Experimental demonstration of subcarrier multiplexed quantum key distribution system

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

ITEAM Research Institute, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain
**Corresponding author: jcapmany@iteam.upv.es*

Received February 2, 2012; revised March 31, 2012; accepted April 13, 2012;
posted April 13, 2012 (Doc. ID 162406); published May 30, 2012

We provide, to our knowledge, the first experimental demonstration of the feasibility of sending several parallel keys by exploiting the technique of subcarrier multiplexing (SCM) widely employed in microwave photonics. This approach brings several advantages such as high spectral efficiency compatible with the actual secure key rates, the sharing of the optical fainted pulse by all the quantum multiplexed channels reducing the system complexity, and the possibility of upgrading with wavelength division multiplexing in a two-tier scheme, to increase the number of parallel keys. Two independent quantum SCM channels featuring a sifted key rate of 10 Kb/s/channel over a link with quantum bit error rate <2% is reported.

OCIS codes: 060.4230, 270.5568.

Quantum key distribution (QKD) exploits the laws of quantum mechanics with the objective of sharing a random sequence of bits between two users with a certifiable security [1,2]. 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 [3–8]. Initially investigated for point-to-point links, there is an increasing interest in its extension to network environments [9–11] including passive optical networks [12–13], where the use of multiplexing techniques can bring an added value for multiuser operation. Initial results [14] for wavelength division multiplexing (WDM) systems, combining one or more classical information channels with a solitary QKD channel have identified spontaneous Raman scattering as the dominant impairment from the strong signals. Very recently, a WDM based QKD system using three different wavelengths in the C-band has been reported [15], featuring promising results, which include a 200 Kb/s key generation rate with a 14.5 dB transmission loss using 1.22 GHz pulse generation rate. Nevertheless, WDM multiplexing alone is spectrally inefficient as it consumes a full wavelength channel for an individual key in the range of 100 of Kb/s to a few Mb/s.

In a previous work [16], we theoretically proposed the distribution of more than one key per wavelength by means of subcarrier multiplexed quantum key distribution (SCM-QKD) [17]. Here, we experimentally demonstrate, for the first time to our knowledge, the feasibility of the SCM-QKD approach to achieve the simultaneous distribution of two parallel keys by using frequency channels very closely packed in the optical spectrum.

The operation principle of SCM-QKD can be explained referring to Fig. 1, which shows a scheme of the experimental setup assembled to demonstrate the feasibility of the SCM-QKD approach by multiplexing different independent keys. Four main blocks can be distinguished, which correspond to the quantum transmitter (Alice), the quantum receiver (Bob), both interconnected by an 11 Km access network link [10 Km single-mode fiber (SMF28e) followed by 1 Km dispersion compensating fiber (DCF)], the classical reference channel, and the overall electronic control system.

In the experiment, Alice's transmitter produced weak coherent-state pulses by strong attenuation of a laser source previously pulsed using a time gating electronic signal to drive a 20 dB extinction ratio electro-optic 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 was 1557.30 nm. Quantum states to encode the binary secret keys were prepared at Alice's location by amplitude modulating the faint laser pulses using a 20 GHz bandwidth external electro-optic modulator (AM), biased at quadrature. We employed two RF subcarriers ($f_{RF1} = 10$ and $f_{RF2} = 15$ GHz), generated by independent voltage controlled oscillators (VCOs). The laser source radiation was externally modulated by the RF subcarriers.

For parallel key distribution, each RF subcarrier transmits a different key, which is generated by randomly phase modulating the output of each VCO among four

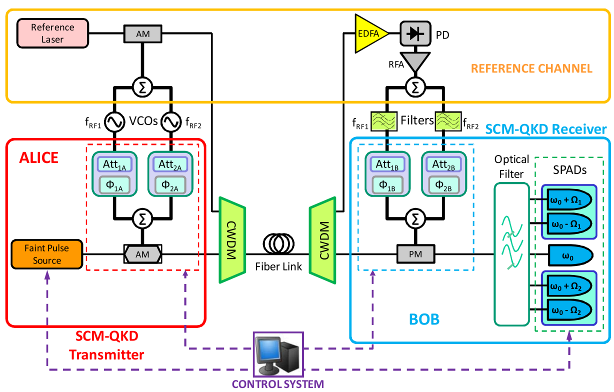

Fig. 1. (Color online) Experimental SCM-QKD system to distribute different keys in parallel: AM, amplitude modulator; PM, phase modulator; VCOs, voltage controlled oscillators; $Att_{(1/2)(A/B)}$, electrical attenuators; CWDM, coarse wavelength division mux/demux; EDFA, erbium doped fiber amplifier; RFA, RF amplifier; SPAD, single photon avalanche detector; and $\Phi_{(1/2)(A/B)}$, RF phase shifters.

0146-9592/12/112031-03$15.00/0

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 [16]. 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.

The control system enabled the pseudo random generation and independent variation of phase shifts Φ_{1A} and Φ_{2A} onto each subcarrier in synchronicity with the arrival of the faint pulses. 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). 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} taking values of 0 or π. 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 were 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 [7] 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 link. The CWDM multiplexer mixed two optical bands with a 20 nm wavelength separation and had insertion losses of 0.5 dB. 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 the quantum and reference channels [18]. Note from Fig. 1 that the reference channel is optically amplified first by means of an erbium doped fiber amplifier (EDFA) and electrically by an RF amplifier (RFA) after detection at Bob's receiver.

The total system loss was 6.5 dB (2.5 dB in the 11 km fiber link and 4.5 dB in Bob's receiver), which includes the CWDM components, the phase modulator, and the spectral filtering stage.

In order to prove the feasibility of the SCM-QKD approach by independently phase encoding, both RF subcarriers were considered with an averaged photon number of one photon per pulse to implement BB84 protocol with strong reference, which, according to [19], is unconditionally secure. Figure 2 shows the sifted key rate of the individual subcarriers (~10 Kbit/s at f_{RF1} and $f_{RF2} = 15$ GHz) and the aggregate sifted key rate (~20 Kbit/s) when both subcarriers are transmitted simultaneously. Furthermore, the aggregate sifted key rate is very close to the maximum multiplexing gain (3 dB) corresponding to the number of subcarriers ($N = 2$) as predicted theoretically [16]. The corresponding quantum bit error rate (QBER) is plotted in Fig. 2(b) featuring a value below 2% for all count rates, which implies visibilities higher than 96% according to the signal level. This reflects the fact that the drifts due to temperature and vibrations are properly compensated by the reference channel. Additionally, in our experimental setup, the dark count minimizing the afterpulsing effects was below 10^{-5} and the dispersion was compensated. Also, the Raman effect was reduced below the dark count for each optical sideband by proper adjusting the input power of the reference channel.

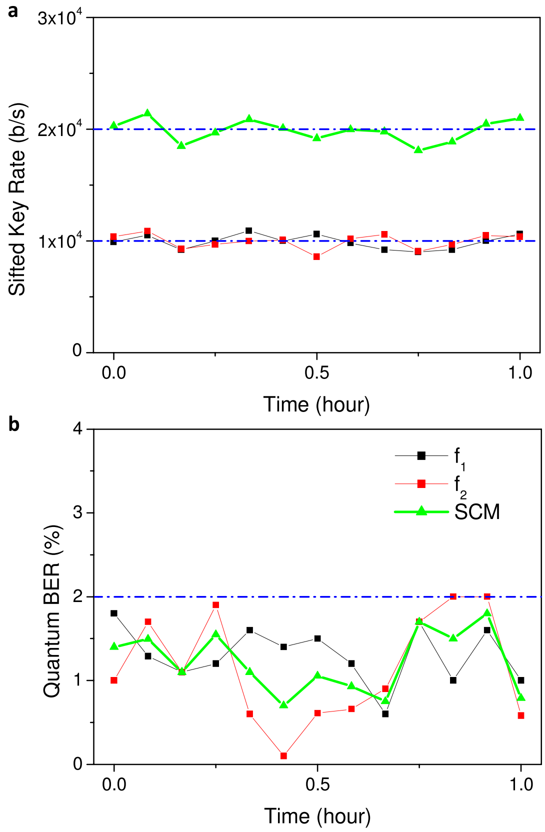

Fig. 2. (Color online) (a) Evolution of the sifted key rate for each individual SCM-QKD channel and the multiplexed sifted key rate when SCM multiplexing technique is considered. (b) Measurement of the corresponding QBER for each single channel and for the multiplexed rate.

Note that independent key distribution using a tightly spectral separation (5 GHz) according to both electrical subcarriers is thus demonstrated for the first time to our knowledge [20]. Indeed, the spectral filtering stage was designed to reduce the crosstalk due to adjacent subcarriers and intermodulation products (located outside of the sidebands) below 23 dB in respect to signal photon probability. In order to achieve this objective, we designed an optical filter based on apodized fiber Bragg gratings (FBGs) comprising three stages. 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 RF band featuring over 20 dB of rejection ratio and a spectral bandwidth around 2.5 GHz. Therefore, there were five ports, one for each band and one more for the optical carrier as shown in Fig. 1. Each FBG was centered at one fixed wavelength with 1 pm of accuracy, which required a temperature control system with 0.1 °C accuracy implemented by placing each apodized FBG inside of the individual thermal box managed by a temperature controller.

Finally, we computed the values for the secret key rate of the SCM scheme (without considering error correction) using the expressions developed in [19] for BB84 with strong reference. We obtained an average reduction around 40% compared to sifted key as expected. The aggregate secret key rate was around 16 Kb/s. In this context, we would like to point out that despite the fact that we experimentally demonstrated moderate single and aggregate sifted key rates, the capacity of the system can be increased by at least 2 orders of magnitude by using commercially available components such as phase shifters with a switch time of 25 ns, SPADs with high-speed gating at frequencies up to 100 MHz, and optical filters with 32 output ports in a single device with a very narrow channel spacing (~5 GHz).

The importance of these results is significant for several reasons, which are now stated. First, SCM relies on a technique that 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 parallel 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 [21]. Thus, in this case, since the typical channel separation in dense WDM 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 (~50 GHz) and optical filters with very narrow channel spacing (~1–2 GHz). This estimation shows that the SCM-QKD technique could provide an order of magnitude improvement in terms of the final key rate. Second, 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.

In conclusion, we have experimentally demonstrated, for the first time to our knowledge, the feasibility of a multiple QKD system based on subcarrier multiplexing. The proposed approach permits an increase in 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 standalone WDM over QKD is that the same photon source is shared by 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. Furthermore, the capacity of SCM-QKD systems can be increased by introducing WDM as a second tier multiplexing domain. The obtained results confirm that MWP is a promising technology to enhance the viability of quantum systems.

This work was supported by the Spanish Ministry of Science & Innovation and the Generalitat Valenciana through projects CONSOLIDER INGENIO 2010 Quantum Information Technologies and PROMETEO GVA 2008-092 MICROWAVE PHOTONICS.

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, Rev. Mod. Phys. **74**, 145 (2002).
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
3. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
4. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
5. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
6. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photon. **1**, 343 (2007).
7. O. Guerreau, J.-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer, and F. J. Malassenet, IEEE J. Sel. Top. Quantum Electron. **9**, 1533 (2003).
8. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
9. P. D. Townsend, D. J. D. Phoenix, K. J. Blow, and S. Cova, Electron. Lett. **30**, 1875 (1994).
10. P. D. Townsend, Opt. Fiber Technol. **4**, 345 (1998).
11. P. D. Townsend, Nature **385**, 47 (1997).
12. V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, IEEE J. Quantum. Electron. **43**, 130 (2007).
13. W. Chen, Z. F. Han, T. Zhang, H. Wen, Z. Q. Yin, F.X Xu, Q. L. Wu, Y. Liu, Y. Zhang, X. F. Mo, Y. Z. Gui, G. Wei, and G. C. Guo, IEEE Photon. Technol. Lett. **21**, 575 (2009).
14. B. Qi, W. Zhu, L. Qian, and H-K. Lo, New J. Phys. **12**, 103042 (2010).
15. K. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, Opt. Lett. **37**, 223 (2012).
16. A. Ortigosa-Blanch and J. Capmany, Phys. Rev. A **73**, 024305 (2006).
17. J. Capmany and D. Novak, Nat. Photon. **1**, 319 (2007).
18. I. Choi, R. J. Young, and P. D. Townsend, Opt. Express **18**, 9600 (2010).
19. J. Capmany and C. R. Fernández-Pousa, IEEE J. Lightwave. Technol. **29**, 3061 (2011).
20. J. Mora, A. Ruiz-Alba, W. Amaya, V. Garcia-Muñoz, A. Martínez, and J. Capmany, in *Proceedings of the IEEE Topical Meeting on Microwave Photonics* (IEEE, 2010), pp. 286–289.
21. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).