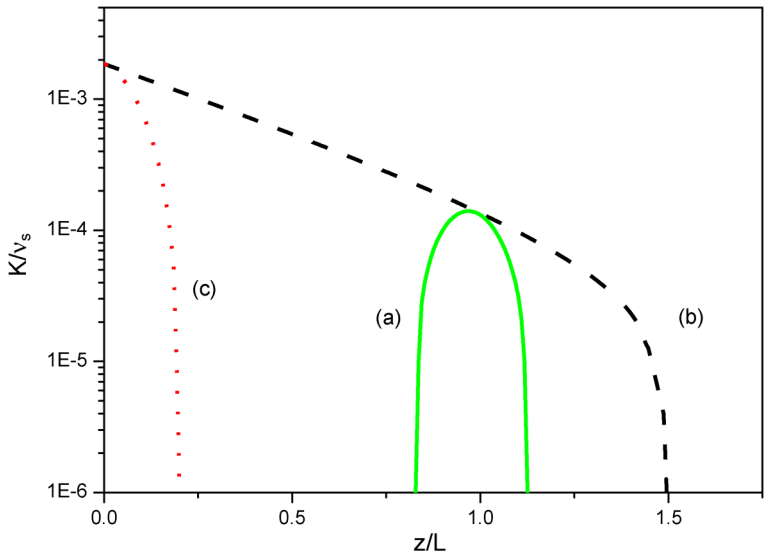
IEEE Photonics Journal
An IEEE Photonics Society Publication

Dispersion Supported BB84 Quantum Key Distribution Using Phase Modulated Light

Volume 3, Number 3, June 2011

J. Mora
A. Ruiz-Alba
W. Amaya
J. Capmany, Fellow, IEEE



DOI: 10.1109/JPHOT.2011.2146764
1943-0655/$26.00 ©2011 IEEE

Dispersion Supported BB84 Quantum Key Distribution Using Phase Modulated Light

J. Mora, A. Ruiz-Alba, W. Amaya, and J. Capmany, *Fellow, IEEE*

ITEAM Research Institute, Universidad Politécnica de Valencia, 46022 Valencia, Spain

DOI: 10.1109/JPHOT.2011.2146764
1943-0655/$26.00 ©2011 IEEE

Manuscript received March 30, 2011; revised April 18, 2011 and April 19, 2011; accepted April 19, 2011. Date of publication April 25, 2011; date of current version May 10, 2011. Corresponding author: J. Capmany (e-mail: jcapmany@dcom.upv.es).

Abstract: We propose and experimentally demonstrate that, contrary to what was thought up to now, an efficient BB84 operation is feasible using the double phase modulator (PM–PM) configuration in frequency-coded quantum key distribution systems without dispersion compensation. This is achieved by exploiting the chromatic dispersion provided by the fiber linking Alice and Bob. Thus, we refer to this system as dispersion supported or as the DS BB84 PM–PM configuration.

Index Terms: Microwave photonics, quantum communications, phase modulation.

1. Introduction

Quantum cryptography features the 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].

QKD deals with the need to distribute a key between a transmitter (Alice) and a receiver (Bob) with complete confidentiality. If Alice and Bob encode their bits in states of a quantum system, a third party, i.e., the eavesdropper (Eve) interested in gaining access to the information they share, will modify the quantum state and, therefore, will destroy its information. At the same time, the eavesdropper will neither be able to keep a perfect copy of the sequence nor to send it again in order to avoid being detected, as this is not allowed by the noncloning theorem [2].

Photonics is the principal enabling technology for long distance QKD using optical fiber links. A particularly interesting approach is the so-called frequency coding (FC-QKD) technique proposed by Mérolla *et al.* [3], which relies on encoding the information bits on the sidebands of either phase [4] or amplitude [5] radio frequency (RF) modulated light. In essence, Alice randomly changes the phase of the electrical signal used to drive a light modulator among four phase values $(0, \pi)$ and $(\pi/2, 3\pi/2)$, which form a pair of conjugated basis. When arriving to Bob, he modulates the signal again using the same microwave signal frequency, and thus, his new sidebands will interfere with those created by Alice [3]. The frequency-coded approach has the additional added value that its capacity can be upgraded by adding more microwave subcarriers: an approach which is known as Subcarrier Multiplexed QKD (SCM-QKD) [6]–[8].

The original proposal by Mérolla *et al.* [3] based on the use of a pair of simple phase modulators (PM–PM configuration) was, in principle, suited only for the implementation of the B92 protocol [9]. In fact, to demonstrate the implementation of the BB84 protocol, it had to be modified by replacing the phase modulators by unbalanced modulators (UM–UM configuration) [5], [10], which, in addition, need to be properly biased for successful operation.

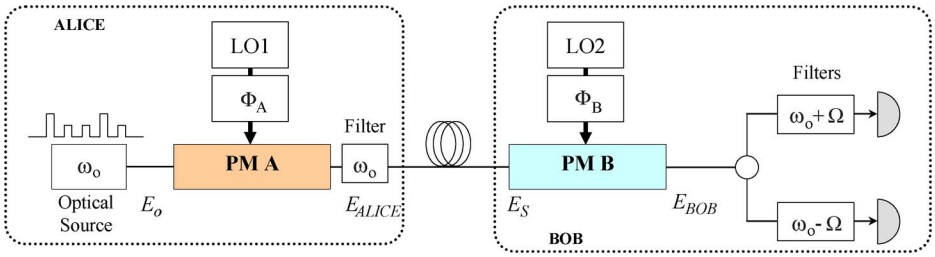


Fig. 1. Scheme of the frequency-coded system using a pair of phase modulators (PM–PM configuration). Alice and Bob are separated by a dispersive link of length L.

In this paper, we demonstrate, contrary to what was thought up to now, that BB84 operation is feasible using the PM–PM configuration. This is achieved by exploiting the chromatic dispersion provided by the fiber linking Alice and Bob. Thus, we refer to this system as dispersion supported or DS PM–PM configuration. This result is important for two reasons: first of all because it allows implementation of the BB84 protocol using the simplest frequency-coded configuration (PM do not require bias voltage) and, second, because the conditions under which this is possible are compatible with those to be found in practice, since Alice and Bob will be, in general, separated by a dispersive optical fiber link. Moreover, even though the use of a fainted laser source is assumed, our approach turns out to be robust against PNS attacks [11], provided that decoy state transmission (implemented by varying the intensity of the optical carrier in the Alice's transmitter) is employed [12], [13].

2. System Configuration and Model

The system under consideration is shown schematically in Fig. 1, and we briefly recall its operation [3]. Alice's transmitter contains a monochromatic optical source that emits photons with an angular frequency ω_o. The optical source emits pulses with variable intensity in order to implement decoy states. Note that an optical filter with tunable amplitude and centered at the optical carrier is needed at the output of Alice's transmitter to control the average photon number of the optical carrier to avoid an eavesdropper by monitoring the carrier component that is regarded as classical light. The optical source is externally modulated by a phase modulator (PMA), which is fed by means of a local oscillator LO1. The local oscillator gives an RF signal of frequency Ω in which Alice can introduce a random phase shift Φ_A to encode the binary secret key. This way, the encoded states are prepared entirely by Alice by means of an electrical phase shifter which gives the phase shift Φ_A. The output signal of Alice's transmitter can be described when low modulation index m_A is considered as

$$E_{\text{ALICE}}(t) = E_o e^{-j\omega_o t} \cdot \sqrt{t_A} \cdot \{1 + jm_A \cdot \cos(\Omega t + \Phi_A + \Phi_{\text{REF}})\} \quad (1)$$

where E_o is the amplitude of the electrical signal related to the average number of photons per bit, and t_A is related to the optical losses of the PMA. The phase Φ_{REF} is coming from the LO1, and it is used as reference phase of the system.

After propagation through a fiber link of length L, the light is again externally modulated by another PM2 at Bob's receiver. PMB is driven also with a frequency Ω but with variable phase Φ_B coming from an LO2. Then, the output optical signal after PMB is given by

$$E_{\text{BOB}}(t) = E_o e^{-j\omega_o t} \cdot e^{j\beta_o L} e^{-\frac{\alpha L}{2}} \sqrt{t_A t_B} \cdot \cdot \left\{1 + jm_A e^{j\frac{1}{2}\beta_2 L\Omega^2} \cdot \cos(\Omega t - \Phi_o + \Phi_A + \Phi_{\text{REF}})\right\}\{1 + jm_B \cdot \cos(\Omega t + \Phi_B)\} \quad (2)$$

where α is the optical fiber losses, t_B is related to the optical losses of the PMB, and m_B is the modulation index of the PMB. The term β_o is the propagation constant of the fiber link at the optical frequency ω_o, and the parameter β_1 is related to the phase $\Phi_o = \beta_1 L\Omega$, which corresponds with the optical group delay at ω_o after transmission [5]. From (2), we can observe that fiber

chromatic dispersion β_2 introduces a phase factor after propagation between the sidebands and the carrier of the optical signal coming from Alice's transmitter. The phase reference is taken as $\Phi_{REF} = \Phi_o - 1/2\beta_2 L\Omega^2$.

The final stage in the system is composed of an optical coupler and a set of optical filters centered at the optical sidebands $\omega_o + \Omega$ and $\omega_o - \Omega$, which are employed to measure the intensity of each optical sideband carrying the secret key. The output of each filter is then sent to a photon counter. Therefore, the optical power normalized for each sideband is given by

$$P(\omega_o + \Omega) = \frac{1}{2}[1 + V\cos(\Phi_B - \Phi_A)]$$
$$P(\omega_o - \Omega) = \frac{1}{2}\left[1 + V\cos(\Phi_B - \Phi_A + \beta_2 L\Omega^2)\right]. \quad (3)$$

Here, the parameter V corresponds represents the visibility of each band, which can be written as

$$V = \frac{2m_A m_B}{m_A^2 + m_B^2}. \quad (4)$$

The BB84 protocol needs that Alice generates randomly four states corresponding to the codification of bits "0" and "1" by means of two conjugated bases, and Bob measures the incoming states with the random choice of one of the conjugated bases. The procedure of measurements with each bases has to be complementary, i.e., when Alice and Bob select the same base for encode and decode, respectively, the measurement of the bit has to be completely defined. In FC-QKD systems, this complementary measurement for each base is realized through the probability of detecting one photon in the upper sideband and the probability of detecting one photon in the lower sideband. This condition is characteristic of those met in systems operating with the BB84 scheme. Under this consideration, we can see that BB84 protocol can be implemented successfully in our approach when the following condition is satisfied:

$$\beta_2 L\Omega^2 = (2n+1)\pi, \qquad n = 0, \pm 1, \pm 2 \ldots. \quad (5)$$

In addition, when the visibility is unity $(m_A = m_B)$, (3) can be written as

$$P(\omega_o + \Omega) = \cos^2\left(\frac{\Phi_B - \Phi_A}{2}\right)$$
$$P(\omega_o - \Omega) = \sin^2\left(\frac{\Phi_B - \Phi_A}{2}\right). \quad (6)$$

Alice's states are prepared by selecting four possible values of phase (Φ_A) 0, π and $\pi/2$, $3\pi/2$, which form this pair of conjugated bases [8]. On the other hand, Bob measures the incoming state with the random choice of one conjugated base through two possible values of phase Φ_B, 0, and $\pi/2$. The correct choice of the basis by Bob results in either $\Phi_B - \Phi_A = 0$ or $\Phi_B - \Phi_A = \pi$, depending on whether a bit "0" or "1" is sent by Alice. This implies, according to (6), that either the lower sideband $(\omega_o - \Omega)$ or the upper sideband $(\omega_o + \Omega)$ is eliminated, respectively, due to interference. When Bob chooses the incorrect basis, then $\Phi_B - \Phi_A = \pm\pi/2$, and none of the sidebands is eliminated since the detection probability is equal for upper and lower sideband. From (3), we observe that both sidebands have the same value when the fiber dispersion is negligible or compensated, i.e., when the term $\beta_2 L\Omega^2$ can be considered close to zero or negligible, as assumed, for instance, in [3]. Therefore, BB84 protocol cannot be implemented efficiently since the amplitudes of both sidebands are always equal, regardless of which particular base is chosen.

In principle, (5) seems to be a restriction of the system since fiber link length L and the operation frequency Ω are joined. However, alternative dispersive elements such as linearly chirped fiber Bragg grating (FBG) can be considered so that the link dispersion can be controlled. Therefore, (5) provides a design criterion for the system. If the overall link dispersion $\beta_2 L$ is fixed, then (5) gives the required value of the subcarrier frequency. This way, the system can use the tuning of the

modulation frequency to satisfy the condition of (5) by using tunable filters. On the other hand, if Ω is fixed, then from (5), we get the value of the minimum required link dispersion. Implementing the QKD system with a pair of phase modulators brings up several advantages in terms of cost and system complexity. For instance, phase modulators are cheaper than unbalanced modulators (UMs), and there is no need to fulfill the counterphase bias condition required when using two UMs. This point is certainly important since the modulator bias voltage tends to drift with time due to environmental impairments, and keeping this condition would require in practice an additional simultaneous bias tracking circuitry. On the other hand, from a point of practical view, the fluctuations, which can affect to the condition (5) related to the frequency stability of the local oscillator or environmental perturbation over the dispersion parameter and fiber length, can be readily estimated. For instance and calling $\Theta = \beta_2 L\Omega^2$, we have that the sensitivity is related to $\partial S = \partial\beta_2/\beta_2 + \partial L/L + 2\partial\Omega/\Omega$. For a typical fiber in the third telecommunications window, $\beta_2 = -21$ ps^2/km, and $\beta_3 = 0.06$ ps^3/km. For a typical source wavelength fluctuation of $d\lambda = 0.1$ nm and, consequently, $d\omega = 12.5 \cdot 10^9/(2\pi)$ s^{-1}, this yields $\partial\beta_2/\beta_2 = \beta_3 d\omega/\beta_2 \sim 5 \cdot 10^{-6}$. Regarding the fiber link length, this can be determined with a precision of around 1 m for a typical link length of 50 km, which yields $\partial L/L \sim 2 \cdot 10^{-5}$. Finally, RF generators provide frequency stability within 1 kHz, which results in the last term $2\partial\Omega/\Omega \sim 10^{-6}$. Thus, the expected overall sensitivity is around 10^{-5}, which is of no practical concern. Therefore, our DS PM–PM configuration is interesting due to practical considerations of stability and permits avoidance of the dispersion compensation since we exploit its properties to reconcile the PM–PM tandem structure with the BB84 protocol.

In order to show that our DS PM–PM solution converges to conventional FC-QKD configurations such as the UM–UM configuration with dispersion compensation, we analyze the secret key rate when Alice and Bob are separated by a distance $L = \pi/\beta_2\Omega^2$ for a given Ω and β_2. The evolution of QBER in function of the distance z can be obtained with a simple computation that yields the value

$$\mathrm{QBER}(z) = \frac{1}{2}\frac{[1 - C(z)] \cdot p^{\mathrm{signal}}(z) + d_{\mathrm{B}}}{p^{\mathrm{signal}}(z) + d_{\mathrm{B}}} \text{ with } p^{\mathrm{signal}}(z) = \rho\mu_{\mathrm{A}} t_{\mathrm{B}} e^{-\alpha z} \tag{7}$$

where p^{signal} is the probability of signal photon detection, and d_{B} is the dark count probability [8]. Note that p^{signal} depends on the detector efficiency ρ, which is the photon mean number μ_{A} of the subcarrier Ω from Alice's transmitters and the optical losses related to the second modulator and the transmission fiber. In our case, we define the contrast C as

$$C(z) = \frac{V \cdot \sin^2\left(\frac{1}{2}\beta_2 z\Omega^2\right)}{1 + V\cos^2\left(\frac{1}{2}\beta_2 z\Omega^2\right)}. \tag{8}$$

In Fig. 2, we show the evolution of the expected detection rate for a FC-QKD system when decoy states are employed according to our predicted evolution of the QBER from (8) and the theoretical analysis previously reported from [12]. The secret key rate K is plotted normalized to the repetition rate of the pulsed source ν_{s} for the DS PM–PM configuration (solid line) as a function of the link distance z for the case where $\beta_2 L\Omega^2 = \pi$, $d_{\mathrm{B}} = 10^{-5}$, and $V = 98\%$. For the sake of comparison with conventional FC-QKD systems, broken-trace curves are included showing the normalized secret key for the BB84 system based on the UM–UM configuration [5] with compensated (dashed line) and noncompensated (dotted line) dispersion. First, we can observe that dispersion compensation is needed to transmit a secret key for high-reach distance in conventional BB84 system based on FC-QKD. However, it becomes clear that the dispersion supported scheme converges to the standard BB84 system performance around $z = L$, which corresponds with the maximum value that the contrast C takes in (8), which corresponds with the visibility V. Note that the type of fiber used as transmission link is determined by the dispersion value and the fiber length. Nevertheless, other kinds of dispersive elements such as chirped FBGs can be incorporated to increase the flexibility of dispersion requirement in the system.

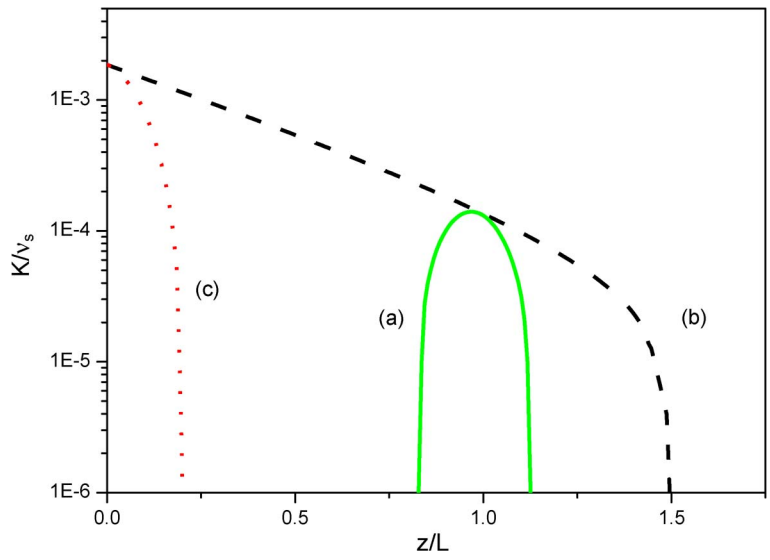


Fig. 2. Evolution of the secret key rate for (a) the DS PM–PM configuration as a function of the link distance z and (b) for the FC-QKD BB84 system when the dispersion is (b) compensated and (c) noncompensated.

3. Experimental Results

In order to validate the proposal, we have tested the QKD system under classical operation regime. Note that similar results are to be obtained when attenuating the signals as long as they can be represented by coherent states. The experimental demonstration was implemented with an optical laser delivering an output power of 5 dBm at 1550 nm. This external cavity laser has a wavelength stability of 100 MHz/h and an optical output stability of 0.05 dB/h. Both modulators PMA and PMB were electrooptic phase modulators with a 20-GHz electrical bandwidth and a 2.5-dB optical insertion losses. The half-wave voltage was 7.4 V. Two local oscillators were used to apply to an RF signal of 15 GHz for each modulator. The modulation indexes m_A and m_B for each modulator were close to 0.15 in order to guarantee a maximum visibility, as shown in (4). A standard single-mode fiber is used as fiber link which had a length around 15 km to comply with (5) with $n = 0$, and the spectra were recorded using an optical spectrum analyzer (OSA). The corresponding dispersion has been measured obtaining a value around -21 ps^2/km at 1550 nm.

The optical filters used in FC-QKD systems are based on FBGs which can offer a large suppression ratio at a small frequency separation, as we reported in [14]. Each FBG is tuned in wavelength using thermoelectric controllers with an accuracy of 0.1 °C, showing a wavelength stability of 1 pm, which is in order with the stability of the optical source. Our photonic filter is composed of a first stage with a strong selection for the optical carrier centered at the frequency ω_o and a second stage which permits to separate the upper and lower subcarrier.

Fig. 3 shows the power spectrum density measured at the OSA for three different fiber lengths when Bob chooses the correct base for the same state that Alice (right side graphs) or the orthogonal state (left side graphs) which corresponds with a phase difference $\Phi_B - \Phi_A$ of 0 or π, respectively. The phase shifter used in the experiment permits a control of the electrical phase with a step of 1.4° for a 360° operation range. The phase shifters have a time response with a rise and fall time around 200 ns.

In Fig. 3(a), we can observe that BB84 protocol can be implemented when the condition $\beta_2 L\Omega^2 = \pi$ is experimentally satisfied. The phase difference $\Phi_B - \Phi_A = 0$ corresponds with the transmitted bit "0" while the phase difference $\Phi_B - \Phi_A = \pi$ corresponds with the transmitted bit "1." According to (6), the optical sidebands $\omega_o + \Omega$ and $\omega_o - \Omega$ appear or not, depending on the constructive or destructive interference imposed by the phases chosen between Alice and Bob.

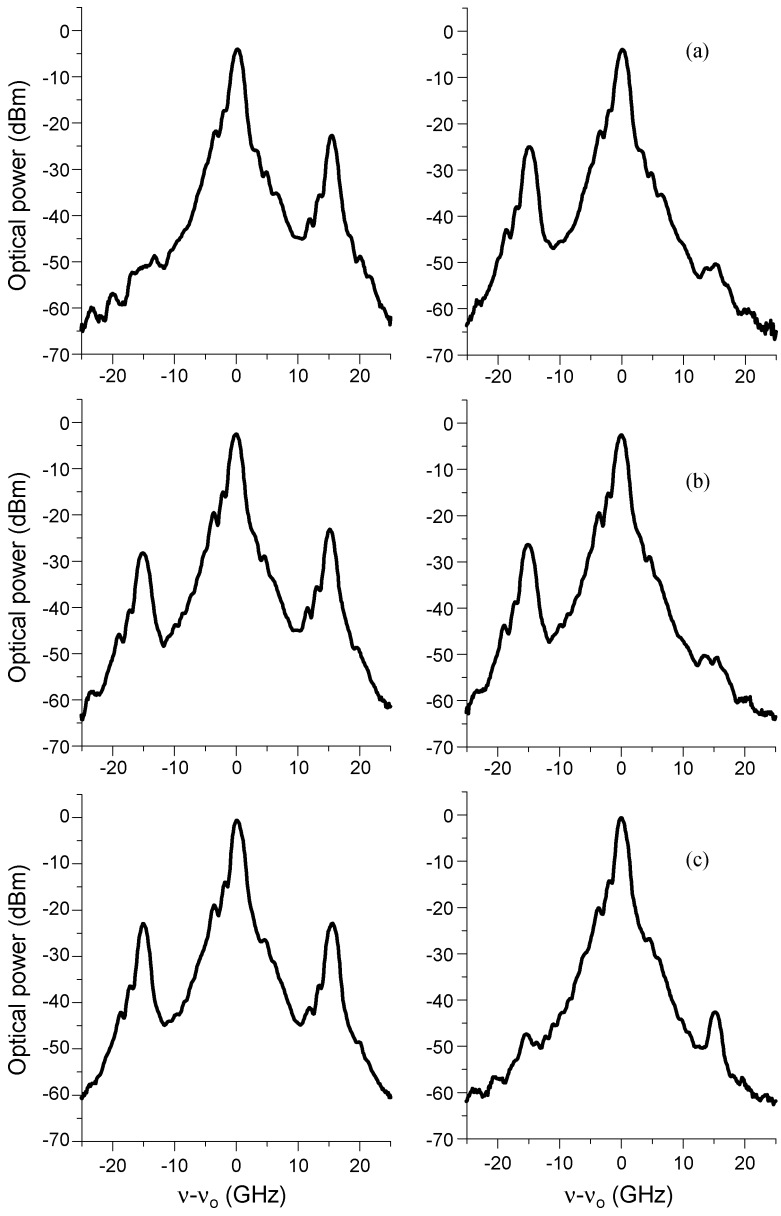


Fig. 3. Power spectra for a fiber link with a length (a) 15 km, (b) 7.3 km, and (c) 0 km. The term $\beta_2 L\Omega^2$ has the values close to π, $\pi/2$, and 0, respectively. Left side graphs correspond with the transmission of a bit "0" with $\Phi_B - \Phi_A = 0$, and the right side graphs correspond with the transmission of a bit "1" with $\Phi_B - \Phi_A = \pi$.

Note that the decision threshold between the bit "0" and "1" is maximum, achieving a contrast close to the visibility, which is around 0.99. However, the contrast of the interference is reduced when the length of the fiber link is far from that required by (5), as shown in Fig. 3(b) and (c). Indeed, the use of a fiber lengths of 7.3 km or a few of meters implies that the term $\beta_2 L\Omega^2$ is close to $\pi/2$ and 0 for Fig. 3(b) and (c), respectively. Note that the lower and upper sidebands do not permit the frequency coding of the bits "0" and "1" to be distinguished clearly. In addition, due to the optical fiber losses, the optical power of the optical carrier is -0.7, -2.6, and -4.0 dBm, respectively.

The theoretical and experimental values of the amplitudes of the detected sidebands are plotted in Fig. 4(a) (lower sideband) and Fig. 4(b) (upper sideband), respectively, as a function of the phase mismatch between Alice and Bob's RF modulating signals. Results are included for the three

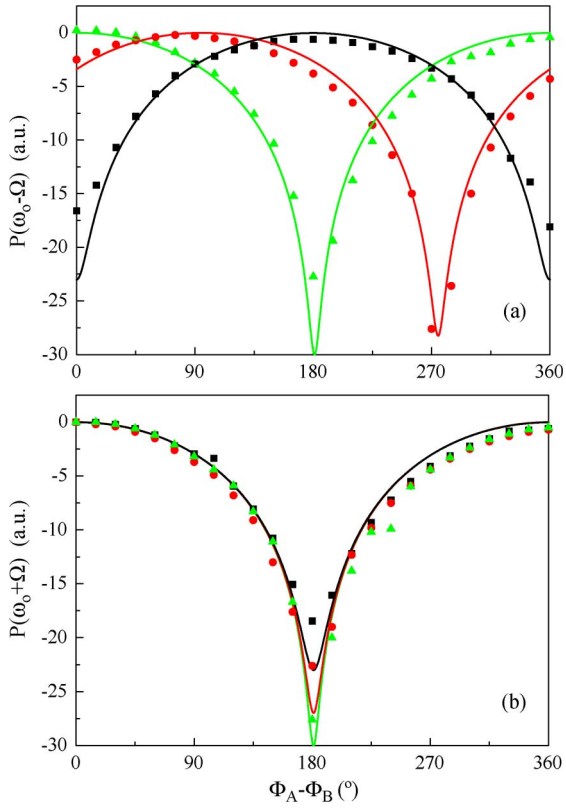


Fig. 4. Amplitude of sidebands for different phase shifts between Alice and Bob after 15 km (■), 7.3 km (●), and 0 km (▲). (a) Left optical sideband and (b) right optical sideband. (Solid traces represent theoretical results.)

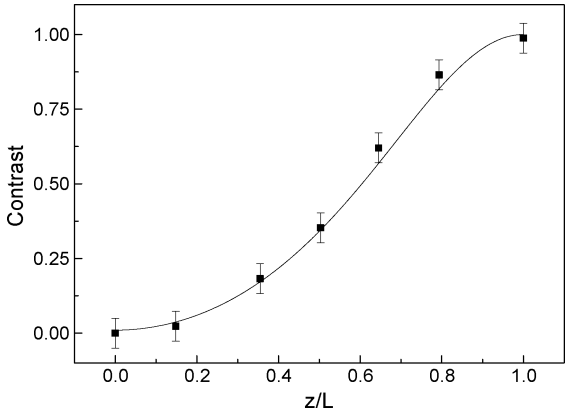


Fig. 5. Theoretical and experimental evolution of the contrast function given by (8).

different fiber link lengths previously considered. An excellent agreement can be observed between theoretical and experimental results. Furthermore, only for the case where the link length is that designed to fulfill the condition imposed by (5) can one appreciate the complementary characteristic of the sideband amplitudes, which is a distinctive feature of the BB84 operation.

As additional supporting experimental evidence, Fig. 5 plots the theoretical and experimental evolution of the contrast function given by (8) with an experimental visibility close to 99%. Note again the excellent agreement between both results.

4. Summary and Conclusion

In summary, we have proposed and demonstrated that BB84 operation is feasible using the PM–PM configuration without dispersion compensation, which was thought to be valid only up to now for the implementation of the B92 protocol. The unconditional security is guaranteed since our DS PM–PM approach is compatible with the decoy states implementation through the random intensity control of the optical carrier. By exploiting the chromatic dispersion which takes place in an optical fiber link, experimental results have been provided to support our proposal, showing excellent agreement with the theoretical predictions.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbiden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan. 2002.
[2] W. K. Wootters and W. H. Zurek, "A single quantum cannot be clones," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
[3] J.-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes, "Single-photon interference in sidebands of phased-modulated light for quantum cryptography," *Phys. Rev. Lett.*, vol. 82, no. 8, pp. 1656–1659, Feb. 1999.
[4] 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.
[5] 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. 2003.
[6] A. Ortigosa-Blanch and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 73, no. 2, p. 024305, Feb. 2006.
[7] J. Capmany, "Photon nonlinear mixing in subcarrier multiplexed quantum key distribution systems," *Opt. Express*, vol. 17, no. 8, pp. 6457–6464, Apr. 2009.
[8] J. Capmany, A. Ortigosa-Blanch, J. Mora, A. Ruiz, W. Amaya, and A. Martínez, "Analysis of subcarrier multiplexed quantum key distribution systems: Signal, intermodulation, and quantum bit error rate," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1607–1621, Nov. 2009.
[9] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.
[10] J.-M. Mérolla, L. Duraffourg, J. P. Goedgebuer, A. Soujaeff, F. Patois, and W. T. Rhodes, "Integrated quantum key distribution system using single sideband detection," *Eur. Phys. J. D*, vol. 18, no. 2, pp. 141–146, Feb. 2002.
[11] A. Acín, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 1, p. 012309, Jan. 2004.
[12] 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. 2009.
[13] M. Curty, T. Moroder, X. Ma, H.-K. Lo, and N. Lütkenhaus, "Upper bounds for the secure key rate of the decoy-state quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, p. 032335, Mar. 2009.
[14] 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. Meeting Microw. Photon.*, Oct. 2010, pp. 286–289.