QKD using polarization encoding with active measurement basis selection

To cite this article: A Duplinskiy et al 2017 J. Phys.: Conf. Ser. 917 062058

View the article online for updates and enhancements.
QKD using polarization encoding with active measurement basis selection

A Duplinskiy\textsuperscript{1,2}, V Ustimchik\textsuperscript{1}, A Kanapin\textsuperscript{1,3}, Y Kurochkin\textsuperscript{1}

\textsuperscript{1}Russian Quantum Center (RQC), Business Center «Ural», 100, Novaya st., Skolkovo, Moscow reg., 143025, Russia
\textsuperscript{2}Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141700, Russian Federation
\textsuperscript{3}Lomonosov Moscow State University, GSP-1, Leninskie Gory, Moscow, 119991, Russian Federation

Abstract. We report a proof-of-principle quantum key distribution experiment using a one-way optical scheme with polarization encoding implementing the BB84 protocol. LiNbO\textsubscript{3} phase modulators are used for generating polarization states for Alice and active basis selection for Bob. This allows the former to use a single laser source, while the latter needs only two single-photon detectors. The presented optical scheme is simple and consists of standard fiber components. Calibration algorithm for three polarization controllers used in the scheme has been developed. The experiment was carried with 10 MHz repetition frequency laser pulses over a distance of 50 km of standard telecom optical fiber.

1. Introduction
Quantum cryptography is a part of quantum information technology which has been successfully practically implemented within the laboratories all over the world. Quantum key distribution (QKD) allows secret key sharing between two distant users – the transmitter (Alice) and the receiver (Bob), while guaranteeing unconditional security based on the fundamental laws of nature. In this paper we present a new optical scheme for the practical implementation of the BB84 protocol and present out preliminary experimental results.

Nowadays QKD distribution is performed at GHz frequencies, nevertheless polarization tracking at such speed is a challenging task. The simplest scheme uses four independent laser sources, one for each state of polarization, required for BB84 protocol implementation \cite{1}. However it has been shown that proving the indistinguishability of light emitted from different sources is non-trivial, while it is vital for key secrecy. Another approach has been proposed, using fiber phase modulators’ Pockels cells for state of polarization changing \cite{2-5}. Electro-optical modulators based on LiNbO\textsubscript{3} crystals may be used as free space Pockels cells, while operating at GHz frequencies and requiring low driving voltages (V\textpi<5V). Alice produces two pairs of orthogonal states – two circular and two diagonal, depending on the phase shift applied to one of the components with the modulator and sends pulses to Bob, who selects which basis – diagonal or circular is used. Once Alice’s and Bob’s bases match – they get the same result with high probability, according to the scheme extinction ratio. If the bases are different the probability of both detectors click is equal. These bits are cancelled during the sifting procedure.

The main drawback of this solution is polarisation mode dispersion which occurs within the lithium niobate crystal due to its birefringence. It causes pulse polarization distortion, resulting in a high quantum bit error rate (QBER). Different methods of compensating have been proposed including HiBi
fiber [2] and Faraday mirrors [5]. In the presented scheme polarization controller is adjusted so that two identical modulators of Alice and Bob compensate each others optical path difference along different axes.

The BB84 protocol was chosen due to its proven unconditional security [1]. Polarization encoding provides opportunity to use the scheme for both fiber and free space quantum channels, while the simplicity and compactness makes it perspective for satellite implementations. One-way optical scheme based on the lithium niobate modulators has a potential to work at GHz laser pulse repetition frequencies. Calibration algorithms for polarization controllers allow the system to compensate the drifts of polarization state both for quantum channel and for Alice’s and Bob’s devices. This procedure applied if needed and maintains the (QBER) at a level suitable for key transmission.

2. Optical scheme
We present a polarization encoding QKD system where both Alice and Bob use fast electro-optical LiNbO$_3$ phase modulators. The whole scheme consists of standard fiber elements (Fig.1). Alice creates one of four polarization states – two diagonal and two circular, applying voltages to her modulator, corresponding to 0, $\pi/2$, $\pi$ and $3\pi/2$ phase shifts. Modulator exploitation for generating these states allows Alice to use a single laser source, solving the problem of pulse indistinguishability. Bob uses his modulator for active basis selection, applying 0 and $\pi/2$ phase shifts. This allows Bob to use only two detectors in contrast to four in the passive basis selection scheme. The polarization mode dispersion issue with LiNbO$_3$ crystals described in previous works [2,5] has been solved with a proper calibration of the polarization controller between the modulators of Alice and Bob (PC 2), allowing two crystals to compensate each other’s’ birefringence by rotating polarization vector by 90°.

![Figure 1. Optical scheme. Laser (L) generates optical pulses, which pass through the polarization controller (PC 1), that guides the light at an angle of 45° into the phase modulator (PM 1) to generate two pairs of orthogonal states. Variable optical attenuator (IM) has two modes of operation – calibration and key distribution. PC 2 compensates the polarization drifts within the quantum channel (QC) and rotates the polarization state by 90° to compensate lithium niobate birefringence. Bob’s phase modulators (PM 2) is used for basis selection and PC 3 transforms the polarization state so that polarization beam splitter (PBS) apportion the states to single-photon detectors (D1, D2).](image)

3. Calibration procedure
Three polarization controllers shown on the scheme have to be adjusted properly in order to make the QKD procedure possible. A calibration algorithm has been developed in order to carry out this procedure automatically. The system uses bright laser pulses in order to increase information collecting speed from the single-photon detectors. The calibration program processes the data and adjusts the voltages of the polarization controller channels. The system monitors the QBER and launches the calibration system automatically when the error value increases above a certain level. The intensity of the optical pulses is switched with an optical attenuator.
The controllers are adjusted one by one, to compensate polarization drifts within the devices of Alice and Bob (PC 1 and PC 3, respectively) and the quantum channel (PC 2).

4. QKD experiment
The proof-of-principle experiment has been conducted with laser pulses repetition frequency of 10 MHz. The key distribution has been carried out over a distance of 50 km of standard single-mode optical fiber. The system automatically performs the calibration procedure and maintains QBER below 5% for hours, applying recalibration if needed.

![Histogram](image)

**Figure 2.** Histogram, illustrating all eight possible combinations of states, generated by Alice and Bob, using their modulators. The picture show statistics for both detectors. Bins with logical 1 on the first detector correspond to logical 0 on the second detector and vice versa. Each pulse consists of five columns in order to monitor the polarization mode dispersion effects.

The approximate rate of calibration regime is about 20% of total time, which means that 80% of time system generates the key.
To conduct the experiment modular QKD setup, developed within the laboratory has been used. Electronics is driven by National Instruments FPGA, that provides control of electro-optical modulators, laser source and polarization controllers, while also caring out data acquisition, and active feedback calibration loop.
Histograms for all possible states measured by Bob is shown on the Fig.2.

5. Conclusion
Novel polarization encoding scheme based on fiber lithium niobate modulators proposed in the paper has opportunity to reach GHz frequencies with proper driving electronics. Current experiment prove it’s robustness with the developed calibration techniques, making the scheme promising for future commercial applications.

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] Gisin N, Ribordy G, Tittel W, & Zbinden H 2002 Reviews of modern physics 74(1) p. 145
[2] Jofre M, Gardelein A, Anzolin G, Molina-Terriza G, Torres J P, Mitchell M W, & Pruneri V 2010 Journal of Lightwave Technology 28(17) p 2572
[3] 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).

[4] Zhizhong Yan, Evan Meyer-Scott, Jean-Philippe Bourgoin, Brendon L. Higgins, Nikolay Gigov, Allison MacDonald, Hannes Hübel, and Thomas Jennewein, "Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links," J. Lightwave Technol. 31, 1399-1408 (2013).

[5] Jindong Wang, Xiaojuan Qin, Yinzhu Jiang, Xiaojing Wang, Liwei Chen, Feng Zhao, Zhengjun Wei, and Zhiming Zhang, "Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units," Opt. Express 24, 8302-8309 (2016).