Relativity principles in quantum cryptography: towards proven unconditional security in practical QKD

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 27, 2015)

Quantum cryptography started to gain popularity as it became clear that it may offer unconditional security for key distribution. However, only a few model cases, such as the original BB84 protocol, were comprehensively studied and received solid proofs of their unconditional security. Many popular practical protocols with weak coherent pulses have a too complex structure for their universal and comprehensive cryptanalysis. We show that the use of relativity principles in quantum cryptography may greatly simplify its security analysis, especially for the case of coherent quantum states. We propose a relativistic QKD protocol superior to the previous one as a step towards proven unconditional security for practical protocols.

Quantum cryptography is an actively developing research area quickly advancing in both theory and experiment. At the same time, there is still a significant lag between introduction of new QKD protocols and their comprehensive cryptanalysis and security proofs. New protocols become more and more complex to analyze, while there are only a few, since the 1980s, that have solid proofs of their security [1]. Unfortunately, universal proofs that were given for the case of true single photon sources [2] cannot be adapted for weak coherent pulses used in practice, so even one of the most studied BB84 protocol [3] until recently didn't have a complete security framework for its practical implementations.

Many demonstrated experimental realizations, especially those with record communication distances, have potentially arguable security bases since the protocols used are too complicated for their comprehensive security analysis. Proofs given so far for the popular decoy state [4], COW [5], and DPS [6] protocols are based on somewhat truncated models and study a too detailed picture rather then universally approach the problem regardless of the way how particular hardware works and how an eavesdropper approaches her goals [7]. The problem of finding the fundamental upper bound on Eve's information for a chain-like construction as in COW or DPS protocols seems to be beyond the reach of today's quantum information theory tools [8].

In this work we advocate for additional tools that make QKD protocols intrinsically simpler for cryptanalysis and show that introduction of relativity principles into QKD can make the security proof much more straightforward. As a potential solution we propose a single-pass relativistic QKD protocol, which differs from the previous double-pass one by its ability to support much higher throughput without collisions typical for the schemes where the SPD is located near the signaling laser.

The main goal of the relativistic protocol, as shown in [9], is in prohibition of causal connection between Eve's measurements of quantum states in the channel and her actions on those states. This is realized by the temporal spread of wavepackets and their travel in the channel with the speed of light, i.e. the speed that cannot be surpassed by any causal connection.

From cryptanalysis point of view this means that the intercept-and-resend strategy becomes inaccessible for Eve. Most notably, it prohibits unambiguous measurements, which typically pose significant limitations on conventional quantum cryptography with weak coherent pulses, for example, rendering B92 protocol [10] insecure for many practical applications. Another threat, which is often overlooked, is in the internal loss and non-ideal detectors in the Bob's setup: even with the lossless channel and, say, 10% Bob's detection efficiency, Eve may easily succeed in the attack if she can unambiguously measure more than 1/10th of the quanta send; whenever she gets a conclusive result she re-sends a relatively bright state to make Bob's detectors fire with high enough probability. Although it may be possible to detect Eve's intrusion using more than one SPD in Bob's setup, this again may become a too partial measure that lacks the desired generality.

Without being able to alter quantum states in the channel depending on the result of her measurement, Eve is strictly bounded in the amount of the information she can pull out from the quantum channel. It is given by the Holevo bound [11], which is a fundamental value independent on Eve's strategies and abilities. This greatly simplifies the whole picture making further security proof only a technical routine. One of the main consequences is the proven ability of the protocol to guarantee security of generated keys regardless of the channel loss, provided that the measured BER is above a certain threshold. More details on this are given in [9].

One of the major limitations of the original relativistic protocol [9] was its double-pass structure, which implied that only a single pulse appeared in the channel. First it

propagated from Bob to Alice in the form of a classical pulse used for the clock synchronization purpose. Then it traveled back as a weak coherent pulse, realizing QKD itself. The scheme had both the signaling laser and the SPD connected to the two inputs of the same interferometer, so when the laser emitted pulses the detector had to be inactive, because of a significant cross talk between the two.

The proposed protocol free from this limitation is schematically illustrated in Fig. 1. It consists of the two stages: backward transmission of a classical synchronization sequence, and then a series of forward quantum transmissions from Alice to Bob. This structure allows to send long quantum sequences after the synchronization step was performed; it also eliminates previous quantum line rate limitations, allowing for a continuous high data rate transmissions of quantum states.

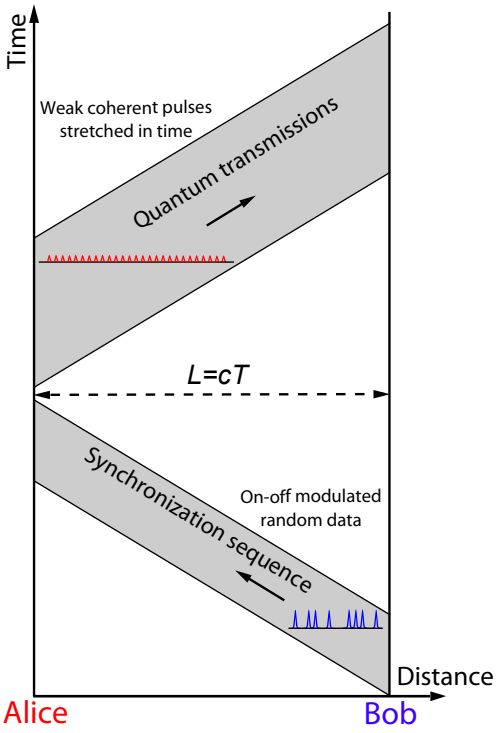

FIG. 1: Space-time diagram of the proposed single-pass relativistic protocol stages: synchronization and quantum transmission. The space-time structure of each optical pulse is not shown; for details see [9].

It should be clear that synchronization in relativistic protocols plays the key role, enabling the advertised key security. Any actions of Eve must not be able to offset Alice's clock from the Bob's, which would effectively mean a complete break-in of the protocol. The second required component of synchronization is the exact knowledge of the distance cT between Alice and Bob, which is needed to tell apart the 'delayed' transmissions, which could be intercepted and re-sent by Eve, from the genuine ones: c is the speed of light and T is the time of flight between Alice and Bob.

In the proposed protocol synchronization is performed in the following way: first Bob sends Alice an on-off modulated classical sequence with random data. Alice records the sequence with a photodiode PIN2. Due to the relativity principle Alice cannot receive any data bits earlier than the moment they left Bob's setup plus T, regardless of Eve's actions. Alice and Bob agree beforehand on how much time they wait after the start (or the end) of the synchro sequence to begin quantum transmissions. So Alice cannot start transmitting earlier than Bob expects her to do. It may happen only later, in which case even the genuine Alice's packets will be dropped by Bob as delayed. Alice also uses the synchronization sequence to balance her interferometer with Bob's one by adjustment of the DC bias on her phase modulator and taking a feedback signal from PIN1.

A mandatory step before creating a key from a series of quantum transmissions is to compare via the public channel the received synchronization sequence with the transmitted one. If the two do not match, it may be a sign of intrusion into the system, so this part of the key should be discarded.

After the synchronization part of the protocol has been performed Alice transmits her quantum sequence randomly choosing the state of her phase modulator between the two different and agreed upon phase shifts. Bob also randomly chooses the state of his phase modulator for each received bit and performs detection exactly at the expected time of arrival. As the two interferometers are already balanced, Bob may only see a detector click when he chooses the same phase as Alice, so both Alice and Bob create their raw keys after Bob announces all transmissions where he received a click.

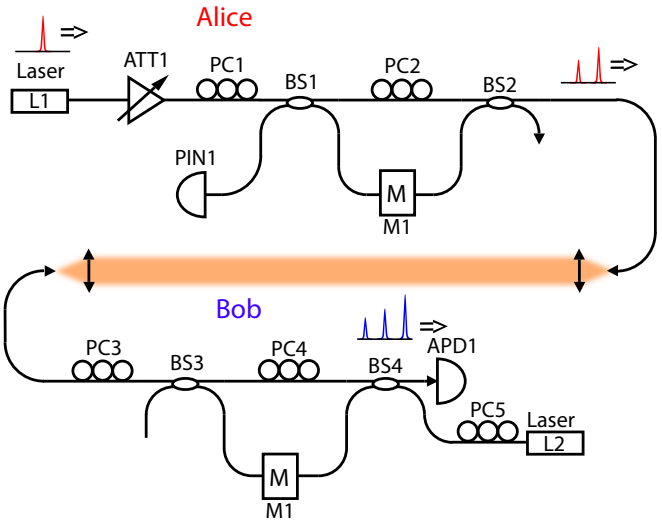

FIG. 2: The proposed experimental setup for the relativistic QKD protocol. ATT – variable attenuator, BS – beam splitter, PC – polarization controller, M – phase modulator, PIN – PIN photodiode, APD – single photon avalanche photodiode.

The proposed protocol may be realized with the setup shown in Fig. 2. Since free-space channels typically preserve polarization, the proposed setup may be constructed with polarization maintaining fibers and splitters, thus eliminating the need of polarization controllers. Placement of phase modulators inside the interferometers helps to reduce the internal losses in the system.

We are working on the experimental demonstration of this protocol and hopefully we'll be showing the results at the conference. This work is partially supported by the RFBR, grant no. 14-02-00765.

[1] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Commun.*, vol. 3, p. 634, 2012.

[2] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 1984, pp. 175–179.

[4] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005.

[5] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, p. 194108, 2005.

[6] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, p. 037902, 2002.

[7] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, "Security of distributed-phase-reference quantum key distribution," *Phys. Rev. Lett.*, vol. 109, no. 26, p. 260501, 2012.

[8] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.

[9] 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.

[10] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 1992.

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