Free space relativistic quantum cryptography with faint laser pulses



2013 Laser Phys. Lett. 10 075205

(http://iopscience.iop.org/1612-202X/10/7/075205)

Laser Phys. Lett. **10** (2013) 075205 (5pp) doi:10.1088/1612-2011/10/7/075205

LETTER

# Free space relativistic quantum cryptography with faint laser pulses

**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, Russia

E-mail: sergei.molotkov@gmail.com

Received 15 March 2013
Accepted for publication 16 March 2013
Published 11 June 2013
Online at stacks.iop.org/LPL/10/075205

**Abstract**
A new protocol for quantum key distribution through empty space is proposed. Apart from the quantum mechanical restrictions on distinguishability of non-orthogonal states, the protocol employs additional restrictions imposed by special relativity. The protocol ensures generation of a secure key even for the source generating non-strictly single-photon quantum states and for arbitrary losses in quantum communication channel.

## 1. Introduction

The unconditional security of quantum key distribution is based on two fundamental no-go theorems of quantum mechanics: (i) impossibility of cloning an arbitrary unknown quantum state [1] and (ii) impossibility of reliable distinguishability of non-orthogonal quantum states [2].

However, in practice quantum states emitted by the source are not strictly single-photon ones which, together with losses in the quantum communication channel, breaks the key security for all basic quantum key distribution protocols (B92 [2], BB84 [3], SARG04 [4], decoy state [5], phase-time coding [6]) if the quantum channel length and/or losses exceed some critical values.

For lossless channels, quantum cryptography protocols employing single-photon orthogonal states with the spatial extent exceeding the channel length were suggested earlier [7, 8].

## 2. Relativistic quantum key distribution

A new relativistic quantum key distribution protocol utilizing additional constraints imposed by special relativity is proposed below. We shall first describe the protocol for a single-photon source and a quantum channel with arbitrary losses, and then extend it to a multi-photon source.

(1) Alice and Bob keep under full control spatial domains required to prepare and detect quantum states (figure 1). The distance between points $i_A$ and $f_B$ is $L$. Their clocks are synchronized[4].

(2) Alice prepares at a publicly known time $t_A = 0$ in the vicinity of point $i_A$ a localized single-photon quantum state $|i_A\rangle$. Then she applies at random one of the two unitary operations, $U_A^0$ or $U_A^1$, transforming the localized state at time $t_A = 0$ into one of the extended states at time $t'_A$:$|\bar{0}_A\rangle$, $|\bar{1}_A\rangle = U_A^{0,1}|i_A\rangle = \frac{1}{\sqrt{2}}(|1_A\rangle \pm e^{\pm i\varphi}|2_A\rangle)$. The states $|1_A\rangle$ and $|2_A\rangle$ have the same shape as $|i_A\rangle$ and only differ due to a spatio-temporal shift along the two branches of the light cone,

$$|\bar{0}_A\rangle, |\bar{1}_A\rangle = \begin{pmatrix} |1_A\rangle\langle i_A| & 0 \\ 0 & \pm e^{\pm i\varphi}|2_A\rangle\langle i_A| \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} |i_A\rangle \\ |i_A\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |1_A\rangle \\ \pm e^{\pm i\varphi}|2_A\rangle \end{pmatrix}. \quad (1)$$

[4] The requirement for Alice and Bob's clocks to be synchronized can be lifted by employing a two-pass scheme.

 

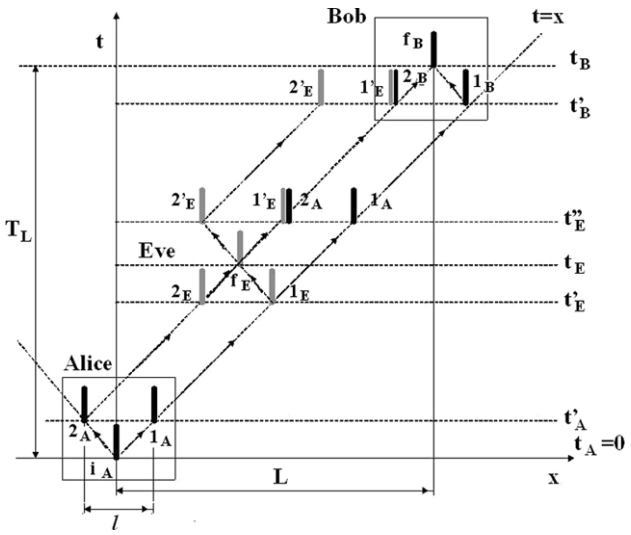


**Figure 1.** Spatio-temporal diagram explaining the protocol. The speed of light is taken to be $c = 1$.

The column vectors in equation (1) represent single quantum states. The top and bottom rows correspond to states referring to the same time but localized around different spatial points.

(3) By the time $t'_B$ the states are entirely found in the spatial domain controlled by Bob, $|\bar{0}_{t'_B}\rangle, |\bar{1}_{t'_B}\rangle = \frac{1}{\sqrt{2}}(|1_{t'B}\rangle \pm e^{\pm i\varphi}|2_{t'_B}\rangle)$.

Bob performs a unitary transformation which does not depend on input state and maps the extended quantum states into states localized around the point $(f_B, t_B)$,

$$|\bar{0}_{t'_B}\rangle, |\bar{1}_{t'_B}\rangle = \begin{pmatrix} |f_B\rangle\langle 1_{t'_B}| & 0 \\ 0 & |f_B\rangle\langle 2_{t'_B}| \end{pmatrix} \times \frac{1}{\sqrt{2}} \begin{pmatrix} |1_{t'_B}\rangle \\ \pm e^{\pm i\varphi}|2_{t'_B}\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |f_B\rangle \\ \pm e^{\pm i\varphi}|f_B\rangle \end{pmatrix}. \quad (2)$$

Then Bob performs at random and independently of Alice one of the two local measurements at point $(f_B, t_B)$. The measurements are similar to those used in the standard B92 protocol [2],

$$I = \mathcal{P}_{0,1} + \mathcal{P}^{\perp}_{0,1}, \qquad \mathcal{P}^{\perp}_{0,1} = I - \mathcal{P}_{0,1};$$
$$\mathcal{P}_{0,1} = \tfrac{1}{2} \begin{pmatrix} 1 & \pm e^{\mp i\varphi} \\ \pm e^{\pm i\varphi} & 1 \end{pmatrix} |f_B\rangle\langle f_B|. \quad (3)$$

The conditional probability for Bob obtaining a conclusive outcome 0 (or 1) provided that Alice sent 0 (or 1) is $P\{0_B|0_A\} = \mathrm{Tr}\{|\bar{0}_{t'_B}\rangle\langle\bar{0}_{t'_B}|\mathcal{P}^{\perp}_1\} = P\{1_B|1_A\} = \mathrm{Tr}\{|\bar{1}_{t'_B}\rangle\langle\bar{1}_{t'_B}|\mathcal{P}^{\perp}_0\} = \cos^2(\varphi)$. The probability of an inconclusive outcome is $P\{?_B|0_A\} = \mathrm{Tr}\{|\bar{0}_{t'_B}\rangle\langle\bar{0}_{t'_B}|\mathcal{P}_{0,1}\} = P\{?_B|1_A\} = \mathrm{Tr}\{|\bar{1}_{t'_B}\rangle\langle\bar{1}_{t'_B}|\mathcal{P}_{1,0}\} = \sin^2(2\varphi)$. Inconclusive outcomes are discarded. Bob also discards all counts whose delay at point $(f_B, t_B)$ *exceeded* $t_B - l/c$, *l being the state extent*.

(4) If the resulting error $Q_B < Q_c$ (see below), the errors are corrected through a public channel. Then the distilled key secrecy is amplified [9].

## 3. Intercept–resend attack

To distinguish between the states, Eve should have access to entire states $\frac{1}{\sqrt{2}}(|1_E\rangle \pm e^{\pm i\varphi}|2_E\rangle)$. Access to the front 'part' $\frac{1}{\sqrt{2}}|1_E\rangle$ only is not sufficient to identify the state. To get access to the second 'half' of the state $\pm\frac{1}{\sqrt{2}}e^{\pm i\varphi}|2_E\rangle$, Eve should transform the state which is extended in both space and time into a state localized at the point $(f_E, t_E)$ (figure 1). This cannot be done faster than the temporal extent of the past light cone covering the entire considered state (figure 1). There exist no physically realizable operators mapping extended states into localized ones in shorter time; such an operator would have non-zero matrix elements between the points separated by a space-like interval. After gathering the two 'halves' of the state at point $(f_E, t_E)$, Eve performs her measurements. Because of the states' non-orthogonality, the minimal possible error in distinguishing the states is [10] $Q_\varphi = \frac{1}{2}(1-\sqrt{1-|\langle\bar{0}_A|\bar{1}_A\rangle|^2}) = \sin^2(\varphi/2)$. Depending on the measurement outcome, Eve can prepare a state consisting of two halves which is similar to the initial state created by Alice. Due to the special relativity restrictions, Eve cannot prepare an extended state earlier than by time $t''_E$. However, at time $t''_E$ the state prepared by Eve will differ from Alice's original state $\frac{1}{\sqrt{2}}(|1_A\rangle \pm e^{\pm\varphi}|2_A\rangle)$ by a spatio-temporal translation through a distance equal to the state length (figure 1). Since Bob performs his measurement in a certain temporal gap only, Eve's states which are shifted in time will yield the same outcome for all states since the second half of Eve's state $\pm e^{\pm i\varphi}|2'_E\rangle$ cannot arrive in time for Bob's measurement. As a result, the probability of Bob making an error with the delayed states is $Q_B = \frac{1}{2}$.

The speed of light in the atmosphere $c'$ differs from that in vacuum, $c$. For Eve to be unable to compensate for the lack of time needed to transform the state, its length $l$ should satisfy the condition $l > c(T'_L - T_L)$, $T'_L = (L+l)/c$, $T'_L = (L+l)/c'$, where $c' = c(1-\xi)$, so that $l > \xi L$. The value of $\xi$ in the Earth's atmosphere at heights $h \leq 10$ km for $\lambda \approx 0.8$ $\mu$m is $\xi \approx 10^{-4}$, while for $h > 10$ km, $c' = c$. Hence Eve can only make up for the lack of time at height $h$ by replacing the quantum channel with the ideal one (i.e., vacuum). The minimal state length $l_{\min}$ is limited by the condition $l_{\min} \geq \xi \times 10$ (km) $= 1$ m. For $l > l_{\min}$ the key can be distributed over arbitrarily large distances.

### *3.1. Inefficiency of the transparent attack*

The most general and powerful eavesdropping strategy in non-relativistic quantum cryptography is the collective attack [11]. For each state sent by Alice to Bob, Eve prepares an ancilla and lets it interact with the arriving state. After the interaction the ancilla and the state end up in an entangled state. The perturbed state sent by Alice travels further to Bob while the modified ancilla is stored by Eve in quantum

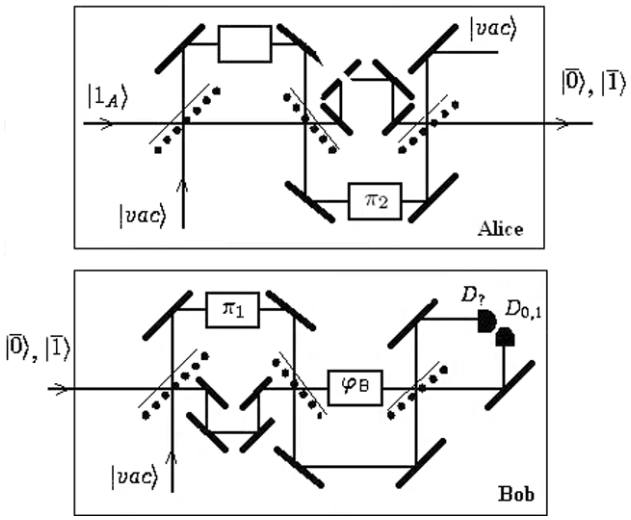


**Figure 2.** Optical diagram for the preparation and detection of quantum states. The reflecting side of symmetric beam splitters changing the state phase by $\pi$ is shown with a solid line while the dashed line represents the side which does not affect the phase.

memory. After all states are sent by Alice and measured by Bob, Eve performs collective measurements of all ancillae residing in her quantum memory. In the relativistic case this attack is inefficient and actually reduces to the previous intercept–resend strategy. The attack is described by a unitary operator, e.g., for state 0

$$U_{\mathrm{BE}}(|\bar{0}_{t'_{\mathrm{E}}}\rangle \otimes |A\rangle_{\mathrm{E}}) = |\bar{0}_{t'_{\mathrm{E}}}\rangle \otimes |\varphi_{00}\rangle_{\mathrm{E}} + |\bar{1}_{t'_{\mathrm{E}}}\rangle \otimes |\varphi_{01}\rangle_{\mathrm{E}},$$
$$U_{\mathrm{BE}}(|1_{t'_{\mathrm{E}}}\rangle \otimes |A\rangle_{\mathrm{E}}) = |1_{t'_{\mathrm{E}}}\rangle \otimes |\tilde{\varphi}_{00}\rangle_{\mathrm{E}} + |2_{t'_{\mathrm{E}}}\rangle \otimes |\tilde{\varphi}_{01}\rangle_{\mathrm{E}}, \quad (4)$$

where $|\bar{0}_{t'_{\mathrm{E}}}\rangle, |\bar{1}_{t'_{\mathrm{E}}}\rangle$ are Alice's states at time $t'_{\mathrm{E}}$ and $|\varphi_{ij}\rangle_{\mathrm{E}}, |\tilde{\varphi}_{ij}\rangle_{\mathrm{E}}$ are Eve's states, $(i, j = 0, 1)$. Taken into account here is the fact that signal states are linearly expressed through the localized basis states $|1_{t'_{\mathrm{E}}}\rangle, |2_{t'_{\mathrm{E}}}\rangle$. If the unitary operator in equation (4) were physically realizable, it would necessarily have non-zero matrix elements $(\langle 2_{t'_{\mathrm{E}}}|[{}_{\mathrm{E}}\langle\tilde{\varphi}_{01}|U_{\mathrm{BE}}|A\rangle_{\mathrm{E}}]|1_{t'_{\mathrm{E}}}\rangle = {}_{\mathrm{E}}\langle\tilde{\varphi}_{01}|\tilde{\varphi}_{01}\rangle_{\mathrm{E}})$ between points $(1_{\mathrm{E}}, t'_{\mathrm{E}})$ and $(2_{\mathrm{E}}, t'_{\mathrm{E}})$ separated by a space-like interval, which contradicts the fundamental relativistic causality principle. In principle, Eve can transform the extended states into those localized around the spatio-temporal point $(f_{\mathrm{E}}, t_{\mathrm{E}})$ and then perform a unitary transformation $U_{\mathrm{BE}}$. After that, the localized states can be transformed into extended ones. However, this procedure would result in a delay and, finally, an error $Q_{\mathrm{B}} = \frac{1}{2}$ in Bob's measurements just as in section 3.

### *3.2. Intercept–resend attack employing quantum states prepared in advance*

Eve prepares in advance her state $\frac{1}{\sqrt{2}}(|1_{\mathrm{A}}\rangle + |2_{\mathrm{A}}\rangle)$ which arrives at the same place as Alice's original state by time $t_{\mathrm{E}}$. Then Eve gathers Alice's state in a single point $(f_{\mathrm{E}}, t_{\mathrm{E}})$ and performs measurements at this point. Depending on the measurement outcome, Eve changes locally at point $(f_{\mathrm{E}}, t_{\mathrm{E}})$ the phase of the second half of her earlier prepared state which later is received by Bob without any delay. Let the fraction of qubits eavesdropped by Eve be $\delta$. For these qubits Bob's and Eve's error is $\delta$. In the rest of the qubits, whose fraction is $1 - \delta$, Bob's error is 0 while Eve's error is $1/2$.

### *3.3. Effects of losses in the quantum channel*

The analysis of signal attenuation is similar to the intercept–resend attack. Here the role of Eve is played by the medium itself. Transformation of an extended state into a localized one requires finite time. After the absorption of a transformed state the absorber ('atom') goes into one of the two states depending on whether the absorbed state was 0 or 1. Eve measures the 'atom' state, the error in discriminating its states being not less than $Q_\varphi$. Resending the states prepared by Eve will result in a delay and, consequently, Bob's error being equal to $1/2$. Formally, it is possible to imagine a situation where both the front and the rear 'halves' of the state are absorbed at a certain moment of time at different spatial points of the medium. In that case, to identify the absorbed state one should have access to spatially separated points of the absorber which would require a finite time $l/c$ anyway.

### *3.4. The secret key length*

Let the sequences obtained by Alice, Bob and Eve after discarding inconclusive outcomes be $X^N = \{0, 1\}^N$, $Y^N = \{0, 1\}^N$ and $E^N = \{0, 1\}^N$. Then the conditional Alice–Bob and Alice–Eve probabilities for eavesdropped qubits are $P(e|x) = P(y|x) = 1 - Q_\varphi$ $(e = y = x)$; $P(e|x) = P(y|x) = Q_\varphi$ $(e, y \neq x)$. The transition probabilities for the rest of the qubits are $P(e|x) = \frac{1}{2}$ $(\forall e, x)$; $P(y|x) = 1$ $(y = x)$, $P(y|x) = 0$ $(y \neq x)$. The secret key length in the limit $N \to \infty$ is (for details, see [11])

$$r = \lim_{N\to\infty} \left(H(E^N|X^N) - H(Y^N|X^N)\right)/N$$
$$= \lim_{N\to\infty} \left(I(X^N; Y^N) - I(X^N; E^N)\right)/N, \quad (5)$$

where $H(Y^N|X^N), H(E^N|X^N), I(X^N; Y^N), I(X^N; E^N)$ are conditional and mutual information. Equation (5) takes into account error correction with random Shannon codes and privacy amplification for the distilled key as well as the relations $H(Y^N|X^N) = -\delta N h(Q_\varphi)$, $H(E^N|X^N) = (1-\delta)N - \delta N h(Q_\varphi)$, where $h(x) = -x\log(x) - (1-x)\log(1-x)$. It is convenient to eliminate the parameter $\delta$ by expressing it through Bob's measured error $Q_{\mathrm{B}} = Q_\varphi \cdot \delta + 0 \cdot (1-\delta)$. One has $r = 1 - \frac{Q_{\mathrm{B}}}{Q_\varphi} + \frac{Q_{\mathrm{B}}}{Q_\varphi} h(Q_\varphi) - h(Q_{\mathrm{B}})$. The critical measured error level below which the key distribution security is guaranteed is $Q_{\mathrm{c}} = Q_\varphi$.

## 4. Optical scheme

The optical diagram is presented in figure 2.

We shall work in the single-photon subspace. The unitary operators describing the optical scheme operation are

$$U_{\mathrm{s}}^{\pm} = \frac{1}{\sqrt{2}} \begin{pmatrix} I & \pm I \\ \mp I & I \end{pmatrix}, \qquad U_{\varphi_{\mathrm{A,B}}} = \begin{pmatrix} I & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\varphi_{\mathrm{A,B}}} I \end{pmatrix},$$
$$U_{j\to j+1} = \begin{pmatrix} I & 0 \\ 0 & \sum_{j=-\infty}^{\infty} |j+1\rangle\langle j| \end{pmatrix},$$

$$U_{\pi_1} = \begin{pmatrix} I & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi}|1\rangle\langle 1| + I(\neq 1) \end{pmatrix},$$

$$U_{\pi_2} = \begin{pmatrix} I & 0 \\ 0 & I(\neq 2) + \mathrm{e}^{\mathrm{i}\pi}|2\rangle\langle 2| \end{pmatrix},$$

$$I(\neq i) = \sum_{j=-\infty, j\neq i}^{\infty} |j\rangle\langle j|. \tag{6}$$

The identity operator in the full space including the vacuum state is $\bar{I} = |\mathrm{vac}\rangle\langle\mathrm{vac}| + I$, and $I = \sum_{j=-\infty}^{\infty}|j\rangle\langle j|$ is the identity operator in the single-photon subspace, $\{|j\rangle\}$ is a set of localized states separated by spatial distance $l$. $U_{\mathrm{s}}^{\pm}$ describes a symmetric beam splitter while $U_{\varphi_{\mathrm{A,B}}}$ represents a phase modulator changing the relative phase of states which travelled along different interferometer arms ($\varphi_{\mathrm{A,B}} = \varphi$ for 0 and $\varphi_{\mathrm{A,B}} = \pi - \varphi$ for 1). $U_{\pi_2}$ describes a phase modulator affecting the relative phase between $|1\rangle$ and $|2\rangle$ in the superposition state in only one of the interferometer arms which is realized by applying a voltage to the modulator when the second 'half' of the state is passing through it[5]. $U_{j\to j+1}$ is the shift operator in one of the arms. Alice employs the following transformation of states:

$$U_{\mathrm{s}}^{+}U_{\pi_2}U_{\mathrm{s}}^{-}U_{\varphi_{\mathrm{A}}}U_{j\to j+1}U_{\mathrm{s}}^{+}\begin{pmatrix}|1_{\mathrm{A}}\rangle\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}(|1_{\mathrm{A}}\rangle + \mathrm{e}^{\mathrm{i}\varphi_{\mathrm{A}}}|2_{\mathrm{A}}\rangle)\\0\end{pmatrix}. \tag{7}$$

The state amplitudes (figure 2) in $D_?$ (top row) and $D_{0,1}$ (bottom row) are

$$U_{\mathrm{s}}^{+}U_{\varphi_{\mathrm{B}}}U_{j\to j+1}U_{\mathrm{s}}^{-}U_{\pi_1}U_{\mathrm{s}}^{+}\frac{1}{\sqrt{2}}\begin{pmatrix}(|1_{\mathrm{A}}\rangle + \mathrm{e}^{\mathrm{i}\varphi_{\mathrm{A}}}|2_{\mathrm{B}}\rangle)\\0\end{pmatrix} = \frac{1}{2}\begin{pmatrix}(\mathrm{e}^{\mathrm{i}\varphi_{\mathrm{A}}} + \mathrm{e}^{\mathrm{i}\varphi_{\mathrm{B}}})|2_{\mathrm{B}}\rangle\\-(\mathrm{e}^{\mathrm{i}\varphi_{\mathrm{A}}} - \mathrm{e}^{\mathrm{i}\varphi_{\mathrm{B}}})|2_{\mathrm{B}}\rangle\end{pmatrix}. \tag{8}$$

Actually, the outlined scheme implements the measurements described by equations (2) and (3). If $\varphi_{\mathrm{A}} = \varphi$ is 0 (or $\varphi_{\mathrm{A}} = \pi - \varphi$ is 1), and Bob chose $\varphi_{\mathrm{B}} = \varphi$ (or $\varphi_{\mathrm{B}} = \pi - \varphi$), the probability of a count occurring in $D_?$ is identically equal to unity, while that in $D_{0,1}$ is zero. On the contrary, if $\varphi_{\mathrm{A}} = \varphi$ (or $\varphi_{\mathrm{A}} = \pi - \varphi$), while $\varphi_{\mathrm{B}} = \pi - \varphi$ (or $\varphi_{\mathrm{B}} = \varphi$), the probability of a conclusive outcome (count) in $D_{0,1}$ is $\cos^2(\varphi)$, while that of inconclusive outcomes in $D_?$ is $\sin^2(\varphi)$.

## 5. Multi-photon case

The initial states prepared by Alice are attenuated coherent laser pulses with average photon number $\mu = |\alpha|^2$: $|\bar{i}_\alpha\rangle_{\mathrm{A}} = \mathrm{e}^{-\frac{\mu}{2}}\left(|\mathrm{vac}\rangle + \sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|\bar{i}\rangle_{\mathrm{A}}^{\otimes n}\right)$, $i = 0, 1$. Eve can employ any of the attacks described earlier, but there exists a more efficient one. Eve can split the arriving state with a beam splitter possessing the splitting coefficient $\eta$. Coherent states are affected by the beam splitter in a self-similar way, i.e. states obtained by Eve and leaving the splitter to Bob are $|\bar{i}_{\alpha\sqrt{1-\eta}}\rangle_{\mathrm{E}} \otimes |\bar{i}_{\alpha\sqrt{\eta}}\rangle_{\mathrm{B}}$ ($i = 0, 1$), respectively. In this way Eve introduces neither delays nor any errors in Bob's measurements. Eve stores her states in quantum memory and performs *collective measurements* at the very end of the protocol, discarding the states whose counterparts produced inconclusive outcomes in Bob's measurements. The transformations used by Bob are similar to those defined by equations (7) and (8). Standard avalanche detectors do not resolve the number of photons in the pulse and are not sensitive to the vacuum component. The probability of conclusive outcomes in $D_{0,1}$ is $\mathrm{e}^{-\mu}(\mathrm{e}^{\mu\eta\cos^2(\varphi)} - 1)$, while that of inconclusive outcomes is $\mathrm{e}^{-\mu}(\mathrm{e}^{\mu\eta\sin^2(\varphi)} - 1)$. Eve cannot obtain information exceeding Holevo's boundary [12] for the density matrix ensemble $\rho_{i_{\sqrt{1-\eta}\alpha}} = |\bar{i}_{\sqrt{1-\eta}\alpha}\rangle_{\mathrm{EE}}\langle\bar{i}_{\sqrt{1-\eta}\alpha}|$ ($i = 0, 1$): $\chi(\rho_{\sqrt{1-\eta}\alpha}) < \lim_{\eta\to 0}\chi(\rho_{\sqrt{1-\eta}\alpha}) = \chi(\rho_\alpha) = h(\zeta)$, $\zeta = (1-\varepsilon)/2$, $\varepsilon = |_{\mathrm{A}}\langle\bar{0}_\alpha|\bar{1}_\alpha\rangle_{\mathrm{A}}| = \mathrm{e}^{-\mu\cos^2(\varphi)}$. The secret key length per one qubit sent by Alice is (see [11])

$$r = \lim_{N\to\infty}\left(I(Y^N|X^N) - N\chi(\rho_\alpha)\right)/N = 1 - h(\zeta). \tag{9}$$

It is interesting to note that Bob should not necessarily monitor the average number of qubits reaching him. For large average numbers of photons in signal states the secret key length tends to zero, $r \propto \mathrm{e}^{-\mu\cos^2(\varphi)}$, although formally it is always larger than zero. Security is guaranteed for arbitrary $\mu$ but the key generation rate decays exponentially with $\mu$ (for example, $\mu = 1$ yields $r \approx 0.37N$ while $\mu = 2$ results in $r \approx 0.14N$). It is important that the channel attenuation does not appear in the security criterion at all, and the key length depends on the initial quantum states only. In the multi-photon case Eve herself acts as an attenuator by partly absorbing the arriving states. However, in contrast to Bob who discards inconclusive outcomes, Eve cannot follow a similar strategy. Collective measurements can only reduce the state discrimination error in Eve's measurements compared with individual measurements.

[5] Such a transformation was implemented in the work [13].

## Acknowledgment

This work was supported partially by the Russian Foundation for Basic Research (project No. 11-02-00455).

## References

[1] Wooters W K and Zurek W H 1992 *Nature* **299** 802
[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[3] 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, Dec.)* p 175
[4] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[5] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[6] Kronberg D A and Molotkov S N 2009 *J. Exp. Theor. Phys.* **109** 557
[7] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
[8] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383

[9] Bennett C H, Brassard G, Crépeau C and Maurer U 1995 *IEEE Trans. Inf. Theory* **41** 1915
[10] Helstrom C W 1976 *Quntum Detection and Estimation Theory* (New York: Academic)
[11] Renner R 2005 Security of quantum key distribution arXiv:quant-ph/0512258
[12] Holevo A S 2002 *Introduction to Quantum Information Theory* (Moscow: MTNMO) (in Russian)
Holevo A S 1998 *Usp. Mat. Nauk* **53** 193
[13] Nambu Y, Hatanaka T, Yamazaki H and Nakamura K 2004 Quantum cryptogrphic system based on silica-based planar lightwave circuits arXiv:quant-ph/0404015