QKD network on mixed encoding schemes

E.O. Kiktenko[1,2], N.O. Pozhar[1], M.N. Anufriev[1], A.V. Duplinskiy[1,3], A.A. Kanapin[1,4], A.V. Miller[1], V.E. Rodimin[1], A.S. Sokolov[1], V.E. Ustimchik[1], S.S. Vorobey[1], A.V. Losev[1], A.S. Trushechkin[1,2], A.K. Fedorov[1], V.L. Kurochkin[1], Y.V. Kurochkin[1]

[1]*Russian Quantum Center (RQC), 100 Novaya St., Skolkovo, Moscow 143025, Russia*
[2]*Steklov Mathematical Institute of Russian Academy of Sciences, Moscow 119991, Russia*
[3]*Moscow Institute of Physics and Technology, Dolgoprudny, Moscow Region, 141700, Russia*
[4]*Lomonosov Moscow State University, GSP-1, Leninskie Gory, Moscow, 119991, Russian Federation*
[5]*Institute for Quantum Science and Technology, University of Calgary, Calgary AB T2N 1N4, Canada*
e-mail: yk@rqc.ru

One of the most important challenges in the development of QKD networks is establishing secret keys beyond laboratory conditions. Thereby it is important to use a QKD protocol that guarantees secrecy in urban fibers with significant losses.

We present the results on creating a heterogeneous quantum network across urban channels between two bank offices in Moscow. The developed QKD network uses the trusted repeater paradigm, where transport of secret keys between multiple users is realized over an intermediate trusted node. QKD networks can be presented as a connected graph, the vertices of which are nodes, and the edges are QKD links. The developed three-node QKD network is composed of two QKD links, each link connecting two nodes (see Fig. 1). The first link of the network generates quantum keys using the polarization-encoding scheme, and the second link employs the phase-encoding scheme [1]. In our experimental tests, the recently presented modular QKD device [2] and open-source platform for post processing have been used. Topology of the developed QKD network is illustrated in Fig. 1.

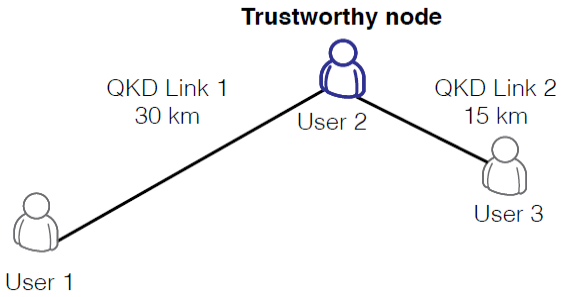

Figure 1 Quantum keys transport between three users over an intermediate trusted node. The first link generates quantum keys using the polarization-encoding scheme, whereas the second link employs the phase-encoding scheme.

The first link of the developed QKD network generates quantum keys using the polarization-encoding scheme on the basis of the BB84 protocol [3]. Alice uses LiNbO3 phase modulator to generate two pairs of orthogonal polarization states with a single laser source, solving the issue of pulses' indistinguishability (see Fig. 2a). Bob's device similarly select measurement basis with a modulator and rotates the output state of polarization backwards, for PBS to distinguish different bits. Only two SPDs are used due to the active basis selection, in contrast to the passive one. This link provides key exchange over 30 km in urban fibers with losses on the level of 13 dB.

The second link relies on another optical layout for QKD, the phase-encoding scheme (see Fig. 2b) with the use of the seminal BB84 protocol. This scheme has been already used for QKD across urban fiber channels [4]. This link allows establishing of the secret keys over 15 km in urban fibers with losses on the level of 7 dB. The post-processing procedure is described in Ref. [5].

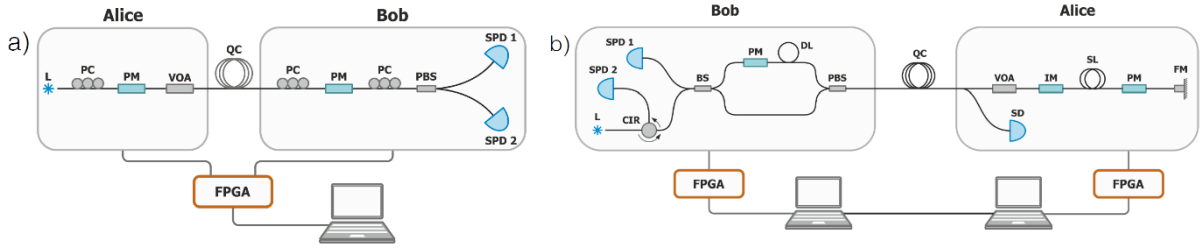

Figure 2 In (a) the first QKD link for generation quantum keys using the polarization-encoding scheme is presented, where L is the light source, PC is the polarization controller, PM is the phase modulator, VOA is the variable optical attenuator, QC is the quantum channel (urban fiber channel), PBS is the polarization beamsplitter, and SPD is the single photon detector. In (b) the second QKD link employing the phase-encoding scheme is presented, where CIR is the circulator, BS is the beamsplitter, DL is the delay line, SL is the storage line, SD is the synchro detector, IM is the intensity modulator, and FM is the Faraday mirror.

We acknowledge financial support from Ministry of Education and Science of the Russian

Federation (Agreement 14.582.21.0009, ID RFMEFI58215X0009).

[1] A. Duplinskiy, V. Ustimchik, A. Kanapin, and Y. Kurochkin, “Fast polarization QKD scheme based on LiNbO 3 phase modulators,” *Proc. SPIE*, vol. 10224, no. 102242W, 2016.

[2] A. S. Sokolov, A. V. Miller, A. A. Kanapin, V. E. Rodimin, A. V. Losev, A. K. Fedorov, V. L. Kurochkin, and Y. V. Kurochkin, “Modular quantum key distribution setup for research and development applications,” *arXiv:1612.04168*, 2016.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984*, 1984, pp. 175–179.

[4] V. L. Kurochkin, Y. V. Kurochkin, A. V. Miller, A. S. Sokolov, and A. A. Kanapin, “Effect of crosstalk on QBER in QKD in urban telecommunication fiber lines,” *SPIE Proc.*, vol. 10224, no. 102242U, 2016.

[5] E.O. Kiktenko, A.S. Trushechkin, Y.V. Kurochkin, and A.K. Fedorov, “Post-processing procedure for industrial quantum key distribution systems”, J. Phys. Conf. Ser. 741, 012081 (2016).