Fast polarization QKD scheme based on $LiNbO_3$ phase modulators

A. Duplinskiy[1,2], V. Ustimchik[1,2], A. Kanapin[1,3] and Y. Kurochkin[1]

[1]Russian Quantum Center (RQC), Business Center «Ural», 100, Novaya st., Skolkovo, Moscow reg., 143025, Russian Federation
E-mail: a.duplinsky@rqc.ru
[2]Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141700, Russian Federation
[3]Lomonosov Moscow State University, GSP-1, Leninskie Gory, Moscow, 119991, Russian Federation

ABSTRACT

An optical scheme for polarization encoding BB84 protocol is described. Fiber electro-optical $LiNbO_3$ phase modulators based on Pockels cells provide both polarization states generation for Alice and basis choosing for Bob at high frequency, requiring low operation voltages ($V_\pi < 5V$). Proposed scheme uses only one laser source, which guarantee the indistinguishability of the pulses and active basis choosing allows the system to have two single photon detectors in contrast to the four in the standard polarization encoding schemes. Two phase modulators compensate each others' polarization mode dispersion, caused by the natural birefringence of the lithium niobate crystal. The system consists of standard components and has simple configuration. The principle of operation is experimentally demonstrated.

Keywords: quantum key distribution, polarization coding, $LiNbO_3$, EOM, birefringence

INTRODUCTION

Quantum key distribution (QKD) is an actively developing technology, with many different protocols and methods of encoding. BB84 is the first but still the most widely used and robust QKD protocol which security has been completely proven [1]. Practical realizations of BB84 could be divided into two major fields – phase and polarization coding. The former is widely used for QKD along the optical fiber, while the latter is preferable for atmosphere communication, including satellite quantum cryptography. Nowadays optical schemes implementing BB84 using polarization encoding have some practical drawbacks due to the fact that most components, which allow to change the state of polarization are low-frequency (polarization controllers) or require high voltages for operation (free space Pockels cells).

The simplest polarization encoding BB84 scheme that operates at high frequency for Alice requires four different laser sources, each of them generating one of the desired states of polarization [3]. This leads to a problem of proving the indistinguishability of pulses which are sent from different sources. For example, if the pulse shape differs much from laser to laser, the eavesdropper would be able to measure which bit has been sent without disturbing the polarization state.

At the Bob's side high frequency is usually reached using passive basis choosing. A 50/50 beam splitter allows the pulse to choose one of the paths, which stand for different bases measurements. This requires two detectors for each path, which results into four single photon detectors for the scheme [3]. Proposed two-detector implementation with the same idea uses time-bin-shift, which decreases the detector's effective operation frequency [4].

Fiber electro-optical $LiNbO_3$ phase modulators include Pockels cells which due to the small size allow to work with low voltages ($V_\pi < 5V$) in contrast to the free space optics. At the same time they provide up to 20 GHz operation frequency, which makes them highly perspective for polarization encoding QKD applications.

Usage of fiber phase modulators based on $LiNbO_3$ Pockels cell to implement fast polarization tracking source has been proposed [2], which allows one to use single laser source for polarization encoding implementation, solving the problem

International Conference on Micro- and Nano-Electronics 2016, edited by Vladimir F. Lukichev, Konstantin V. Rudenko
Proc. of SPIE Vol. 10224, 102242W · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2266517

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term

of indistinguishability. However authors observed output signals to be significantly disturbed by polarization mode dispersion (PMD) in lithium niobate, which is proposed to compensate using HiBi fiber.

We present a polarization encoding QKD system where both Alice and Bob use phase electro-optical $LiNbO_3$ modulators for polarization tracking. Alice creates one of four polarization states – two bases of two orthogonal states. Bob uses his modulator to choose the basis in which he measures the state. This allows Bob to use only two detectors instead of four in the scheme with the passive choice. Proper calibration of polarization controller between Alice and Bob allows two phase modulators to compensate each other's PMD.

CLASSICAL STATES DESCRIPTION

Electro-optical $LiNbO_3$ phase modulators employ Pockels effect for operation. Refractive index of lithium niobate along one of the optical axes changes proportionally to the applied electric field. This effect is usually used to change the polarization state, varying the phase shift between two polarization components. Here we describe how it can be used for a practical polarization encoding scheme.

Jones matrix of lithium niobate phase modulator along the crystal optical axes is[1]:

$$\begin{Vmatrix} e^{i\varphi_{or}} & 0 \\ 0 & e^{i(\varphi_{ex}+\Delta\varphi)} \end{Vmatrix} \quad (1)$$

Where $\Delta\varphi$ is a voltage-induced phase shift and φ_{or} and φ_{ex} – phase shifts along ordinary and extraordinary axes, respectively.

Polarization state at the input of phase modulator could be represented as Jones vector, ignoring the constant phase:

$$\begin{Vmatrix} A \\ Be^{i\varphi_0} \end{Vmatrix} \quad (2)$$

A and B are real amplitudes alone ordinary and extraordinary axes of lithium niobate and φ_0 is a phase difference between the components.

We place a polarization controller and a polarization beam splitter (PBS) after the phase modulator. Two arms of the PBS end with detectors D1 and D2.

Assume that we managed to apply two different voltages to the phase modulator and adjust polarization controller so that with the first one the signal is completely in the D1 and with the second in the D2 or vice versa. Two states at the input of PBS could be written as $\sqrt{A^2+B^2}\begin{Vmatrix} e^{i\chi} \\ 0 \end{Vmatrix}$ and $\sqrt{A^2+B^2}\begin{Vmatrix} 0 \\ e^{i\phi} \end{Vmatrix}$, ($\chi, \phi$ random). These vectors are orthogonal. Considering polarization dependent losses to be negligible Jones matrix of optical fiber could be presented as a composition of birefringent plates and rotation matrixes. Due to the fact that these types of matrixes are unitary, the composition will also be an unitary matrix. We also consider that this matrix remains constant between the two pulses, because polarization drifts are slow enough. Therefore, if orthogonal states enter the PBS this means that states at the output of phase modulator were also orthogonal according to the properties of unitary matrixes.

The pulses' state after the modulator would be:

[1] To simplify equations we suppose components and fiber to be lossless. Polarization independent losses do not change the direction of the Jones vector, but only reduce its length. All states would experience the same reduction, so the final result would remain true for the system with nonzero losses.

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term

$$\begin{Vmatrix} e^{i\varphi_{or}} & 0 \\ 0 & e^{i(\varphi_{ex}+\Delta\varphi_1)} \end{Vmatrix} \begin{Vmatrix} A \\ Be^{i\varphi_0} \end{Vmatrix} = \begin{Vmatrix} A \\ Be^{i(\varphi_0+\Delta\varphi_1)} \end{Vmatrix} \quad (3)$$

$$\begin{Vmatrix} e^{i\varphi_{or}} & 0 \\ 0 & e^{i(\varphi_{ex}+\Delta\varphi_2)} \end{Vmatrix} \begin{Vmatrix} A \\ Be^{i\varphi_0} \end{Vmatrix} = \begin{Vmatrix} A \\ Be^{i(\varphi_0+\Delta\varphi_2)} \end{Vmatrix} \quad (4)$$

Where $\Delta\varphi_1$ and $\Delta\varphi_2$ depend on the applied voltages. Orthogonality of these vectors mean that:

$$A^2 + Be^{i(\varphi_{ex}+\varphi_0+\Delta\varphi_1)}\left(Be^{i(\varphi_{ex}+\varphi_0+\Delta\varphi_2)}\right)^* = 0 \quad (5)$$

$$A^2 + B^2e^{i(\Delta\varphi_1-\Delta\varphi_2)} = 0 \quad (6)$$

The only solution for positive amplitudes is A = B and $\Delta\varphi_1 - \Delta\varphi_2 = \pi n, n \in \mathbb{Z}$. Practically this means that to implement orthogonal polarization basis one need the same amplitudes of polarization components along the ordinary and extraordinary axes of the lithium niobate at the input of phase modulator and V_π difference in voltages on phase modulator between two states. Note that the input state is not necessary to be diagonal – phase shift between two components could be random. It's just a matter of proper calibration of the polarization controller before PBS. And vice versa – managing to completely distinguish two pulses by polarization means that the amplitudes along the axes were equal and the voltage difference is V_π.

Placing another polarization controller at the input of the phase modulator we are able to establish a desired state - when the amplitudes alone both axes are the same. Let's see how intensity on the detectors will change when we apply different phase shifts to the modulator.

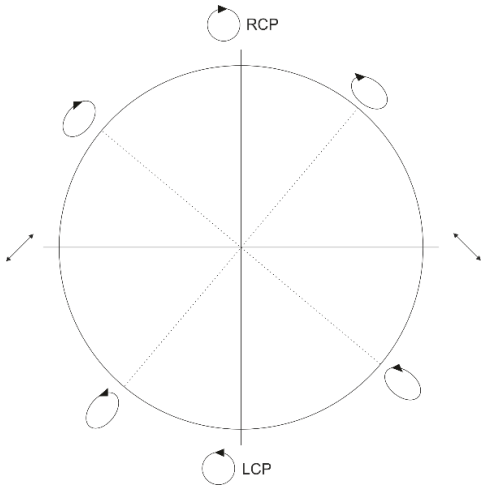

Figure 1. Polarization states generated by Alice. In general these are two pairs of orthogonal ellipses.

$\vec{a}_1 = A \begin{Vmatrix} 1 \\ e^{i\varphi_0} \end{Vmatrix}$ – the first state after the phase modulator;

$\vec{a}_2 = A \begin{Vmatrix} 1 \\ e^{i(\varphi_0-\Delta\varphi)} \end{Vmatrix}$ – the second state after the phase modulator when we apply phase shift $(-\Delta\varphi)$ relatively to the first state. The intensity of these pulses is $I_0 = 2A^2$.

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term

We calibrate polarization controller after the phase modulator so that the first state would have its whole intensity I_0 on the first detector. Vector $\vec{a}_1$ transforms into $\vec{b}_1$, in the coordinates of the polarization beam splitter axes:

$$\vec{b}_1 = A\sqrt{2}\begin{Vmatrix} e^{i\chi} \\ 0 \end{Vmatrix} \tag{7}$$

This would transform the $\vec{a}_2$ vector into some arbitrary state $\vec{b}_2$ that could be written as:

$$\vec{b}_2 = \begin{Vmatrix} He^{i\theta} \\ Ve^{i\phi} \end{Vmatrix} \tag{8}$$

The intensity on the first detector for the second state is $I = H^2$.

Unitary transformation preserves inner product. This means that $\vec{a}_1\vec{a}_2 = \vec{b}_1\vec{b}_2$ and also $(\vec{a}_1\vec{a}_2)^2 = (\vec{b}_1\vec{b}_2)^2$

$$\vec{a}_1\vec{a}_2 = A^2(1 + e^{i\Delta\varphi}) \tag{9}$$

$$\vec{b}_1\vec{b}_2 = AH\sqrt{2}e^{i(\chi+\theta)} \tag{10}$$

$$A^2((1 + \cos(\Delta\varphi))^2 + \sin^2(\Delta\varphi)) = 2H^2 \tag{11}$$

$$H^2 = 2A^2\cos^2\frac{\Delta\varphi}{2} \tag{12}$$

$$I = I_0\cos^2\frac{\Delta\varphi}{2} \tag{13}$$

Equation (13) means that the signal on the detectors will have completely the same distribution with the phase shift on the modulator as if we used an interferometric phase encoding scheme [3].

To implement a QKD scheme Alice and Bob need two phase modulators – one for each side. If we connect them with a single mode optical fiber, practically input and output states of polarization will be different. Changing external conditions, will also cause polarization drifts in time. To compensate these effects we place a polarization between the modulators.

To match the axes along which phase shift is being introduced for Alice and Bob, polarization controller between them has to be calibrated so that Jones matrix of the quantum channel would be identity matrix. But the static difference in the ordinary and extraordinary indexes of lithium niobate causes PMD (Fig.2) which may severely disturb the pulse, increasing the bit error rate, especially for short pulses [2]. Practically this may not be compensated via Pockels effect, because static birefringence is much stronger and the procedure would require hundreds of volts. One of the advantages of the presented scheme is that two identical phase modulators may compensate each other's PMD. To achieve this the Jones matrix of the quantum channel should rotate the SOP by $\pm 90°$. Note that it is also allowed to introduce different phase shifts for these two axes, as it may be compensated with the polarization controller before PBS:

$$\begin{Vmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{Vmatrix}\begin{Vmatrix} 1 & 0 \\ 0 & e^{i\Delta\sigma} \end{Vmatrix} = \begin{Vmatrix} 0 & \mp e^{i\Delta\sigma} \\ \pm 1 & 0 \end{Vmatrix} \tag{14}$$

As a result both polarization components pass through one fast and one slow lithium niobate axes, zeroing PMD.

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term

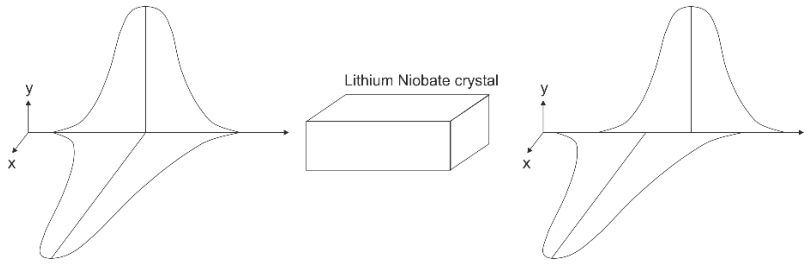

Figure 2. Polarization mode dispersion

We implement BB84 protocol: Alice uses 4 voltages (0, $V_\pi/2$, V_π, $3V_\pi/2$) where 0 and V_π stand for 0 and 1 in one basis and $V_\pi/2$ and $3V_\pi/2$ in the other and Bob chooses basis applying one of two possible voltages – 0 or $V_\pi/2$. Generated states are shown on the figure 1. In general states won't be two diagonal and two circular as in [2], because polarization maintaining fiber at the input of modulator was not used. In the current implementation the set of states may be different after every calibration.

Once all polarization controllers are adjusted as described above the detectors will completely distinguish states when Alice and Bob used the same basis. Furthermore as a result of (13) in case bases do not match the intensity of the pulses would be divided equally between two detectors. The results in BB84 interpretation are shown in the table 1.

OPTICAL SCHEME

We describe the scheme for polarization encoding based on the analysis described in the previous paragraph (fig. 3).

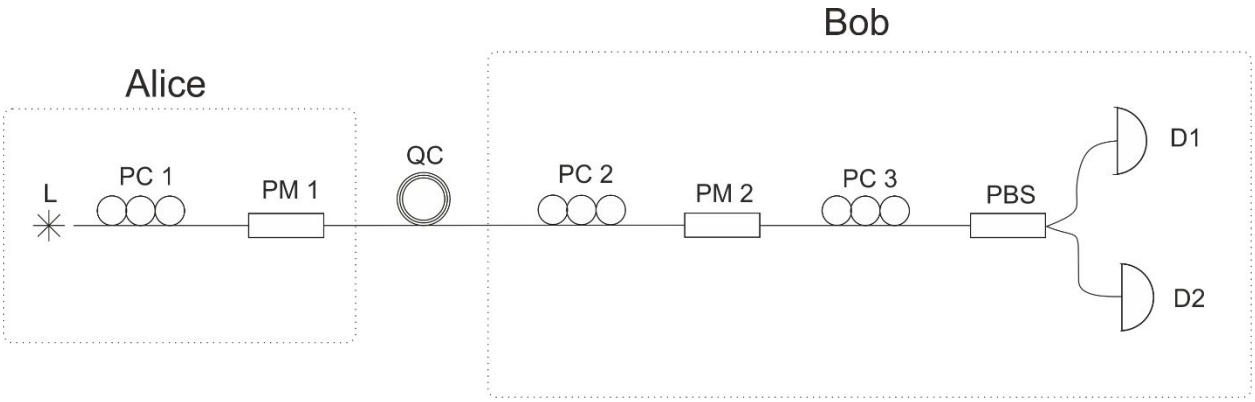

Figure 3. QKD scheme for classical regime tests. L – laser, PC – polarization controller, PM – electro-optical phase modulator, PBS – polarization beam splitter, D – detector, QC – quantum channel.

Alice's device includes a coherent polarized light source, polarization controller and phase modulator. Polarization controller PC_1 transforms the initial state of polarization from the source so that it enters phase modulator PM_1 with equal amplitudes along the optical axes of lithium niobate. Applying 0, $V_{\pi/2}$, V_π, $V_{3\pi/2}$ voltages on the phase modulator Alice generates 4 states of polarization, where 0, V_π and $V_{\pi/2}$, $V_{3\pi/2}$ stand for two pairs of orthogonal states (two bases), implementing the BB84 protocol.

Bob uses PC_2 to compensate polarization drifts in the quantum channel and rotate the polarization plane by 90° in order to prevent polarization mode dispersion of lithium niobate. Applying 0 and $V_{\pi/2}$ voltages on the electro-optical phase modulator PM_2 Bob chooses the basis of measurement. PC_3 transforms the states at the output of the PM_2 so that if Alice

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term

and Bob used the same basis – the pulses' final state on the polarization beam splitter will match one of its axes, allowing Bob to get the right bit, by the detector click. In case bases didn't match the probabilities of both detectors' click would be equal.

To implement QKD regime intensity modulator should be placed after the laser source.

EXPERIMENT

Proof-of-concept experiment has been conducted in the bright light regime. The table and the figure below illustrate all possible combinations of states generated by Alice and bases chosen by Bob. The pulse repetition frequency is 10 MHz, pulse width is 5 ns. The laser's wavelength is around 1550 nm and quantum channel between Alice and Bob consists of 25km of SMF28 optical fiber.

Bit number	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Alice's bit	1	1	0	0	1	1	0	0
Alice's basis	(0, π)	(π/2, 3π/2)	(0, π)	(π/2, 3π/2)	(0, π)	(π/2, 3π/2)	(0, π)	(π/2, 3π/2)
Alice's phase	0	π/2	π	3π/2	0	π/2	π	3π/2
Bob's basis	(0, π)	(0, π)	(0, π)	(0, π)	(π/2, 3π/2)	(π/2, 3π/2)	(π/2, 3π/2)	(π/2, 3π/2)
Bob's phase	0	0	0	0	π/2	π/2	π/2	π/2
Phase diff.	0	π/2	π	3π/2	-π/2	0	π/2	π
Bob's bit	1	-	0	-	-	1	-	0

Table 1. All possible combinations of bits and bases for Alice and Bob

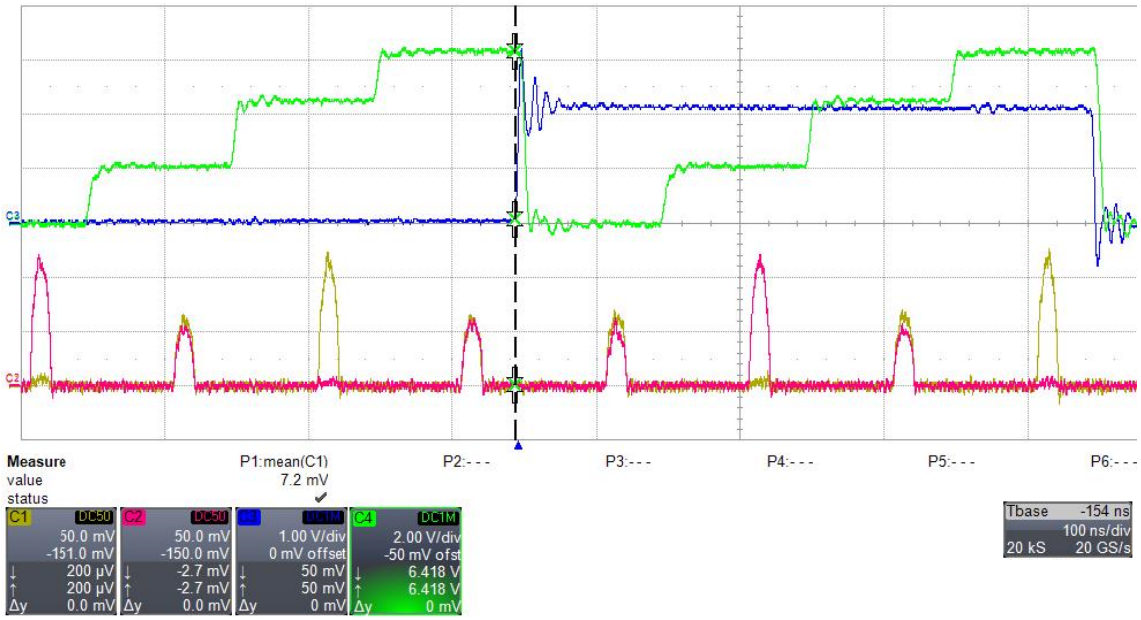

Figure 4. Yellow and red lines stand for D1 and D2 signals. Green and blue – voltages applied to the phase modulators of Alice and Bob, respectively. The figure illustrates all possible combinations of states and bases for BB84 protocol.

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term

CONCLUSION

The scheme for fast polarization encoding has been proposed and successfully demonstrated in experiment. Alice sends weak coherent pulses, switching polarization states via Pockels effect in the fiber electro-optical $LiNbO_3$ phase modulator, generating four different states required for the BB84 protocol. Bob chooses the basis of measurement with his phase modulator and measures the state using polarization beam splitter and two single photon detectors. Proper calibration of polarization controller allows phase modulators to compensate each others' polarization mode dispersion. The system has simple configuration, uses single laser source and only two detectors.

ACKNOWLEDGMENTS

The support from Ministry of Education and Science of the Russian Federation in the framework of the Federal Program (Agreement 14.582.21.0009, ID RFMEFI58215X0009) is acknowledged.

REFERENCES

[1] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Physical review letters 85(2) , 441-444 (2000).

[2] 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," Journal of Lightwave Technology 28(17), 2572–2578 (2010).

[3] N. Gisin, et al. "Quantum cryptography," Reviews of modern physics 74(1), 145 (2002).

[4] Ma L., Chang T., Mink A., Slattery O., Hershman B., & Tang, "Experimental demonstration of a detection-time-bin-shift polarization encoding quantum key distribution system," IEEE Communications Letters 12(6), 459-461 (2008).

Downloaded From: http://proceedings.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/90843/ on 03/28/2017 Terms of Use: http://spiedigitallibrary.org/ss/term