Practical Quantum Key Distribution based on the BB84 protocol

A. Ruiz-Alba, D. Calvo, V. Garcia-Muñoz, A. Martinez, W. Amaya, J.G. Rozo, J. Mora, J. Capmany
Instituto de Telecomunicaciones y Aplicaciones Multimedia, Universidad Politécnica de Valencia, 8G Building-access D-Camino de Vera s/n-46022 Valencia (Spain)
Corresponding author: jcapmany@iteam.upv.es

Abstract

This paper provides a review of the most important and widely used Quantum Key Distribution systems and then describes our recently proposed scheme based on Subcarrier Multiplexing that opens the possibility of parallel Quantum Key Distribution. We report the first-ever experimental implementation of parallel quantum key distribution using this technique showing a maximum multiplexing gain.

Keywords: Optical fiber communications, quantum information, quantum key distribution, subcarrier multiplexing.

1. Introduction

Quantum Cryptography features a unique way of sharing a random sequence of bits between users with a certifiably security not attainable with either public or secret-key classical cryptographic systems. This is achieved by means of Quantum Key Distribution (QKD) techniques, which rely on exploiting the laws of quantum mechanics [1]. Indeed, only systems based on QKD techniques can offer unconditional security without imposing any computational assumptions [2].

A main limitation of QKD systems, and still to be solved, is the fact that bit rates are very low compared to those used in classical telecommunications [3]. One of the main restrictions to date relies on photon sources and the so-called photon guns are far from ready. An alternative and also a complementary approach to increase the bit rate is to make QKD systems work in parallel. This simple engineering approach becomes a challenge when working with quantum systems: The system should work in parallel but still rely on just one source and 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.

In this context, recent progress in the literature [4] remarks that photonics is a key enabling technology for implementing commercial QKD systems to become a competitive technology in Information Security. For this to happen at a reasonable cost, it is fundamental to take advantage of the currently available generation of photonic components developed for applications in the telecommunications field. Therefore, our overall objective is to implement and demonstrate practical QKD systems based on available optical communication devices and optical multiplexing techniques feature securing operation outperforming currently available alternatives.

The paper is organized as follows. In section 2 we provide some basic notions of QKD, including the description of the generic settings and techniques so far proposed for its implementation and the most typical protocol, known as BB84. In section 3, we present different configurations reported in the literature that allow the

implementation of the BB84 protocol by using optical polarization, optical phase or frequency modulation as encoding techniques. Section 4 presents the theoretical principles of a quantum key distribution system that opens the possibility of parallel: quantum key distribution based on subcarrier multiplexing (SCM) technique or SCM-QKD. In section 5 we report some preliminary results of an experimental prototype for a SCM-QKD implementation operating with two radiofrequency subcarriers. The obtained results in quantum and classical regime demonstrate the system feasibility.

2. SRR-loaded CPW models

Figure 1 illustrates a typical QKD system. Two partners who are traditionally called Alice and Bob want to establish a secret key at a distance. They need to be connected by two channels: a quantum channel, allowing them to share quantum signals; and a classical channel, -which needs to be authenticated-, (i.e Alice and Bob must certifiably identify themselves). On the other hand, a third person can listen to the conversation but cannot participate in it. The quantum channel, however, is open to any possible manipulation from a third party. Specifically, the task of Alice and Bob is to guarantee security against an adversarial eavesdropper, usually called Eve, tapping on the quantum channel and listening to the exchanges on the classical channel [2, 3].

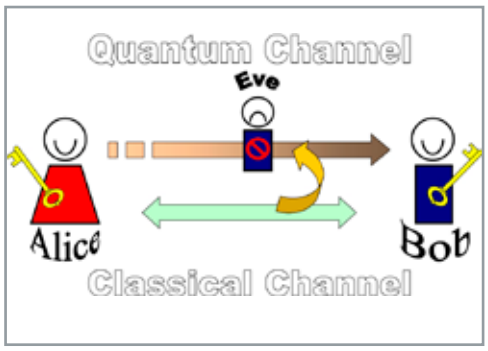

Figure 1. *Diagram of a QKD system where Alice and Bob are connected by a quantum channel into which Eve can tap without any restriction other than the laws of physics; and by an authenticated classical channel, into which Eve can only listen to.*

The fact that security can be based on general principles of quantum physics suggests the possibility of unconditional security, i.e. the possibility of guaranteeing security without imposing any restriction on the power of the eavesdropper. Indeed, the origin of security of QKD can be traced back to some fundamental principles of quantum physics. Firstly, a well-know principle of quantum physics establishes that measurement in general modifies the state of the measure systems and secondly, the no-cloning theorem which states that one cannot duplicate an unknown quantum state while keeping the original intact [5]. Both these arguments are exploited in the BB84 protocol, probably the best known and most widely employed scheme in QKD systems.

The BB84 protocol is a discrete variable coding named after its inventors Charles Bennet and Gilles Brassard and the year of its first publication (1984) [1]. In this protocol, Alice prepares and sends to Bob a set of random qubits. These are selected from the following set of four states:

$$\text{Base 1} \longleftrightarrow \begin{cases} |\psi_0\rangle = |0\rangle \\ |\psi_1\rangle = |1\rangle \end{cases}$$

$$\text{Base 2} \longleftrightarrow \begin{cases} |\psi_+\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \\ |\psi_-\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right] \end{cases} \qquad [1]$$

The first two states in (1) form one base of a quantum two dimensional system while the other two from a second one. Therefore, the conditions $\langle\psi_0|\psi_1\rangle = 0$ and $\langle\psi_+|\psi_-\rangle = 0$ corresponding to scalar products between states have to be satisfied. At the same time, the states in the different basis of (1) are not orthogonal and have maximum overlapping. As a consequence, there is no measurement procedure that can determine with 100% certainty the specific state which is prepared by Alice and it is sent to Bob.

For every incoming state from Alice, Bob randomly chooses one of the two basis to measure, either Base 1 or Base 2, performs the measurement and records the results. This measurement procedure employed by Bob allows the determination of the bit sent by Alice. Once quantum communication has finished, Bob and Alice use a public channel to communicate certain properties relative to the states that she has sent and he has measured. Specifically, Bob announces the position of the detected bits and the basis used, this stream is called raw key. Alice and Bob retain the bits for which the basis employed in the encoding and the decoding processes coincide and discard the rest. In this base reconciliation, Alice does not reveal the particular value of the state and Bob does not indicate the results of the measurement. This roughly results in a subset of around half of the bits originally detected by Bob. This subset is called the sifted key.

In the process of qubit sending from Alice to Bob an eavesdropper, known as Eve, can intercept some or all of them interfering the communication process. Eve can implement this attack through a kind of channel measurement, for example a projective measurement carried over the qubit, by means of an intercept and re-resend scheme. As it has been mentioned before, in the second part of this protocol Alice and Bob

The properties of these structures can be controlled by properly de–signing the loading elements

Left-handed substances have negative index of refraction, negative phase advance, and the reversal of the Doppler shift and Vavilov-Cerenk–ov effect

make public the basis employed to encode and detect the bits respectively the outcome of this process resulting in the generation of the raw key. In principle, it is thought possible for the eavesdropper Eve to know part of the key but the QKD system permits Alice and Bob to detect the presence of Eve. Note that Eve has to choose one of the basis to perform the projective measurement and determine incoming state. Therefore, she has a 50% probability of employing the incorrect base in her measurements resulting in a disagreement between what Bob detects and Alice has sent. In this way, Alice and Bob have a very simple way to detect the presence of Eve by performing an error detection check by sharing a subset of the bits. If the error rate of this process is small then Alice and Bob can perform other processes known as error correction and privacy amplification over the rest of the bits in the key that have not been made public. Privacy amplification is a classical operation and can be carried out, for example, by taking pairs of bits in the key and performing an OR exclusive operation. If Alice and Bob obtain the same result they retain the pair of bits. Otherwise they discard both of them. The unconditional security of the BB84 protocol has been proved with many different techniques [6, 7].

3. Review of Fiber Optic Quantum Key Distribution Systems

Basically, the BB84 protocol has been implemented through different experimental schemes that we describe in this section.

3.1. Polarization Encoding Systems

A QKD system with the BB84 protocol using the polarization of photons is shown in figure 2. Alice's transmitter consists of four laser diodes which emit short classical photon pulses polarized at $-\pi/4$, 0, $\pi/4$, and $\pi/2$. For a given bit, a single diode is triggered. The pulses are then attenuated by a set of filters to reduce the average number of photons lower than 1, and sent along the quantum channel to Alice. It is essential that the pulses remain polarized for Bob to be able to extract the information encoded by Alice.

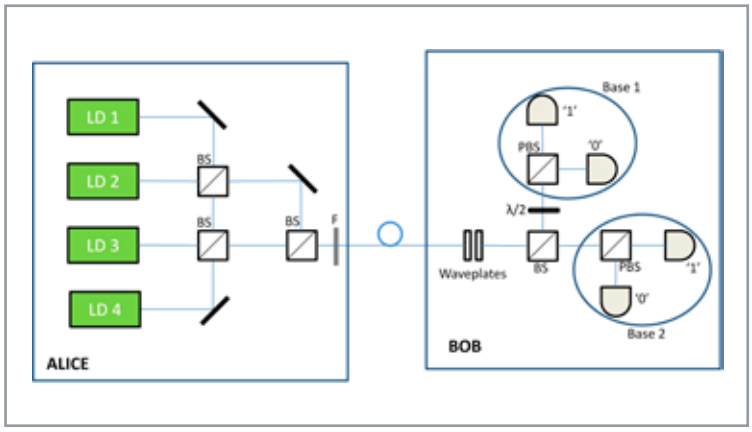

Figure 2. *Layout of a typical BB84 QKD system based on Polarization encoding.*

When the pulses reach Bob's location they are extracted from the fiber and travel through a set of waveplates used to recover the initial polarization states by compensating for the transformation induced by the optical fiber. After that, the pulses reach a symmetric beamsplitter (BS), implementing the random base choice. The Base 1 is performed with the rotation of the polarization state with a waveplate by $\pi/4$. Transmitted photons are analyzed in this vertical-horizontal base with a polarizing BS and two photon-counting detectors. Also, the photons are analyzed with a second set of polarizing BS and photon-counting detectors that characterize Base 2. As example, we consider a photon polarized at $\pi/4$ that Alice emits and launches into the optical fiber link. At Bob's end, if it chooses the output of the BS corresponding to Base 2 (vertical-horizontal), it will experience an equal probability of reflection or transmission at the polarizing BS, yielding a random outcome. On the other hand, if it chooses the diagonal Base 1, its state will be rotated to $\pi/4$. The polarizing BS will then reflect it with unit probability, yielding a deterministic outcome.

Antoine Buller and co-workers [8] have used such a system to perform QKD experiments over optical fibers. They created a key over a distance of 1100 meters with photons at 800 nm. In order to increase the transmission distance, they repeated the experiment with photons at 1300 nm and created a key over a distance of 23 km [9]. Record rates over 1Mb/s have been reported by Tang et al from NIST [10] and a distance record or 200 Km featuring a key rate of 15 bit/s has been very recently reported by Liu et al [11].

3.2. Phase Encoding Systems

Although the original BB84 coding scheme was designed to exploit the quantum properties of single photon polarization states, phase coding schemes can also be realized [12]. These coding schemes are based on the properties of interferometers and the coding is implemented by changing the relative optical path lengths or phase between the internal arms of the interferometer. Two typical layouts to implement a BB84 protocol are shown in figure 3 which are based on a Mach-Zehnder interferometer (single or unbalanced).

Figure 3(a) shows how Alice and Bob can control a phase modulator in their respective half of the interferometer. If Alice sends a single photon into this device an interference phenomenon will be observed, the photon will be detected at only one of Bob's photodetectors, either "0" or "1", with a probability that varies with the phase difference $\Delta\varphi=\varphi_A-\varphi_B$ in an identical fashion to the classical interference pattern.

If, for example, $\Delta\varphi=0$ the photon will arrive at detector "0", whereas if $\Delta\varphi=\pi$ the photon will arrive at detector "1". For intermediate values of the photon behaves probabilistically; for example, if

$\Delta\varphi=\pi/2$ or $\Delta\varphi=-\pi/2$ the photon is equally likely to be observes at "0" or "1". If any measurement is applied to this system to determine which arm the photon is "in" then the interference, or phase, information is destroyed.

The main problem of this configuration is that it is practically impossible to keep the path difference stable when Alice and Bob are separated by more than a few meters. In order to overcome this limitation, Bennet proposed the use of two unbalanced Mach-Zehnder interferometers, one for Alice and one for Bob, connected in series by a single optical fiber, as shown in figure 3(b).

Townsed and co-workers [13], were the first to test this system over a fiber optic spool of 10 Km. To our knowledge, record values using this approach have been reported in [14] where a secure key rate of 1.02Mbit/s for a fiber distance of 20 km and 10.1 kbit/s for 100 km have been demonstrated by Shields an co-workers at Toshiba.

3.3. Frequency Coded Systems

As we have shown in previous subsection, phase-based systems for QKD require phase synchronization and stabilization. Because of the high frequency of optical waves (approximately 200 THz at 1550 nm), this condition is difficult to fulfill. To overcome this limitation Goedgebuer and co-workers [15] proposed an alternative solution where the value of the bits is coded in the relative phase between sidebands of a central optical frequency subject to radiofrequency modulation. This is known as the frequency coding approach illustrated in figure 4.

The technique implements the BB84 protocol as follows [16]: A source emits short pulses of classical monochromatic light with angular frequency ω_0. A first electrooptical modulator EOMA modulates the phase of this beam with a radiofrequency $\Omega<<\omega_0$ and a small modulation depth. Two sidebands are thus generated at frequencies $\omega_0\pm\Omega$. The phase modulator is driven by a radio-frequency local oscillator LO_A whose phase φ_A can be varied among four phase values 0, π and $\pi/2$, $3\pi/2$, which form a pair of conjugate basis. Finally, the beam is attenuated so that the sidebands contain much less than one photon per pulse, while the central peak remains classical. After the transmission link, the beam experiences a second modulation applied by an electrooptical modulator EOM_B. This phase modulator is driven by a second radio-frequency local oscillator LO_B with the same frequency Ω and phase φ_B which can be varied among two phase values 0 and $\pi/2$ which represent the choice between the two encoding basis.

These oscillators must be synchronized. After passing through this device, the beam contains the original central frequency ω_0, the sidebands created by Alice, and the sidebands created by Bob. The sidebands at frequencies $\omega_0\pm\Omega$ are mutually coherent and thus interfere. Bob can then record the interference pattern in these sidebands after removal of the central frequency and the higher-order sidebands with an optical filter. The advantage of this setup is that the interference is controlled by the phase of the radio frequency oscillators. Their frequency is six orders of magnitude smaller than the optical frequency and thus considerably easier to stabilize and synchronize [17].

Merolla and co-workers, using this approach, have reported in [18] a secure key rate of 19.2bit/s for a fiber distance of 50 km.

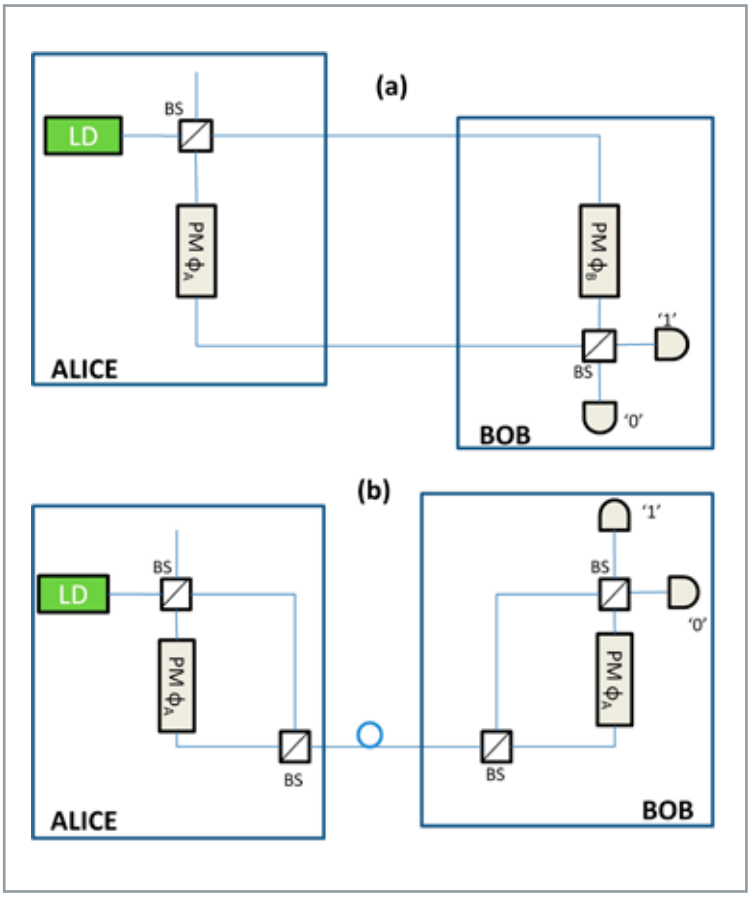

Figure 3. *Layout of a QKD system using Phase coding for (a) single Mach-Zehnder configuration and (b) unbalanced Mach-Zehnder configuration.*

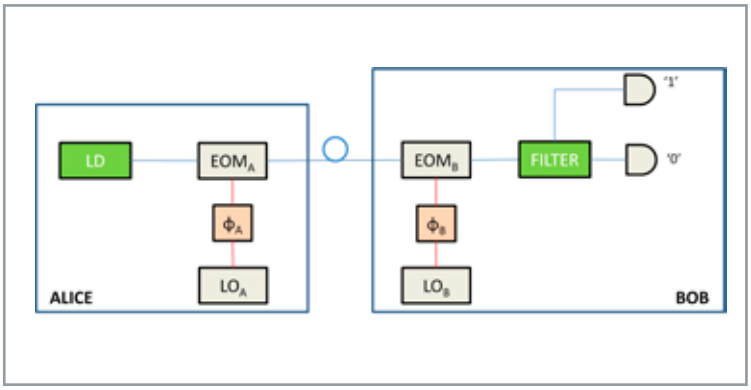

Figure 4. *Layout of a Frequency Coded QKD transmission system.*

4. Description of SCM-QKD Systems

We have proposed to apply the the concept of subcarrier multiplexing to extend the capacity of frequency coding schemes for QKD systems. We show here that by taking advantage of the fact that quantum mechanics allows for multiple-frequency measurements, multiple subcarrier frequencies can be simultaneously used to increase the bit rate without compromising the security of the protocol. SCM-QKD can be explained referring to figure 5. A faint pulse laser source emitting at frequency $\omega_0=2\pi f_0$ is externally modulated by N radiofrequency subcarriers by Alice. Each subcarrier with angular frequency $\Omega_i=2\pi f_i$, is generated by a local oscillator (LO_i) and randomly phase modulated among four possible values 0, π and $\pi/2$, $3\pi/2$ which let the encoding of the bits and form a pair of conjugated basis required to implement a BB84 protocol. 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 among two possible values 0 and $\pi/2$, which represent the choice between the two basis, to decode the bits. As a consequence, an interference single-photon signal is generated at each of the sidebands (upper and lower) of each subcarrier.

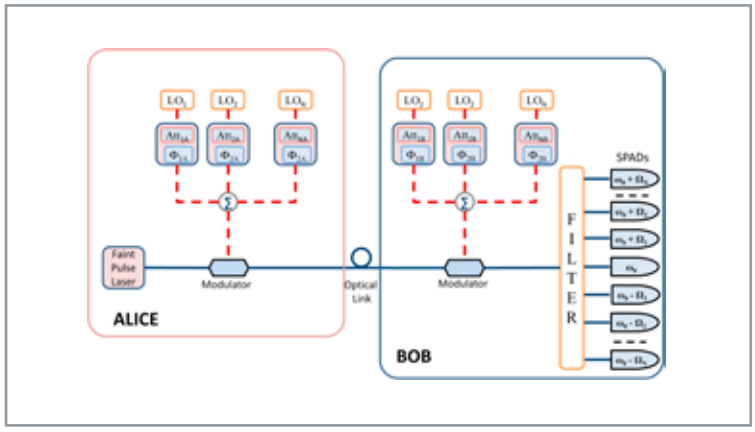

Figure 5. *SCM-QKD system layout (electrical signal is in dashed line, optical signal in solid line). SPAD: Single Photon Avalanche Detector.*

According to the results derived in [19], the detection probabilities at each of the detectors placed after the filters centered at the Upper Sideband (USB) and the Lower Sideband (LSB) for each subcarrier, which correspond to $\omega_0+\Omega_i$ and at $\omega_0-\Omega_i$, respectively, are given by:

$$\text{Base } 2 \longleftrightarrow \begin{cases} |\psi_+\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \\ |\psi_-\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right] \end{cases} \quad (2)$$

In the above expression, ρ is the detection efficieny, μ_i represents the mean photon number per bit emitted by the laser source for subcarrier Ω_i, T_i is the end-to-end optical link transmission efficiency for subcarrier Ω_i, V is the visibility, and $\Delta\Phi_i$ represents the mismatch between the phases inscribed by Alice and Bob into the subcarrier at Ω_i. The correct choice of the basis by Bob for subcarrier Ω_i results in either $\Delta\Phi_i=0$ or $\Delta\Phi_i=\pi$ depending on whether a '0' or '1' is sent by Alice. This implies, according to (2), that either the LSB or the USB is eliminated respectively due to interference. When Bob chooses the incorrect base, then $\Delta\Phi_i=\pm\pi/2$ and none of the sidebands is eliminated since the detection probability is equal for USB and LSB.

For the sake of simplicity and for illustrative purposes, we consider here the case where Alice and Bob implement the system using six different microwave signals with frequencies $f_i=\Omega_i/2\pi$. With this approach we have performed extensive simulations that include all the relevant parameters previously discussed as shown in Figure 6. When the relative phase difference $\Delta\Phi_i$ used by Alice and Bob is either 0 or π, the carrier and either upper frequencies or lower frequencies sidebands are detected. When $\Delta\Phi_i=\pm\pi/2$ then the carrier and all the sidebands are detected. However, as pointed out earlier, the main advantage of using this system is that it provides the possibility to Alice of sending different bits using two or more independently encoded different radio-frequency tones.

Specifically, figure 6(a) illustrates the case where there is a perfect matching between the basis employed by Alice and Bob for each subcarrier and Alice is sending the sequence 000000. In this case, all the frequencies f_i have a relative phase difference $\Delta\Phi_i= 0$ and consequently upper sidebands appear in the right side of the optical frequency spectrum. In the case represented in figure 6(b), there is a perfect matching between the basis employed by Alice and Bob for each subcarrier and Alice is sending the sequence 111111. The relative phase difference $\Delta\Phi_i = \pi$ for all subcarriers and consequently lower sidebands appear in the left side of the optical frequency spectrum.

On the other hand, figure 6(c) and 6(d) represents the case when the same sequence 011010 is sent from Alice to Bob where the first bit corresponds to the electrical subcarrier f6 and the last bit to the electrical subcarrier f1. Figure 6(c) shows the case where Bob chooses the incorrect base for all the subcarriers. In this case, the relative phase difference $\Delta\Phi_i =\pm\pi/2$ and according to (2) the probability is equal for USB and LSB and 12 optical sidebands appear as we can see in figure 6(c). In figure 6(d), Bob makes the correct base decision for odd subcarriers f_1, f_3 and f_5 (note a single optical sideband is obtained) and the incorrect for even subcarriers f_2, f_4 and f_6 (note two optical sidebands are obtained).

Therefore, the final transmitted bits are {100} since the 50% of the transmitted key is discarded due to the basis reconciliation.

In this context, the independence of the bits transmission between different subcarriers is clearly seen since the multiple subcarriers does not lead to interference between bits. The system can be secure against photon number splitting attacks if the reference optical carrier is filtered and detected since Bob gets a time reference for detection and he will gather information about possible attacks of the fiber link at the same time [20].

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 above objective is fulfilled. For a single channel the rate of the sifted key as a function of distance is given by:

$$R_{sifted}(\Omega_i) = \frac{1}{2}\rho T_i \mu_i f_{rep} \tag{3}$$

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 $I_{max}(A,E,\Omega_i)$ [6], which is given by

$$R_{net}(\Omega_i) = R_{sifted}(\Omega_i)\cdot\left[I(A,B,\Omega_i) - I^{max} I(A,E,\Omega_i) \right] \tag{4}$$

For the multiplexed system, the overall useful key rate is then given by:

$$R_{net}^{MUX} = \sum_{i=1}^{N} R_{net}(\Omega_i) \tag{5}$$

In figure 7 we have plotted with a blue line the useful key rate for $N=1$ with the following (typical) parameters; $f_{rep}=10MHz$, $V=98\%$, detector efficiency $\rho=0.1$, $\alpha=0.2\ dB/km$ and $T=10\ dB$. The curve features an exponential decrease first, and then, due to error correction and privacy amplification, the bit rate fell rapidly to zero.

For the sake of comparison with the frequency coding case *(i.e. N=1)*, we consider in figure 7 also the high *(N=50)*, intermediate *(N=30)* and low *(N=15)* count SCM-QKD options. All the curves show a similar behavior, the useful rate

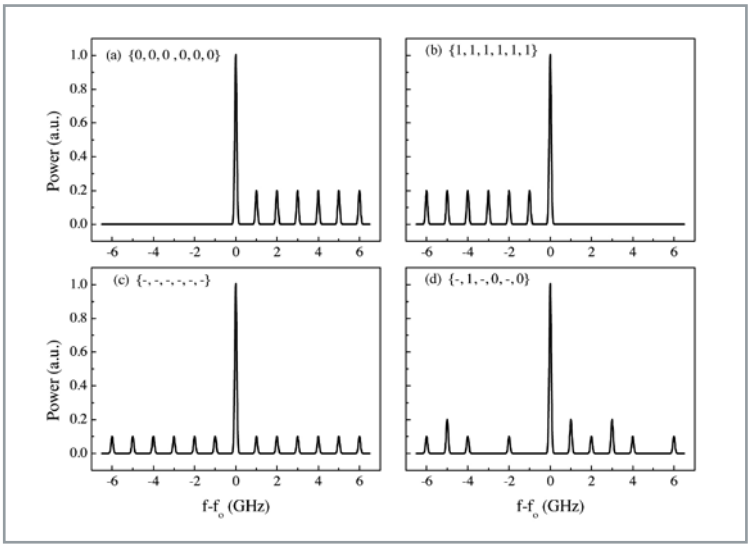

Figure 6. *Simulated power spectra for perfect matching between the basis employed by Alice and Bob for each subcarrier and Alice is sending (a) the sequence 000000 and (b) the sequence 111111. In case (c), Bob makes the incorrect basis decision for all the subcarriers and in case (d), Bob makes the correct basis decision for subcarriers f_1, f_3 and f_5. For cases (c) and (d), the sequence is 011010.*

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 for of link lengths spanning up to 85 Km. Nonlinear signal mixing effects start to be noticeable in the useful bit rate for modulation indexes close to 10%.

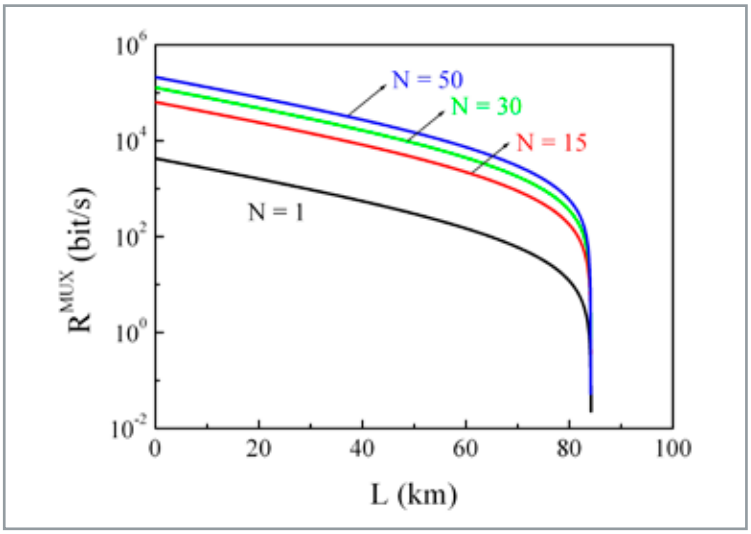

Figure 7. *Overall useful key rate values versus the optical fiber link length in Km, obtained for the three frequency plan (N=15, N=30 and N=50) systems and for the case of a frequency coded (N=1) system when the index modulation is m= 2 %.*

The multiplexing gain can be defined mathematically as:

$$M_G = \frac{R_{net}^{MUX}}{R_{net}(\Omega_1)} \quad (6)$$

where $R_{net}(\Omega_1)$ is the useful rate when $N=1$.

For instance, figure 8 shows the evolution of the multiplexing gain computed at L=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 that is faster the higher number of channels. These results, which have been computed for a particular source pulse repetition frequency ($f_{rep} = 10$ *MHz)*, scale with this parameter in terms of usable key bit rate.

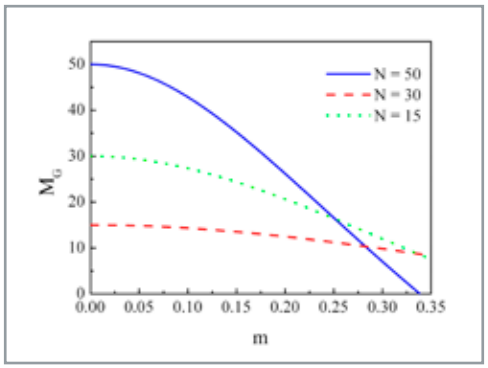

Figure 8. *Multiplexing gains in the overall useful key rate values versus the modulation index computed at z=30Km for the three frequency plan (N=15, N=30 and N=50) systems.*

5. Experimental demonstration

In order to demonstrate the SCM-QKD principle of operation, we have assembled an experimental testbed transmitting two subcarriers, which is shown in figure 9. It consists of two blocks, named Alice and Bob, interconnected by several meters of optical fiber. Alice's transmitter contains a tunable laser source with an emission wavelength of 1557.2 nm and 5 dBm of optical power. The laser output is strongly attenuated in order to achieve the quantum regime and pulsed with an amplitude modulator biased at the minimum transmission point. The electrical driving signal of the pulsed modulator is generated by the control system. The optical signal is modulated by a Phase Modulator (PM), the RF input of which is fed by two RF subcarriers at f1=10 and f2=15 GHz, respectively, which are produced by two independent local oscillators. To encode the binary secret key, Alice introduces a random and independent phase shift Φ_{1A} and Φ_{2A} for each subcarrier. An electrical attenuator is placed at the input of each phase shifter $(Att_{1A}$ and $Att_{2A})$ so as to control independently the modulation indexes of both subcarriers $(m_{1A}$ and $m_{2A})$

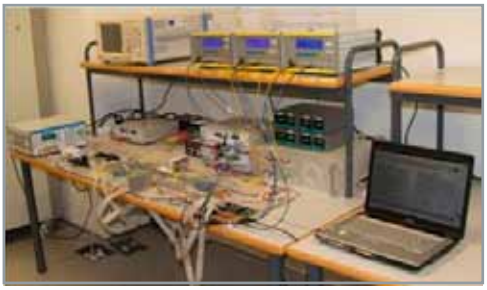

Figure 9. *Experimental setup assembled in the laboratory to test the feasibility of a two channel subcarrier multiplexed quantum key distribution system*

On the other hand, Bob has a similar configuration as Alice, but in this case the input signal of Bob is modulated by means of an Amplitude Modulator (AM) biased in quadrature. Bob can insert its own random phase shifts Φ_{1B} and Φ_{2B} and the attenuations Att_{1B} and Att_{2B} to control the RF signal driving its modulator. The phase shifts inserted in Alice and Bob are implemented using four eight-bit tunable RF phase shifters.

The four phase shifters are computer controlled independently and are capable of providing full 360º phase shifts with a 1.4º resolution step. The control system also provides full system synchronization and clock generation. The phase shifts inserted by Alice and Bob were implemented using four eight-bit tunable phase shifters. In figure 10 we can see a general a visual system description.

The system's performance was checked in the classical regime with the aid of an optical spectrum analyzer (OSA), featuring a 10 pm resolution, placed at the output of Bob's modulator. In figure 11 we can observe the theoretical and experimental signal for all the possible phase differences $\Delta\Phi_1 = \Phi_{1B} - \Phi_{1A}$ and $\Delta\Phi_2 = \Phi_{2B} - \Phi_{2A}$ corresponding to $f_1=10$ and $f_2=15$ *GHz*, respectively. The modulation indexes are around 3 % to guarantee a full multiplexing gain. The presence and absence of optical sidebands due to constructive and destructive interference can be readily checked which corresponds with the case that Alice and Bob choose the same base. The presence of equal amplitude sidebands corresponds with the case that the basis 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 classical regimen.

One of the main practical difficulties for the implementation of FC-QKD, and in particular SCM-QKD, is the filtering of each of the RF sidebands

Potential use of these miniaturized high-Q cells can be foreseen in biosensors and planar frequency filtering structures

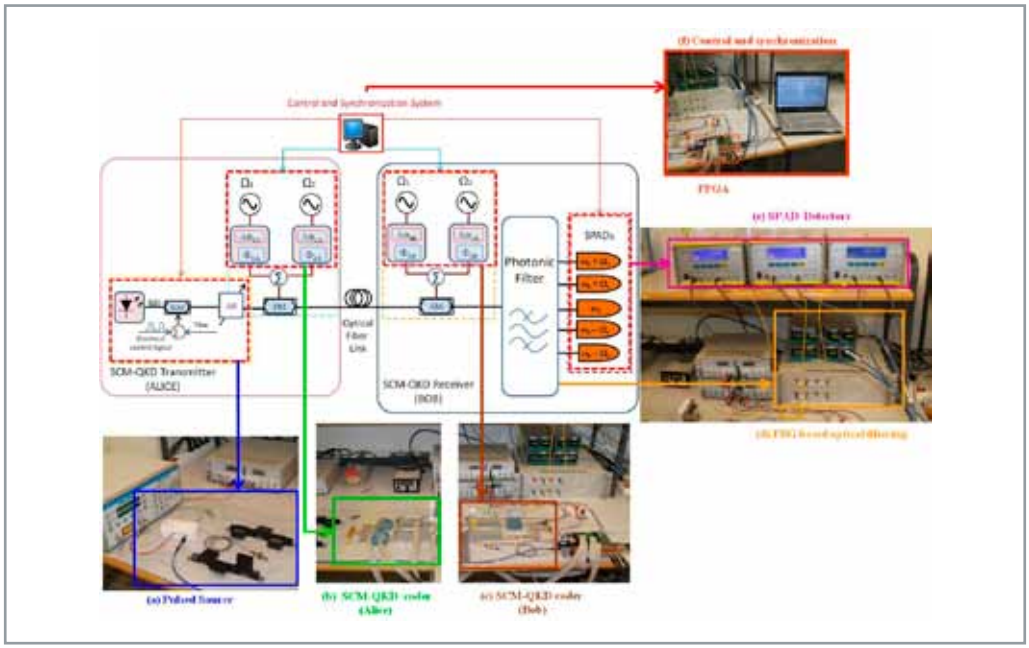

Figure 10. *Experimental setup assembled in the laboratory to test the feasibility of a two channel subcarrier multiplexed quantum key distribution system*

in the optical domain at the output of Bob's modulator. A photonic filter structure based on Fiber Bragg Gratings (FGBs) has been designed and fabricated to separate each sideband with an extinction ratio of 25 dB while introducing minimum insertion losses [21]. At each output of the filter structure we placed a Single Photon Avalanche Detector (SPAD) acting as photon counter.

We also checked the system performance in the quantum regime by attenuating the pulsed signal of Alice's source and placing SAPD's at the output of the filters as described in figure 10. The output pulses had a 1.3 ns FWHM with a repetition rate of 1 MHz. The SPADs worked with a detection gate width of 2.5 ns which was synchronized with the source, and a dead time of 10 μsec to avoid afterpulsing. The SPADs detection efficiency ρ was close to 10%, the dark count probability was 1.2×10^{-5}, and the measurement time per point was set to 25 s. The mean photon number is $\mu_1 = 0.35$ for 10 GHz and $\mu_2 = 0.25$ for 15 GHz. Note that these values are enough to guarantee unconditional security provided that decoy states [7] transmission is introduced in order to relax the requirements of the mean photon number at Alice's output.

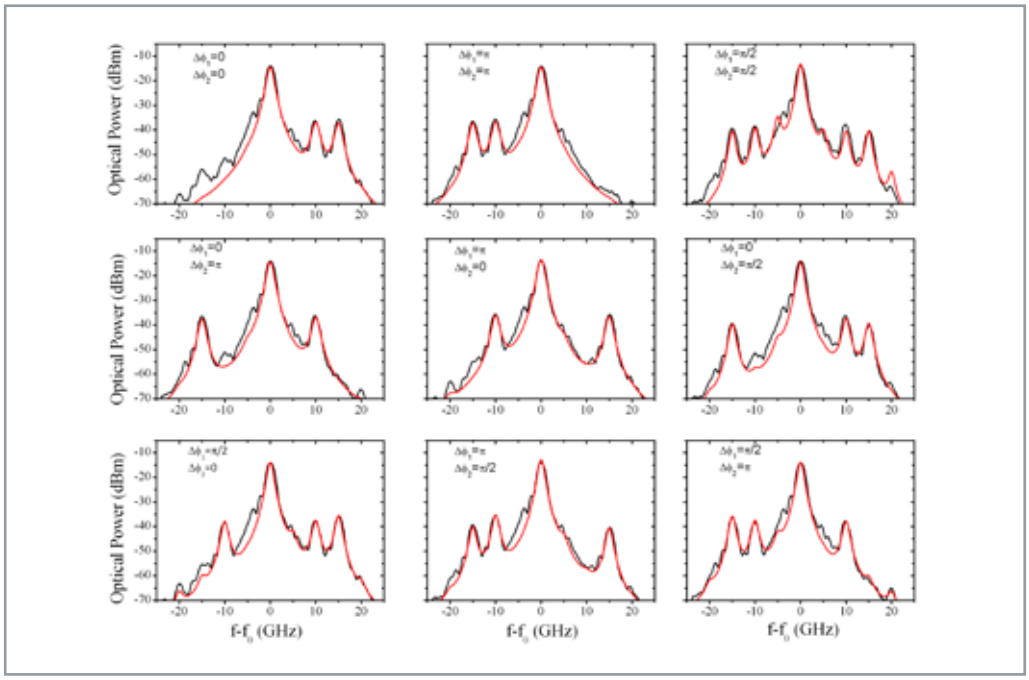

Figure 11. *Experimental (black line) and theoretical (red line) results and for a two subcarrier SCM-QKD system for different phase match values between Alice and Bob. Subcarrier frequencies are 10 and 15 GHz respectively.*

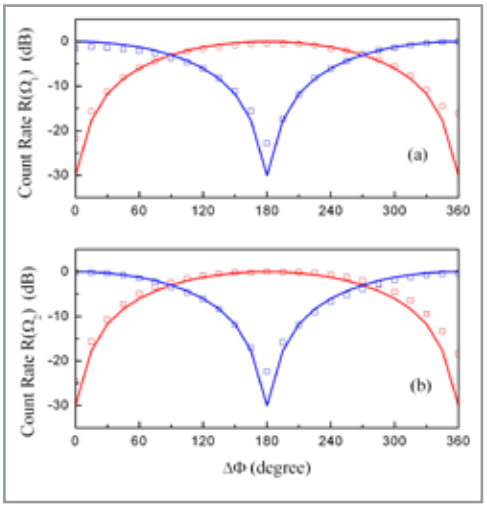

Figure 12. *Normalized SPADs count rate for (a) 10 GHz subcarrier and (b) 15 GHz subcarrier. Experimental upper band results are in marks (□) and lower band results are in marks (o). The corresponding theoretical predictions are in solid and dashed line, respectively.*

In figure 12 we plot the count rates $R(\Omega_1)$ and $R(\Omega_2)$ coming from the normalized accumulated counts for the 10 GHz and 15 GHz sidebands as a function of the phase difference. We can observe a visibility better than 98%. In addition, we have found that the maximum multiplexing rate $R_{MUX} = R(\Omega_1) + R(\Omega_2)$ is around 60 kbit/s coming from the individual single rates for each subcarrier R(W1) = 35 kbits/s and $R(\Omega_1)$ = 25 kbit/s. Therefore, we have obtained a maximum multiplexing gain close to 3 dB which corresponds with the number of subcarriers N=2.

6. Conclusions

In this paper we have presented an overview of QKD technologies based on the BB84 protocol. We have described operating mechanisms, performance metrics and provided a brief discussion of its security against eavesdropping. We have also briefly described some state of the art configurations proposed in the literature to optically implement these systems by means of Polarization, Phase and Frequency encoding techniques.
The theoretical description of SCM-QKD systems which employ N subcarriers to independently encode N parallel keys or to multiply by N the rate of a single key has been subsequently addressed, showing the theoretical potentiality of this multiplexing technique to increase considerably the key rate. In addition, we have described the SCM-QKD demonstrator assembled at ITEAM premises which employs two radiofrequency subcarriers at 10GHz and 15 GHz in combination with a microwave photonic filter allowing the separation of each optical sideband in the optical domain. The system was tested under classical and quantum regimes by means of a faint pulse source with a rate of 1 MHz and a pulse width around 1.5 ns. The experimental measurements show the feasibility of obtaining visibility values close to 98% as required for the successful operation of these systems. Moreover, the theoretical predictions are in agreement with the experimental results demonstrating the real viability of the system.

Acknowledgments

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] 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, IEEE, New York, pp.175-179, 1984.
[2] V. Scarani, H.Bechmann- Pasquinucci, N.J. Cerf, N. Lütkenhaus, M. Peev, "The security of practical quantum key distribution", Reviews of modern physics vol. 81, pp. 1301-1310, 2009.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, "Quantum Cryptography", Rev. Mod. Phys., vol. 74, pp. 145-195, 2002.
[4] J. Capmany and D. Novak, "Microwave Photonics combines two worlds", Nature Photonics, vol. 1, pp. 319-330, 2007.
[5] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", Nature London, vol. 299, pp. 802-803, 1982.
[6] Shor, P. W., and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", Phys. Rev.Lett., vol. 85, pp. 441–444, 2000.
[7] Kraus, B., N. Gisin, and R. Renner, Phys. Rev. Lett., vol. 95, pp. 080501, 2005 .
[8] Muller, A., J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", Europhys. Lett., vol. 23, pp. 383–388, 1993
[9] Muller, A., H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed underlake telecom fibre", Europhys. Lett., vol. 33, pp. 335–339, 1996.
[10] X. Tang, L.Ma, A. Mink, A. Nakassis, H. Xu,B. Hershman, J. C. Bienfang, D. Su, R.F.Boisvert, C.W. Clark, and C. J. Williams, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s", Opt.Express, vol. 14, pp. 2062-2070, 2006.
[11] Y. Liu, T.Y.Chen, J.Wang,W.Q. Cai, X. W., L.K Chen, J. H. Wang, SB. Liu, H. Liang, L. Yang, C.-Z Peng, K.C., Z.-B Chen, and J.-W. Pan,"Decoy-

state quantum key distribution with polarized photons over 200 km", Opt. Express, vol. 18, pp. 8587-8594, 2010.
[12] Townsend, P., "Quantum cryptography on optical fiber networks", Opt. Fiber Technol. Mater, Devices Syst. vol. 4, pp 345–370, 1998.
[13] Townsend, P., J. G. Rarity, and P. R. Tapster, "Single photon interference in a 10 km long optical fiber interferometer", Electron. Lett. vol. 29, pp. 634–639, 1993.
[14] 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 . Express vol. 16, pp. 18790-18979, 2008.
[15] 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., vol. 82, pp. 1656-1659, 1999.
[16] 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.
[17] 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.
[18] Johann Cussey, Frédéric Patois, Nicolas Pelloquin and Jean-Marc Merolla. "High Frequency Spectral Domain QKD Architecture with Dispersion Management for WDM Network", OFC/NFOFC 2008.
[19] 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. vol. 15, pp. 1607-1621, 2009.
[20] O.L. Guerreau, F.J. Malassenet, S.W. McLaughlin, J.M. Merolla, "Quantum key distribution without a single-photon source using a strong reference," IEEE Photonics Technology Letters, vol.17, no.8, pp.1755-1757, Aug. 2005.
[21] J. Mora, A. Ruiz-Alba, W. Amaya, V. Garcia-Muñoz, A. Marti_nez, J. Capmany, "Microwave photonic filtering scheme for BB84 Subcarrier Multiplexed Quantum Key Distribution," Microwave Photonics (MWP), 2010 IEEE Topical Meeting on , vol., no., pp.286-289, 5-9 Oct. 2010.

Biographies

Antonio Ruiz-Alba was born in Madrid, Spain on 1982. He received the Licenciado en Ciencias Fisicas degree from the Universidad Autónoma de Madrid on 2007 and the M.Sc. degree in technologies, Systems and Network of Communication in the Universitat Politécnica de Valencia (UPV) in 2009. Since May 2008, he has been with the Optical and Quantum Communication Group at the iTEAM Research Institute, where he is currently working toward his Ph.D. degree in the field of quantum communication. His main re search interest is quantum key distribution systems and optical communications.

David Calvo was born in Alfaro, La Rioja, Spain in 1982. He received the M. Sc. degree in Computing Engineering from the Universidad Jaume I, Castellón, in 2006. He received the M. Sc. degree in Electronic Engineering from the Universidad de Valencia in 2009. From 2008 to 2009 he was at European Centre for Nuclear Research (CERN) in Switzerland where he worked in electronic design for electromagnetic calorimeter of ALICE detector. In 2009 he joined the Optical and Quantum Communication Group at the Universidad Politécnica de Valencia where he worked in the field of coupled resonator optical waveguides. He is currently working in quantum key distribution.

Víctor García-Muñoz was born in Alacant, Spain on 1977. He received the M. Sc. in physics degree from the Universidad de Valencia, Spain and the Nuclear Physics Master Degree from the Université de Paris XI, France both in 2001. In 2002 he was at the Universita di Pavia as part of the European Research Network MMCODEF working in the field of microwaves. He completed his Ph.D. in the Photonics Technology Group at the Universidad Politécnica de Madrid in 2008. His dissertation subject was related with the applications of Fiber Bragg Gratings (FBGs) to the processing of ultrafast optical signals. From june 2008 to August 2009 we worked at the Université polytechnique de Mons, Belgium where he was envolved in the study and reduction of the polarization related properties

of FGBs and in the applications of in-fiber sensing techniques to the fabrication of composite pieces. In september 2009 he joined the Optics and Quantum Communications Group at the Universidad Politecnica de Valencia as a Juan de la Cierva fellow where he works in the field of quantum key distribution and Optical Code Division Multiple Access (OCDMA).

Alfonso Martínez García was born in Cartagena, Murcia Spain, on 1976. He received the M. Sc. in Telecommunications Engineering from the Universidad Politécnica de Valencia (Spain) in 2000. Since 2001, he has been working at the Optical and Quantum Communications Group (OQCG) in the iTEAM Research Institute from Universidad Politécnica de Valencia. Since 2004, he is working as a teaching assistant at the Communications Department from Universidad Politécnica de Valencia. He is currently pursuing the Ph.D. degree in the field of optical packet switching. He has published more than 40 papers and conference contributions. His main research interests include Fiber Bragg Gratings applications, microwave photonics, wavelength conversion, quantum key distribution, optical packet switching and WDM-SCM networks.

Waldimar Amaya 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. 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 (OQCG), Institute of Telecommunications and Multimedia Research Institute - iTEAM, where he developed his PhD thesis and he obtained his PhD degree in telecommunications from the Universidad Politecnica de Valencia (UPV) Valencia, Spain, in 2008. Since 2009 he works with the OCQG – iTEAM as fellow research where he has continued with his work in optical signal processing and more recently in the field of quantum key distribution.

Juan Guillermo Rozo Chicué was born in Cali (Colombia) in 1985. He received the B.Sc. degree in Computer Engineering from the Universidad Libre Seccional (UL) Cali in 2008. Since June 2010, he has been with the Optical and Quantum Communications Group at the iTEAM Research Institute, where he is currently working toward his M.Sc. degree in Technologies, Systems and Networks of Communication in the Universidad Politécnica de Valencia (UPV), Valencia, Spain. His main research interests are cryptography and secure communications.

José Mora was born in Torrent, Valencia, Spain, on 1976. He received the M. Sc. in Physical Sciences from the Universidad de Valencia (Spain) in 1999. From 1999 to 2004, he worked in the Deparment of Applied Physic from the Universidad de Valencia. He holds a PhD. degree in Physics from the Universidad de Valencia in 2005 and he received the Extraordinary Doctorate Prize of the Universidad de Valencia in 2006. Since 2004, he joined as a researcher at the Optical and Quantum Communications Group in the Institute of Telecommunications and Multimedia Research Institute (ITEAM) from the Universitat Politècnica de València. He has published more than 100 papers and conference contributions covering a wide range of fields related to fiber bragg gratings for sensing applications, optical signal processing, microwave photonics, optical networks and quantum cryptography using photonic technology.