Research Article | Vol. 25, No. 23 | 13 Nov 2017 | OPTICS EXPRESS 28886
Optics EXPRESS

Low loss QKD optical scheme for fast polarization encoding

A. DUPLINSKIY,[1,2,*] V. USTIMCHIK,[1,3] A. KANAPIN,[1,4] V. KUROCHKIN[1] AND Y. KUROCHKIN[1]

[1]*Russian Quantum Center (RQC), Business Center Ural, 100, Novaya Street, Skolkovo, Moscow Region, 143025, Russia*
[2]*Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141700, Russia*
[3]*IRE RAS, Mokhovaya St, 11 – 7, Moscow, 125009, Russia*
[4]*Lomonosov Moscow State University, GSP-1, Leninskie Gory, Moscow, 119991, Russia*
**a.duplinsky@rqc.ru*

Abstract: We present a new optical scheme for BB84 protocol quantum key distribution (QKD). The proposed setup consists of a compact all-fiber polarization encoding optical scheme based on $LiNbO_3$ phase modulators, single laser source and two single-photon detectors. The optical scheme consists of standard telecommunication components and is suitable for both fiber and free-space quantum communication channels. Low losses (~2 dB) in Bob's device increase both the key generation rate and the distance limit. A new technique for solving the polarization mode dispersion (PMD) issue in $LiNbO_3$ is implemented, allowing two crystals to neutralize the effect of each other. Several proof-of-concept experiments have been conducted at a 10 MHz repetition frequency over 50 km of standard optical fiber under laboratory conditions and over 30 km of urban fiber with high losses (13 dB), which is a link within a QKD network. To achieve this, calibration algorithms have been developed, allowing the system to work autonomously and making it promising for practical applications.

OCIS codes: (270.0270) Quantum optics; (270.5568) Quantum cryptography.

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).
2. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," Phys. Rev. Lett. **98**(1), 010503 (2007).
3. A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Continuous operation of high bit rate quantum key distribution," Appl. Phys. Lett. **96**(16), 161102 (2010).
4. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**(2), 172–177 (2017).
5. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," Phys. Rev. Lett. **98**(1), 010504 (2007).
6. H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtfeiser, and H. Weinfurter, "Free space quantum key distribution: Towards a real life application," Fortschr. Phys. **54**, 840–845 (2006).
7. C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter, "Long Distance Free Space Quantum Cryptography," Proc. SPIE **4917**, 25 (2002).
8. S. Nauerth, M. Furst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in free-space BB84 quantum cryptography," New J. Phys. **11**(6), 065001 (2009).
9. M. S. Lee, M. K. Woo, J. Jung, Y. S. Kim, S. W. Han, and S. Moon, "Free-space QKD system hacking by wavelength control using an external laser," Opt. Express **25**(10), 11124–11131 (2017).
10. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," Phys. Rev. Lett. **81**(15), 3283 (1998).
11. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," Nature **419**(6906), 450 (2002).

#304476 https://doi.org/10.1364/OE.25.028886
Journal © 2017 Received 16 Aug 2017; revised 11 Oct 2017; accepted 13 Oct 2017; published 7 Nov 2017

Optics EXPRESS

12. R. Hughes, J. Nordholt, D. Derkacs, and C. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. **4**(1), 43 (2002).
13. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**(7), 481–486 (2007).
14. C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," Opt. Express **16**(21), 16840–16853 (2008).
15. M. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtfeiser, "Daylight operation of a free space, entanglement-based quantum key distribution system," New J. Phys. **11**(4), 045007 (2009).
16. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," Nat. Photonics **7**, 382–386 (2013).
17. X. Liu, C. Liao, J. Mi, J. Wang, and S. Liu, "Intrinsically stable phase-modulated polarization encoding system for quantum key distribution," Phys. Lett. A **54**, 373 (2008).
18. X. B. Liu, C. H. Liao, Z. L. Tang, J. D. Wang, Z. J. Wei, and S. H. Liu, "Polarization coding and decoding by phase modulation in polarizing sagnac interferometers," Proc. SPIE **6827**, 68270I (2007).
19. Z. Yan, E. Meyer-Scott, J. P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hübel, and T. Jennewein, "Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links," J. Lightwave Technol. **31**(9), 1399–1408 (2013).
20. J. Wang, X. Qin, Y. Jiang, X. Wang, L. Chen, F. Zhao, Z. Wei, and Z. Zhang, "Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units," Opt. Express **24**(8), 8302–8309 (2016).
21. M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, "100 MHz Amplitude and Polarization Modulated Optical Source for Free-Space Quantum Key Distribution at 850 nm," J. Lightwave Technol. **28**(17), 2572–2578 (2010).
22. I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, "Proof-of-concept of real-world quantum key distribution with quantum frames," New J. Phys. **11**, 095001 (2009).
23. A. Duplinskiy, V. Ustimchik, A. Kanapin, and Y. Kurochkin, "Fast polarization QKD scheme based on LiNbO3 phase modulators," Proc. SPIE **10224**, 102242W (2016).
24. E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution", https://arxiv.org/abs/1612.03673.
25. E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, V. L. Kurochkin, Y. V. Kurochkin, and A. K. Fedorov, "Demonstration of a quantum key distribution network in urban fibre-optic communication lines," Quantum Electron. **47**, 798–802 (2017).
26. E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, "Quantum-secured blockchain", https://arxiv.org/abs/1705.09258.
27. N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
28. A. S. Trushechkin, E. O. Kiktenko, and A. K. Fedorov, "Practical issues in decoy-state quantum key distribution based on the central limit theorem," Phys. Rev. A **96**, 022316 (2017).
29. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett. **91**(4), 041114 (2007).
30. C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," Supercond. Sci. Technol. **25**(6), 063001 (2012).
31. G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**(3), 1867–1873 (2008).
32. G. B. Xavier, N. Walenta, G. V. De Faria, G. P. Temporão, N. Gisin, H. Zbinden, and J. P. Von der Weid, "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," New J. Phys. **11**(4), 045015 (2009).

1. Introduction

QKD is a rapidly developing technology. It allows unconditional secrecy of sharing keys between distant users – the transmitter (Alice) and the receiver (Bob), the security being guaranteed by fundamental laws of quantum physics. In QKD, Alice and Bob generate a secret key by transmitting information encoded in the states of single photons or weak coherent pulses. The most widely used encoding methods are: phase coding, in which information is contained in the phase difference between two modes interfering with each other, time-bin encoding, where bits are encoded in the time slots and polarization coding, in which the information is carried by the state of polarization (SOP) [1].

Polarization encoding is common for free-space applications, since the atmosphere, unlike telecommunicational optical fibers, keeps the polarization stable. However, even polarization

Optics EXPRESS

drift in a fiber quantum channel (QC) can be overcome with the help of polarization stabilization techniques. Moreover, this problem is not unique for polarization encoding schemes – usually phase encoding and time-bin QKD setups also require SOP recovery since Bob's devices frequently include polarization dependent elements [2–4]. Polarization encoding requires only single time slot, while phase encoding and time-bin BB84 need two or more [4].

Achieving quantum key production at competitive rates requires high frequency generation of polarization states, which is a challenge. Polarization controllers available on the market do not allow GHz state preparation frequencies, common for present-day QKD setups. The simplest fast QKD configuration for Alice utilizes four independent laser sources, one for each SOP required for BB84 protocol [5–7]. However, it appears to be hard to guarantee the indistinguishability of pulses emitted from different lasers, resulting in the system's vulnerability [8,9]. Bob as well needs to modify the SOP arriving at his station to select the measurement basis. Due to the same demand of high speed, it is usually done passively with the help of a beamsplitter (BS) [10–16]. The main drawback of this method is that the number of single-photon detectors (SPDs) increases by a factor of two – from two to four. This results in a higher quantum bit error rate (QBER) as the number of noise clicks rise. Moreover, SPDs are practically the most expensive part of QKD devices.

An alternative idea to use Pockels effect of fast electro-optical $LiNbO_3$ phase modulators for switching the polarization has been proposed with two main methods implementing this idea. The first one is based on the balanced interferometers [17,18]. Two orthogonal polarization components enter different arms of the interferometer with the help of a polarization beam splitter, after that one of the components experiences a phase shift induced by the modulator. As a result, two diagonal and two circular states can be generated. However, fiber Mach-Zendner interferometers are very sensitive and require phase stabilization [19], while interferometers with constant phase difference use free-space components that increase losses [17,18,20]. Jofre et al. proposed a different approach to switching the SOP with the help of phase modulators [21]. The transmitter based on this technique produces orthogonal states as polarization maintaining fiber is aligned at an angle of 45° directly to the $LiNbO_3$ crystal inside the modulator. A phase difference between orthogonal polarization components is produced, since modulation affects only one axis. The critical issue of this method is polarization mode dispersion (PMD) caused by the birefringence of the crystal. Suggested solutions, including polarization maintaining fiber (PMF) compensating patch cords [21] and Faraday mirrors [20,22] complicate the optical scheme (see sec. 4).

We present a simple configuration polarization encoding scheme based on $LiNbO_3$ phase modulators both in Alice's and Bob's devices, which use a single laser source and only two SPDs, while solving the PMD issue described above. Another advantage is that in contrast to the transmitter based on the phase modulator described in [21], there is no need to carry out any specific manipulation to align the PMF and the modulator's crystal, as a polarization controller or PMF patch cord spliced at an angle could be used (see sec. 2, 3). This significantly simplifies the technology and makes it possible to use modulators in regular configuration, which are available on the market. The result is a compact all-fiber system which consists of only standard telecommunication fiber components with low losses of about 2 dB on Bob's side.

A proof-of-concept experiment has been carried out at a 10 MHz laser pulses repetition frequency over 50 km of single-mode optical fiber. The system operates autonomously with the help of calibration algorithms, developed to set the polarization controllers' voltages. Once the QBER exceeds a threshold value set by the user, recalibration is applied automatically (see sec. 6, 7). The average QBER in our work is 2% with a sifted key rate of 0.5 Kbit/s. Furthermore, the system has been tested as a part of an urban QKD network [26]. Experimental demonstration confirms the suitability of the setup for practical applications. In

Optics EXPRESS

addition, electronics can be upgraded to reach much higher pulse rates, as the scheme is limited only by the modulators' maximum frequency, which can reach 10-40 GHz.

2. Experimental setup

The basic setup is shown on Fig. 1. Alice produces linearly polarized optical pulses using a 1550 nm laser source. The subsequent polarization controller (PC 1) is configured in such a way that the amplitudes of the field along the ordinary and extraordinary axes of the crystal inside the modulator (PM 1) are equal. This allows using the phase modulator for generating two pairs of orthogonal polarization states – "linear" and "circular" bases (see sec.3). The final element in Alice's apparatus is a variable optical attenuator that has two modes of operation – key sharing and system calibration. During the former, light is attenuated to 0.1 photon per pulse, while the latter is performed with stronger pulses (more than 1 photon per pulse, depending on the losses) to speed up the tuning procedure. As soon as the error rate reaches an acceptably low level, the attenuation is switched back to the key distribution regime value.

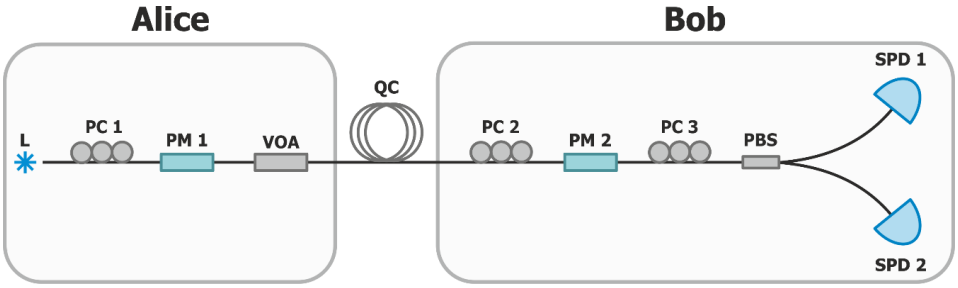

Fig. 1. QKD optical scheme for BB84 protocol with polarization encoding. Laser source (L) emits polarized optical pulses at 1550 nm. Polarization controller (PC 1) transforms the polarization state so that the amplitudes along the crystal axes of Alice's phase modulator (PM 1) are equal to each other. This allows Alice to encode bits of the secret key in the SOP with the help of the modulator. To weaken the pulse, a variable optic attenuator (VOA) is used. The intensity is reduced to calibration or key generation level, depending on the operation mode. After the quantum channel (QC), the second piezo-driven polarization controller (PC 2) compensates SOP drifts and rotates it so that the polarization components along the lithium niobate crystal axes switch places, compensating the birefringence of $LiNbO_3$. Bob's modulator PM 2 is used for basis selection. Finally, polarization controller PC 3 converts SOPs for polarization beam splitter (PBS) to distinguish states with the help of single-photon detectors (SPD1, SPD2). Standard single-mode fiber is suitable for all elements included; however, three polarization controllers are used.

At the input of the Bob's device is a polarization controller (PC 2), that compensates the changes that SOP of the pulse undergoes within the QC. In addition, it is used to rotate the polarization components by 90° relative to their positions at the input of the Alice's modulator (PM 1). As a result, the component that passed along the fast axis of lithium niobate inside Alice's modulator travels along the slow axis of the identical crystal within Bob's modulator and vice versa, so the two $LiNbO_3$ crystals of the modulators compensate each other's polarization mode dispersion (sec. 4). Bob uses his modulator (PM 2) to select the measurement basis, deciding whether to apply a phase shift corresponding to a $\lambda/4$ plate, thereby switching between "linear" and "circular" bases (see sec. 3). The final polarization controller (PC 3) rotates the polarization, preparing the light for projective measurement in the corresponding basis with the use of a polarization beam splitter (PBS) and two single-photon detectors (SPD 1, SPD 2). The procedure is similar to using a half-wave plate in free-space (Fig. 2), rotating polarization by 45°, to fit our logical state polarizations into one of two PBS output channels depending on the state (sec. 3). For continuous operation, all polarization controllers are piezo-driven and are automatically adjusted by feedback algorithm described in the sec. 5.

Optics EXPRESS

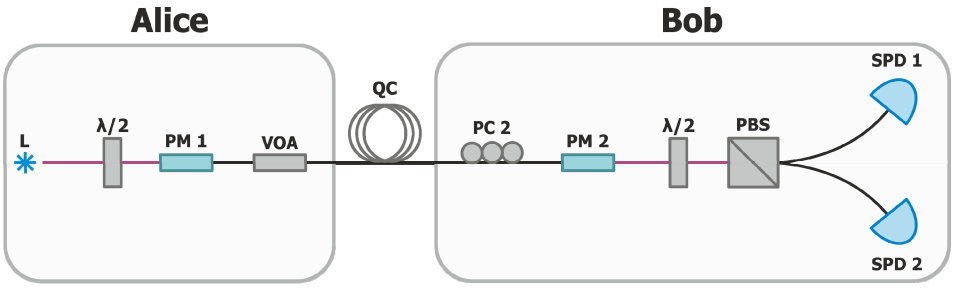

Fig. 2. A version of the optical scheme with free space elements and single polarization controller. Controllers PC1 and PC3 (from Fig. 1) have been replaced with free-space optical elements – half-wave plates and PBS cube. Alice and Bob use PMF inside their devices, that is shown with purple lines.

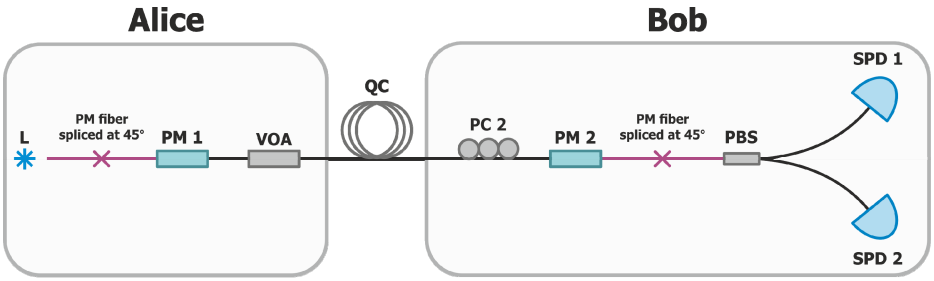

Fig. 3. Full-fiber version of the optical scheme with single polarization controller. Controllers PC1 and PC3 (from Fig. 1) have been replaced with fiber splices at a 45° angle. Alice and Bob use PMF inside their devices, that is shown with purple lines.

Polarization controllers PC 1 and PC 3 only affect the fiber inside the devices of Alice and Bob, so they could be replaced with passive optical components and PMF. Half-wave plates rotate the SOP and PMF retains the amplitudes along both axes constant. However, using free-space optics is less practical, due to its sensitivity and high losses of fiber in-out interfaces. Therefore, the most promising design is replacing controllers with PMF fiber splices at 45°, which provides the same effect (Fig. 3). In addition, any combinations of scheme versions could be used. Detailed analysis of these solutions is given in the sections 3 and 5.

3. Phase modulator for polarization state changing

Polarization state at the input of phase modulator can be represented as a Jones vector. Here and below we use the reference frame associated with the modulator's crystal axes. Ignoring the constant phase, the polarization state vector at the input of the modulator is expressed as follows:

$$\begin{Vmatrix} A \\ Be^{i\varphi_1} \end{Vmatrix} \tag{1}$$

Here A and B are the real amplitudes along the ordinary and extraordinary axes of lithium niobate and φ_1 is the phase difference between the components [23]. To describe the influence of the phase modulator on the polarization we use Jones matrix:

$$\begin{Vmatrix} e^{i\varphi_{or}} & 0 \\ 0 & e^{i(\varphi_{ex}+\Delta\varphi)} \end{Vmatrix} \tag{2}$$

Optics EXPRESS

Here $\Delta\varphi$ is a voltage-induced phase shift and φ_{or} and φ_{ex} – phase shifts along ordinary and extraordinary axes, respectively, at zero voltage. For simplicity, we describe a system without losses, since fixed losses do not affect the polarization state but only weaken the pulse's intensity. Polarization dependent losses (PDL) are considered to be negligible, as confirmed by experimental results.

The phase shift $\Delta\varphi$ will affect only one of the vector components. In order for the phase modulation to switch SOP to an orthogonal one, it is necessary and sufficient that the magnitudes of the vector components along the axes are equal, while the applied phase shift is π [23]:

$$|A| = |B|, \quad \Delta\varphi = \pi. \tag{3}$$

In such a configuration the phase modulator acts like a $\lambda/2$ plate, reflecting the polarization state symmetrically relative to the crystal axis. Therefore applying 0 or π phase shifts we produce a pair of states which forms the first basis for BB84 protocol (At this step we neglect the birefringence of the $LiNbO_3$ as it would be discussed in detail in sec.4):

$$\begin{aligned} \psi_1 &= \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + e^{i\varphi_1}|\updownarrow\rangle\right) \\ \psi_2 &= \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + e^{i(\varphi_1+\pi)}|\updownarrow\rangle\right) \end{aligned} \tag{4}$$

To create the second basis states, we add an extra $\pi/2$ phase shift (similarly to $\lambda/4$ plate) to both of the states listed above:

$$\begin{aligned} \chi_1 &= \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + e^{i(\varphi_1+\pi/2)}|\updownarrow\rangle\right) \\ \chi_2 &= \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + e^{i(\varphi_1+3\pi/2)}|\updownarrow\rangle\right) \end{aligned} \tag{5}$$

In Fig. 4, the set of corresponding SOPs is shown on the Poincare sphere. The four states are located on a meridian that includes diagonal and circular polarization states and are separated by 90° angles. The common offset angle is determined by φ_1. In the special case when $\varphi_1 = 0$, the first basis corresponds to linear diagonal states and the second to right and left circular polarizations (Fig. 5(a)). For simplicity, we shall thereafter call the bases "linear" and "circular" even for nonzero φ_1.

Optics EXPRESS

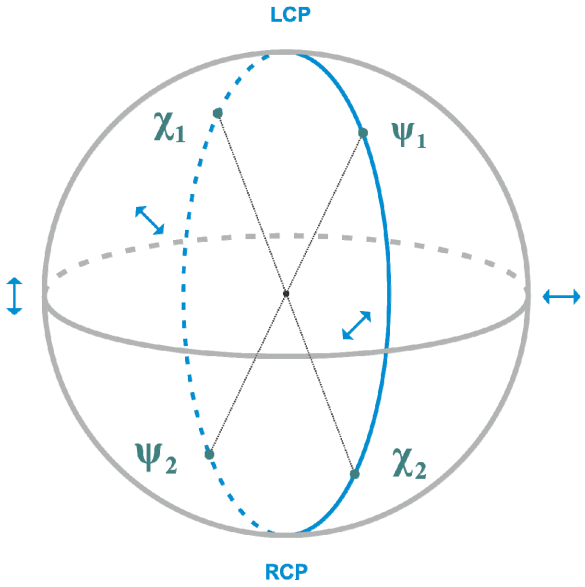

Fig. 4. The four states produced by Alice displayed on the Poincare sphere

Such a configuration of states is suitable for the BB84 protocol. That is, if Bob's apparatus is set to distinguish the states in one of the two bases, the states in the other basis will randomly produce an event in either detector with a probability ½.

Note that actually φ_1 does not have to be zero and in general case the states that fit our requirements are two pairs of orthogonal ellipses (Fig. 5(b)). This fact significantly simplifies the procedure of guiding the light into the modulator and is exploited within the experimental setup that we present.

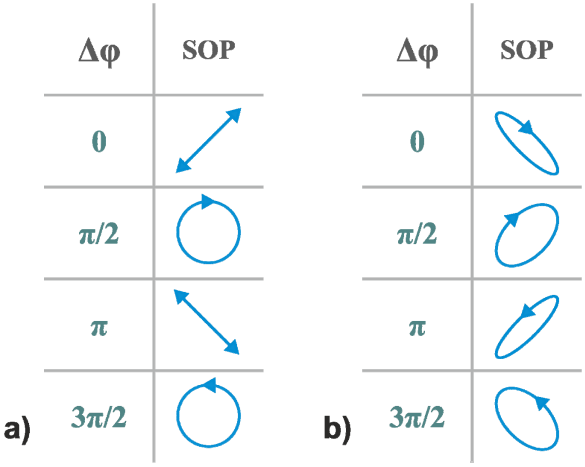

Fig. 5. .Polarization patterns at the $LiNbO_3$ phase modulator output. a) special case $\varphi_1 = 0$; b) arbitrary φ_1

In order to fulfill condition (3), it is necessary to guide the light into the crystal in a way that the amplitudes along the crystal axes are equal. Similarly, for Bob to decipher the information correctly, an inverse transformation is required, turning the states into horizontal and vertical. As discussed above, this can be realized in free space by means of a half-wave plate, of in fibers via a polarization controller, or simply splicing two PMFs at a 45° angle.

Optics EXPRESS

4. Compensating polarization dispersion in a $LiNbO_3$ crystal

The lithium niobate crystal used in the phase modulators has a significant difference in the refraction indices of the ordinary and extraordinary axes. As a result, PMD is observed when light enters the crystal at an angle to its axes. The difference in the optical paths of the axes within a modulator is about 0.5 mm (less than 2 ps), so for pulses wider than a nanosecond the PMD itself does not produce significant error rate. However, power modulation of a semiconductor laser diode, which is used to generate the pulses, results in phase variation with time, i.e. in chirping of these pulses. This effect combined with a shift between the two orthogonal polarization components caused by the PMD leads to a significant degree of polarization degradation as SOP changes dramatically within a single pulse. This in turn causes a high error rate.

Several methods for compensating the occurring dispersion have been proposed. For example, PMF also possesses a difference in the refractive index of the two axes, so two modes could be aligned by choosing a patch cord of certain length [21]. Another alternative is guiding the pulse through the modulator a second time after being reflected from a Faraday mirror, so both components pass the ordinary and extraordinary axes one time each [22].

The solution presented in this work does not require any additional elements in the scheme. The polarization components entering Bob's phase modulator are rotated by 90° relative to the way they enter the modulator in the Alice's device. The component that passes through the ordinary axis in Alice's crystal passes through the extraordinary axis in Bob's crystal, and vice versa. As a result, the optical paths of both components are evened out, with the help of identical modulators and correct tuning of the polarization controller between them.

The absence of extra components minimizes losses in Bob's device, increasing the key bitrate. The minimum loss is limited by the commercial lithium niobate modulator. The insertion loss of the fiber-coupled phase modulators is usually a bit less than 2dB for the best models. This results in about 2dB losses for the optical scheme of Bob's device. The calibration task for the polarization controller is discussed in detail in sec. 5.

5. The calibration procedure

The correct operation of the scheme requires the voltages of the piezo-driven polarization controllers to be set up in such a way that the polarization of the light entering both modulators and the PBS fits the requirements described above. Calibration is performed automatically. The input data for the tuning is the SPDs count statistics. To increase the amount of detector clicks and speed up the process, the light intensity is significantly increased for the duration of the calibration with the help of a voltage-driven attenuator. The intensity of the calibrating pulses sent by Alice is chosen depending on the losses in the quantum channel. Analyzing this data, the program adjusts the polarization controllers' voltages.

Goal

Let us briefly summarize the requirements for the SOPs described above:

1) At the input of Alice's phase modulator, the components along ordinary and extraordinary axes are equal

2) At the input of Bob's modulator, the components swap

3) Bob's measurements differentiate BB84 orthogonal states with extinction higher than 98%.

These requirements can be formulated mathematically by defining the Jones matrices for each of the scheme's sections.

Optics EXPRESS

The first section connects the laser source and Alice's phase modulator. We assume the incident light to be linearly polarized. To fulfill the criterion 1 the transformation of this section has to be:

$$\frac{\sqrt{2}}{2}\begin{Vmatrix} e^{i\varphi_1} & 1 \\ 1 & e^{-i\varphi_1} \end{Vmatrix} \tag{6}$$

The second section lies between Alice's and Bob's modulators and includes QC. According to the condition 2 the overall transformation of this part should be:

$$\begin{Vmatrix} 0 & 1 \\ e^{i\varphi_2} & 0 \end{Vmatrix} \tag{7}$$

Finally, the condition 3 is implemented by section between Bob's modulator and the PBS:

$$\frac{\sqrt{2}}{2}\begin{Vmatrix} e^{i\varphi_3} & 1 \\ 1 & e^{-i\varphi_3} \end{Vmatrix} \tag{8}$$

All three sections may introduce arbitrary relative phase shifts (φ_1, φ_2, φ_3) between the polarization components, but in order for PBS to distinguish the states correctly their sum should be divisible by 2π:

$$(\varphi_1 + \varphi_2 + \varphi_3) \vdots 2\pi \tag{9}$$

This is required as production of the matrices (6), (7) and (8) should be equal to identity matrix. Note that φ_1 mentioned in sec. 3 is a result of the transformation (6) that is applied in the first section.

Tuning

As we cannot directly measure the elements of the Jones matrices for every section, we need to establish a set of observed values to implement the calibration. We tune one controller after another relying on the single photon detector counting statistics. To get enough information we need to switch on phase modulators and match the detector statistics to the phase shifts that we apply.

Alice applies four different voltages to the phase modulator, corresponding to phase shifts of 0, π/2, π and 3π/2. Bob applies two voltages, corresponding to 0 and π/2.These shifts do not mean correct polarization states production and detection, since polarization controllers are not tuned correctly yet. We begin the calibration by amassing the statistics of detector clicks corresponding to each pair of voltages, receiving a histogram of eight columns (Fig. 6), as shown in the Table 1.

The tuning of PC2 is based on the idea that, if correctly set up, the two phase modulators apply their phase shifts to orthogonal polarization components of light (sec. 4). Therefore, the pulses that experienced the pairs of shifts (0, 0) and (π/2, π/2) should not be distinguishable. This means that these two pulses will have the same statistics of clicks.

In addition, the following pairs are indistinguishable:

1) with a relative phase shift of π/2: (π/2, 0) and (π, π/2);

2) with relative phase shift of π: (π, 0) and (3π/2,π/2);

3) with relative phase shift of 3π/2: (3π/2, 0) and (0, π/2).

Optics EXPRESS

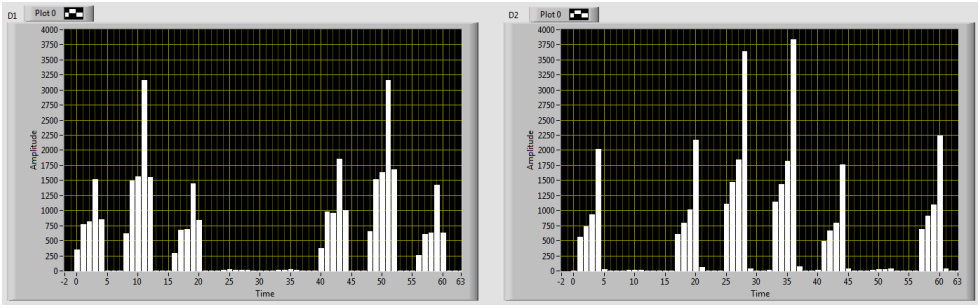

Fig. 6. Histogram of eight pulses for two detectors, illustrating all possible combinations of Alice's and Bob's phase shifts, corresponding to the Table 1.

Table 1. All possible combinations of Alice's and Bob's states. Letters "C" and "L" stand for "circular" and "linear" states, respectively. For more detail, see sec. 3.

Pulse number	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Alice's bit	0	1	1	0	0	1	1	0
Alice's basis	C	L	C	L	C	L	C	L
Bob's basis	L	L	L	L	C	C	C	C
Bob's bit after sifting	-	1	-	0	0	-	1	-

Thus, we tune PC 2 aiming to equalize the click statistics for these combinations. Once PC 2 is set up correctly, PC 1 and PC 3 may be tuned in any order. The first one maximizes the difference between logical 1 and 0 in the correct bases, while the third one finishes the procedure, minimizing the error rate. The last controller that is tuned fits Eq. (11) equation for the current setups of the two controllers that were calibrated before.

The setup upgrades using passive elements (Fig. 2, Fig. 3) significantly simplifies the calibration process, as only one controller has to be tuned. Indeed, sections 1 and 3 are already consistent with matrices (6) and (8). The only polarization controller in the scheme has to minimize the error rate, which means that it meets the (7) type, also fulfilling the condition (9). Recalibration may be caused by the changes in the QC or by drifts of φ_1 or φ_3, that are not guaranteed to remain stable.

Algorithm

Three channels of the polarization controllers are used. The controller successively minimizes the parameter for each channel using gradient descent.

Each controller uses its own parameter for minimization. Thus, for PC2, which attempts to align four pairs of columns on the histogram, the parameter was chosen to be equal to the squared sum of differences of corresponding columns, averaged over a short period to reduce the influence of noise on this parameter. The time has been chosen manually to ensure a balance between precision and performance speed. PC1 aims to achieve a maximal difference between logical 0 and 1 columns when Alice and Bob bases are the same. The parameter is the difference, taken with a minus sign. PC3 directly minimizes the error rate.

6. Experimental results

A proof-of-principle experiment has been conducted at a 10 MHz repetition frequency. The key distribution has been carried out over a distance of 50 km of standard single-mode optical fiber in spool (10 dB losses) with 0.1 photons per pulse. The system automatically performed

Optics EXPRESS

the calibration procedure and maintained QBER below 5% for hours, applying recalibration as needed. Average time that the system has spent in the key distribution mode is about 80%, while the other 20% has been required for recalibrations as the quantum channel has not been isolated from external influences, including mechanical and temperature ones. The effective key generation frequency was reduced to 5 MHz due to the processing issues. The sifted key generation rate of 0.5 Kbit/s and 2% QBER have been obtained with 20 ns detection window. The system uses ID Quantique ID230 single-photon detectors with 10% efficiency, 13 μs dead time, 15 Hz dark count rate and 5% afterpulsing probability. Data acquisition, control of the phase modulators, attenuator, laser source and polarization controllers is carried out via a National Instruments FPGA, the software being written in LabVIEW. The calculated lower bound for QBER in this setup is about 1% mainly due to afterpulses.

Further, an environment experiment has been carried out for a 30 km urban line with high losses (13 dB). To suppress the noise caused by the nearby telecommunicational fiber channels, WDM optical filter at 1554.94 nm has been used on the Bob's side. The laser has been tuned with the help of temperature controller to fit the filter's wavelength. The residual illumination has been about 200Hz. To reduce its impact, system has been upgraded to a 5 ns detection window. In order to guarantee the key secrecy, the average number of photons per pulse has been lowered to 0.02. Under these conditions, 106 bit/s sifted key rate has been obtained, taking calibration time into account (265 bit/s raw key during key distribution regime). Figure 7 illustrates QBER statistics vs. time during urban tests for 20 hours, the average value being 5.5%. The experiment has shown approximately the same proportion of data transfer and calibration time – about 20% has been spent for tuning. For this experiment the lower bound for the QBER is about 4,5% mostly caused by the noise from the telecommunicational channel, together with the low intensity of the key pulses. The post-processing procedure applied to the sifted key consists of information reconciliation, parameter estimation, privacy amplification, and authentication check stages [24]. As a result, secret key has been generated with 0.02 Kbit/s rate.

The system is currently used as a link within a QKD network across the urban fiber channels [25]. The developed QKD network is based on the trusted repeater paradigm and allows establishing a common key between users over an intermediate trustworthy node. The second link is a "plug and play" phase encoding scheme. The developed network has been used for the first quantum-secure blockchain experiments [26].

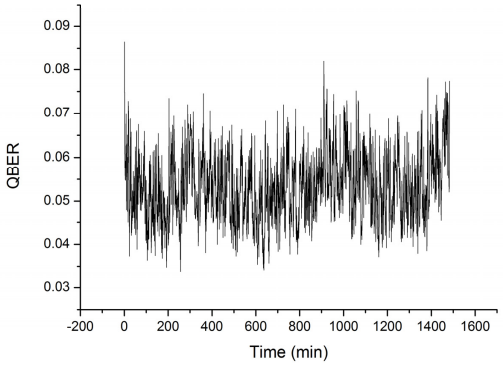

Fig. 7. QBER statistics with time during the urban tests with 13 dB losses and 0.02 photons per pulse.

We used a model described in [27] to find the upper bound for number of photons per pulse that guarantees the secrecy of the key, without decoy states. As soon as SPDs are the part of the Bob's device, which is trusted, we assumed constant detector efficiency. The upper

Optics EXPRESS

bound for allowed number of photons per pulse decreases as the losses in the quantum channel increase. The next upgrade of the device is going to include the intensity modulator to generate decoy states, allowing more photons per pulse, which means higher key generation rate [28].

Upgrade of the driving electronics will provide higher repetition frequencies that will also significantly increase the secret key rate. Losses within the quantum channel, detector dead time and non-perfect efficiency drop the key generation speed, so the best possible count rate for GHz laser repetition frequencies is practically below 100 MHz. For long distances or just for channels with high losses this value could be much less than kHz. For these purposes commercial free-run detectors with time resolution below nanosecond could be used, but the maximum count rate for InGaAs - based detectors is much less than 1 MHz due to the dead time. On the other hand, detectors with gating frequencies beyond GHz could be used [29]. Furthermore, superconducting nanowire single-photon detectors can reach count rate even beyond 100 MHz [30].

It should be noted, that during the last decade many ways to stabilize the SOP for QKD have been proposed, including those that can act during the key distribution, allowing the system to operate without interruptions [31,32]. These methods usually require bright pulses for stabilization at a different wavelength. To avoid extra band-pass filtering and minimize losses, we have used quantum signal to calibrate system without bright pulses. Our algorithm is based only on the elements that are required for key distribution, making it possible for Alice to become flashdrive-size. However, for different applications other stabilization procedures may be implemented to improve characteristics of the system.

7. Conclusions

A novel optical scheme implementing the polarization encoding BB84 protocol has been presented. Alice uses a $LiNbO_3$ phase modulator to generate two pairs of orthogonal polarization states with a single laser source, solving the issue of pulses' indistinguishability. A polarization controller or a PMF splice at an angle of 45° guide the pulses into the modulator with equal amplitudes along the crystal axes. Bob's device similarly selects the measurement basis with a modulator and rotates the output SOP in order for the PBS to distinguish different bits. Only two SPDs need to be used due to the active basis selection. Low losses (~2 dB) in Bob's apparatus allow increasing the communication distance and the bitrate. In addition, a novel approach solving the issue of PMD caused by the $LiNbO_3$ birefringence is implemented. A polarization controller following the quantum channel rotates the SOP by 90° equalizing the optical paths of two polarization modes within the crystals. A significant advantage of the scheme is that it consists of only standard telecommunication components and is suitable for both fiber and free space QCs.

Proof-of-concept experiments have been conducted at 10 MHz over 50 km of optical fiber in a spool and 30 km of urban fiber line. The system has been used as a part of a QKD network. To achieve continuous operation for several hours, calibration algorithms have been developed, allowing the system to work autonomously. The algorithm has proved itself reliable under both laboratory and urban conditions, spending approximately 20% of time for recalibration. The scheme seems suitable for future upgrades to higher frequencies and decoy-state protocols, being promising for practical applications.

Funding

The research leading to these results has received funding from Russian Science Foundation under project 17-71-20146.