Security of quantum key distribution with a laser reference coherent state, resistant to loss in the communication channel

Laser Phys. Lett. **12** (2015) 065201 (6pp) doi:10.1088/1612-2011/12/6/065201

Security of quantum key distribution with a laser reference coherent state, resistant to loss in the communication channel

S N Molotkov[1,2] **and T A Potapova**[3]

[1] Institute of Solid State Physics of Russian Academy of Sciences, Chernogolovka, Moscow district, 142432, Russia
[2] Computer Science Department of M.V. Lomonosov Moscow State University, Moscow 119899, Russia
[3] Computer Science Department, National Research University, Higher School of Economics, Moscow 123458, Russia

E-mail: sergei.molotkov@gmail.com

Received 30 March 2015, revised 4 April 2015
Accepted for publication 8 April 2015
Published 23 April 2015

Abstract

The problem of quantum key distribution security in channels with large losses is still open. Quasi-single-photon sources of quantum states with losses in the quantum communication channel open up the possibility of attacking with unambiguous state discrimination (USD) measurements, resulting in a loss of privacy. In this letter, the problem is solved by counting the classic reference pulses. Conservation of the number of counts of intense coherent pulses makes it impossible to conduct USD measurements. Moreover, the losses in the communication channel are considered to be unknown in advance and are subject to change throughout the series parcels. Unlike other protocols, differential phase shift (Inoue *et al* 2002 *Phys. Rev. Lett.* **89** 037902, Inoue *et al* 2003 *Phys. Rev.* A **68** 022317, Takesue *et al* 2007 *Nat. Photon.* **1** 343, Wen *et al* 2009 *Phys. Rev. Lett.* **103** 170503) and coherent one way (Stucki *et al* 2005 *Appl. Phys. Lett.* **87** 194108, Branciard *et al* 2005 *Appl. Phys. Lett.* **87** 194108, Branciard *et al* 2008 *New J. Phys.* **10** 013031, Stucki *et al* 2008 *Opt. Express* **17** 13326), the simplicity of the protocol makes it possible to carry out a complete analysis of its security.

Keywords: quantum key distribution, unambiguous measurements, unambiguous state discrimination

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum cryptography—quantum key distribution is intended to transmit secret keys through a quantum communication channel. Moreover, the channel is not controlled by legitimate users so the eavesdropper can make any modifications to the channel. An auxiliary classic authentic channel is also open and available for listening [1]. The secrecy of the keys is guaranteed by fundamental restrictions of quantum mechanics on distinguishability of non-orthogonal quantum states [1, 2]. The no-cloning theorem [3] guarantees that any acquisition of information about one of the sets of non-orthogonal quantum states will inevitably lead to a perturbation of the quantum states, which are detected at the receiving side. The inevitable perturbation of non-orthogonal states when extracting information from them is not limited to single-photon states and is valid for any of the non-orthogonal states, including multiphoton states. At the same time, the detection of disturbance of multiphoton states requires a corresponding set of measurements. In the case of a pair of non-orthogonal states, measurements that will detect any disturbance of the states should be kept to the projection on the subspace orthogonal to this multiphoton state. Such measurements are practically impossible to realize today, though there are no fundamental prohibitions against it. Nowadays measurements are limited to avalanche detectors, which do not distinguish even the number of photons, not to mention the more complex measurements. Today real systems of quantum cryptography use strongly attenuated coherent states, which are quasi-single-photon states with Poisson statistics on the number of photons.

There is another factor that is lacking in the no-cloning theorem [3]—losses. This theorem does not forbid obtaining reliable information about one of the non-orthogonal states, but with a probability of outcome of less than one. More precisely, if the set of quantum states is linearly independent then it is a necessary and sufficient condition for the existence of unambiquous measuremnets (UM or USD—unambiguous state discrimination) [4]. Strongly attenuated coherent states, which are used as information states in quantum cryptography protocols satisfy these conditions [5]. If losses in the quantum channel exceed a certain critical value then it is impossible to detect an eavesdropper and to guarantee the secrecy of the keys [5]. The USD attack is as follows. The eavesdropper breaks the quantum channel near the transmitting and receiving stations. If the eavesdropper near the transmitter receives a conclusive outcome then the eavesdropper near the receiver resends the true state. If an inconclusive outcome is received (the probability of an outcome is Pr(?)), then nothing resends. Starting with a certain level of losses, the eavesdropper knows all of the quantum states, does not make mistakes, is not detected and knows the key. Note that the eavesdropper can make USD not only due to the losses in the quantum channel but can also use the internal losses in the receiver.

Thus, the closer probability Pr(?) of an inconclusive outcome to unity, the larger the losses (respectively, the lengths of the communication channel) the protocol guarantees. To overcome this problem a series of protocols that increase the probability of an inconclusive outcome have been proposed. The differential phase shift (DPS) protocol [6–8] and derived from it the coherent one way (COW) protocol [9–12] can bring Pr(?) arbitrarily close to unity by increasing the length of the sequence of quantum states. Since in DSP and CW protocols bits of the key are encoded in the relative phase of the neighbouring coherent states, the proof of secrecy becomes much more complicated [6–12]. The critical error in DPS and COW protocols is still unknown, even in the channel without loss. Thus, a large Pr(?) in DPS and COW protocols is too big a cost because of the unprovability of the security of the protocols [6–12].

So far we have discussed the fiber optics system of quantum cryptography. For quantum cryptography systems, the additional fundamental constraints dictated by the special theory of relativity when working through open space, solves the problem of USD. Relativistic causality prohibits the transfer information faster than the speed of light. In contrast to the above-mentioned protocols in relativistic quantum cryptography, unambiguous measurements inevitably lead to delays and errors on the receiving side [13–15].

Previous nonrelativistic protocols (DPS, CW and others) were aimed at reducing the role of unambiguous measurements. Below we present a radical solution of the problem. The basic idea is to disable unambiguous measurements. Implementation and analysis of the security of the protocol is simple and transparent enough. In this protocol unambiguous measurements inevitably lead to errors on the receiving side.

The idea is to combine the quantum part of the protocol with the classical part. More precisely, in any system of quantum cryptography (fiber or open space) an intense classical coherent state is used as a synchronization pulse. The presence of such an intense state due to the technical part of the protocol (gated avalanche detectors), generally speaking, is not included in the quantum cryptographic part of the protocol. The intensity of the synchronization pulse is always enough in order for all of the clocks in each series of parcels to be registered. Otherwise, the system indicates a failure of synchronization, and a whole series of parcels is discarded. The idea is to use the intense coherent state (synchronization pulse) in quantum cryptographic parts of the protocol.

2. Fiber-optic protocol implementation

Protocol implementation is shown in figure 1. The laser generates a localized in time intensive coherent state $|\alpha^*\rangle$ ($|\alpha^*|^2 \gg 1$, where for convenience it is denoted $\alpha^* = \sqrt{2}\,\zeta\alpha$, $\zeta \gg 1$, $\alpha \approx 1$). A Mach–Zehnder interferometer with different arm lengths converts the localized in time intensive coherent state into two time-shifted coherent states. The lower arm of the interferometer has a built-in variable attenuator, which weakens the intensive coherent state to the strongly attenuated coherent state—$|\alpha\rangle_{\rm qu}$ ($|\alpha|^2 < 1$).

In the output of the interferometer there are a pair of coherent states—intensive classical and quantum (strongly attenuated coherent state)—$|\alpha\rangle_{\rm qu} \otimes |\zeta\alpha\rangle_{\rm cl}$. After the interferometer, the pair state goes through a phase modulator. At the time of the passage of the quantum state to the phase modulator, a voltage pulse is applied, resulting in an additional phase shift in the quantum coherent state. Information on key bits is encoded in a phase of the strongly attenuated coherent quantum state—$0 \to \varphi_A^0$, $1 \to \varphi_A^1$.

Coming in channel states consist of the time-shifted classical coherent state and quantum state—the strongly attenuated coherent state

$$\left|\zeta\alpha\right\rangle_{\rm cl} \otimes \left|{\rm e}^{{\rm i}\varphi_A^{0,1}}\alpha\right\rangle_{\rm qu}.$$

Both states ($|\zeta\alpha\rangle_{\rm cl} \otimes |{\rm e}^{{\rm i}\varphi_A^{0,1}}\alpha\rangle_{\rm qu}$) go the same way in the communication channel and in the channel with linear loss, intensive and strongly attenuated coherent states are attenuated self-similar

$$\left|\zeta\alpha\right\rangle_{\rm cl} \otimes \left|{\rm e}^{{\rm i}\varphi_A^{0,1}}\alpha\right\rangle_{\rm qu} \to \left|\zeta\alpha T(L)\right\rangle_{\rm cl} \otimes \left|{\rm e}^{{\rm i}\varphi_A^{0,1}}\alpha T(L)\right\rangle_{\rm qu}, \quad T(L) = 10^{-\delta L/10},$$

where L is the length of the communication channel, δ is a loss factor (for fiber SMF-28 $\delta \approx 0.2$ db km^{-1}).

At the receiving side the states are divided into two channels

$$|\zeta\alpha T(L)\rangle_{\rm cl} \otimes |{\rm e}^{{\rm i}\varphi_A^{0,1}}\alpha T(L)\rangle_{\rm qu} \to \left(\begin{array}{l} \left|\dfrac{\zeta\alpha T(L)}{\sqrt{2}}\right\rangle_{\rm cl} \otimes \left|{\rm e}^{{\rm i}\varphi_A^{0,1}}\dfrac{\alpha T(L)}{\sqrt{2}}\right\rangle_{\rm qu} \\ \left|-\dfrac{\zeta\alpha T(L)}{\sqrt{2}}\right\rangle_{\rm cl} \otimes \left|-{\rm e}^{{\rm i}\varphi_A^{0,1}}\dfrac{\alpha T(L)}{\sqrt{2}}\right\rangle_{\rm qu} \end{array}\right) \begin{array}{l}\text{channel 1} \\ \text{channel 2}\end{array}.$$

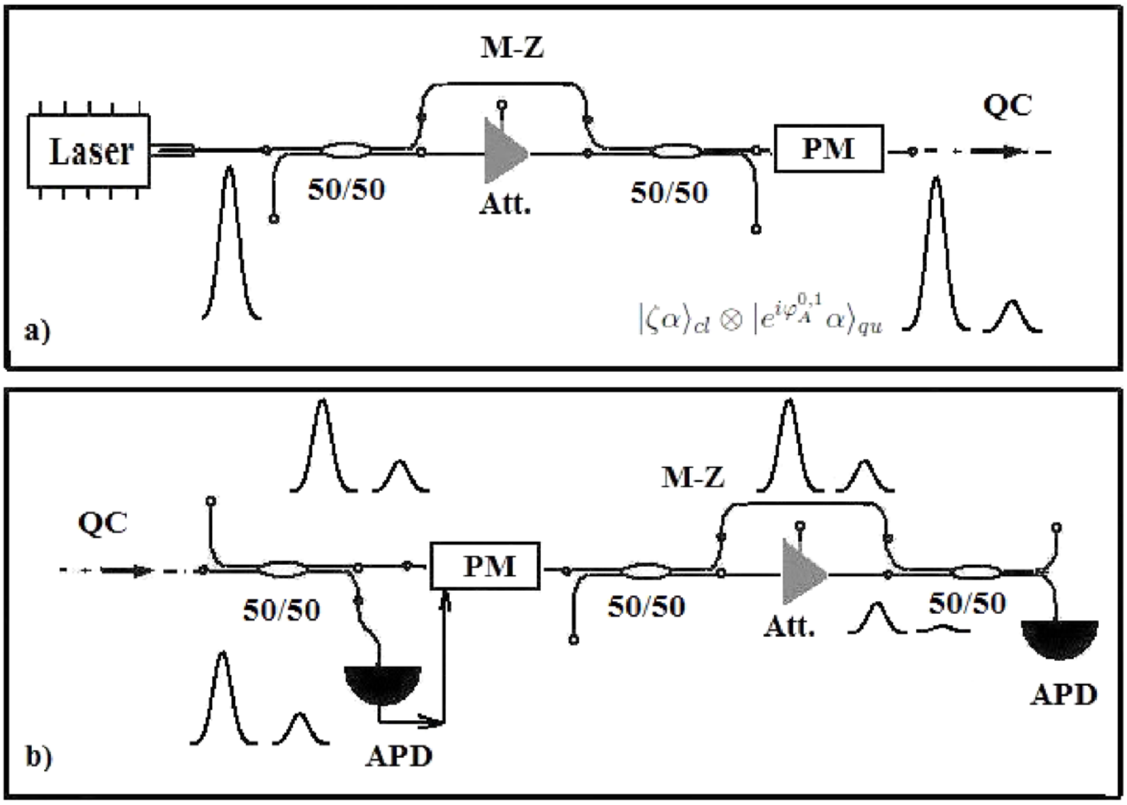
M-Z
Laser
50/50
Att.
50/50
PM
QC
$|\zeta\alpha\rangle_{cl} \otimes |e^{i\varphi_A^{0,1}}\alpha\rangle_{qu}$
a)
QC
50/50
PM
APD
M-Z
50/50
Att.
50/50
APD
b)

Figure 1. Functional diagram of the fiber system, (a) transmitting station, (b) receiving station. Designations: laser—source of coherent states, 50/50—symmetrical beam splitters, MZ—Mach–Zehnder interferometer with different length arms, PM—phase modulators, Att.—slow variable attenuator, APD—avalanche photon detectors, QC—quantum communication channel.

Part of the intensive coherent state arrives at the detector, which produces a gating voltage pulse for the phase modulator. The phase modulator is activated at the time when the strongly attenuated coherent state passes $\left|\mathrm{e}^{\mathrm{i}\varphi_{\mathrm{i}A}^{0,1}}\frac{\alpha T(L)}{\sqrt{2}}\right\rangle_{\mathrm{qu}}$, which is transformed to a state $\left|\mathrm{e}^{\mathrm{i}(\varphi_A^{0,1}-\varphi_B^{0,1})}\frac{\alpha T(L)}{\sqrt{2}}\right\rangle_{\mathrm{qu}}$.

The attitude of intensive and quantum (strongly attenuated) coherent states persists in the course of the communication channel's passage—$\zeta = \frac{|\zeta\alpha T(L)|}{|\alpha T(L)|}$. The attenuator in the short arm attenuates the classical and quantum coherent states passing through this arm in ζ times. It is important to note that the attenuation is determined only by the ratio of the amplitudes of the initial coherent states.

The intensive coherent state goes into $\left|\frac{\zeta\alpha T(L)}{2}\right\rangle_{\mathrm{cl}} \to \left|(\mathrm{e}^{\mathrm{i}\varphi_A^{0,1}} - \mathrm{e}^{\mathrm{i}\varphi_B^{0,1}})\frac{\alpha T(L)}{2}\right\rangle_{\mathrm{cl}}$,

$$\begin{pmatrix} \left|\frac{\zeta\alpha T(L)}{2}\right\rangle_{\mathrm{cl}} \otimes \left|(\mathrm{e}^{\mathrm{i}\varphi_A^{0,1}} - \mathrm{e}^{\mathrm{i}\varphi_B^{0,1}})\frac{\alpha T(L)}{2}\right\rangle_{\mathrm{qu-cl}} \otimes \left|\frac{-\alpha T(L)}{2\zeta}\right\rangle_{\mathrm{qu}} \\ \left|\frac{\zeta\alpha T(L)}{2}\right\rangle_{\mathrm{cl}} \otimes \left|(\mathrm{e}^{\mathrm{i}\varphi_A^{0,1}} + \mathrm{e}^{\mathrm{i}\varphi_B^{0,1}})\frac{\alpha T(L)}{2}\right\rangle_{\mathrm{qu-cl}} \otimes \left|\frac{\alpha T(L)}{2\zeta}\right\rangle_{\mathrm{qu}} \end{pmatrix} \begin{matrix} \text{empty output} \\ \text{detector output} \end{matrix},$$

$\left|(\mathrm{e}^{\mathrm{i}\varphi_A^{0,1}} \pm \mathrm{e}^{\mathrm{i}\varphi_B^{0,1}})\frac{\alpha T(L)}{2}\right\rangle_{\mathrm{qu-cl}}$ are the states which appeared in the course of interference of the initial strongly attenuated information coherent state and the attenuated initial intensive reference coherent state.

At the output of the Mach–Zehnder interferometer, the pair of states interfere (constructively and destructively) and are registered by avalanche photo-detectors in the central time-window (see figure 1).

The protocol uses a pair of non-orthogonal states. Alice with equal probability selects one of the phases of the φ_A^0 or φ_A^1. Bob independently from Alice with equal probability selects one of the two phases φ_B^0 or φ_B^1. Phase values are selected in such a way that there was

$$\frac{|\mathrm{e}^{\mathrm{i}\varphi_A^0} + \mathrm{e}^{\mathrm{i}\varphi_B^0}|}{2} = 1, \quad \frac{|\mathrm{e}^{\mathrm{i}\varphi_A^1} + \mathrm{e}^{\mathrm{i}\varphi_B^1}|}{2} = 1,$$

$$\frac{|\mathrm{e}^{\mathrm{i}\varphi_A^0} + \mathrm{e}^{\mathrm{i}\varphi_B^1}|}{2} = 0, \quad \frac{|\mathrm{e}^{\mathrm{i}\varphi_A^1} + \mathrm{e}^{\mathrm{i}\varphi_B^0}|}{2} = 0.$$

If Alice's and Bob's phases are identical, there is constructive interference and the detector clicks. Otherwise, when the phases of Alice and Bob are not the same, there is destructive interference, and the detector does not click.

Detection of an eavesdropper occurs on the parcels that do not produce clicks in the detector, i.e. then Alice's and Bob's phases do not coincide.

3. Informal reasons for the security of the protocol with respect to unambiguous measurements

An eavesdropper must be able to distinguish between two non-orthogonal quantum states in the communication channel $\left|\zeta\alpha\right\rangle_{\mathrm{cl}} \otimes \left|\mathrm{e}^{\varphi_A^0}\alpha\right\rangle_{\mathrm{qu}}$ or $\left|\zeta\alpha\right\rangle_{\mathrm{cl}} \otimes \left|\mathrm{e}^{\varphi_A^1}\alpha\right\rangle_{\mathrm{qu}}$. Assume in favor of the eavesdropper that the phase α is known, for example, from the classical coherent state. In this case, the eavesdropper must be able to distinguish between two non-orthogonal pure coherent quantum states $\left|\mathrm{e}^{\varphi_A^0}\alpha\right\rangle_{\mathrm{qu}}$ or $\left|\mathrm{e}^{\varphi_A^1}\alpha\right\rangle_{\mathrm{qu}}$.

The probability of an inconclusive outcome is

$$\Pr(?) = |{}_{\mathrm{qu}}\langle \mathrm{e}^{\varphi_A^0}\alpha | \mathrm{e}^{\varphi_A^1}\alpha\rangle_{\mathrm{qu}}| = \mathrm{e}^{-2\mu\sin^2\left(\frac{\varphi_A^0-\varphi_A^1}{2}\right)}, \quad \mu = |\alpha|^2 < 1.$$

The eavesdropper can not block the intensive coherent state otherwise the whole series will be discarded by Alice and Bob. In the case of an inconclusive outcome, an eavesdropper is obliged, instead of a true state $\left|\mathrm{e}^{\varphi_A^0}\alpha\right\rangle_{\mathrm{qu}}$ or $\left|\mathrm{e}^{\varphi_A^1}\alpha\right\rangle_{\mathrm{qu}}$, to send a quantum state at random. A fake quantum state causes clicks of the detector in the passes where such clicks should be absent.

For example, if instead of a true state, the eavesdropper resends fake state $\left|\mathrm{e}^{\varphi_A^0}\alpha\right\rangle_{\mathrm{qu}}$, and Bob chose phase $\left|\mathrm{e}^{\varphi_A^1}\alpha\right\rangle_{\mathrm{qu}}$, then the detector produces an error click. *Thus, if there are any losses in the communication channel, an eavesdropper will never be able to know the key and will not produce errors on the receiving side.* If it were not the classic impulse which interferes after attenuation with the quantum coherent state, an eavesdropper could block the parcel which received an inconclusive outcome (?). In the presence of the classic reference state, unambiguous measurements lead to errors at the receiver.

It should be noted that for a classic state, it is enough to use the coherent state before entering the avalanche detector having $\zeta^2\mu \approx 50 \div 60$ photons. In this case, the single-photon detector fires in each pass.

This means when the length of the line is 100 km, Alice's classic coherent state must contain $\zeta^2\mu \approx 5 \cdot 10^3 \cdot \div 6 \cdot 10^3$ photons to guarantee detector clicks in each parcel.

4. The length of the secret key in the asymptotic limit of long sequences

Any protocol of quantum key distribution consists of the following stages:

(a) Transfer of quantum states from Alice to Bob and their measurement on the receiving side.
(b) Discarding of empty passes.
(c) Estimation of the error probability and error correction through public classic channel.
(d) Estimation of Eve's information changing after error correction.
(e) Privacy amplification.

Quantum state Alice–Bob–Eve after stage (a) is described by the joint density matrix $\rho^n{}_{XX'E}$, where X^n, X'^n are Alice's and Bob's bit strings. A string X' is possible with errors, where $\rho_E^n = \mathrm{Tr}_{XX'}\{\rho_{XX'E}^n\}$ is Eve's quantum system. Taking into account Eve's information obtained from the quantum channel and classical information during error correction, Alice and Bob perform compression of keys (privacy amplification). After privacy amplification Eve has no information about the final secret key. The protocol should satisfy the correctness and secrecy criteria [16]. Correctness means that Alice's and Bob's keys are identical with probability of at least $1 - \varepsilon_{\mathrm{corr}}$,

$$\Pr[X^n \neq X'^n] < \varepsilon_{\mathrm{corr}}, \tag{1}$$

where X^n and X'^n are Alice's and Bob's bit strings after error correction. The criterion for security of the keys is the trace distance—the distance to the ideal situation. The ideal situation is where Eve's quantum system is not correlated with Alice's bit string,

$$\Delta = \frac{1}{2}\left\|\rho_{XE}^n - \rho_U^n \otimes \rho_E^n\right\|_1 < \varepsilon_{\mathrm{secr}}. \tag{2}$$

According to leftover hash lemma [16, 17] after hashing with two-universal hash functions [18] trace distance becomes

$$\Delta = \frac{1}{2}\sqrt{2^{-\left(H_{\min}^{\varepsilon}(X^n|C^nE^n) - R_n\right)}}, \tag{3}$$

here $H_{\min}^{\varepsilon}(X^n|C^nE^n)$ is smooth conditional min entropy, including error correction information C^n transmitted from Alice to Bob through a public channel.

Under the definition where λ is the minimum number such that $\lambda I_X \otimes \tilde{\rho}_{\mathrm{CE}}^n - \tilde{\rho}_{\mathrm{XCE}}^n > 0$, $\left\|\tilde{\rho}_{\mathrm{CE}}^n - \rho_{\mathrm{CE}}^n\right\|_1 < \varepsilon$, and $\mathrm{Tr}(\tilde{\rho}_{\mathrm{CE}}^n) = 1$. The protocol is ε secret [3], if the length of the final secret key R_n is not greater than

$$R_n \leqslant H_{\min}^{\varepsilon}(X^n|C^nE^n) - 2\log(1/2\varepsilon). \tag{4}$$

Conditional entropy $H_{\min}^{\varepsilon}(X^n|C^nE^n)$ satisfies the inequality [16],

$$H_{\min}^{\varepsilon}(X^n|C^nE^n) \geqslant H_{\min}^{\varepsilon}(X^n|E^n) - \mathrm{leak}_n - 2\log(1/2\varepsilon), \tag{5}$$

where leak_n is classical information in bits transmitted through a public channel during error correction, and it is defined only by the procedure of error correction. Formula (4) has an intuitively transparent interpretation. The $H_{\min}^{\varepsilon}(X^n|C^nE^n)$ is a lack of information, which is not enough for Eve, having a quantum system E and classical information C (ρ_{CE}^n), to fully know the bit string of Alice.

The length of the private key in the asymptotic limit ($n \to \infty$, ε, $\varepsilon_{\mathrm{cor}} \to 0$), is the following

$$R = \lim_{n\to\infty} \frac{R_n}{n} = H(X|E) - \mathrm{leak}. \tag{6}$$

Allowing the observed probability of error Q. Error corrections in the asymptotic limit require disclosure of nh (Q) bits through a public channel; $h(Q) = -Q\log Q - (1-Q)\log(1-Q)$ is the Shannon binary entropy function. *An eavesdropper cannot block the quantum channel because the presence of the reference coherent state leads to Eve's information*

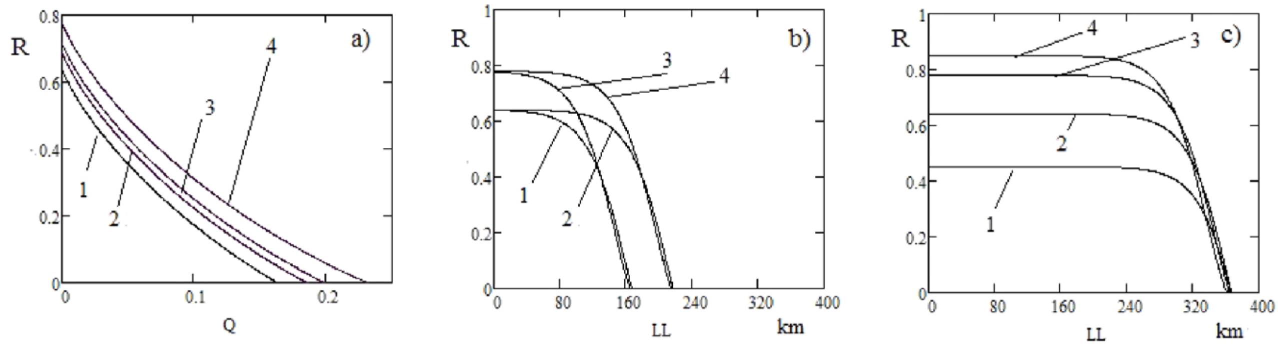

Figure 2. (a) Secret key length as a function of observed error. Parameters are the following: 1—$\mu = 0.5$; 2—$\mu = 0.4$; 3—$\mu = 0.35$; 4—$\mu = 0.25$. p_d is the probability of dark counts, $\Delta\varphi = \varphi_A^0 - \varphi_A^1$. (b) Secret key length as a function of quantum channel length. Parameters for curves 1, 2, 3, 4 are the following: 1—$p_d = 10^{-5}$, $\mu = 0.5$, $\Delta\varphi = \pi$; 2—$p_d = 10^{-6}$, $\mu = 0.5$, $\Delta\varphi = \pi$; 3—$p_d = 10^{-5}$, $\mu = 0.25$, $\Delta\varphi = \pi$; 4—$p_d = 10^{-6}$, $\mu = 0.25$, $\Delta\varphi = \pi$. (c) Parameters for curves 1, 2, 3, 4 are the following: 1—$p_d = 10^{-9}$, $\mu = 1.0$, $\Delta\varphi = \pi$; 2—$p_d = 10^{-9}$, $\mu = 0.5$, $\Delta\varphi = \pi$; 3—$p_d = 10^{-9}$, $\mu = 0.25$, $\Delta\varphi = \pi$; 4—$p_d = 10^{-9}$, $\mu = 0.15$, $\Delta\varphi = \pi$.

being restricted by the fundamental Holevo quantity [19]. The information deficit of Eve is

$$H(X|E) = 1 - \overline{C}(\varphi_{0,1}, \mu)$$
$$= 1 + \left(\frac{1-\xi}{2}\right)\log\left(\frac{1-\xi}{2}\right) - \left(\frac{1+\xi}{2}\right)\log\left(\frac{1+\xi}{2}\right), \quad (7)$$

where $\xi = \Pr(?)$ is denoted. Finally for the length of the private key, in terms of a registered parcel, we have

$$R(Q) = 1 - h(Q) - \overline{C}(\varphi_{0,1}, \mu). \quad (8)$$

It is important to emphasize that in formula (8), evaluation of the eavesdropper's information does not depend on the observed errors on the receiving side. The upper bound of the eavesdropper's information may not exceed Holevo's information—classical accessible information that can be extracted from quantum ensemble. The length of the secret key as a function of the observed error at the receiver is presented in figure 2(a).

5. The length of the quantum communication channel in which there is guaranteed secret key distribution

Let's estimate the quantum channel length up to which there is guaranteed secret key distribution. In the absence of an eavesdropper, the error occurs only because of dark noise. The following estimate is obtained for the error probability due to dark noise

$$Q(L) = \frac{1}{2}\frac{p_d}{(p_d + n_{\text{reg}}(L))}, \quad n_{\text{reg}}(L) = 1 - \mathrm{e}^{-\eta \cdot \eta_{\text{APD}} \cdot \mu(L)}, \quad (9)$$

$$\mu(L) = \mu \cdot 10^{-\frac{\delta \cdot L}{10}},$$

L is the length of the quantum communication channel, $n_{\text{reg}}(L)$ is the detection probability of the avalanche detector, η_{APD} is the quantum efficiency of the detector, η is the beam-splitter coefficient, p_d is the probability of a dark count per gate. The length of the secret key as a function of quantum communication channel length can be obtained by substituting (9) into (8), we have

$$R(Q(L)) = 1 - h(Q(L)) - \overline{C}(\varphi_{0,1}, \mu). \quad (10)$$

The secret key length for different parameter values are shown in figure 2(b).

6. Conclusion

USD measurements in some systems with a certain level of losses in the quantum channel lead to a loss of privacy. An eavesdropper without producing errors, knows the whole key and is not detected. In this protocol, the USD measurements will inevitably lead to an error on the receiving side, which ensures the eavesdropper is detected and the security of the keys. Unlike other protocols, DPS [6–8] and COW [9–12], the simplicity of the protocol makes it possible to carry out a complete analysis of its security.

Acknowledgments

We express our gratitude to S P Kulik for fruitful discussions.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Comput. Sys. and Sign. Proces.* (*Bangalore, India, December*) p 175

[2] Bennett C H 1992 Quantum cryptography using any two non-orthogonal states *Phys. Rev. Lett.* **68** 3121

[3] Wooters W K and Zurek W H 1982 A single quantum cannot be clonned *Nature* **299** 802

[4] Chefles A 1998 Unambiguous discrimination between linearly-independent quantum states *Phys. Lett.* A **239** 339

Chefles A and Barnett S M 1998 Optimum unambiguous discrimination between linearly independent symmetric states *Phys. Lett.* A **250** 223

[5] Scarani Bechmann-Pasquinucci V H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301

[6] Inoue K, Waks E, Yamamoto Y 2002 Differential phase shift quantum key distribution *Phys. Rev. Lett.* **89** 037902
Inoue K, Waks E and Yamamoto Y 2003 Differential-phase-shift quantum key distribution using coherent light *Phys. Rev.* A **68** 022317

[7] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 Quantum key distribution over a 40 dB channel loss using superconducting single-photon detectors *Nat. Photon.* **1** 343

[8] Wen K, Tamaki K and Yamamoto Y 2009 Unconditional security of single-photon differential phase shift quantum key distribution *Phys. Rev. Lett.* **103** 170503

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

[10] Branciard C, Gisin N, Lütkenhaus N and Scarani V 2005 Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography *Appl. Phys. Lett.* **87** 194108

[11] Branciard C, Gisin N and Scarani V 2008 Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography (coherent-one-way and differential-phase-shift) *New J. Phys.* **10** 013031

[12] Stucki D *et al* 2008 High speed coherent one-way quantum key distribution prototype *Opt. Express* **17** 13326

[13] Molotkov S N 2012 Relativistic quantum cryptography *JETP* **112** 370
Molotkov S N 2011 Relativistic quantum cryptography for open space without clock synchronization on the receiver and transmitter sides *JETP Lett.* **94** 469
Molotkov S N 2012 On the resistance of relativistic quantum cryptography in open space at finite resources *JETP Lett.* **96** 342

[14] Molotkov S N and Potapova T A 2013 Free space relativistic quantum cryptography with faint laser pulses *Laser Phys. Lett.* **10** 075205

[15] Radchenko I V, Kravtsov K S, Kulik S P and Molotkov S N 2014 Relativistic quantum cryptography *Laser Phys. Lett.* **11** 065203

[16] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zürich arXiv/quant-ph: 0512258 [quant-ph]

[17] Tomamichel M, Schaffner C, Smith A and Renner R 2011 Leftover hashing against quantum side information *IEEE Trans. Inf. Theory* **57** 5524–35

[18] Carter J L and Wegman M N 1979 Universal classes of hash functions *J. Comput. Syst. Sci.* **18** 143

[19] Holevo A S 1998 Quantum coding theorems *Russ. Math. Surv.* **53** 1295