Experimental realization of a relativistic QKD system with one-way quantum communication

K. S. Kravtsov[1,2], I. V. Radchenko[1,2], S. P. Kulik[1], and S. N. Molotkov[3]
[1] *Faculty of Physics, Moscow State University, Moscow, Russia*
[2] *A.M. Prokhorov General Physics Institute RAS, Moscow, Russia*
[3] *Academy of Cryptography, Moscow, Russia; Institute of Solid State Physics, Chernogolovka, Moscow Rgn., Russia; Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow Russia*
(Dated: April 30, 2016)

A fundamental difference between the original BB84 protocol and virtually all practical ones is the information carrier: the former needs true single photons while the latter have to rely upon weak coherent pulses (WCPs). As WCPs are formally infinite-dimensional quantum systems, there is always a non-zero probability of unambiguous discrimination of the transmitted states in the channel [1–3]. Thus, starting from some level of loss, conventional WCP-based QKD systems inevitably lose their guaranteed security. Corresponding thresholds are well-known for simple protocols as B92 [4] and WCP-based BB84 [3], but, to the best of our knowledge, still far from being found for popular WCP-based COW and DPS protocols, whose security proofs, thus, may be considered incomplete. To avoid this potential security breach at an arbitrary level of the quantum channel loss we argue that additional measures have to be taken in the protocol design to completely disallow masking unsuccessful unambiguous state discrimination (USD) in losses.

A valid approach known from the early days is the B92 with a strong phase reference, where the presence of a strong reference pulse makes it impossible for Eve to send vacuum if the USD fails to get a conclusive result. Another alternative, earlier demonstrated by our group [5], relies upon relativistic limitations, which make sure that Eve obtains the USD result too late to choose whether she sends vacuum or the successfully measured state down the line. In this paper we demonstrate an improved experimental realization of this protocol, where we switched from the double-pass to a one-way configuration and implemented an active free-space channel tracking system, allowing stable operation of the single-mode quantum channel over 110 m.

Switching to a one-way quantum channel makes the system more protected from Eve's actions, compared to the double-pass one, where Eve could manipulate classical pulses traveling from Bob to Alice. It also greatly improved the operation rate of the system, as there is no need to wait the round-trip time to send more data into the channel. The backward communication channel required in the protocol is realized via the tracking system, which serves the two goals: to provide necessary secure synchronization between Alice and Bob, and to transmit some service data and control messages in both directions between the parties. Besides data communication, the tracking system is needed to keep the quantum channel up, as, in the contrast to conventional free-space QKD systems, the present one needs to use a single-mode receiver compatible with a fiber-based delay interferometer. Without active tracking, the system was extremely unstable when mounted on standard theodolite tripods and would not operate reliably even for a few minutes. With the tracking system implemented it showed good performance for hours.

A typical challenge when switching from a double-pass (e.g. the "plug-and-play") to a one-way system is the alignment of the receiving side interferometer along with the transmission one. We addressed this problem by a significant modification of the optical scheme. Alice's side now contains only a narrow linewidth CW laser (external cavity diode laser), a phase modulator and an attenuator, as shown in fig. 1. The receiving side has a polarization maintaining fiber based delay interferometer with a phase modulator in one of the arms, which serves for both interferometer alignment (with a quasi-DC bias) and data modulation during the QKD stage. The bias is adjusted according to the number of single photon detector clicks when biased at $\pi/2$ below and above the normal level, which corresponds to the dark interferometer output. A whole cycle of the modulator work is shown in fig. 2.

The main operation parameters are as follows. Each transmitted quantum symbol is a 10 ns long piece of the CW laser signal at $\lambda = 780$ nm with the output intensity of -85.9 dBm, which corresponds to 0.1 photons per pulse. Depth of the phase modulation equals 0.8π. Phase modulated symbols come in packets of 65536 bits each with the average rate of 12.5 MHz. Importantly, symbols in the packet are not equidistant, but rather randomly occupy either the first or the second half of their 80 ns time window, which is necessary for the purpose of secure synchronization [5]. A packet can be sent in any phase modulator cycle, which is 16 ms long (see fig 2). However, the actual packet rate was limited by the time needed to exchange the random data buffers and measurement results with a PC via a USB interface, so the actual rate was about 2 packets/sec.

The whole system consists of two similar stations with a box of electronics and fiber-based elements, and a free-space channel tracking platform placed on a tripod as

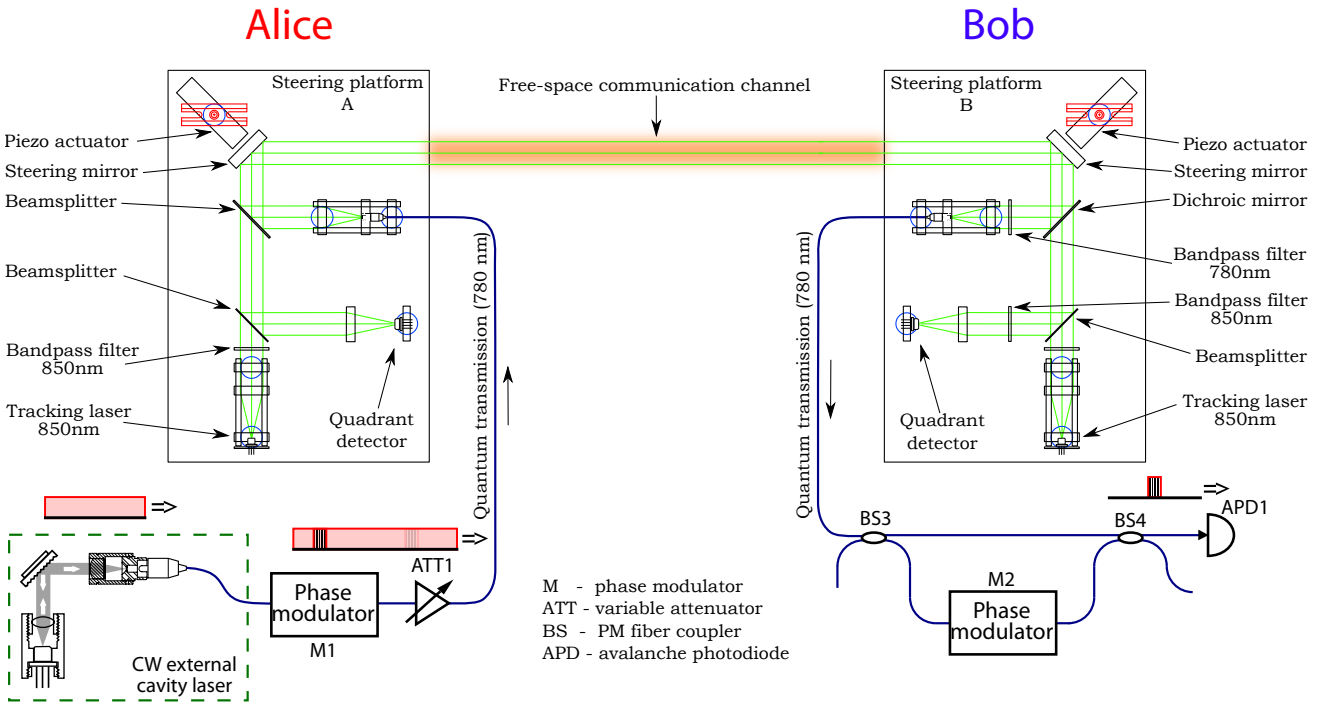

FIG. 1: Experimental setup including both the QKD part and the tracking system.

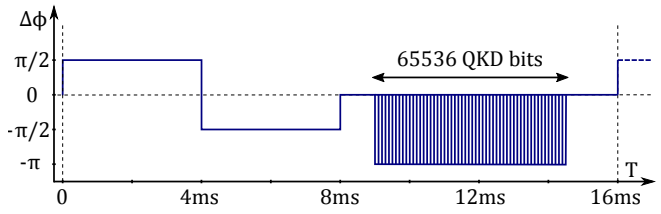

FIG. 2: Operation of the receiving interferometer phase modulator. In each cycle first it measures count frequencies in two quadrature points to adjust the bias, and then proceeds to the QKD sequence.

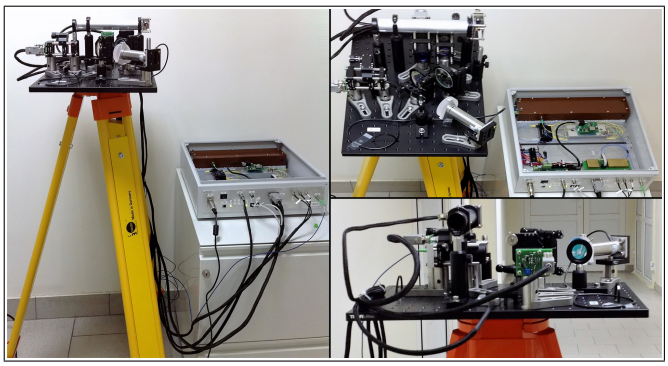

FIG. 3: Station Alice: a tripod with a free-space channel tracking platform and a box with fiber optic components and all electronics.

shown in fig. 3. The obtained performance over 110 m is shown in fig. 4. The average bit error rate was 4.1 % with quite large variation due to the atmospheric turbulence. The (asymptotically) estimated secret key rate is defined by the two parameters: first, a part of the obtained raw key is used for error correction; second, one must remove the information, which could potentially leak to Eve. Since the implemented relativistic scheme disallow Eve's influence on the received quanta in the way that her actions depend on results of her measurements, Eve's information is fundamentally bounded by the Holevo quantity [6]. For the particular setup ($\mu = 0.1$ photon/pulse, $\varphi = 0.8\pi$ phase modulation depth) it is

$$\chi = h\left(\frac{1-\exp(-2\mu\sin^2(\varphi/2)}{2}\right) = 0.41,$$

where $h(p) = -p\log(p) - (1-p)\log(1-p)$. Thus, the estimated secret key rate equals $\mathbf{R} = 1 - \chi - h(\mathrm{BER}) = 0.34$.

Overall, we report an important improvement in experimental realization of the relativistic QKD protocol. The setup now has a one-way configuration, simplified optical part, and a single-mode free-space channel with the active tracking system. The implementation of the relativistic protocol is an important step towards practical use of QKD protocols with clear security grounds, which rely only on simple fundamental facts, rather then on excessively complex and potentially often incomplete security analyses.

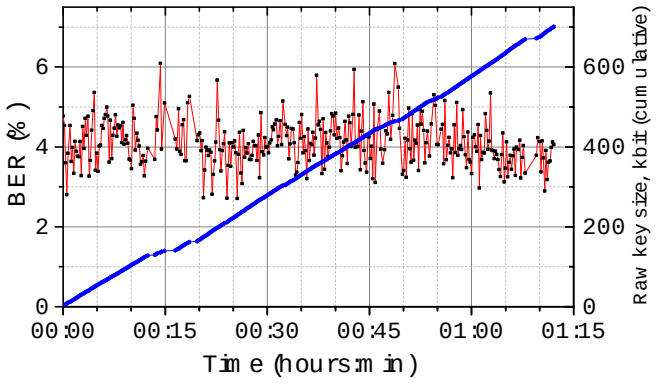

FIG. 4: Bit error rate and the cumulative generated raw key size vs. time. Note that some of the frames are lost due to someone blocking the beam.

[1] A. Chefles and S. M. Barnett, "Optimum unambiguous discrimination between linearly independent symmetric states," *Phys. Lett. A*, vol. 250, pp. 223–229, 1998.

[2] A. Chefles, "Quantum state discrimination," *Contemporary Physics*, vol. 41, no. 6, pp. 401–424, 2000.

[3] M. Dusek, M. Jahma, and N. Lutkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A*, vol. 62, p. 022306, 2000.

[4] A. Peres, "How to differentiate between non-orthogonal states," *Phys. Lett. A*, vol. 128, p. 19, 1988.

[5] I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, "Relativistic quantum cryptography," *Laser Phys. Lett.*, vol. 11, no. 6, p. 065203, 2014.

[6] A. S. Holevo, "Quantum coding theorems," *Russian Math. Surveys*, vol. 53, no. 6, pp. 1295–1331, 1998.