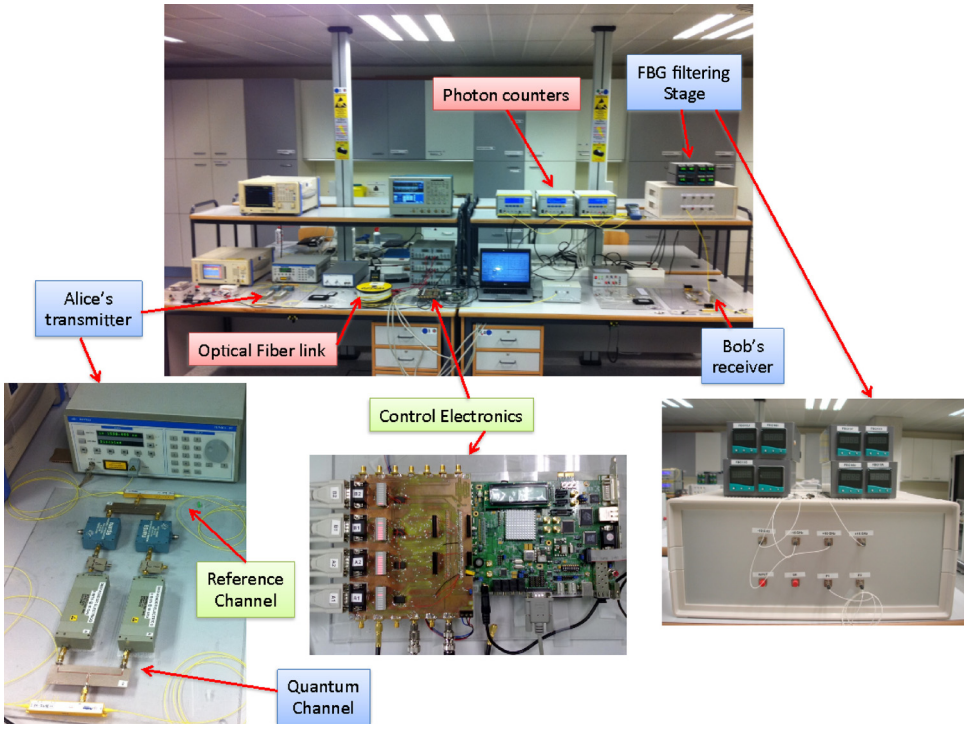
IEEE Photonics Journal
An IEEE Photonics Society Publication

Microwave Photonics Parallel Quantum Key Distribution

Volume 4, Number 3, June 2012

Antonio Ruiz-Alba
José Mora
Waldimar Amava
Alfonso Martínez
Víctor García-Muñoz
David Calvo
José Capmany



DOI: 10.1109/JPHOT.2012.2201255
1943-0655/$31.00 ©2012 IEEE

Microwave Photonics Parallel Quantum Key Distribution

Antonio Ruiz-Alba, José Mora, Waldimar Amaya, Alfonso Martínez, Víctor García-Muñoz, David Calvo, and José Capmany

Optical and Quantum Communications group, ITEAM Research Institute, Universitat Politécnica de Valencia, 46022 Valencia, Spain

DOI: 10.1109/JPHOT.2012.2201255

Manuscript received April 25, 2012; revised May 17, 2012; accepted May 18, 2012. Date of publication May 24, 2012; date of current version May 31, 2012. Corresponding author: J. Capmany (e-mail: jcapmany@dcom.upv.es).

Abstract: The incorporation of multiplexing techniques used in microwave photonics to quantum key distribution (QKD) systems brings important advantages by enabling the simultaneous and parallel delivery of multiple keys between a central station and different end-users in the context of multipoint access and metropolitan networks, or by providing higher key distribution rates in point to point links by suitably linking the parallel distributed keys. It also allows the coexistence of classical information and QKD channels over a single optical fiber infrastructure. In this paper, we show, for the first time to our knowledge, the successful operation of a two-domain (subcarrier and wavelength division) multiplexed strong reference BB84 QKD system. A four-independent channel QKD system featuring a sifted key rate of 10 kb/s/channel over an 11-km link with quantum bit error rate (QBER) $< 2\%$ is reported. These results open the way for multi-QKD over optical fiber networks.

Index Terms: Microwave photonics, quantum key distribution.

1. Introduction

Microwave photonics (MWP) [1], [2], the science and engineering field dealing with the study of photonic devices operating at microwave frequencies, and their application to microwave and optical systems is now expanding to address a number of novel and emerging applications, such as optical packet switching, optical probing, terahertz-wave generation and processing for noninvasive high resolution sensing and quantum communications. Within this last area, one of the most important application is quantum key distribution (QKD) [3], [4], in which techniques that rely on exploiting the laws of quantum mechanics are developed with the objective of sharing a random sequence of bits between two users, Alice and Bob, with a certifiably security not attainable with either public or secret-key classical cryptographic systems. Photonics has proved to be one of the principal enabling technologies for long-distance QKD using optical fiber links and several techniques have been proposed in the literature [5]–[18]. Initially investigated for point-to-point links, there is an increasing interest in its extension to network environments [19]–[22] where the use of multiplexing techniques can bring an added value for multi-user operation. The first reported results [20], [22], [23], based on wavelength division multiplexing (WDM) have explored the impact of one or several classical information channels over a solitary QKD channel, usually placed in a different spectral band, identifying the spontaneous Raman scattering as the dominant impairment from the strong signals. Very recently, a first WDM based QKD system using three different wavelengths in the C-Band has been reported [24], [25], featuring promising results which include a 200 kb/s key

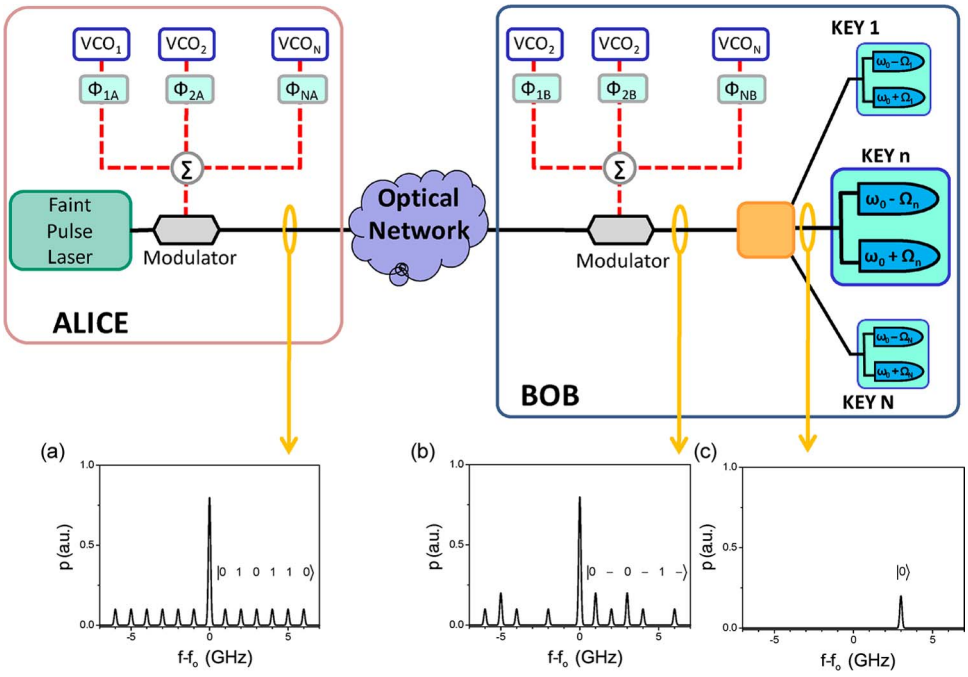


Fig. 1. SCM-QKD system layout to distribute N keys in parallel. Electrical signal is in dashed line and optical signal in solid line. Simulated probability distribution for (a) 6 bits transmitted in parallel by using both conjugated basis, (b) after detection in Bob's side measuring also in both basis and (c) result for a given user which receives correctly the bit "0".

generation rate with a 14.5 dB transmission loss using 1.22 GHz pulse generation rate. WDM multiplexing alone however, has the drawback of consuming a full wavelength channel for each key. A particularly interesting approach to distribute more than one key per wavelength is Subcarrier Multiplexed QKD [26] (SCM-QKD), a technique borrowed from MWP, which brings several advantages such as high spectral efficiency compatible with the actual key rates achieved by QKD systems, the sharing of the optical source by all the multiplexed channels, which reduces the complexity of the system and the possibility of upgrading with WDM in a two-tier scheme, to increase the number of parallel keys and to coexist with other classical information channels over the same fiber infrastructure.

This paper provides the first-ever, experimental demonstration of both SCM-QKD and WDM/SCM-QKD systems. The first case is implemented by independently modulating two subcarriers at 10 and 15 GHz which, in turn, modulate an optical carrier. The compound signal is delivered through an 11-km optical fiber length, representing a standard access network link, after which it is remodulated and the sidebands optically filtered previous to detection. Using a source providing 1 MHz pulse repetition rate we demonstrate the generation of two independent sifted keys at 10 kb/s featuring a quantum bit error rate (QBER) below 2% under a total system loss of 6.5 dB. The system is then WDM upgraded with a second optical carrier to demonstrate four independent 10 kb/s sifted keys with QBER $< 2\%$. In both cases, a classical reference channel used for system stabilization is also sent along the fiber link with a negligible impact due to Raman scattering.

2. Basic Principle

The operation principles of SCM-QKD [26] can be explained referring to Fig. 1. A faint pulse laser source emitting at frequency ω_o is externally modulated by N radio frequency subcarriers Ω_n $(n = 1, 2, \ldots, N)$ at Alice's location such that the mean photon number per pulse emitted by the laser source for subcarrier Ω_n verifies $\mu_n \leq 1$. For parallel key distribution, each subcarrier transmits a different key which is generated by an independent voltage controlled oscillator (VCO) randomly

phase-modulated among four possible values 0, π and $\pi/2$, $3\pi/2$ which form a pair of conjugate bases required to implement the Bennet-Brassard BB84 protocol [26], [27]. As example, Fig. 1(a) depicts the probability distribution for a situation where Alice transmits 6 keys in parallel. The compound signal is then sent by an optical fiber link through an optical network and, upon reaching Bob's location, is externally modulated by N identical subcarriers (now randomly phase-modulated among two possible values: 0 and $\pi/2$) [26], [27] in a second modulator. As a consequence, an interference single-photon signal is generated at each one of the sidebands (upper and lower) of each subcarrier with a certain probability as shown in Fig. 1(b). For a given parallel key, the detection probabilities at each one of the detectors placed after the filters centered at the Upper Sideband (USB) and the Lower Sideband (LSB) corresponding to $\omega_o + \Omega_n$, and $\omega_o - \Omega_n$, respectively, are given by

$$\begin{aligned} p_{USB}(\omega_0 + \Omega_n) &= \rho\mu_n T_n \cdot (1 + V\cos\Delta\Phi_n)/2 \\ p_{LSB}(\omega_0 - \Omega_n) &= \rho\mu_n T_n \cdot (1 - V\cos\Delta\Phi_n)/2. \end{aligned} \tag{1}$$

In the above expression, ρ is the detection efficiency, T_n is the end-to-end optical link transmission efficiency for subcarrier Ω_n, V is the system visibility, and $\Delta\Phi_n = \Phi_{An} - \Phi_{Bn}$ represents the mismatch between the phases Φ_{An} and Φ_{Bn} inscribed by Alice and Bob, respectively, into the subcarrier at Ω_n.

For a given subcarrier $\Omega_n = 2\pi f_n$, if Alice and Bob's bases match, then the photon will be detected with probability 1 by either the detector placed after the filter centered at $\omega_o + \Omega_n$, or by the detector placed after the filter centered at $\omega_o - \Omega_n$ depending on whether a "0" or a "1" is, respectively encoded. 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. Note that Fig. 1(b) plots the measured bits at Bob's side when the base choices match in three channels and Fig. 1(c) corresponds with the key $n = 3$ receiving correctly the bit "0."

Thus, the SCM-QKD system permits to combine all the parallel keys to compose a superkey, the bit rate of which will be given by the sum of the individual keys for each single channel. A further advantage of the SCM-QKD technique is that it can be combined with M WDM carriers to provide a two-tier multiplexing scheme featuring either the distribution of M superkeys between a central office and *M* end users or an overall aggregate key rate multiplied by an NM factor in a point to point link.

3. Experiment

3.1. Experimental Setup

Fig. 2 shows the first experimental setup assembled to demonstrate the feasibility of the SCM-QKD approach by multiplexing two independent keys. Four main blocks can be distinguished which correspond to the quantum transmitter (Alice), the quantum receiver (Bob), both interconnected by a 11 km fiber length representing a typical access network link, the classical reference channel and the overall electronic control system (see Appendix).

Alice's transmitter produced weak coherent-state pulses by strongly attenuating a laser source previously pulsed using a time gating electronic signal to drive a 20 dB extinction ratio electrooptic Mach–Zehnder modulator. The output pulses had 1.3 ns FWHM and a repetition rate of 1 MHz. The nominal 3 dB laser linewidth was 10 MHz and the emission wavelength 1548.78 nm.

Quantum states to encode the binary secret keys were prepared at Alice's location by amplitude modulating the fainted laser pulses using a 20 GHz-bandwidth external electrooptic modulator (AM), biased at quadrature and fed through the RF port by two subcarriers, generated from independent local oscillators of frequencies $f_1 = 10$ and $f_2 = 15$ GHz. To implement the different versions of the BB84 protocols [16], [27], [28], each sideband must contain a mean photon number of $\mu \leq 1$ per pulse. In particular, for the case of BB84 protocol with strong reference [28], [29] which was the one considered in our experiment, $\mu = 1$.

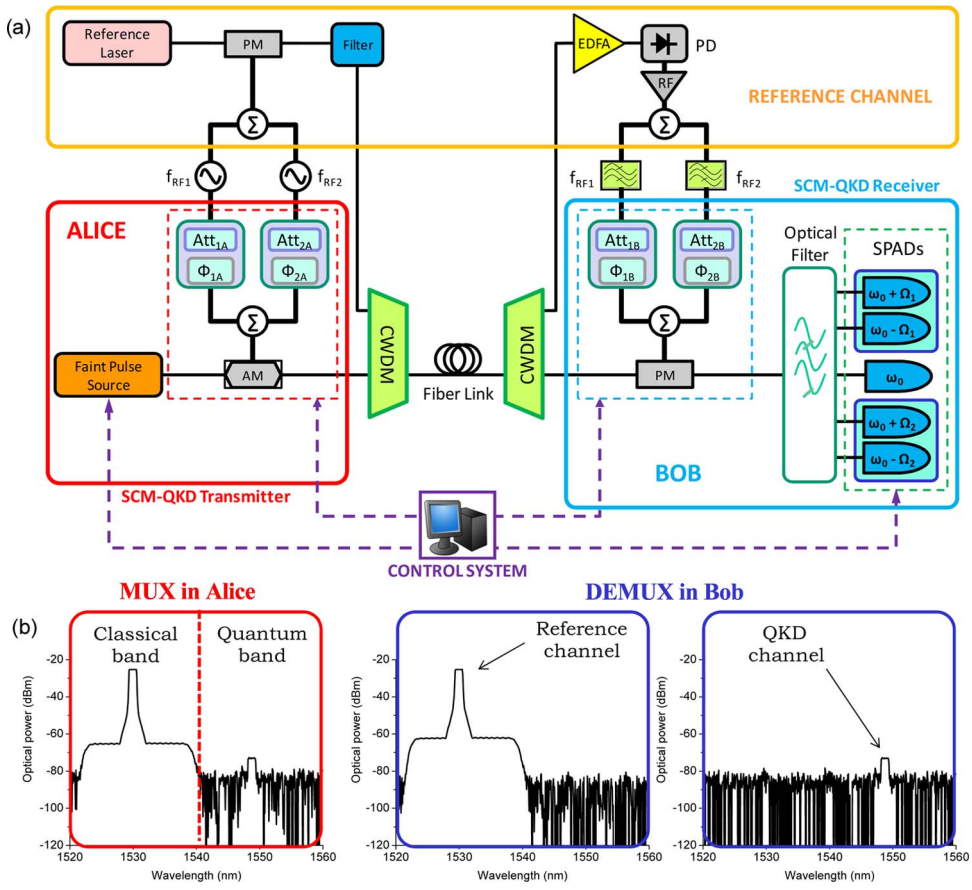


Fig. 2. (a) Experimental setup assembled in the laboratory to test the feasibility of a two keys in parallel transmission by means a SDM-QKD system $(N = 2)$. (b) Optical spectra for classical and quantum bands when are multiplexed in Alice and Bob, respectively. Note that power level of quantum channel which would be below the noise floor is intentionally augmented to show its spectral location.

The control system enabled the pseudorandom generation and independent impression of time varying phase shifts Φ_{1A} and Φ_{2A} onto each subcarrier in synchronicity with the arrival of the fainted pulses. Note that a true random generation is required in a real implementation. Eight-bit, digitally tunable phase shifters (500 ns switching speed) capable of providing full 360° phase shifts with a 1.4° resolution step were employed for that purpose. Electrical attenuators (Att_{1A} and Att_{2A}) were placed at the input of both phase shifters to independently control the amplitude of the RF signal driving each subcarrier. Bob's receiver has a similar configuration as Alice but in this case the optical signal after propagating through the fiber link is modulated by means of a 20-GHz-bandwidth Phase modulator (PM). The use of PM at Bob's side reduces the control and management of the local user since it does not require polarization biasing. Bob selects the basis for each subcarrier to realize the measurement of the transmitted qubit by synchronously inserting independent random phase shifts Φ_{1B} and Φ_{2B}. After filtering, the photon detection was realized by placing an ID Quantique (id201) Single Photon Avalanche Detector (SPAD) for each optical sideband. The quantum efficiency and the dark count probability of the SPADs was 10% and 10^{-5}, respectively, which were operated using a time gate of 2.5 ns and synchronized with the faint pulse source by means of the control system.

A classical reference channel was required to convey a synchronization signal from Alice to Bob and also to stabilize the link against fiber length fluctuations [18] by providing Bob with exact replicas of the 10 and 15 GHz electrical subcarriers produced at Alice's side. The reference and quantum channels were coarse wavelength multiplexed (CWDM) to share the same optical fiber

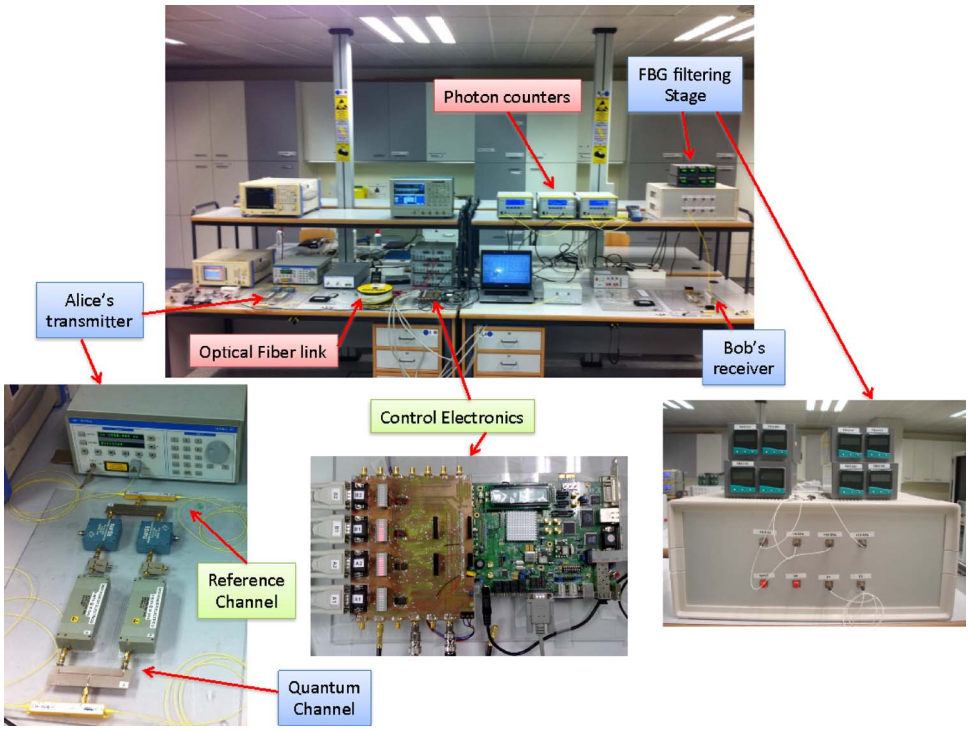


Fig. 3. Pictures of the experimental setup assembled in the laboratory to test the feasibility of a two keys in parallel transmission by means a SDM-QKD system (upper part) and details of some of its main constituents (lower part).

link. The CWDM multiplexer mixed two optical bands with a 20 nm wavelength separation and insertion losses of 0.5 dB. As shown in Fig. 2(b), the optical band centered at 1551 nm was used to transmit the quantum channels while the adjacent band at 1531 nm was used for the reference channel. After fiber transmission, a CWDM demultiplexer separated both quantum and reference channels. Fig. 3 displays the pictures of the demonstrator and of some of its main constituents.

3.2. Limiting Factors

The design of the SCM-QKD implies the solution of several challenging limitations that can drastically reduce the useful key rate: The implementation of narrowband optical filters with high extinction ratios for the selection of the RF sidebands, the control of the Raman effect due to the reference channel over the quantum band, the control of environmental fluctuations in the optical path and the compensation of chromatic dispersion.

To optically filter each one of the sidebands with enough extinction ratio at the output of Bob's modulator we designed and implemented a photonic filter structure composed of different fiber Bragg grating (FBG) stages [30] as shown in Fig. 4(a). The filter allows the extraction of the optical carrier as strong reference to guarantee unconditional security and features a high-extinction filtering of each sideband providing uniform output probability for each sideband (see Appendix). We checked the filter performance in the classical regime with the aid of a 10 pm resolution ANDO optical spectrum analyzer (OSA), placed at each output of the filter.

Fig. 4(b) shows the measured spectra for all filtered bands at ± 10 GHz and ± 15 GHz with respect to optical carrier. All sidebands display the same power (probability) with an extinction ratio of 25 dB while introducing minimum insertion losses ($T_{FILTER} = 1.5$ dB).

Also, we evaluated the photon crosstalk due to the Raman effect that the reference channel generates in each optical filtering output of Bob's receiver for the SCM channels corresponding to

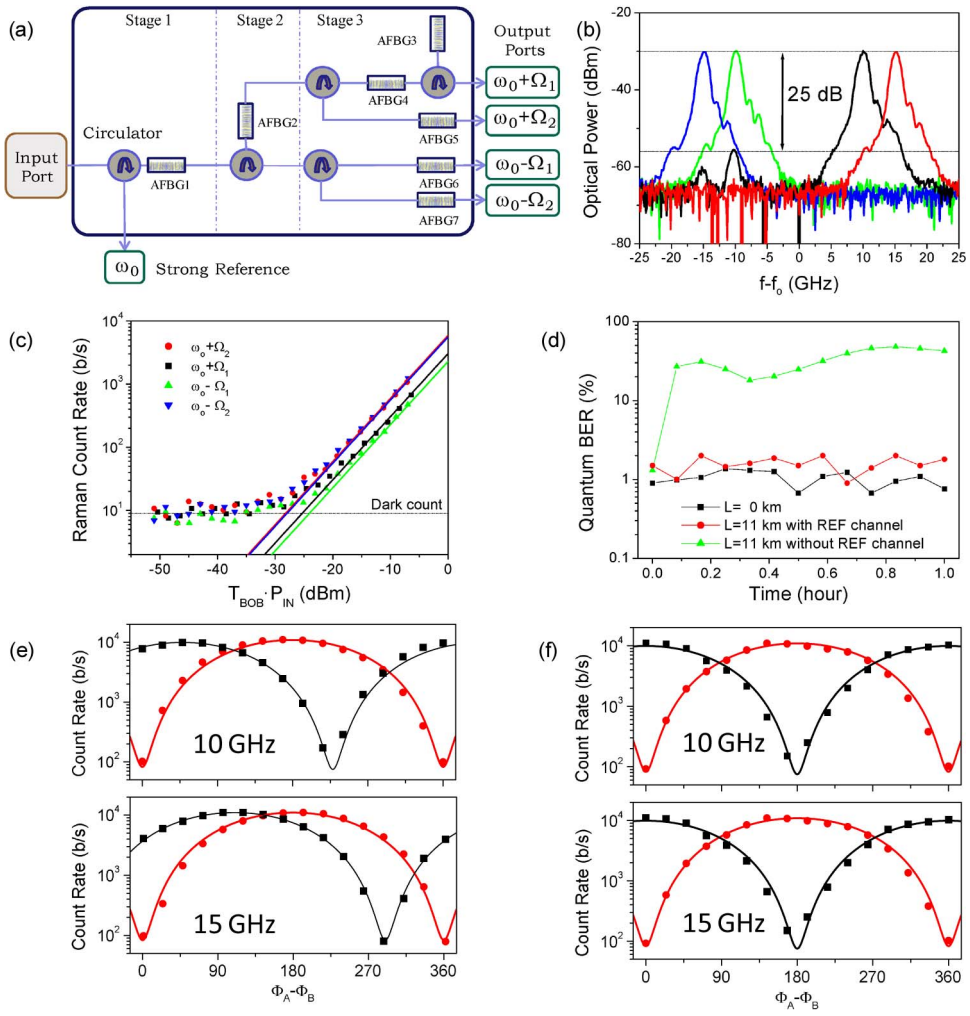


Fig. 4. (a) Filter structure employed to discriminate each subcarrier. (b) Optical spectra for each optical sideband in classical regime after the filter structure. The central frequency is gauged to the carrier ω_0. (c) Experimental count rate (points) corresponding to each optical filtering output as a function of the optical power of reference channel and Bob's losses (lines are theoretical simulations). (d) QBER when reference channel is enable or disable on one hour for 11 km compared to back to back configuration. (e) Count rate of sidebands for each subcarrier when the dispersion is not compensated and (f) when is compensated. Theoretical predictions are plotted in lines.

the 1548.78 nm wavelength [22]. Fig. 4(c) depicts the count rate measured for each optical sideband as a function of the product of the classical power P_{IN} of the reference channel and the amount of optical losses T_B at Bob's receiver. The behavior is very similar among the sidebands although slight differences are found due to optical filtering nonuniformities. In practice, Bob's losses (around 4.5 dB) relax the requirements to minimize Raman photon count below the dark count for an optical input power close to -25 dBm. For this reason, the reference channel is optically amplified first after demultiplexing and electrically after detection at Bob's receiver. For the rest of QKD band we obtain similar results so the minimum value of -25 dBm is valid for the all WDM channels carrying the QKD signals.

The correct stabilizing operation of the reference channel was checked as shown in Fig. 4(d), which depicts the measurement of the QBER (see Appendix) over a one-hour interval, as the system needed a reset to adjust the synchronization and the optical hardware after this period. A clear difference can be observed when the reference channel is inactive (QBER close to 50% for a long time period) as compared to when it is active. For this last case, QBER values were lower than

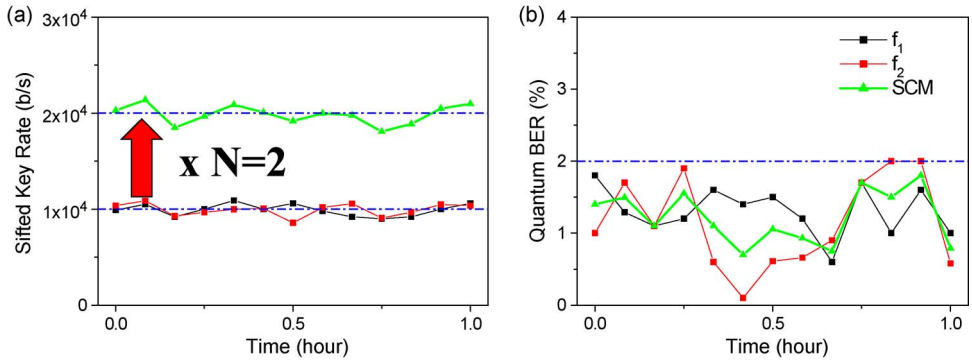


Fig. 5. (a) Evolution of the sifted key rate for each individual SCM-QKD channel and the multiplexed sifted key rate when SCM multiplexing technique is considered. (b) Measurement of the corresponding QBER for each single channel and for the multiplexed rate.

2% and consequently an averaged visibility better than 96% was achieved which are comparable with those of a back to back system $(L = 0\ km)$.

Chromatic dispersion can also degrade the system visibility and must be compensated. In our case a 1 km dispersion compensating fiber (DCF) was added to the 10 km standard fiber link. Fig. 4(e) shows that complementarity between LSB and USB is lost for uncompensated dispersion and Fig. 4(f) how this is recovered for both subcarriers when dispersion is compensated. Measured QBER values of around 17% and 35% for the 10 and 15 GHz subcarriers in the uncompensated case are reduced to values around 1.5% for both subcarriers when the dispersion is compensated.

3.3. SCM-QKD and WDM/SCM-QKD Multiplexed Key and Quantum Bit Error Rates

Performance of both SCM-QKD and WDM/SCM-QKD was tested, by measuring the individual sifted key rates and QBER (see Appendix), after transmission through an 11 km optical fiber link. In the first stage, the feasibility of the SCM-QKD approach was proved by independently phase encoding two RF subcarriers with an averaged photon number of 1 photon per pulse at 1-MHz repetition frequency. The wavelength of the optical carrier was 1557.30 nm. The optical system loss was 6.5 dB which corresponds to 2.5 and 4 dB due to the 11-km fiber link and the Bob's receiver, respectively, which includes the CWDM components, the PM and the optical filtering stage. Taking into account the quantum efficiency of the SPAD $(\rho = 0.1)$, the total system losses were 7.5 dB. Fig. 5(a) shows the sifted key rate of the individual subcarriers ($\sim$10 kbit/s at $f_1 = 10$ and $f_2 = 15$ GHz) and the aggregated sifted key rate ($\sim$20 kbit/s) when both subcarriers are transmitted simultaneously. The independent key distribution using such a tightly spectral separation (5 GHz) is thus demonstrated for the first time to our knowledge. Furthermore, the aggregated sifted key rate is very close to the maximum multiplexing gain (3 dB) corresponding to the number of subcarriers $N = 2$ as theoretically predicted [26]. The corresponding QBER is plotted in Fig. 5(b) featuring a value below 2% for all count rates which implies visibilities higher than 96% according to the signal level. As expected, this reflects the fact that the drifts due to temperature and vibrations are properly compensated by the reference channel.

In order to further prove the scalability and flexibility of the proposed system, a WDM/SCM-QKD system was assembled in a two-tier configuration. First, two independent SCM-QKD transmitters (each one generating two independently phase-encoded multiplexed subcarriers at $f_1 = 10$ and $f_2 = 15$ GHz) were implemented at Alice's location centered at 1548.78 (CH1) and 1557.30 (CH2) nm, respectively. These channels were wavelength multiplexed using a Dense Wavelength Division Multiplexer (DWDM) based on FBGs and then, all quantum channels were multiplexed via CWDM with the reference channel as shown in Fig. 6(a). In a similar way than single SCM-QKD channel, the classical and quantum bands were recovered with a CWDM demultiplexer and each quantum channel was filtered by means of a SCM-QKD receiver after a DWDM demultiplexer. Fig. 6(b) and (c) plot the individual sifted key rates obtained for each one of

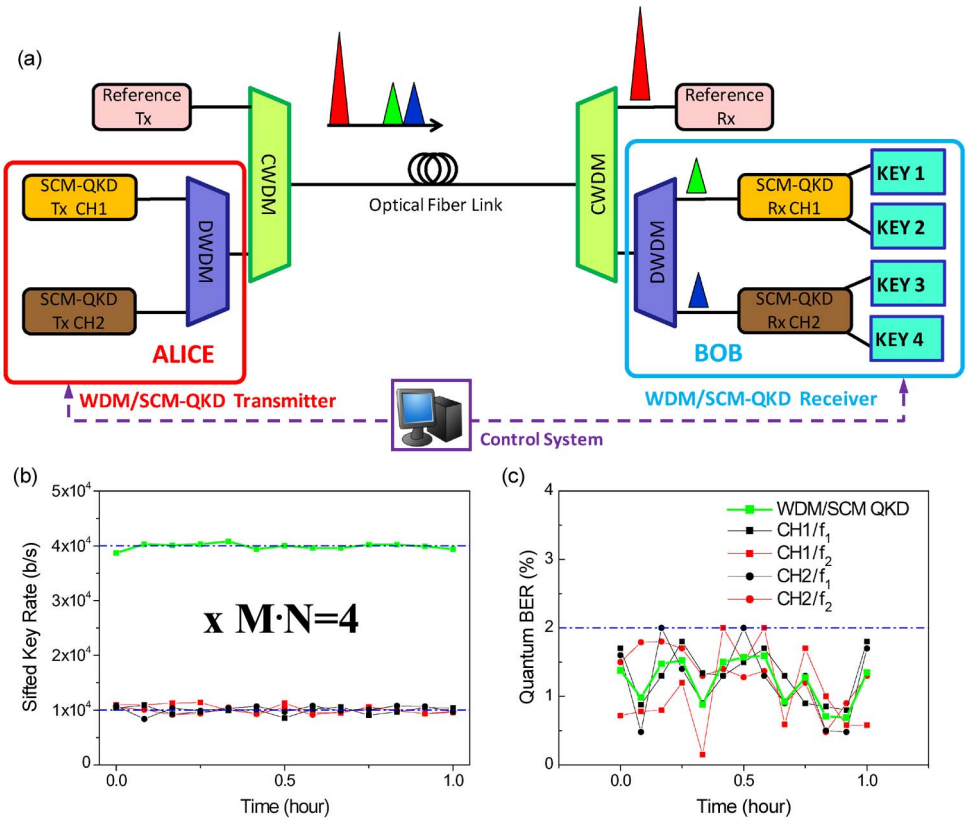


Fig. 6. (a) QKD scheme for both WDM and SCM multiplexing transmission. (b) Sifted key rate for each individual quantum channel and the multiplexed key rate. (c) Measurement of the corresponding QBER for each single channel and for the multiplexed sifted key rate.

the four subcarrier channels and the aggregated sifted key rate which, in this case, is close to the $M{\cdot}N = 4$ value. Note that QBER values lower than 2% are obtained for all the channels.

Finally, we computed the values for secret key rate of SCM and SCM/WDM schemes using weak coherent pulses and a strong reference, which is implemented by the optical carrier wavelength, to perform the analysis of security against PNS attach [29]. We obtained an average reduction around of 40% compared to sifted key as expected (see Appendix). The aggregated secret key rate was around 16 kb/s.

4. Discussion

The reported work has demonstrated that SCM, widely employed in the field of MWP, can be used in the context of QKD, to achieve the simultaneous distribution of parallel keys by using frequency channels closely packed in the optical spectrum. The importance of this advance is very significant for several reasons which are now stated.

First, it relies on a technique which is very well known for its high spectral-efficiency. Since the actual key rates achieved by QKD systems are very modest in comparison with those of classical broadband communications, the use of a multiplexing technique with reduced spectral separation between adjacent channels seems a natural and sustainable choice for the delivery of multiple keys. As an example, to the best of our knowledge, the record result for secure bit rate is around 1 Mb/s for a link distance of 50 km [32]. Thus in this case, since the typical channel separation in DWDM is 100 GHz the intrachannel spectrum efficiency is far limited to around 2–4%. In this sense, the use of SCM technique can increase efficiently this ratio up to values higher than 50% with the use of broadband modulators ($\sim$50 GHz) and optical filters with very narrow channel

spacing (~1–2 GHz). This estimate shows that the SCM-QKD technique could provide an order of magnitude improvement in terms of the final key rate. Secondly, the optical source is shared by all the multiplexed channels which reduces the complexity of the system since all keys are carried on the same wavelength assigned in an optical network providing a reduction of system complexity, management and cost. A third advantage is that the SCM approach can be combined and upgraded with WDM to increase the number of parallel keys and to coexist with other classical information channels over the same fiber infrastructure. Again, this two-tier WDM/SCM combination is borrowed from MWP.

We would like to point out that despite the fact that in the experiments reported here we considered an average number of 1 photon per pulse as required by the BB84 protocol with strong reference, the SCM-QKD system was tested for different values of the mean photon number ranging from 0.1 to 1 photon per pulse, obtaining satisfactory results in all the cases with the obvious reduction in the sifted key rate. Note that we experimentally demonstrated moderate single key rates since the capacity of our system is limited to 1 MHz in our case due to the trigger and deadtime of the SPADs. Using 1-GHz SPADs [32], the secret key rate per channel could be readily increased by 2 or 3 orders of magnitude up to hundreds of kilobits per second. Also, the aggregated sifted key rates can be upgraded currently in at least two orders of magnitude by using components that are commercially available as phase shifters with a switch time of 25 ns and optical filters based on AWGs with 32 output ports in a single device with a very narrow channel spacing (~5 GHz). Note that parallel filtering configuration is more efficient for this particular application since the filtering losses do not scale with the number of output ports as it occurs to filtering stages based on the serial concatenation of FBGs.

5. Summary and Conclusion

To summarize, we have demonstrated, for the first time, the feasibility of a QKD system based on the combination of WDM and SCM multiplexing techniques in order to further enhance the transmission capacity over optical fiber networks. The proposal permits to increase the final key rate of the quantum transmission and the distribution of parallel keys for different users. The advantage of the SCM multiplexing technique against WDM over QKD is that the same photon source is shared by N different keys and consequently, the complexity of the synchronization and control system is reduced drastically when the QKD system is introduced in an optical network. The obtained results confirm that MWP is a promising technology to enhance the viability of the quantum systems. In addition, the SCM multiplexing technique could be adapted to alternative protocols to BB84 such as DPS or COW.

Appendix

Quantum Bit Error Rate Computation, Measurement and Limiting Factors

The quantum bit error rate (QBER) defined as the ratio of wrong bits to the total number of bits received is a measure of the quality of a QKD system which takes into account the most important limiting factors. In practice, these limiting factors come from two sources; environmental instabilities which drift the system away from its ideal operation point and the wrong photon count contribution due to different crosstalk processes. Environmental changes related to the fluctuations of optical path and the state of polarization between both Alice and Bob's modulators can be controlled by means of the reference channel and thus will not be further considered for the QBER computation which in the case of the Bennet-Brassard 1984 (BB84) protocol implemented by subcarrier multiplexing is given by

$$\mathrm{QBER}(\Omega_n) = \frac{1}{2}\frac{(1 - V_{\mathrm{eff}})p_{\mathrm{signal}} + p_X + d_B}{p_{\mathrm{signal}} + p_X + d_B}$$

where p_{signal} is the probability coming from the detection of signal photons, d_B is the dark count probability related to the noise source coming from photon detection and V_{eff} represents the

effective visibility due to the imperfections of the devices employed in the system and the fiber dispersion. p_X is the crosstalk probability and takes into account the photon crosstalk contributions measured at each optical detector which contribute to a false detection. In our case, $p_X = p_{Raman} + p_{filter} + p_{imd} + p_{phn}$ which includes several sources such as Raman effect, the extinction ratio of the optical filtering, intermodulation of SCM multiplexing and the linewidth of the laser source used as quantum carrier, respectively.

In our experimental setup, the dark count minimizing the after-pulsing effects is below 10^{-5} and the dispersion was compensated leading to a visibility higher than 96%. The Raman effect was reduced below the dark count for each optical sideband by properly adjusting the input power of the reference channel. The optical filtering stage has been designed to reduce the crosstalk due to adjacent subcarriers and intermodulation products (located outside of the sidebands) below 23 dB respect to signal photon probability. In order to achieve this objective, we designed an optical filtering based on apodized FBGs comprising three stages [see Fig. 3(a)].The first one provided the strong reference by reflecting the optical carrier with a FBG of a reflection coefficient close to 99.9%. The second stage separated the upper RF bands from the lower RF bands. Finally, the third stage filtered each one RF bands featuring over 20 dB of rejection ratio and a spectral bandwidth around 2.5 GHz. Therefore, there are 5 ports, one for each band and one more for the optical carrier. Each FBG was centered at one fixed wavelength with 1 pm of accuracy which required a temperature control system implemented placing each apodized FBG inside of individual thermal box managed by a temperature controller.

With regard to the linewidth of the optical laser used as a faint pulse source, it had to be considered for the SCM channel close to optical carrier since additional photon counts could be introduced. In our case, a moderate modulation index guarantees that a negligible crosstalk due to this source.

On the other hand, the electrooptical modulators need to have the input polarization aligned along the main axis to reduce the optical losses of the device. We minimize the effects of the polarization changes by means a tracking polarization controller. In addition, we have introduced a polarizer previous to Bob's modulator in order to reduce drastically this photon contribution. In this way, the measurement of count rate is used as a feedback signal to monitor and adjust the polarization controller state. As shown in Figs. 4(b) and 5(c), the key rate has a slight variation around 1 dB which is due to the residual changes that optical polarization of the quantum channel are occurred along the fiber link propagation.

Finally, the measurement of the QBER was experimentally realized by comparing a sequence of bits sent from Alice to the received bits and counting the number of errors at Bob's side. According to the above expression, the predicted QBER value for any quantum channel should be around 2% which is confirmed by all measured results.

In the manuscript, we show the sifted key rate which was obtained after basis reconciliation. The secret key rate was not obtained experimentally since Error Correction (EC) and Privacy Amplification (PA) were not implemented. However, we estimated that the secret key rate is around 31% of the sifted key rate according to the fraction of secure bits [29] considering PNS attack and taking into account that maximum values of QBER were below 2%.

The incorporation of SCM technique in QKD systems implies the use of faint pulse laser source to achieve a real multiplexing. In our case, the use of single photon source can reduce the key rate up to 3 orders of magnitude since the amplitude of each optical sideband is proportional to the modulation index, which is low to minimize the intermodulation between electrical subcarriers. The particular QKD scheme implemented in this paper (BB84 with strong reference pulse) has not yet been proven to be secure. However, as reported in [29], the security analysis of the SCM-QKD systems by means of weak coherent pulses and a strong reference against PNS attack, implies a value of $\mu = 1$ to minimize the fraction of information IE that Eve can extract from multiphoton pulses [28]. Therefore, the secure key rate K is given by the formula [29]

$$\frac{K}{\tilde{\nu}_s} \approx \left\{ \Delta \left[1 - h\left(\frac{QBER}{\Delta} \right) \right] - h(QBER) \right\}$$

where $\Delta = 1 - I_E$ represents the secure fraction in the absence of loss and error and h(x) is the binary entropy function.

Control System

The operation of the SCM-QKD and WDM/SCM-QKD systems was electronically controlled by using Virtex V (XUPV5-LX110T) Field Programmable Gate Arrays (FPGAs) from Xilinx connected to the computers via a RS-232 protocol. The electrical control signals generated by the FPGAs were distributed to the system by means of on purpose Printed Circuit Boards (PCBs). All the controlling signals were synchronized to the operating system frequency, set to 1 MHz and moreover, each one had an independently controllable delay. The main tasks of the control system are now briefly described.

At Alice's side, it provided 1.3 ns width electric pulses used to drive the faint pulse sources. In addition, the phase shifters were independently controlled for each subcarrier by means of different 8 bit signals providing the required phase shifts to implement the two maximally overlapping bases of the BB84 protocol. At Bob's side, the control system tasks included the generation of TTL type signals to trigger the photon counters in synchronicity with the arrival times of the pulses generated at Alice's location. Whenever a count was produced, the control system detected the electric signal provided by the photon counters taking into account its position on the bit stream. The control system was also in charge of storing the streams corresponding to the parallel key bits and base selections performed by Alice by an independent pseudorandom generator implemented in the corresponding FPGAs. At Bob's location, another file is stored with the streams identifying the base choices made by Bob and the count results for USB, LSB and strong Carrier Band (CB) up to a length of raw key close to 4 kbits per user, which is determined by the available memory size of the used FPGA. These files are used in the public discussion for obtaining the sifted key after basis reconciliation process for each user and the calculation of the corresponding QBER.

Acknowledgment

The authors wish to acknowledge the financial support of the Spanish Ministry of Science and Innovation and the Generalitat Valenciana through projects CONSOLIDER INGENIO 2010 Quantum Information Technologies and PROMETEO GVA 2008-092 MICROWAVE PHOTONICS.

References

[1] J. Capmany and D. Novak, "Microwave photonics combines two worlds," *Nat. Photon.*, vol. 1, no. 6, pp. 319–330, Jun. 2007.
[2] J. Yao, "Microwave Photonics," *J. Lightw. Technol.*, vol. 27, no. 3, pp. 314–335, Feb. 2009.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan.–Mar. 2002.
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Jul.–Sep. 2009.
[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, 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, no. 7, p. 793, Feb. 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.
[8] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Single-photon interference in a 10 km long optical fiber interferometer," *Electron. Lett.*, vol. 29, no. 7, pp. 634–636, Apr. 1993.
[9] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, p. 037 902, Jul. 2002.
[10] 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, no. 1, p. 232, 2005.
[11] 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, no. 6, pp. 343–348, Jun. 2007.
[12] 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, no. 8, pp. 1656–1659, Feb. 1999.

[13] 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, no. 2, pp. 104–106, Jan. 1999.
[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 scheme with WDM synchronization," *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1533–1540, Nov./Dec. 2003.
[15] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km telecom fiber," *Appl. Phys. Lett.*, vol. 84, no. 19, pp. 3762–3764, May 2004.
[16] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, "Practical long-distance quantum key distribution system using decoy levels," *New J. Phys.*, vol. 11, no. 4, p. 045 009, Apr. 2009.
[17] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, "Feasibility of 300 km quantum key distribution," *New J. Phys.*, vol. 11, no. 8, p. 085 002, Aug. 2009.
[18] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.*, vol. 11, no. 7, p. 075 003, Jul. 2009.
[19] 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, no. 22, pp. 1875–1877, Oct. 1994.
[20] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, pp. 47–49, Jan. 1997.
[21] P. D. Townsend, "Quantum cryptography on optical fiber networks," *Opt. Fiber Technol.*, vol. 4, no. 4, pp. 345–370, Oct. 1998.
[22] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, no. 10, p. 105 001, Oct. 2009.
[23] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through dense wavelength division multiplexing network," *New J. Phys.*, vol. 12, p. 103 042, 2010.
[24] A. Tanaka, A. Tajima, and A. Tomita, "Colourless interferometric technique for large capacity quantum key distribution systems by use of wavelength division multiplexing," presented at the Proc. 35th European Conf. Optical Communication (ECOC), Vienna, Austria, 2009, Paper 1.4.2.
[25] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "A scalable full quantum key distribution system based on colourless interferometric technique and hardware key distillation," presented at the Proc. 37th European Conf. Exposition Optical Communications, OSA Tech. Dig. (CD) (Optical Society of America), Geneva, Switzerland, 2011, Paper Mo.1.B.3.
[26] A. Ortigosa-Blanch and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," *Phys. Rev. A, Atom. Mol. Opt. Phys.*, vol. 73, no. 2, p. 024 305, Feb. 2006.
[27] 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, 1984, pp. 175–179.
[28] O. Guerreau, F. J. Malassenet, S. W. McLaughlin, and J.-M. Merolla, "Quantum key distribution without a single-photon source using a strong reference," *IEEE Photon. Technol. Lett.*, vol. 17, no. 8, pp. 1755–1757, Aug. 2005.
[29] J. Capmany and C. R. Fernández-Pousa, "Impact of third-order intermodulation on the performance of subcarrier multiplexed quantum key distribution," *IEEE J. Lightw. Technol.*, vol. 29, no. 20, pp. 3061–3069, Oct. 2011.
[30] J. Mora, A. Ruiz-Alba, W. Amaya, V. Garcia-Muñoz, A. Martinez, and J. Capmany, "Microwave photonic filtering scheme for BB84 subcarrier multiplexed quantum key distribution," in *Proc. IEEE Top. Meet. Microw. Photon.*, Montreal, Canada, 2010, pp. 286–289.
[31] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.*, vol. 12, p. 063 027, Jun. 2010.
[32] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," *Appl. Phys. Lett.*, vol. 96, no. 16, p. 161 102, Apr. 2010.