and upper sidebands have an identical expected value that is independent on the base chosen by Bob. Indeed, it is determined by the expected value of the term I^{IM}, which is defined in (19). It is due to the fact that the rest of the terms in (18) have a null expected value. Indeed, considering the procedure results derived in Appendix A, it is straightforward to show that

$$E\left[\sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \cos\left(\Delta\Phi_{lk} - \Phi_{1i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right)\right] = 0 \tag{21}$$

$$E\left[\sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} \cos\left(\Sigma\Phi_{lk} - \Phi_{1i} - \frac{\Delta\Phi_i}{2} - \frac{\pi}{4}\right)\right] = 0. \tag{22}$$

It is interesting to emphasize that the expected value of the interference terms is symmetrical and independent on the base chosen by Bob. Therefore, the expected values of both interference terms are proportional to m^2 and the number of composite second-order terms N_{CSO}.

The number of composite second-order terms N_{CSO} depends on the number of subcarriers employed in the system and also on their frequency spacing. It is composed of the sum of harmonic distortion terms and intermodulation terms. Fig. 3 shows, as an example, the frequency spectrum, number of harmonic distortion terms $N_{\mathrm{CSOHD}}(\Omega_i)$, number of intermodulation terms $N_{\mathrm{CSOU}}(\Omega_i) + N_{\mathrm{CSOD}}(\Omega_i)$, and overall CSO number $N_{\mathrm{CSO}}(\Omega_i)$ for a frequency plan composed of 15 evenly spaced (by 2 GHz) channels spanning from 2 to 30 GHz, representative of a low-count frequency plan. Along the rest of this paper, we will also consider an intermediate channel count frequency plan composed of 30 evenly spaced (by 1 GHz) channels spanning from 1 to 30 GHz and a high-channel count frequency plan composed of 50 evenly spaced (by 1 GHz) channels spanning from 1 to 50 GHz. In practical terms, as it will be discussed in the next section, only the low-channel count option is feasible with the current state-of-the-art technology of commercial optical filters and external modulators, but it is envisaged that middle term developments in these technologies will enable the implementation of intermediate and high-channel count systems. The number of composite second-order terms is different for each channel frequency Ω_i with a maximum number obtained in the

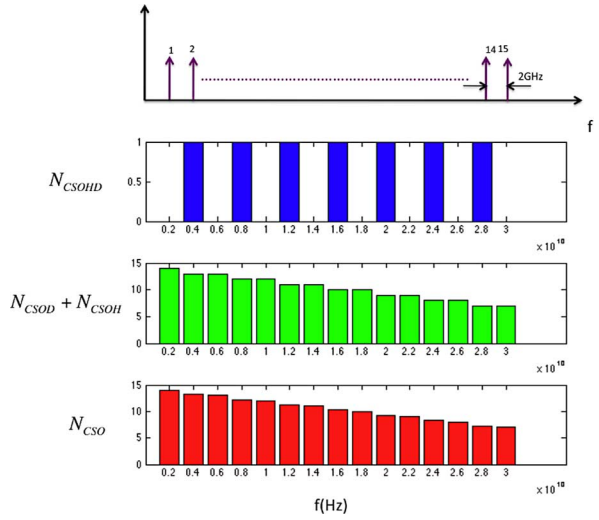


Fig. 3. Frequency spectrum, number of harmonic distortion and intermodulation terms, and overall CSO number $\mathrm{NCSO}(\Omega_i)$ for a frequency plan composed of 15 evenly spaced channels spanning from 2 to 30 GHz.

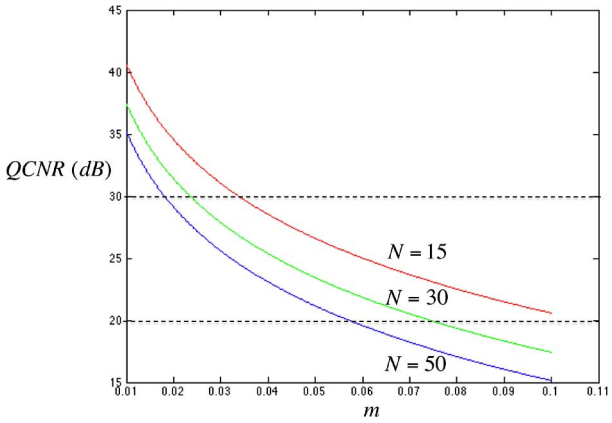


Fig. 4. $\mathrm{QCNR}^i_{\mathrm{CSO}}$ as a function of the modulation index for the three frequency plans described in the text (low, intermediate, and high counts).

lowest frequency channel, which is roughly equal to the number N of channels[2] in the frequency plan.

In analogy with classical systems, it is useful to define a carrier to noise ratio [29] due to composite second-order intermodulation. In this case, we will use the name QCNR, which is given by

$$\mathrm{QCNR}^i_{\mathrm{CSO}} = \frac{I_S}{E\left[I^{\mathrm{IM}}_{\pm\Omega_i}\right]} = \frac{16}{m^2 N_{\mathrm{CSO}}\left(\Omega_i\right)}. \tag{23}$$

This quantity represents the ratio between the probability of detecting a linear photon in the upper sideband for visibility 1 and the probability of detecting a nonlinear photon due to intermodulation in the lower sideband. Fig. 4 plots the value of the $\mathrm{QCNR}^i_{\mathrm{CSO}}$ as a function of the modulation index for the three frequency plans previously described. As expected, it decreases for increasing number of channels and increasing values of the modulation index. For instance, for a minimum value of $\mathrm{QCNR}^i_{\mathrm{CSO}} = 20$ dB, the maximum allowable modulation index is 5.8% in the $N = 50$ frequency plan, $m = 7.5\%$ for the $N = 30$ frequency plan, and $m = 10.5\%$ for the $N = 15$ frequency plan. These values are reduced to 1.9%, 2.5%, and 3.4%, respectively, if a $\mathrm{QCNR}^i_{\mathrm{CSO}} = 30$ dB is targeted.[3]

IV. Quantum Bit Error Rate

The overall performance of the QKD system is given by the QBER. For SCM systems, we have to consider the influence of the intermodulation and harmonic distortion terms as outlined in [30].

A. Derivation of the QBER Expression

To derive a suitable QBER expression for SC-QKD systems, we follow the approach of [31] specialized for each subcarrier channel. At the detector placed after the optical filter selecting the Ω_i channel, the probability that Bob detects a signal has three sources: one coming from the detection of signal photons $p^{\mathrm{signal}}_{\mathrm{exp}}(\Omega_i)$, another coming from the detection of intermodulation photons $p^{\mathrm{imd}}_{\mathrm{exp}}(\Omega_i)$, and finally, those arising from the dark counts of the specific photodetector placed at the output of the filter that selects the subcarrier Ω_I, $p^{d}_{\mathrm{exp}}(\Omega_i)$. The combination of these three sources gives

$$\begin{aligned} p_{\mathrm{exp}}(\Omega_i) = {} & p^{\mathrm{signal}}_{\mathrm{exp}}(\Omega_i) + p^{\mathrm{imd}}_{\mathrm{exp}}(\Omega_i) + p^{d}_{\mathrm{exp}}(\Omega_i) \\ & - p^{\mathrm{signal}}_{\mathrm{exp}}(\Omega_i) p^{\mathrm{imd}}_{\mathrm{exp}}(\Omega_i) - p^{\mathrm{signal}}_{\mathrm{exp}}(\Omega_i) p^{d}_{\mathrm{exp}}(\Omega_i) \\ & - p^{\mathrm{imd}}_{\mathrm{exp}}(\Omega_i) p^{d}_{\mathrm{exp}}(\Omega_i) + p^{\mathrm{signal}}_{\mathrm{exp}}(\Omega_i) p^{\mathrm{imd}}_{\mathrm{exp}}(\Omega_i) p^{d}_{\mathrm{exp}}(\Omega_i). \end{aligned} \tag{24}$$

We assume that, for each subcarrier, the three sources are independent. Let $R_i(k)$ represent the probability that the source sends k photons at subcarrier Ω_i, then the probability that Bob's detector placed after the filter selecting Ω_i is triggered by a signal photon can be expressed in terms of the detector efficiency ρ and the end-to-end optical link transmission efficiency $T_L(\Omega_i)$[4] as

$$p^{\mathrm{signal}}_{\mathrm{exp}}(\Omega_i) = \sum_{k=0}^{\infty} R_i(k) \left[\sum_{l=1}^{k} \binom{k}{l} \left(\rho T_L(\Omega_i)\right)^l \left(1 - \rho T_L(\Omega_i)\right)^{l-1} \right]. \tag{25}$$

In a similar way, if $I_i(k)$ represents the probability that the source produces k photons that leak as intermodulation at subcarrier Ω_i, then the probability that Bob's detector placed after

[2]It is a common practice in CATV industry [29] to take this worst-case value to evaluate the performance of the whole frequency plan in terms of second-order distortion, and we will follow this approach here when plotting the results of the QBER in the next section. In other words, $\mathrm{NCSO}(\Omega_i) = \mathrm{NCSO}_{\max}$ for all Ω_i.

[3]That is, the probability of detecting a linear photon is 1000 times that of detecting a nonlinear photon generated by intermodulation or harmonic distortion.

[4]The transmission efficiency can be expressed as $T_L(\Omega_i) = 10^{-\alpha L/10} T_B T_F(\Omega_i)$ [30], where α represents the fiber loss in decibels per kilometers, L the fiber link length in kilometers, T_B the transmissivity due to Bob modulator losses, and T_F the lumped transmissivity of the optical filters employed in the channel selection. The frequency dependence of T_F and therefore of T_L takes into account the two possible channel selection schemes, serial or parallel. In the second, the use of, for example, an AWG filter makes reasonable to assume that T_B and hence T_L are frequency independent.

the filter selecting Ω_i is triggered by a photon generated by intermodulation is

$$p_{\exp}^{\mathrm{imd}}(\Omega_i)=\sum_{k=0}^{\infty} I_i(k)\left[\sum_{l=1}^{k}\binom{k}{l}\left(\rho T_L(\Omega_i)\right)^l\left(1-\rho T_L(\Omega_i)\right)^{l-1}\right]. \tag{26}$$

Finally, the dark count distribution is simply given by

$$p_{\exp}^{d}(\Omega_i)=d_B. \tag{27}$$

As mentioned earlier, in SCM-QKD systems, the signal source is a strongly attenuated laser pulse; therefore, the photon number can be considered to be Poisson distributed with mean value $\bar{\mu}_i$

$$R_i(k)=\frac{e^{-\bar{\mu}_i}\left(\bar{\mu}_i\right)^k}{k!}. \tag{28}$$

Therefore,

$$p_{\exp}^{\mathrm{signal}}(\Omega_i)=1-e^{-\rho T_L(\Omega_i)\bar{\mu}_i}\approx\rho T_L(\Omega_i)\bar{\mu}_i. \tag{29}$$

In a similar way, we obtained

$$I_i(k)=\frac{e^{-\bar{\mu}_i^{\mathrm{imd}}}\left(\bar{\mu}_i^{\mathrm{imd}}\right)^k}{k!}. \tag{30}$$

According to the results obtained in Appendix A, we have

$$\bar{\mu}_i^{\mathrm{imd}}=\bar{\mu}_i\frac{m^2 N_{\mathrm{CSO}}(\Omega_i)}{16}=\frac{\bar{\mu}_i}{\mathrm{QCNR}_{\mathrm{CSO}}^{i}} \tag{31}$$

Hence,

$$\begin{aligned}p_{\exp}^{\mathrm{imd}}(\Omega_i)&=1-e^{-\rho T_L(\Omega_i)\bar{\mu}_i^{\mathrm{imd}}}\approx\rho T_L(\Omega_i)\bar{\mu}_i^{\mathrm{imd}}\\&=\left(\frac{N_{\mathrm{CSO}}(\Omega_i)\,m^2}{16}\right)\rho T_L(\Omega_i)\bar{\mu}_i\\&=\rho T_L(\Omega_i)\frac{\bar{\mu}_i}{\mathrm{QCNR}_{\mathrm{CSO}}^{i}}.\end{aligned} \tag{32}$$

Now, the error rate stems from three sources again; the first is an error rate for the detected photons, which is due to alignment errors that impact over the interference visibility. In our case, it can be expressed as

$$p_{\mathrm{visibility}}^{\mathrm{error}}(\Omega_i)=\frac{(1-V)}{2}p_{\exp}^{\mathrm{signal}}(\Omega_i). \tag{33}$$

The dark count contribution to the error probability is (only half of these photons contribute to errors)

$$p_{\mathrm{dark}}^{\mathrm{error}}(\Omega_i)=\frac{d_B}{2}. \tag{34}$$

Finally, the contribution of the intermodulation signal to the error is

$$p_{\mathrm{imd}}^{\mathrm{error}}(\Omega_i)=\frac{p_{\exp}^{\mathrm{imd}}(\Omega_i)}{2}. \tag{35}$$

Considering (24), (29)–(31), and (32)–(35), we get the following expression for the QBER:

$$\mathrm{QBER}(\Omega_i)=\frac{\frac{(1-V)}{2}p_{\exp}^{\mathrm{signal}}(\Omega_i)+\frac{d_B}{2}+\frac{p_{\exp}^{\mathrm{imd}}(\Omega_i)}{2}}{p_{\exp}(\Omega_i)}. \tag{36}$$

In the denominator of (36), we can make further simplifications since $d_B\ll 1$ and we can assume that $\rho T_L\bar{\mu}_i\ll 1$. Furthermore, if we take into account the definition of the quantum carrier to noise ratio, we get

$$\mathrm{QBER}(\Omega_i)=\frac{\left\{(1-V)+\left(\frac{1}{\mathrm{QCNR}_{\mathrm{CSO}}^{i}}\right)\right\}\rho T_L(\Omega_i)\bar{\mu}_i+d_B}{2\left[\left\{1+\left(\frac{1}{\mathrm{QCNR}_{\mathrm{CSO}}^{i}}\right)\right\}\rho T_L(\Omega_i)\bar{\mu}_i+d_B\right]}. \tag{37}$$

B. QBER Analysis

We now make use of (37) to analyze the effect of different system design parameters on the QBER performance of the SCM-QKD systems. In all the cases, we consider a parallel detection scheme and the use of modulators with enough modulation bandwidth in order to make the overall losses independent of the subcarrier frequency. We will justify in Section IV-D that the serial approach is not a convenient solution for these kinds of systems as compared to the parallel configuration. In first place, we consider the effect of undesired nonlinear photons generated by intermodulation or harmonic distortion. In Fig. 5(a)–(c), we present the QBER values versus the optical fiber link length in kilometers, obtained for the three frequency plans ($N=15$, 30, and 50) system, previously presented in Section III, and for the case of a frequency coded ($N=1$) system. For the computation of the QBER, we have taken standard values for several parameters. For instance, the visibility is taken as $V=98\%$, the detector efficiency is $\rho=0.13$, $\alpha=0.2$ dB/km and $T_B=9.6$ dB.

We have considered the worst case, i.e., the QBER has been computed for the channel in the frequency plan exhibiting the highest N_{CSO} value. The average number of photons per sideband at the laser output is, unless otherwise stated, $\overline{\mu}=0.05$. In Fig. 5(a), we represent the QBER values when the modulation index for the SCM channels is a 2% (i.e., $m=0.02$). Note that the impact of intermodulation in this case is negligible for low-, middle-, and high-count channel systems. This situation changes for higher modulation indexes. For instance, in Fig. 5(b), we plot the QBER results for the same systems when the modulation index of the SCM channels is a 5%. The impact of the degrading effects of intermodulation is now apparent with a greater impact, the higher the channel counts of the frequency plan. With a modulation index of 8% shown in Fig. 5(c), it can be appreciated that, for instance, the QBER can increase by a factor of almost 50% for $N=50$ as compared to the case where $N=1$. In practice, these results suggest that modulation indexes below 2% must be employed if the SCM-QKD system is to be considered immune to intermodulation and harmonic distortion effects. The combined effect of the channel visibility and intermodulation is considered in Fig. 6(a) and (b).

For these results, we have fixed the number of channels in the SCM-QKD system to $N=15$ and computed the QBER results for different values of the visibility ($V=97\%$, 98%, 99%, and 100%). Fig. 6(a) considers the case where the modulation index for the subcarriers is 2%, while this value is assumed to be 8% in Fig. 6(b). A similar evolution is observed in both cases.

Finally, we consider the effect of the average number of photons per sideband $\bar{\mu}$ on the QBER. Fig. 7(a) and (b) shows

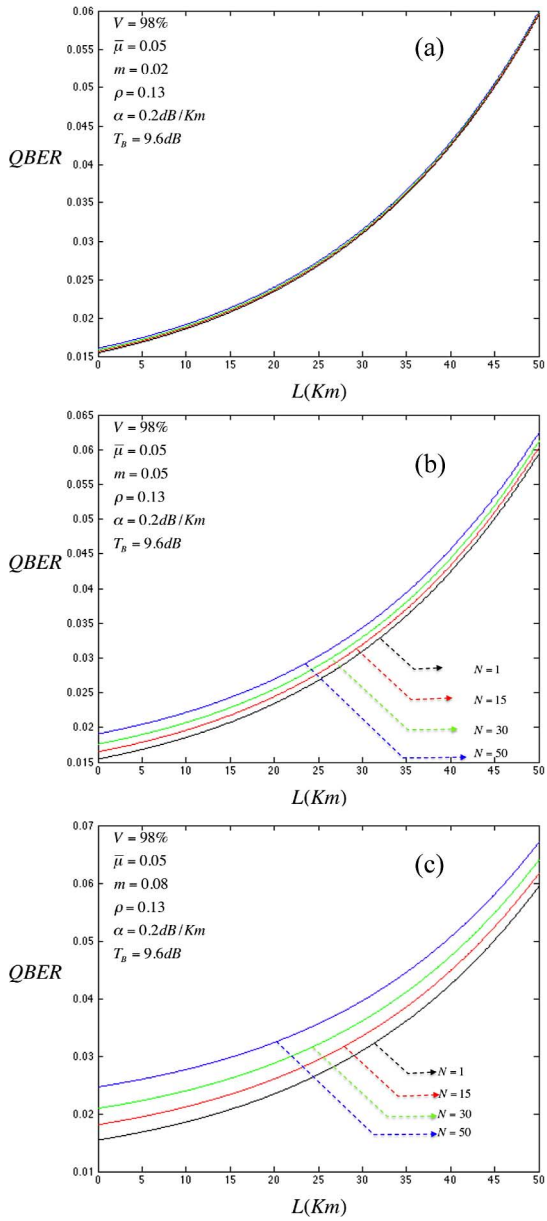


Fig. 5. QBER values versus the optical fiber link length in kilometers, obtained for the three frequency plan ($N = 15$, 30, and 50) systems and for the case of a frequency coded ($N = 1$) system with m equal to (a) 2%, (b) 5%, and (c) 8%.

the results for 15 and 50 channel SCM-QKD systems, respectively. In each figure, we consider both low ($m = 2\%$) and high ($m = 8\%$) modulation index cases and parametrize the curves by $\bar{\mu} = 0.05$, $\bar{\mu} = 0.1$, and $\bar{\mu} = 0.2$.

It is interesting to note that for the low-channel count system ($N = 15$), the evolution of the QBER values with the link distance follows the same trend either for $m = 2\%$ or for $m = 8\%$ in the three cases under consideration. This suggests that there is a relative decoupling between the effects of intermodulation and $\bar{\mu}$. This situation is different for the high-count SCM-QKD system ($N = 50$), where the evolution of the $m = 2\%$ and 8% modulation index QBER values is different, especially in the case of low average number of photons per sideband ($\bar{\mu} = 0.05$) for which there can be a nonnegligible coupling between this quantity and intermodulation.

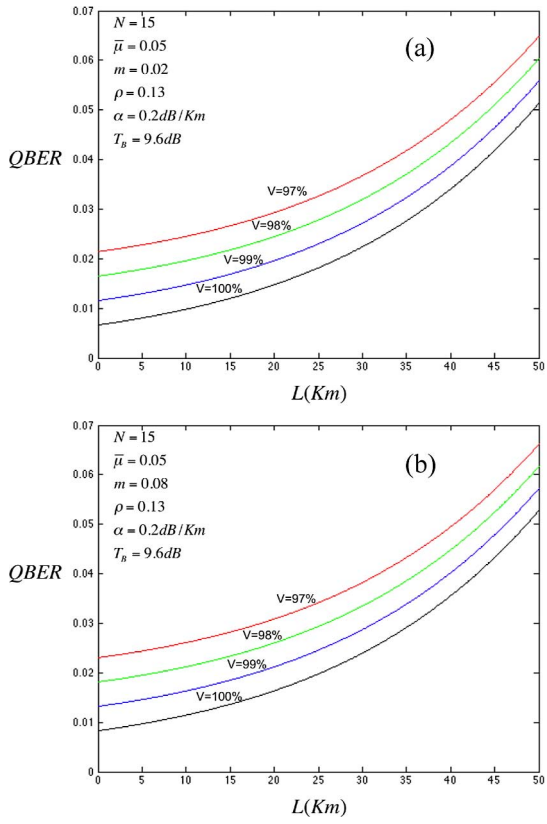


Fig. 6. Combined effect on the QBER of the channel visibility and intermodulation with m equal to (a) 2% and (b) 8%.

C. Useful Key Rates

We now turn our attention to the computation of the achievable key rates using SCM-QKD. In principle, the objective of using multiplexing techniques in the context of these systems is to increase the achievable key rates by a factor of N (N being the number of channels in the multiplex). We now investigate the conditions under which the aforementioned objective is fulfilled.

For a single channel, the rate of the sifted key as a function of distance is given by

$$R_{\text{sift}}(\Omega_i) = \frac{1}{2}\rho T_L(\Omega_i)\bar{\mu}_i f_{\text{rep}} \tag{38}$$

where f_{rep} is the pulse repetition frequency of the optical source. To calculate the useful key rate as a function of distance, we need to know the fraction of bits lost due to error correction and privacy amplification, which depends on the strategy followed by the eavesdropper. In general, we can express the useful key rate as the product of the sifted key rate and the difference between the Alice–Bob mutual information $I(A, B, \Omega_i)$ and Eve's maximal Shannon information $I^{\max}(A, E, \Omega_i)$ [3], which is given by

$$R_{\text{net}}(\Omega_i) = R_{\text{sift}}(\Omega_i)\left[I(A, B, \Omega_i) - I^{\max}(A, E, \Omega_i)\right]. \tag{39}$$

In the case of Eve performing attacks on one qubit after the other, i.e., individual attacks, the following expressions are obtained for the mutual information terms in (38) as a function

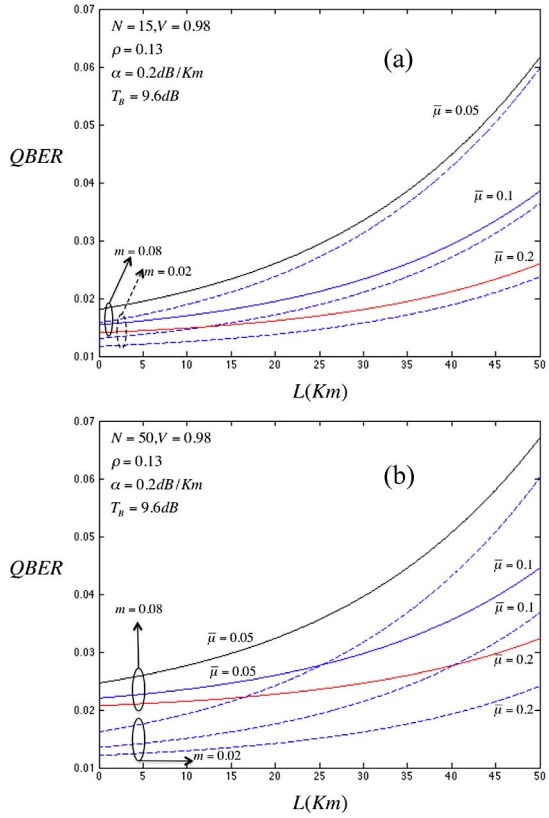


Fig. 7. Effect of the average number of photons per sideband μ on the QBER with N (a) 15 channel system and (b) 50 channel system. In each figure, we consider both low ($m = 2\%$) and high ($m = 8\%$) modulation index cases and parametrize the curves by $\mu = 0.05$, 0.1, and 0.2.

of the QBER [3]

$$I(A,B,\Omega_i) = 1 + \mathrm{QBER}(\Omega_i)\log_2\left(\mathrm{QBER}\left(\Omega_i\right)\right) + \left(1-\mathrm{QBER}(\Omega_i)\right)\log_2\left(1-\mathrm{QBER}(\Omega_i)\right) \tag{40}$$

$$\begin{aligned} I^{\max}(A,E,\Omega_i) &= 1 + \left(\frac{1+2\sqrt{\mathrm{QBER}(\Omega_i)(1-\mathrm{QBER}(\Omega_i))}}{2}\right) \\ &\quad \times \log_2\left(\frac{1+2\sqrt{\mathrm{QBER}(\Omega_i)(1-\mathrm{QBER}(\Omega_i))}}{2}\right) \\ &\quad + \left(\frac{1-2\sqrt{\mathrm{QBER}(\Omega_i)(1-\mathrm{QBER}(\Omega_i))}}{2}\right) \\ &\quad \times \log_2\left(\frac{1-2\sqrt{\mathrm{QBER}(\Omega_i)(1-\mathrm{QBER}(\Omega_i))}}{2}\right). \end{aligned} \tag{41}$$

Equations (40) and (41) together with (37) allow us to obtain the evolution of the useful key rate for a single channel as a function of distance using (38). For the multiplexed system, the overall useful key rate is then given by

$$R_{\mathrm{net}}^{\mathrm{MUX}} = \sum_{\Omega_i} R_{\mathrm{net}}(\Omega_i). \tag{42}$$

For the sake of comparison with the frequency coding case (i.e., $N = 1$), we consider the system performance in terms of useful key rate for a system given by the following (typical) parameters: $f_{\mathrm{rep}} = 10$ MHz, V = 98%, detector efficiency $\rho = 0.13$, $\alpha = 0.2$ dB/km, and $T_B T_F = 9.6$ dB. The evolution of the useful key rates as a function of the link distance is represented for three different values of the modulation index ($m = 2\%$, 10%, and 20%) in Fig. 8(a)–(c), respectively. In each figure, we consider the high- ($N = 50$), intermediate- ($N = 30$), and low- ($N = 15$) count SCM-QKD options as well as the frequency coding alternative ($N = 1$) both under coherent state and single photon operation (in this last case, $f_{\mathrm{rep}} = 1$ MHz. All the curves show a similar behavior, featuring an exponential decrease first, and then, due to error correction and privacy amplification, the bit rates fell rapidly to zero. The curves showing the useful rate variation for different channels are parallel provided the link length is not too close to the limit point imposed by error correction and privacy amplification. The comparison between the useful bit rate achieved for a given multiplex and that achieved for the case $N = 1$ gives the multiplexing gain M_G. Ideally, the multiplexing gain should be given precisely by N.

The main effects of the index of modulation on the system performance are two: on one hand, the multiplexing gain is reduced, so $M_G < N$. On the other hand, the link length span across which M_G is constant is reduced.

For low values of the index of modulation ($m < 10\%$), the multiplexing gain remains constant and equal to the number of channels (N) in the multiplex of link lengths spanning up to 85 km. Nonlinear signal mixing effects start to be notable in the useful bit rate for modulation indexes close to 10%. For instance, as shown in Fig. 8(b), the multiplexing gain as well as the maximum link length for which this gain remain constant (75 km) are reduced.

These effects are more clear in Fig. 8(c) for a modulation index of 20%.

For instance, Fig. 9 shows the evolution of the multiplexing gain computed at $z = 30$ km as a function of the modulation index for the three frequency plans under consideration.

Note that the multiplexing gains remain very close to the ideal values for low values of the index of modulation. In particular, for values up to a 5%, the SCM-QKD system performance is immune to nonlinear signal mixing. Beyond this range, the multiplexing gain decreases at a rate, which is faster, the higher number of channels. These results that have been computed for a particular source pulse repetition frequency ($f_{\mathrm{rep}} = 10$ MHz) do scale with this parameter in terms of usable key bit rate. As an example, if a 1-GHz pulse repetition frequency source is considered and an index of modulation of 0.02 is chosen, the achievable useful key rates for a 30-km fiber link could be up to 2 Mb/s for an $N = 15$ system, 4 Mb/s for an $N = 30$ system, and 7 Mb/s for an $N = 50$ system. These values are beyond those

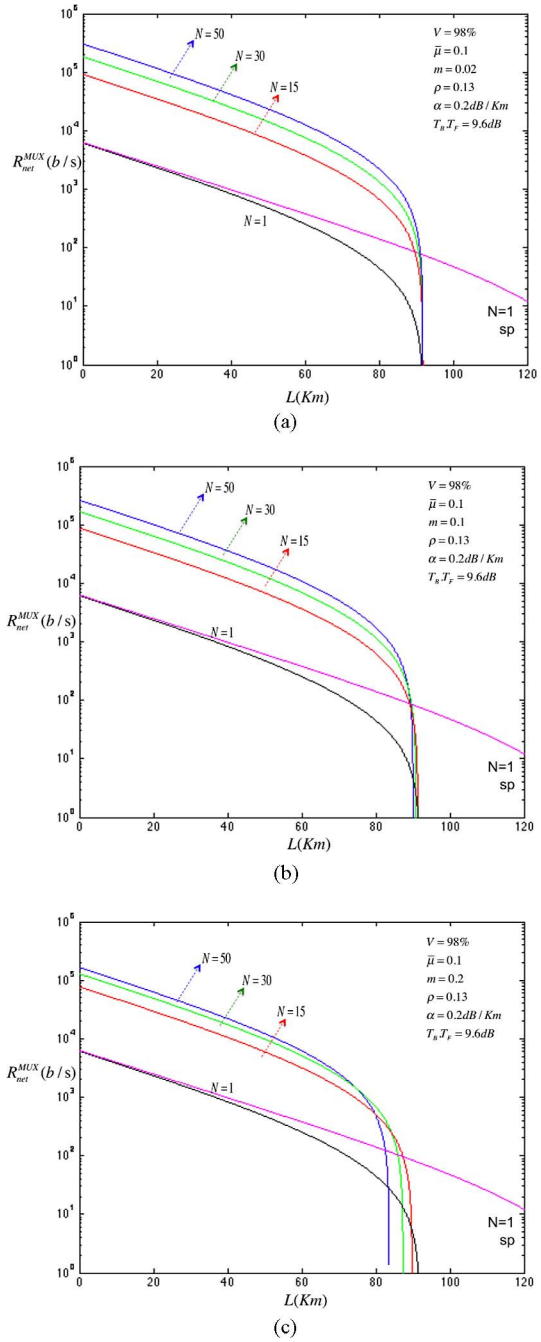


Fig. 8. Overall useful key rate values versus the optical fiber link length in kilometers, obtained for the three frequency plan ($N = 15$, 30, and 50) systems and for the case of a frequency coded ($N = 1$) system with both coherent state and single photon operation. (a) $m = 2\%$. (b) $m = 10\%$. (c) $m = 20\%$. In all cases, the pulse repetition frequency of the optical source is 10 MHz. Other parameters are shown in the insets.

currently reported for state-of-the-art BB84 systems (1 Mb/s at the rate of 20 km [22]).

D. Other Practical Considerations

We now consider the realistic limitations imposed on the ideal system operation by two important factors: the effect of the modulator bandwidth on the system multiplexing capacity

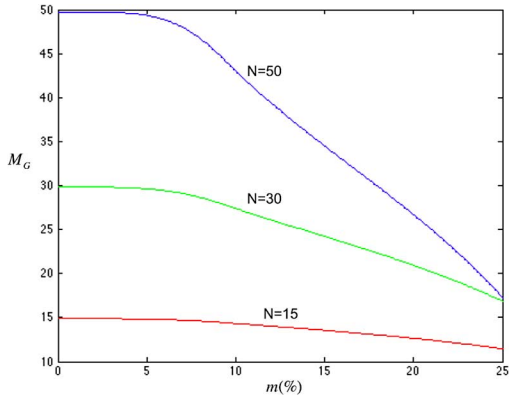


Fig. 9. Multiplexing gains in the overall useful key rate values versus the modulation index computed at $z = 30$ km for the three frequency plan ($N = 15$, 30, and 50) systems.

and the impact of the optical filtering imperfections and losses in the subcarrier selection. Electrooptic modulators are currently commercially available, featuring modulation bandwidths up to 50 GHz [33]. Higher bandwidths have been reported experimentally by various groups for different material systems. For instance, 100-GHz modulation bandwidth devices have been reported both for lithium niobate [34] and polymer [35] modulators with a slightly smaller value for semiconductor-based modulators (i.e., 80 GHz for InP [36] and 50 GHz for GaAs [37]). Thus, for 2-GHz subcarrier spacing, commercial modulators can accommodate up to 25 channels and this figure goes down to ten and five channels if subcarriers are separated by 5 and 10 GHz, respectively. With up to 100-GHz modulation bandwidths, the former figures double.

Regarding the optical filtering operation, two alternatives are possible, as suggested by Fig. 1. In the parallel detection configuration, the subcarrier filtering, together with the spatial separation, can be efficiently achieved by means of an arrayed waveguide grating (AWG) device. The current state of the art in these devices has achieved 32 output ports in a single device with a very narrow channel spacing (10 GHz) selection, featuring more than -30 dB adjacent channel crosstalk and a total typical insertion loss of around 3 dB for the 20 central channels [38]. Channel spacing can be reduced to 5 GHz by spectral interleaving of two devices at the extra penalty of 3 dB. An ultranarrowband device featuring channel spacing of 1 GHz has also been experimentally reported [39], but it is not yet available commercially. For the serial operation, the alternative featuring the required degree of spectral selectivity and low losses is that based on fiber Bragg gratings (FBGs). Uniform FBGs have been reported with a bandwidth as narrow as 1.3 GHz [40]. Lower figures can even be achieved by means of π-shifted configurations [41]. In any case, sophisticated synthesis algorithms exist [42], which render FBG filter designs with the required bandwidth featuring extremely high reflectivities as well (insertion losses around 0.1 dB and lower). The main limitation in the serial configuration is due to the need of employing optical circulators to spatially extract the filtered subcarriers. The best insertion loss figures for state-of-the-art circulators are in the range of 0.3–0.4 dB.

With the aforementioned data and assuming a total insertion loss of 6 dB for Bob's modulator, the parallel approach would, for instance, be able to accommodate around ten subcarriers with a spectral separation of 10 GHz and a total filtering loss of 3 dB with a 50-GHz bandwidth modulator (overall loss 9 dB), 20 subcarriers with a spectral separation of 5 GHz, and a total filtering loss of 6 dB with a 100-GHz bandwidth modulator (overall loss 12 dB). This figure could rise up to 50 channels with a 50-GHz modulator if an ultra-narrowband AWG as that reported in [39] becomes commercially available. In the case of the serial configuration assuming a total loss of 0.5 dB per FBG, only 12 devices can be placed in series for a total filtering loss of 6 dB. However, note that in these cases, the filtering loss would be highly dependent on the subcarrier value. The conclusion is that the parallel filtering configuration is more efficient for this particular application since the filtering losses do not scale with the number of output ports. In principle, the number of subcarriers that can be accommodated with this approach and the current state-of-the-art technology ranges between 10 and 20. However, there is, in principle, no fundamental limitation on the attainable channel separation with AWG devices, so future developments may make ultra-narrowband channel separation devices such as that reported in [38] commercially available. In such a case, systems supporting 50 subcarriers would be feasible at a reasonable loss level. In the low modulation index scenario discussed before, this means that the key rate could be potentially increased by such a figure. Further improvements could be achieved nevertheless by incorporating the wavelength domain (WDM) into the multiplexing hierarchy.

V. Summary and Conclusion

In this paper, we have provided an in-depth theoretical analysis of SCM-QKD systems, taking into account as many factors of impairment as possible, and especially considering the influence of nonlinear signal mixing on the end-to-end QBER and useful key rate. The thorough analysis of SCM-QKD has sequentially considered the different factors affecting the sideband visibility (drifts in the modulator bias points, modulation index mismatch between Alice and Bob subcarriers) and the impact of nonlinear signal mixing leaking into otherwise void subcarrier sidebands. In a similar way to classical photonic radio-over-fiber telecommunication and CATV systems, the impact of this nonlinear signal mixing can be accounted in terms of a QCNR that depends on the specific frequency plan that is implemented. QBER and useful key rate results for three different frequency plans featuring $N = 15$ (low-channel count system), $N = 30$ (intermediate-count channel system), and $N = 50$ (high-count channel system) channels have been provided, which show that photon nonlinear mixing can be of importance in middle- and high-count SCM-QKD systems ($N > 30$) with moderate RF modulation indexes ($5\% < m$). In practical terms, nonlinear signal mixing can be neglected if low modulation indexes ($m < 5\%$) are employed to encode the photons in the subcarrier sidebands and a full multiplexing gain of N (where N is the number of subcarriers) can be achieved for the overall useful key rate. As compared to the useful rate provided by a single-channel practical issues regarding the limitations imposed by the modulators regarding their multiplexing capability and the impact of filter selectivity and losses have also been discussed.

TABLE I
Term Decomposition of (A1)

(1) l=k=l'=k'	N terms
(2) l=k, l'=k'	$N(N-1)$ terms
(3) $l = k,\ l' \neq k' \neq l$	$N(N-1)(N-2)$ terms
(4) $l = l',\ k = k', k \neq l$	$N(N-1)$ terms
(5) $l = l',\ k \neq k' \neq l$	$N(N-1)(N-2)$ terms
(6) $l = k',\ k = l', l \neq k$	$N(N-1)$ terms
(7) $l = k',\ k \neq l' \neq l$	$N(N-1)(N-2)$ terms
(8) $l = k = l',\ l \neq k'$	$N(N-1)$ terms
(9) $l = k = k', l \neq l'$	$N(N-1)$ terms
(10) $l = l' = k',\ l \neq k$	$N(N-1)$ terms
(11) $l' = k' = k, l \neq k$	$N(N-1)$ terms
(12) $l \neq k \neq l' \neq k'$	$N(N-1)(N-2)(N-3)$ terms
(13) $l' = k', l \neq k \neq l'$	$N(N-1)(N-2)$ terms
(14) $k = k', l \neq k \neq l'$	$N(N-1)(N-2)$ terms
(15) $k = l', l \neq k \neq k'$	$N(N-1)(N-2)$ terms

Appendix

Appendix A: Computation of the Interference Average Values in (19)

We aim to compute the average value of the term I^{IM} that appears in the interference terms for lower and upper sidebands. We proceed term by term in the sum. For the first term in the sum, we can find the following expression:

$$E[U] = E\left[\left|\sum_{\substack{l,k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N} e^{j(\Delta\Phi_{l,k})}\right|^2\right]$$

$$= E\left[\sum_{l=1}^{N}\sum_{\substack{k=1 \\ \Omega_l - \Omega_k = \Omega_i}}^{N}\sum_{l'=1}^{N}\sum_{\substack{k'=1 \\ \Omega_{l'} - \Omega_{k'} = \Omega_i}}^{N} e^{j\left(\Delta\Phi_{l,k} - \Delta\Phi_{l',k'}\right)}\right] \tag{A1}$$

The N^4 terms in a quadruple summation can be placed in 15 different classes, as shown in Table I [30]. Not all the aforementioned terms have to be considered since the restriction placed over the values of the interfering frequencies require that $l \neq k$ and $l' \neq k'$ (the downconversion beating between a subcarrier and itself cannot fell inside the subcarrier frequency channel since it is placed at baseband). Thus, terms (1)–(3), (8)–(11), and (13) need not to be considered in (A1).

Lets then proceed with the computation of the remaining terms:

Term (4)

$$E\left[U_{(4)}\right] = E\left[\sum_{l=1}^{N}\sum_{k=1}^{N} e^{j(\Delta\Phi_{l,k}-\Delta\Phi_{l,k})}\right] = N_{\mathrm{CSOD}}\left(\Omega_i\right) \tag{A2}$$

where $N_{\mathrm{CSOD}}(\Omega_i)$ represents the number of composite second-order terms due to downconversion that fell inside channel centered at subcarrier Ω_i.[5]

Term (5)

$$\begin{aligned} E\left[U_{(5)}\right] &= E\left[\sum_{l=1}^{N}\sum_{k=1}^{N}\sum_{\substack{k'=1\\k'\neq k}}^{N} e^{j\left(\Delta\Phi_{l,k}-\Delta\Phi_{l,k'}\right)}\right] \\ &= \mathrm{NE}\left[\sum_{k=1}^{N}\sum_{\substack{k'=1\\k'\neq k}}^{N} e^{j\left(\Phi_{2,k'}-\Phi_{2,k}\right)}\right] \\ &= 2\mathrm{NE}\left[\sum_{k=1}^{N}\sum_{k'>k}^{N}\cos\left(\left(\Phi_{2,k'}-\Phi_{2,k}\right)\right)\right] \\ &= 2N\sum_{k=1}^{N}\sum_{k'>k}^{N} E\left[\cos\left(\left(\Phi_{2,k'}-\Phi_{2,k}\right)\right)\right] = 0. \end{aligned} \tag{A3}$$

For the computation of the aforementioned result, one must take into account that $\Phi_{2,k'}-\Phi_{2,k}$ is an uniformly distributed four-valued random phase variable, and therefore, $E\left[\cos(\Phi_{2,k'}-\Phi_{2,k})\right]=0$.

The average of *term (6)* is given by

$$\begin{aligned} E\left[U_{(6)}\right] &= E\left[\sum_{l=1}^{N}\sum_{k=l}^{N} e^{j2\Delta\Phi_{l,k}}\right] = 2E\left[\sum_{l=1}^{N}\sum_{k>l}^{N}\cos\left(2\Delta\Phi_{l,k}\right)\right] \\ &= 2\sum_{l=1}^{N}\sum_{k>l}^{N} E\left[\cos\left(2\Delta\Phi_{l,k}\right)\right] = 0 \end{aligned} \tag{A4}$$

since $2\Delta\Phi_{l,k}$ is a triangular-distributed three-valued $[-\pi,0,\pi]$ random phase variable and $E\left[\cos(2\Delta\Phi_{l,k})\right]=0$.

The average of *term (7)* is given by

$$\begin{aligned} E\left[U_{(7)}\right] &= E\left[\sum_{l=1}^{N}\sum_{k=1}^{N}\sum_{l'=1}^{N} e^{j\left(\Delta\Phi_{l,k}-\Delta\Phi_{l',l}\right)}\right] \\ &= 2E\left[\sum_{l=1}^{N}\sum_{k=l}^{N}\sum_{l'=k}^{N}\cos\left(\Delta\Phi_{l,k}-\Delta\Phi_{l',l}\right)\right] \\ &= 2\sum_{l=1}^{N}\sum_{k=l}^{N}\sum_{l'=k}^{N} E\left[\cos\left(\Delta\Phi_{l,k}-\Delta\Phi_{l',l}\right)\right] = 0 \end{aligned} \tag{A5}$$

since $\Delta\Phi_{l,k}-\Delta\Phi_{l',l}$ is an uniformly distributed four-valued random phase variable and $E\left[\cos(\Delta\Phi_{l,k}-\Delta\Phi_{l',l})\right]=0$.

[5]This parameter is of common usage in the CATVresearch community and industry.

In a similar way, the average of (12) is

$$\begin{aligned} E\left[U_{(12)}\right] &= 2E\left[\sum_{l=1}^{N}\sum_{k>1}^{N}\sum_{l'>k}^{N}\sum_{k'>l'}^{N}\cos\left(\Delta\Phi_{l,k}-\Delta\Phi_{l',k'}\right)\right] \\ &= 2\sum_{l=1}^{N}\sum_{k>1}^{N}\sum_{l'>k}^{N}\sum_{k'>l'}^{N} E\left[\cos\left(\Delta\Phi_{l,k}-\Delta\Phi_{l',k'}\right)\right] = 0 \end{aligned} \tag{A6}$$

since $\Delta\Phi_{l,k}-\Delta\Phi_{l',k'}$ is an uniformly distributed four-valued random phase variable and $E\left[\cos(\Delta\Phi_{l,k}-\Delta\Phi_{l',k'})\right]=0$.

Using the same reasoning, it can be also shown that

$$E\left[U_{(14)}\right] = E\left[U_{(15)}\right] = 0. \tag{A7}$$

Thus,

$$E\left[U\right] = E\left[\left|\sum_{l,k=1}^{N} e^{j(\Delta\Phi_{l,k})}\right|^2\right] = N_{\mathrm{CSOD}}. \tag{A8}$$

We can now proceed in a similar fashion with the second term in the sum (19)

$$\begin{aligned} E\left[V\right] &= E\left[\left|\sum_{\substack{r,s=1\\ \Omega r+\Omega_s=\Omega_i}}^{N} e^{j(\Sigma\Phi_{l,k})}\right|^2\right] \\ &= E\left[\sum_{r=1}^{N}\sum_{\substack{s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N}\sum_{r'=1}^{N}\sum_{\substack{s'=1\\ \Omega_{r'}+\Omega_{s'}=\Omega_i}}^{N} e^{j\left(\Sigma\Phi_{r,s}-\Sigma\Phi_{r',s'}\right)}\right]. \end{aligned} \tag{A9}$$

The N^4 terms in a quadruple summation can be placed again in 15 different classes, as shown in Table II.

In this case, we cannot neglect term (1) since it represents the harmonic distortion terms, i.e., $\Omega_r+\Omega_s=(r=s)=2\Omega_r$ beatings that fell inside the channel centred at subcarrier Ω_i.

Term (1)

$$E\left[V_{(1)}\right] = E\left[\sum_{\substack{r=1\\ 2\Omega_r=\Omega_i}}^{N} e^{j(\Sigma\Phi_{r,r}-\Sigma\Phi_{r,r})}\right] = N_{\mathrm{CSOHD}}\left(\Omega_i\right) \tag{A10}$$

where $N_{\mathrm{CSOHD}}(\Omega_i)$ represents the number of composite second-order terms due to harmonic distortion that fell inside channel centered at subcarrier Ω_i

Term (4)

$$E\left[V_{(4)}\right] = E\left[\sum_{r=1}^{N}\sum_{\substack{s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} e^{j(\Sigma\Phi_{r,s}-\Sigma\Phi_{r,s})}\right] = N_{\mathrm{CSOU}}\left(\Omega_i\right) \tag{A11}$$

where $N_{\mathrm{CSOU}}(\Omega_i)$ represents the number of composite second-order terms due to upconversion that fell inside channel centered

TABLE II
TERM DECOMPOSITION OF (A12)

(1) r=s=r'=s'	N terms
(2) r=s, r'=s'	$N(N-1)$ terms
(3) $r = s,\ \ r' \neq s' \neq r$	$N(N-1)(N-2)$ terms
(4) $r = r',\ \ s = s', r \neq s$	$N(N-1)$ terms
(5) $r = r',\ \ s \neq s' \neq r$	$N(N-1)(N-2)$ terms
(6) $r = s',\ \ r = r', r \neq s$	$N(N-1)$ terms
(7) $r = s',\ \ s \neq r' \neq r$	$N(N-1)(N-2)$ terms
(8) $r = s = r',\ \ r \neq s'$	$N(N-1)$ terms
(9) $r = s = s', r \neq r'$	$N(N-1)$ terms
(10) $r = r' = s',\ r \neq s$	$N(N-1)$ terms
(11) $r' = s' = s,\ r \neq s$	$N(N-1)$ terms
(12) $r \neq s \neq r' \neq s'$	$N(N-1)(N-2)(N-3)$ terms
(13) $r' = s', r \neq s \neq s'$	$N(N-1)(N-2)$ terms
(14) $s = s', r \neq s \neq r'$	$N(N-1)(N-2)$ terms
(15) $s = r', r \neq s \neq s'$	$N(N-1)(N-2)$ terms

at subcarrier Ω_i.[6] The rest of the terms vanish, so finally, we have

$$E[V] = E\left[\left|\sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} e^{j(\Sigma\Phi_{r,s})}\right|^2\right] = N_{\mathrm{CSOU}}(\Omega_i) + N_{\mathrm{CSOHD}}(\Omega_i). \quad \text{(A12)}$$

Finally, it is straightforward to show that

$$E\left[\sum_{\substack{l,k=1\\ \Omega_l-\Omega_k=\Omega_i}}^{N}\ \sum_{\substack{r,s=1\\ \Omega_r+\Omega_s=\Omega_i}}^{N} \cos\left(\Delta\Phi_{lk} - \Sigma\Phi_{rs}\right)\right] = 0 \quad \text{(A13)}$$

So finally, we get

$$E\left[I^{\mathrm{IM}}\right] = \frac{I_e m^2}{16}\left[N_{\mathrm{CSOD}}(\Omega_i) + N_{\mathrm{CSOU}}(\Omega_i) + N_{\mathrm{CSOHD}}(\Omega_i)\right] = \frac{I_e m^2}{16} N_{\mathrm{CSO}}(\Omega_i). \quad \text{(A14)}$$

REFERENCES

[1] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, pp. 77–88, 1983.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India. New York: IEEE, 1984, pp. 175–179.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[4] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, pp. 3–28, 1992.

[6] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, pp. 793–795, 1997.

[7] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, "Quantum key distribution system clocked at 2 GHz," *Opt. Exp.*, vol. 13, no. 8, pp. 3015–3020, Apr. 2005.

[6] Again, this parameter is of common usage in the CATV research community and industry.

[8] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Single-photon interferente in a 10 km long optical fiber interferometer," *Electron. Lett.*, vol. 29, no. 7, pp. 634–635, Apr. 1993.

[9] P. D. Townsend, D. J. D. Phoenix, K. J. Blow, and S. Cova, "Design of quantum cryptography systems for passive optical networks," *Electron. Lett.*, vol. 30, pp. 1875–1877, Oct. 1994.

[10] P. D. Townsend, "Quantum cryptography on optical fiber networks," *Opt. Fiber Technol.*, vol. 4, pp. 345–370, 1998.

[11] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, pp. 037902-1–037902-3, 2002.

[12] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution over 105 km fibre," *New J. Phys.*, vol. 7, pp. 1–12, 2005.

[13] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photon.*, vol. 1, pp. 343–348, 2007.

[14] J.-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes, "Single-photon interefrence in sidebands of phase-modulated light for quantum cryptography," *Phys. Rev. Lett.*, vol. 82, pp. 1656–1659, 1999.

[15] J.-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, H. Porte, and W. T. Rhodes, "Phase-modulation transmission system for quantum cryptography," *Opt. Lett.*, vol. 24, pp. 104–106, 1999.

[16] O. Guerreau, J.-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer, and F. J. Malassenet, "Long distance QKD transmission using single-sideband detection scheme with WDM synchronization," *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1533–1540, Nov./Dec. 2003.

[17] J. Capmany and D. Novak, "Microwave photonics combines two worlds," *Nat. Photon.*, vol. 1, pp. 319–330, 2007.

[18] J. Capmany, B. Ortega, D. Pastor, and S. Sales, "Discrete-time optical processing of microwave signals," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 702–721, Feb. 2005.

[19] C. H. Bennett, "Quantum cryptography using any two non-orthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, 1992.

[20] J.-M. Mérolla, L. Duraffourg, J. P. Goedgebuer, A. Soujaeff, F. Patois, and W. T. Rhodes, "Integrated quantum key distribution system using single sideband detection," *Eur. Phys. J. D*, vol. 18, pp. 141–146, 2002.

[21] M. Bloch, S. McLaughlin, J. M. Merolla, and F. Patois, "Frequency-coded quantum key distribution," *Opt. Lett.*, vol. 32, pp. 301–303, 2007.

[22] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Opt. Exp.*, vol. 16, no. 23, pp. 18790–18979, 2008.

[23] H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, pp. 230504-1–230504-4, 2005.

[24] A. Ortigosa-Blanch and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 73, pp. 024305-1–024305-4, 2006.

[25] W. Caiqin and X. Zhang, "Impact of nonlinear distortion in radio over fiber systems with single-sideband and tandem single-sideband subcarrier modulations," *J. Lightw. Technol.*, vol. 24, no. 5, pp. 2076–2090, May 2006.

[26] N. J. Frigo, M. R. Phillips, and G. E. Bodeep, "Clipping distortion in lightwave CATV systems: Models, simulations, and measurements," *J. Lightw. Technol.*, vol. 11, no. 1, pp. 138–146, Jan. 1993.

[27] A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications*, 6th ed. Oxford, U.K.: Oxford Univ. Press, 2006.

[28] G. P Agrawal, *Fiber-Optic Communications*, 3rd ed. New York: Wiley, 2002.

[29] W. I. Way, *Broadband Hybrid Fiber/Coax Access System Technologies*. San Diego, CA: Academic, 1998.

[30] J. W. Goodman, *Statistical Optics*. New York: Wiley, 1985.

[31] J. Capmany, "Photon nonlinear mixing in subcarrier multiplexed quantum key distribution systems," *Opt. Exp.*, vol. 17, no. 8, pp. 6457–6464, Apr. 2009.

[32] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 61, pp. 052304-1–052304-10, 2000.

[33] S. Iezekiel, *Microwave Photonics*. Chichester, U.K.: IEEE/Wiley, 2009.

[34] K. Noguchi, O. Mitomi, and H. Miyazawa, "Millimeter-wave $Ti:LiNbO_3$ optical modulators," *IEEE J. Lightw. Technol.*, vol. 16, no. 4, pp. 615–619, Apr. 1998.

[35] D. Chen, H. R. Fetterman, A. Chen, W. H. Steier, L. Dalton, W. Wang, and Y. Shi, "Demonstration of 110 GHz electro-optic polymer modulators," *Appl. Phys. Lett.*, vol. 70, pp. 3335–3337, 1997.

[36] H. N. Klein, H. Chen, D. Hoffmann, S. Staroske, A. G. Steffan, and K. O. Velthaus, "155 μm Mach-Zehnder modulators on InP for optical 40/80 Gb/s trasmission networks," in *Proc. Indiun Phosphide Relat. Mater. Conf.*, 2006, pp. 171–173.
[37] M. Jarrahi, T. H. Lee, and D. A. B. Miller, "Wideband, low driving voltage traveling-wave Mach-Zehnder modulator for RF-Photonics," *IEEE Photon. Technol. Lett.*, vol. 20, no. 7, pp. 517–519, Apr. 2002.
[38] C. R. Doerr and K. Okamoto, "Planar lightwave circuits in fiber-optic communications," in *Optical Fiber Telecommunications*. vol. VA, San Diego, CA: Academic, 2008, ch. 7.
[39] K. Takada, M. Abe, T. Shibata, and K. Okamoto, "1 GHz spaced 16-channel arrayed-waveguide grating for a wavelength reference standard in DWDM network systems," *IEEE Photon. Technol. Lett.*, vol. 20, no. 5, pp. 822–825, May 2002.
[40] A. Suzuki, Y. Takahashi, and M. Nakazawa, "Fabrication of an ultranarrow band fiber Bragg grating filter with a 1.3 GHz bandwidth," *IEIC Tech. Rep.*, vol. 106, pp. 11–16, 2006.
[41] R. Kashyap, *Fiber Bragg Gratings*. San Diego, CA: Academic, 1999.
[42] J. Capmany, M. A. Muriel, and S. Sales, "Highly accurate synthesis of fiber and waveguide Bragg gratings by an impedance reconstruction layer-aggregation method," *IEEE J. Quantum Electron.*, vol. 43, no. 10, pp. 889–898, Oct. 2007.

José Capmany (S'88–M'92–SM'96–F'08) was born in Madrid, Spain, on December 15, 1962. He received the Ingeniero de Telecomunicacion and Ph.D. degrees from the Universidad Politécnica de Madrid, Madrid, in 1987 and 1991, respectively, and the Licenciado en Ciencias Físicas degree from the Universidad Nacional de Educación a DIstancia (UNED), Spain.

From 1988 to 1991, he was a Research Assistant with the Departamento de Tecnologıa Fotonica, Universidad Politécnica de Madrid. In 1991, he moved to the Departamento de Comunicaciones, Universidad Politecnica de Valencia, Valencia, Spain, where he started the activities on optical communications and photonics, founding the Optical Communications Group, and was an Associate Professor from 1992 to 1996, and has been a Full Professor in optical communications, systems, and networks since 1996. In parallel, he was the Telecommunications Engineering Faculty Vice Dean from 1991 to 1996, and has been the Deputy Head of the Communications Department since 1996. Since 2002, he has been the Director of the Institute of Telecommunications and Multimedia Research Institute, Universidad Politécnica de Valencia. His research interests include a wide range of subjects related to optical communications, including optical signal processing, ring resonators, fiber gratings, RF filters, subcarrier multiplexing, wavelength-division multiplexing, and code division multiple access transmission, wavelength conversion, optical bistability, and more recently, quantum cryptography and quantum information processing using photonics. He is the author or coauthor of more then 310 papers published in international refereed journals and conferences.

Prof. Capmany is a Fellow of the Optical Society of America and the Institution of Electrical Engineers. He is an Associate Editor of the IEEE PHOTONICS TECHNOLOGY LETTERS and a member of the Editorial Board of the *Fiber and Integrated Optics, Microwave and Optical Technology Letters*. He has also been a Guest Editor for the IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS. He has been a member of the Technical Programme Committees of the European Conference on Optical Communications, the Optical Fiber Conference, the Integrated Optics and Optical Communications Conference, the Conference on Lasers and Electro-Optics Europe, and the Optoelectronics and Communications Conference. He has also carried out activities related to professional bodies. He is the Founder and the Chairman of the Lasers and Electro-Optics Society Spanish Chapter. He w as a reviewer for more than 25 Science Citation Index Journals in the field of photonics and telecommunications. He was the recipient of the Extraordinary Doctorate Prize of the Universidad Politécnica de Madrid in 1992.

Arturo Ortigosa-Blanch received the Licenciado en Ciencias Fisicas degree from the Universitat de Valencia, Valencia, Spain.

From 1999 to 2002, he was with the Optoelectronics Group, University of Bath, Bath, U.K., where he completed his doctoral thesis in fabrication and linear and nonlinear characterization of photonic crystal fibers (PCFs). From 2002 to 2005, he was a Postdoctoral Researcher in the Applied Physics Department, University of Valencia, where he was involved in the fabrication and characterisation of PCFs and optical-fiber-based sensors. From 2006 to 2008, he was with the Optical and Quantum Communications Group, Universidad Politécnica de Valencia, Valencia, where he was involved in research in the field of quantum key distribution, and is currently with the Institute of Telecommunications and Multimedia Research Institute.

José Mora was born in Torrent, Valencia, Spain, in 1976. He received the M.Sc. degree in physics and the Ph.D. degree from the Universidad de Valencia, Valencia, in 1999 and 2005, respectively.

He received the extraordinary doctorate prize from the Universidad de Valencia in 2006. Since 2004, he has been a Researcher with the Optical and Quantum Communications Group, Institute of Telecommunications and Multimedia Research Institute, Universidad Politécnica de Valencia, Valencia. He is the author or coauthor of more than 100 papers and conference contributions, covering a wide range of fields related to fiber gratings, optical signal processing, microwave photonics filters, optical networks, and quantum key distribution.

Antonio Ruiz-Alba received the Licenciado en Ciencias Fisicas degree from the Universidad Autónoma de Madrid, Madrid, Spain.

Since 2008, he has been with the Optical and Quantum Communications Group, Institute of Telecommunications and Multimedia Research Institute, Universidad Politécnica de Valencia, Valencia, Spain, where he is engaged in research on subcarrier multiplexed quantum key distribution Systems.

Waldimar Amaya (M'00) was born in Bogotá, Colombia. He received the Electronics Engineer, Mobile Telecommunications Specialist, and M.Sc. degrees from the Distrital University, Bogotá, Colombia, in 1999, 2000, and 2006, respectively, and the Ph.D. degree in telecommunications from the Universidad Politecnica de Valencia (UPV) Valencia, Spain, in 2008.

For two years, he was a Hybrid Fiber Coaxial Community Access Television Operator. Later, he was an Assistant Lecturer at two universities in Colombia. In 2005, he joined the Optical and Quantum Communications Group, Institute of Telecommunications and Multimedia Research Institute, UPV.

Alfonso Martínez was born in La Palma (Murcia), Spain, on December 3, 1976. He received the Ingeniero de Telecomunicacion degree from the Universidad Politécnica de Valencia (UPV), Valencia, Spain, in 2000. He is currently working toward the Ph.D. degree with the Optical Communications Group, Institute of Telecommunications and Multimedia Research Institute, UPV.

His current research interests include fiber Bragg gratings applications, subcarrier multiplexing, wavelength conversion, microwave photonics, and wavelength-division multiplexing networks.

Experimental Demonstration of Subcarrier Multiplexed Quantum Key Distribution

A. Ruiz-Alba, J. Mora, J. Capmany, W. Amaya, A. Ortigosa-Blanch
ITEAM Research Institute
Universidad Politécnica de Valencia
Edificio 8G, Acceso D
Valencia, Spain
jcapmany@dcom.upv.es

***Abstract*— We provide for the first time, to our knowledge, an experimental demonstration of the feasibility of Subcarrier Multiplexed Quantum Key Distribution (SCM-QKD).**

I. INTRODUCTION

Quantum cryptography features an unique way of sharing a random sequence of bits between users with a certificable security not attainable with either public or secret-key classical cryptographic systems [1, 2]. This is achieved by means of quantum key distribution (QKD) techniques. In essence, QKD relies on exploiting in a positive sense the laws of quantum mechanics, which are often viewed in other contexts of physics as limiting or negative [3]. Photonics has proved to be one of the principal enabling technologies for long-distance QKD using optical fiber links. One of the most interesting approaches originally proposed by Merolla et al [4], also known as frequency coding, relies on encoding the information bits on the sidebands of either phase [4] or amplitude [6] radio-frequency (RF) modulated light. Here Alice, the key sender, randomly changes the phase of the electrical signal used to drive a light modulator among four phase values, which form a pair of conjugated bases and sends the signal through a fiber link. When it arrives at Bob, the key receiver, he modulates the signal again using the same microwave signal frequency and thus his new sidebands will interfere with those created by Alice [4]. Originally used for implementing the Bennett 1992 B92 protocol [7], [4], it was subsequently improved by adjusting the modulator characteristics which let them demonstrate the implementation of the Bennett-Brassard 1984 BB84 protocol [2], [8].

The conceptual approach of frequency coding can be considerably improved in terms of signal speed by incorporating a multiplexing technique widely employed in microwave photonics [9] and known as subcarrier multiplexing (SCM) to provide parallel QKD. In [10] we have proposed the extension of frequency coding to multiple subcarriers, showing that it opens the possibility of parallel quantum key distribution and, therefore, of a potential substantial improvement in the bit rate of such system. In this paper we provide for the first time, to our knowledge, an experimental demonstration of the feasibility of Subcarrier Multiplexed Quantum Key distribution. The experiment shows the correct operation as far as microwave sideband interference and suppression is concerned for a two subcarrier (@ 10 and 15 GHz respectively) system in terms of the different values of the phase-shift bases selected by Alice and Bob.

II. THEORETICAL FUNDAMENTALS

A. Basic Overall system operation

The concept behind subcarrier multiplexed quantum key distribution (SCM-QKD) can be explained referring to Fig. 1. A faint pulse laser source, emitting at frequency w_o is externally modulated by N radiofrequency subcarriers by Alice. Each subcarrier, generated by an independent voltage controlled oscillator (VCO) is randomly phase modulated, Φ_{1i}, among four possible values $0, \pi$ and $\pi/2, 3\pi/2$, which, as mentioned above, form a pair of conjugated bases. The compound signal is then sent through an optical fiber link and upon reaching Bob's location, is externally modulated by N identical subcarriers in a second modulator. These subcarriers are phase modulated Φ_{2i} among two possible values 0 and $\pi/2$ which represent the choice between the two encoding bases.

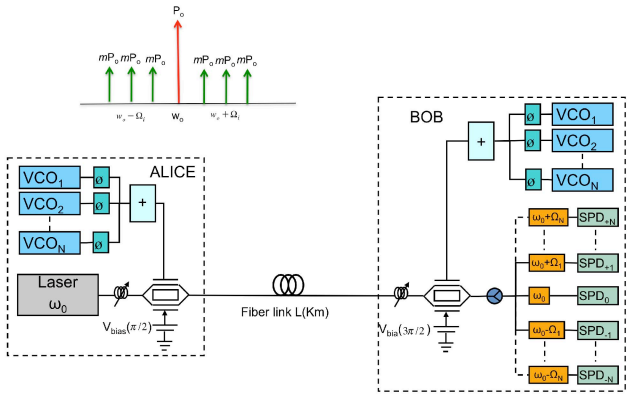


Figure 1. SCM_QKD system Layout [20].

As a consequence, an interference single-photon signal can be generated at each of the sidebands (upper and lower) of each subcarrier. For a given subcarrier $\Omega_i = 2\pi f_i$, if Bob and Alice's bases match, then the photon will be detected with probability 1 by either the detector placed after the filter centered at $w_o + \Omega_i$ or by the detector placed after the filter centered at $w_o - \Omega_i$. If, on the contrary, Bob and Alice's bases do not match there will be an equal probability of ½ of detecting the single photon at any of the two detectors and this detection will be discarded in a subsequent procedure of public discussion.

B. System Equations

According to the results derived in [10] if I_e represents the input optical intensity to Alice's modulator, and the modulation index of each subcarrier is assumed to be equal to *m*, then the output intensities for the upper and lower sidebands at frequency Ω_i after optical filtering and detection are given by:

$$I^S_{\Omega_i} = \frac{I_e m^2}{8}\sin^2\frac{\Delta\Phi_i}{2}$$
$$I^S_{-\Omega_i} = \frac{I_e m^2}{8}\cos^2\frac{\Delta\Phi_i}{2} \qquad (1)$$

In the above equations, $\Delta\Phi_i$ represents the mismatch between the phases inscribed by Alice and Bob into the subcarrier at Ω_i. The correct choice of base by Bob for subcarrier Ω_i results in either $\Delta\Phi_i = 0$ or $\Delta\Phi_i = \pi$ depending on whether a "0" or a "1" is sent by Alice. This, in turn implies, according to (1) that the upper or lower sideband is eliminated respectively due to interference.

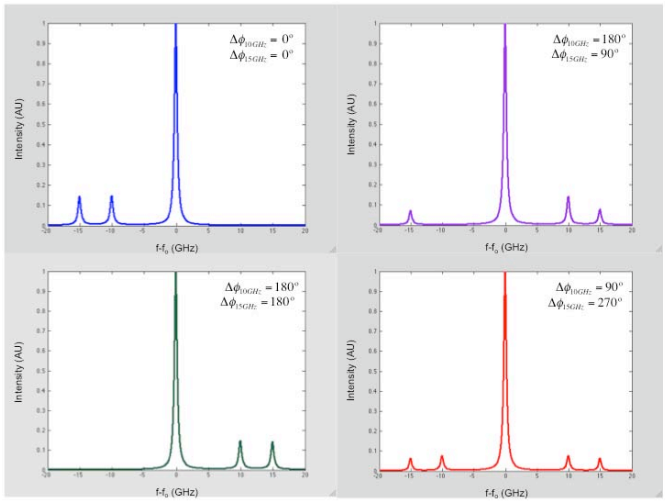


Figure 2. Theoretical spectral results for a 2 subcarrier SCM_QKD system and different phase mismatch values between Alice and Bob. Subcarrier frequencias are 10 and 15 GHz respectively.

When Bob chooses the incorrect basis, then $\Delta\Phi_i = \pm\pi/2$ and therefore none of the sidebands is eliminated. Figures 2 and 3 show several examples for an ideal two subcarrier QKD system. The subcarriers are 10 and 15 GHz respectively. The inset in each figure displays for each subcarrier the phase mismatch between Alice and Bob.

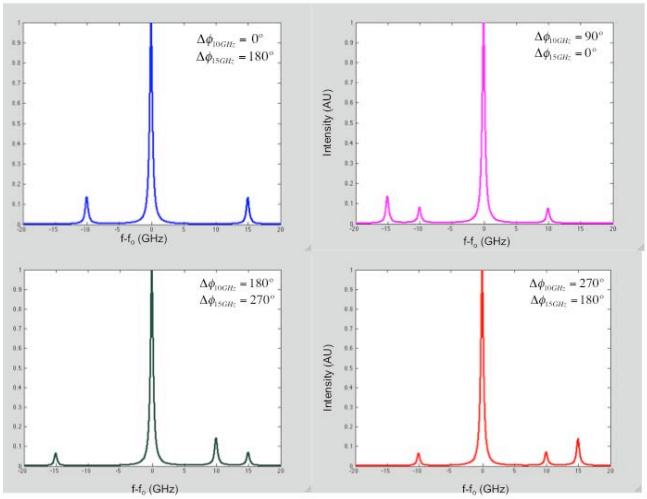


Figure 3. More theoretical spectral results for a 2 subcarrier SCM_QKD system and different phase mismatch values between Alice and Bob. Subcarrier frequencias are 10 and 15 GHz respectively.

III. EXPERIMENT

To test the feasibility of the SCM-QKD technique we assembled in the laboratory the layout shown in figure 4.

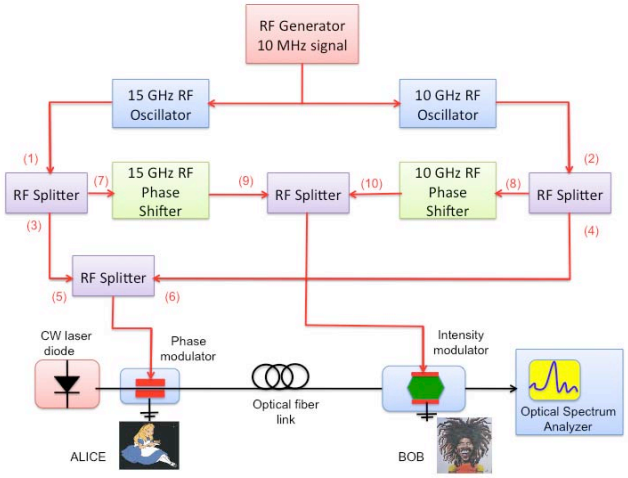


Figure 4. Experimental setup assembled in the laboratory to test the feasibility of a two channel subcarrier multiplexed quantum key distribution system.

A. *Setup Description*

Referring to figure 4, a 10 MHz RF generator is used to provide a driving signal to the two microwave oscillators producing the subcarriers at 10 and 15 GHz (points (1) and (2)) respectively. Two RF splitters placed at the output of both oscillators equally divide their output powers and direct half of the power towards Alice's modulator (points (3) and (4)) and half of the power towards Bob's modulator (points (7) and (8)). In our laboratory setup the phase-shifts introduced by Alice are fixed (not tunable) and the different values were achieved by introduction of proper lengths of RF cable between points (3)-(5) and points (4)-(6) respectively. In any case the system was calibrated in order to assure equal RF amplitudes for both subcarriers at the input of Alice's modulator. Phase shifts introduced at Bob's location however were tunable since two eight bit tunable phase shifters were placed between points (7)-(9) for the 10 GHz subcarrier and between points (8) and (10) for the 15 GHz subcarrier. Both phase shifters were computer controlled and were capable of providing full 360º phase shifts with a 1.4º resolution step. Bob's phase shifters were programmed to achieve the different phase mismatches to be tested in order to compare with the theoretical results provided by figures 2 and 3. The optical part is comprised of a CW laser diode operating at 1539.1 nm and providing 5 dBm output power. It should be pointed out that the experiments reported here are designed to confirm the proper spectral operation under a laser source operation. In this respect it is not necessary to attenuate the optical source power down to the single photon emission level. Alice's signal is introduced into the optical carrier by means of a 10 GHz JDSU Lithium Niobate Phase modulator. After propagation through a dispersive compensated fiber-optic link, the signal enters Bob's modulator which in this case is push-pull intensity modulator. The output signal from Bob's modulator is directed to an ANDO Optical Spectrum Analyzer featuring a 0.01 nm resolution.

B. *Experimental Results*

The results obtained for the phase shifts corresponding to figures 2 and 3 are shown in figures 5 and 6 respectively.

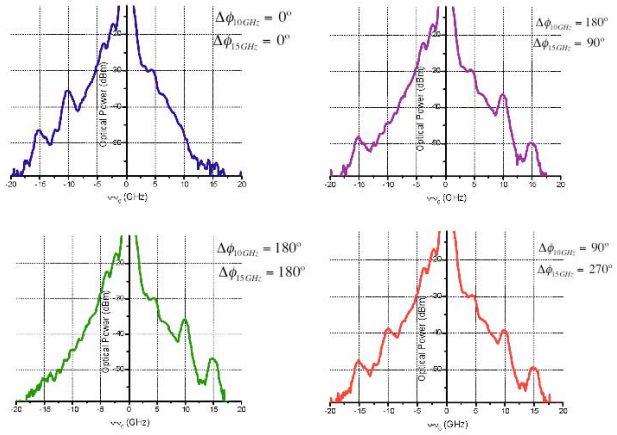


Figure 5. Experimental results corresponding to the 2 subcarrier SCM_QKD and the different phase mismatches between Alice and Bob of figure 2.

The experimental results are affected by the optical spectrum analyzer resolution which results in a convolution of the real spectrum with a 0.01 nm (i.e. 1.25 GHz) lorentzian function. Note as well that experimental results are plotted in logarithmic rather than natural units. Nevertheless, the presence and absence of RF sidebands due to constructive and destructive interference can be readily checked as well as the presence of equal amplitude sidebands when the bases chosen by Alice and Bob do not match. The matching between experimental and theoretical results is remarkable and shows the feasibility of SCM QKD systems in the single photon operation limit.

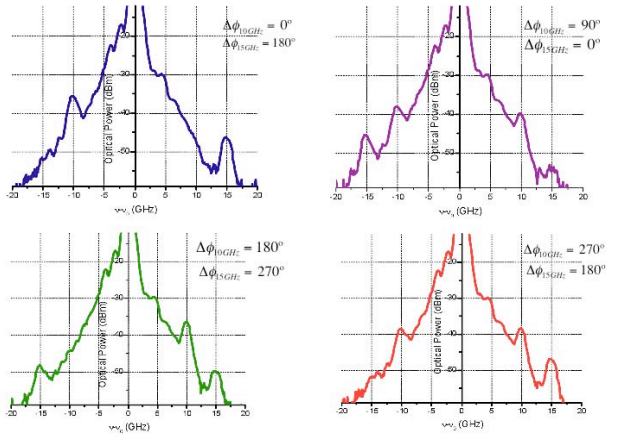


Figure 6. Experimental results corresponding to the 2 subcarrier SCM_QKD and the different phase mismatches between Alice and Bob of figure 3.

IV. SUMMARY AND CONCLUSIONS

In summary, we have provided for the first time, to our knowledge, an experimental demonstration of the feasibility of Subcarrier Multiplexed Quantum Key distribution.

ACKNOWLEDGMENT

This work was supported in part by the Spanish Government through Quantum Optical Information Technology (QOIT), a CONSOLIDER-INGENIO 2010 Project and in part by the Generalitat Valenciana through the PROMETEO 2008/092 research excellency award.

REFERENCES

[1] S. Wiesner, 'Conjugate coding ', SIGACT News 15, 77-88,1983.

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

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, 'Quantum Cryptography' ,Rev. Mod. Phys. Vol. 74, pp. 145-195, 2002.

[4] J-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes, 'Single-photon interefrence in Sidebands of Phase-Modulated Light for Quantum Cryptography', Phys. Rev. Lett. Vol. 82, pp. 1656-1659, 1999.

[5] J-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, H. Porte, and W. T. Rhodes, 'Phase-modulation transmission system for quantum cryptography,Opt. Lett. Vol. 24, pp. 104-106, 1999.

[6] O. Guerreau, J-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer, and F. J. Malassenet, ' Long distance QKD transmission using single-sideband detection detection scheme with WDM synchronization' ,IEEE J. Sel. Top. Quantum Electron. Vol. 9, pp. 1533-1540, 2003.

[7] C. H. Bennett, Phys., 'Quantum cryptography using any two non-orthogonal states', Rev. Lett. Vol. 68, (3121), 1992.

[8] J-M. Mérolla, L. Duraffourg, J. P. Goedgebuer, A. Soujaeff, F. Patois, and W. T. Rhodes, 'Integrated quantum key distribution system using single sideband detection', Eur. Phys. J. D Vol. 18, pp. 141-146, 2002.

[9] A. Ortigosa-Blanch and J. Capmany, 'Subcarrier multiplexing optical quantum key distribution', Phys. Rev. A, (024305), 2006.

[10] J. Capmany and D. Novak, 'Microwave Photonics combines two worlds', Nature Photonics, Vol. 1, pp. 319-330, 2007.