ISSN 0021-3640, JETP Letters, 2014, Vol. 100, No. 6, pp. 413–419. © Pleiades Publishing, Inc., 2014.
Original Russian Text © S.N. Molotkov, 2014, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2014, Vol. 100, No. 6, pp. 457–464.

On the Stability of Fiber-Optic Quantum Cryptography at Arbitrary Losses in a Communication Channel: Exclusion of Unambiguous Measurements

S. N. Molotkov

Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia
Academy of Cryptography of the Russian Federation, Moscow, 121552 Russia
Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, 119991 Russia
e-mail: sergei.molotkov@gmail.com

Received August 8, 2014

Since a source of quantum states is not strictly single-photon and losses exist in a communication channel, an attack with unambiguous measurements is possible, leading to loss of security. The problem of the stability of quantum key distribution protocols in a channel with large losses is still unsolved. A radical solution of this problem has been proposed by completely excluding unambiguous measurements by an eavesdropper. The problem is solved by means of counting of classical reference pulses. The conservation of the number of classical sync pulses results in the impossibility of unambiguous measurements. In this case, losses in the communication channel are considered as a priori unknown and can vary during a series of messages.

DOI: 10.1134/S0021364014180076

INTRODUCTION

In modern systems of fiber-optic quantum cryptography (quantum key distribution systems), the security of keys is guaranteed *even with ideal detectors without their own dark noise* only at certain lengths of a communication channel that do not exceed a certain critical length [1]. This is due to the *joint action of two factors*. First, strongly weakened laser radiation—a coherent state $|\alpha\rangle$ ($\mu = |\alpha|^2 \approx 0.1$–$0.5$ is the average number of photons)—which is not strictly single-photon state, but is a quasi-single-photon state with a Poisson distribution in the number of photons, is used as a source of information quantum states. Second, losses exist in the communication channel.

Information quantum states to which information on a future key is encoded constitute a set of nonorthogonal linearly independent coherent states $\{|\varphi_i\rangle = |\alpha_i\rangle\}_{i=1}^{N}$.[1] Nonorthogonality is necessary for the impossibility of unambiguous distinguishability of states. The linear independence of states is a necessary and sufficient condition of unambiguous measurements [2].

Any quantum mechanical measurement by a physical instrument is formally described by a certain decomposition of unity. The decomposition of unity id for unambiguous measurements has the form

$$\mathrm{id} = \sum_{j=1}^{N+1} \mathcal{M}_j, \tag{1}$$

where $\mathcal{M}_j$ are positive operator-valued measures. The unambiguous measurements have the property

$$\begin{gathered}\Pr(j|i) = \mathrm{Tr}\{|\varphi_i\rangle\langle\varphi_i|\mathcal{M}_j\} = P_j\delta_{ji}, \\ i = 1, \ldots, N, \\ \Pr(N+1|i) = \mathrm{Tr}\{|\varphi_i\rangle\langle\varphi_i|\mathcal{M}_{N+1}\} = P_{?i}, \\ i = 1, \ldots, N.\end{gathered} \tag{2}$$

Measurements mean that, if one of 1, …, N (*conclusive*) outcomes occurs, a state is identified unambiguously, but with the probability smaller than unity. If the $(N+1)$th (*inconclusive*) outcome occurs, it is impossible to identify a state inducing this outcome.

If losses exist in the channel, i.e., some states do not reach the receiver side, an eavesdropper can act as follows. He breaks the communication channel near the transmitter and receiver sides (we recall that the quantum communication channel in quantum cryptography is not controlled). The eavesdropper performs unambiguous measurements near the transmitter side. If an unambiguous outcome is obtained, he reports the result to his partner near the receiver side. The partner prepares the corresponding state and sends it to the receiver side. If the inconclusive outcome (?) is

[1] In practice, packets of coherent states rather than single-mode coherent states are used. However, since an optical scheme is linear, it is sufficient to consider one mode of coherent states in order to avoid the complication of calculations by insignificant details.

obtained, nothing is sent to the receiver side. In this case, if the probability of losses in the communication channel is equal to the probability of the inconclusive outcome (Pr(?) = Pr(Loss)), the number of the states reaching the receiver side is the same in the presence and absence of the eavesdropper. The eavesdropper knows all transmitted states and does not make errors on the receiver side; i.e., he remains undetected. The system does not ensure the security of keys beginning with a certain level of losses in the communication channel.

Thus, unambiguous measurements break the security of quantum cryptography protocols. This problem remains topical. The main protocols and the reason for their instability with respect to unambiguous measurements, as well as a new protocol that excludes unambiguous measurements, will be briefly analyzed below.

BRIEF ANALYSIS OF MAIN QUANTUM KEY DISTRIBUTION PROTOCOLS WITH PHASE ENCODING

B92 Protocol

This protocol was proposed in [3] and involved a pair of nonorthogonal states. The quantum ensemble is $\{p_0 = p_1 = \frac{1}{2}, |\varphi_0\rangle, |\varphi_1\rangle\}$, where p_0 and p_1 are the probabilities of the appearance of respective states. The optimal unambiguous measurements minimizing the probability of an inconclusive outcome [2] have the form

$$\begin{aligned} \mathrm{id} &= \mathcal{M}_0 + \mathcal{M}_1 + \mathcal{M}_?, \quad \mathcal{M}_0 = \frac{\mathrm{id} - |\varphi_1\rangle\langle\varphi_1|}{1 - |\langle\varphi_0|\varphi_1\rangle|}, \\ \mathcal{M}_1 &= \frac{\mathrm{id} - |\varphi_0\rangle\langle\varphi_0|}{1 - |\langle\varphi_0|\varphi_1\rangle|}, \quad \mathcal{M}_? = \mathrm{id} - \mathcal{M}_0 - \mathcal{M}_1. \end{aligned} \tag{3}$$

In view of $p_0 = p_1$, the probability of an inconclusive outcome is

$$\Pr(?) = |\langle\varphi_0|\varphi_1\rangle|. \tag{4}$$

If phase encoding of coherent states is used, $|\varphi_0\rangle = |\exp(i\varphi_0)\alpha\rangle$ and $|\varphi_1\rangle = |\exp(i\varphi_1)\alpha\rangle$. Correspondingly, the probability of the inconclusive outcome is $\Pr(?) = \exp\left(-\frac{\mu|e^{i\varphi_0} - e^{i\varphi_1}|^2}{2}\right)$, whereas the probability of losses in the channel is $\Pr(\mathrm{Loss}, L) = \exp\{-\mu[T(L)]\}$, where $\mu = |\alpha|^2$ is the average number of photons (typical values $\mu = 0.1$–0.5), $T(L) = 10^{-\delta L/10}$, L is the length of the communication channel, and δ is the damping constant (typical value $\delta = 0.2$ dB/km for the SMF-28 single-mode fiber).

A protocol is not secret if $\Pr(\mathrm{Loss}, L) \geq \Pr(?)$. From this condition, the critical length of the communication channel L_c to which the security of distributed keys is guaranteed can be obtained. If the length of the communication channel satisfies the condition $L \geq L_c$, the eavesdropper knows the entire key, does not generate errors on the receiver side, and remains undetected.

BB84 Protocol and Protocols on Geometrically Uniform States

The BB84 protocol was proposed in [4] and is currently the most studied [5–7]. This protocol uses two conjugate bases (+ and ×) with ensembles of states inside each of them: $\left\{p_0(+) = p_1(+) = \frac{1}{2}, |\alpha\rangle, |-\alpha\rangle\right\}$, $\left\{p_0(\times) = p_1(\times) = \frac{1}{2}, |i\alpha\rangle, |-i\alpha\rangle\right\}$.

This protocol can be generalized to a larger number of information states, protocols based on geometrically uniform states (GUS protocols) [8]. States in the BB84 protocol are described by equidistant points on a circle with the radius $|\alpha|$ in the complex plane α. All states can be obtained from one state, e.g., $|\alpha\rangle$, by successive unitary rotations. In particular, $|i\alpha\rangle = U\left(\frac{\pi}{2}\right)|\alpha\rangle$, $|-\alpha\rangle = U^2\left(\frac{\pi}{2}\right)|\alpha\rangle$, and $|-i\alpha\rangle = U^3\left(\frac{\pi}{2}\right)|\alpha\rangle$. The number of bases ($N_b$) and the number of states ($2N_b$) can be larger than the number $N_b = 2$ in the BB84 protocol. Because of the geometrically uniform structure of information states, there is an exact analytical solution for optimal unambiguous measurements for this family of protocols [2]. An increase in the number of states reduces the probability of conclusive outcomes (correspondingly, increasing the probability of inconclusive outcomes). Nevertheless, at any N_b value, there is the critical length of the communication channel above which the protocol loses security. The eavesdropper knows the entire key, does not generate errors on the receiver side, and is not detected.

This family of protocols is convenient for the analysis of their stability owing to the geometrically uniform structure. The length of the communication channel can seemingly be arbitrarily increased by increasing the number of bases. At the same time, even with ideal photodetectors without dark noise, an increase in the number of bases reduces the efficiency of key generation. In the limit $N_b \longrightarrow \infty$, the critical length formally tends to infinity, $L_c \longrightarrow \infty$. However, the key generation rate approaches zero in this case. Consequently, this family of protocols does not solve the problem of security in long communication channels (correspondingly, with large losses).

Differential Phase Shift and Coherent One-Way Protocols

The differential phase shift (DPS) protocol [9–11] and coherent one-way (COW) protocol [12–15], which is a derivative of the DPS protocol, were also developed in order to "exclude" unambiguous measurements. The DPS protocol is an analog of a protocol used in classical telecommunications. In the DPS protocol, information on the key is encoded in the relative phase difference of a series of weakened coherent states:

$$|e^{i\varphi_1}\alpha_1\rangle \otimes |e^{i\varphi_2}\alpha_2\rangle \otimes \ldots \otimes |e^{i\varphi_{n-1}}\alpha_{n-1}\rangle \otimes |e^{i\varphi_n}\alpha_n\rangle,$$

where $\varphi_i = -\pi, \pi$. The ith bit of the key is 0 at $\varphi_i - \varphi_{i+1} = 0, 2\pi$ and is 1 at $\varphi_i - \varphi_{i+1} = \pm\pi$.

Since bases are absent in the protocol, the key generation rate does not decrease with an increase in the length of the series. Unambiguous measurements cannot be performed with an individual message. However, unambiguous measurements with the entire series simultaneously are possible. In this case, the probability of a conclusive outcome apparently decreases exponentially with an increase in the length of the series. It is also noteworthy that, at large losses and long series, it is unnecessary to perform unambiguous measurements with the entire series simultaneously. The entire sequence can be divided into quite short series and unambiguous measurements can be performed with these series. In this case, the critical error of the protocol to which secret key distribution is guaranteed approaches zero. The last property is alerting. In view of the mutual connection between individual messages, this protocol does not satisfy the quantum de Finetti theorem (for details, see [7]), which allows the reduction of the analysis of the stability of the protocol to attacks on individual messages. For this reason, the stability of the protocol is analyzed incompletely (see, e.g., [1], where this protocol was called a challenge for theorists).

The COW protocol [12–15] is a complication of the DPS protocol. It is based on the same idea of mutual dependence of individual messages at the detection of the eavesdropper. This protocol uses three states including two information states, $|\text{vac}\rangle \otimes |\alpha\rangle$ for 0 and $|\alpha\rangle \otimes |\text{vac}\rangle$ for 1, and one control $|\alpha\rangle \otimes |\alpha\rangle$, where $|\text{vac}\rangle$ is the vacuum state of the field (empty message). The stability of this protocol is also analyzed incompletely for the same reasons as for the DPS protocol.

RELATIVISTIC QUANTUM CRYPTOGRAPHY IN OPEN SPACE

Relativistic quantum cryptography completely solves the problem of security of key distribution through open space with arbitrary losses [16]. The only limitation is due to dark noise of single-photon detectors. (We recall that the above protocols lose security *even with ideal single-photon detectors* when losses are larger than the critical value.) In addition to fundamental exclusions of quantum mechanics of the distinguishability of quantum states, relativistic quantum cryptography involves additional fundamental constraints imposed by relativistic causality [16]. These protocols were specially developed for key distribution through open space. In addition to errors on the receiver side at the detection of actions of the eavesdropper, the protocols proposed in [16] detect delays of states in the channel. In this case, an additional parameter—the distance between the receiver and transmitter sides—appears in the problem. At first glance, the fixation of delays requires the general synchronization of clocks on the transmitter and receiver sides, which should be performed through a classical communication channel that is not controlled by legitimate users. However, it appeared [16] that delays can be detected without the general synchronization of clocks by the two-pass measurement scheme (see the implementation of the protocol in [17]). The protocol guarantees the security of keys at arbitrary losses in the communication channel and a not strictly single-photon source of information quantum states. It can be believed that relativistic quantum cryptography for open space completely solves the problem of exclusion of unambiguous measurements. The picture is physically quite transparent. Unambiguous measurements require access to a quantum state as a whole. If the quantum state is smeared in the Minkowski spacetime (having a finite length), access of the eavesdropper to the state as a whole is equivalent to access (scanning) to a finite part of spacetime. This requires a finite time because of the limit velocity of signal propagation. This circumstance inevitably results in delays (shift) of measurement times on the receiver side, which are detected.

Unfortunately, relativistic quantum cryptography in open space can hardly be transferred to fiber-optic systems. Since the velocity of propagation in a fiber is one and a half times lower than that in open space, it is necessary to strongly stretch quantum states so that the eavesdropper cannot compensate time delays associated with the difference between the speeds of light in a fiber and open space.

NEW PROTOCOL: QUANTUM KEY DISTRIBUTION WITH A CLASSICAL REFERENCE STATE

The analysis above shows that the problem of the loss of security in a channel with losses has not yet been solved. All attempts at a solution are reduced to an increase in the number of information states in order to exclude (more precisely, to reduce) the effect of unambiguous measurements, which results in an increase in the probability of inconclusive outcomes. In the DPS and COW protocols, information is smeared on the entire transmitted sequence. However,

this does not exclude the possibility of unambiguous measurements of the entire sequence simultaneously. Since information is smeared on the whole sequence, the analysis of the stability of the protocol is difficult. Although these protocols were actively studied, even the critical error in a channel without losses is unknown for them. Partial results were obtained for the DPS protocol in the single-photon case. It was shown [11] that the critical error is quite small ($\approx 4.12\%$) when a single-photon state is smeared on n messages. Any results for the COW protocol in the single-photon case are unknown to us. The critical error for the BB84 protocol in the single-photon case is $\approx 11\%$. According to the studies of other protocols, the critical error can only decrease in the case of quasi-single-photon coherent states.

Since states in all messages are coupled to each other, the quantum de Finetti theorem [7], which makes it possible to reduce the analysis of the stability of the protocol to the analysis of states in individual messages, is inapplicable. Finally, partial results of the studies of the stability of the protocol in the channel with losses show that the critical error to which the security of keys can be guaranteed tends to zero with an increase in losses. This indirectly indicates that the protocol does not ensure the security of keys in long communication channels with large losses.

Although the DPS and COW protocols are used in European and Japanese quantum cryptography systems [9–15], uncertainty with their cryptographic security hardly provides a foundation for guaranteed security systems.

A fundamentally new solution to the problem of unambiguous measurements in quantum cryptography is proposed below. The implementation of this protocol and, particularly, the analysis of its stability are fairly simple, which is important in practice. *The preceding protocols were developed in order to reduce the role of unambiguous measurements. The "exclusion" of unambiguous measurements meant only a decrease in the probability of conclusive outcomes and, correspondingly, an increase in the probability of inconclusive outcomes. In the present protocol, unambiguous measurements are completely excluded.*

The idea is the superposition of the quantum and classical parts of the protocol. In any quantum cryptography system (fiber-optic or in open space), an intense (classical) coherent state $|\alpha_{cl}\rangle$ (with a macroscopically large average number of photons $\mu_{cl} = |\alpha_{cl}|^2 \gg 1$) with the same wavelength as information states is used as an intense classical light sync pulse. In some systems, such a pulse is transmitted through a separate auxiliary channel. The use of such intense state is due to the technical part of the protocol—gating of avalanche detectors. This state does not generally enter into the quantum cryptographic part of the protocol. *In this case, the intensity of the state is always such that all sync pulses in each series of messages should be detected. Otherwise, the system signalizes failure in synchronization and the entire series of messages is rejected.* Since the intense classical state is always present, it is reasonable to directly use it in the quantum cryptographic part of the protocol. The protocol is first described below, its implementation is then discussed, and its stability is finally analyzed.

Protocol.

(i) A long series of individual independent messages is transmitted. Each message consists of a pair of states shifted in time by means of a Mach–Zehnder interferometer (see below); these are an information state $|e^{i\varphi_{0,1}}\alpha_q\rangle$ ($|\alpha_q|^2 < 1$) and an intense classical state $|\alpha_{cl}\rangle$ ($|\alpha_{cl}\rangle \gg 1$) – $|e^{i\varphi_{0,1}}\alpha_q\rangle \otimes |\alpha_{cl}\rangle$. Information on the bits of a key is encoded in the phase of a quantum state: $0 \longrightarrow \varphi_0$ and $1 \longrightarrow \varphi_1$.

(ii) Losses $T(L)$ in the communication channel can vary during key distribution.

(iii) Coherent states passing through the communication channel with linear losses are weakened self-similarly: $|e^{i\varphi_{0,1}}\alpha_q\rangle \otimes |\alpha_{cl}\rangle \longrightarrow |e^{i\varphi_{0,1}}\alpha[T(L)]_q\rangle \otimes |\alpha[T(L)]_{cl}\rangle$.

(iv) States on the receiver side are divided by a beam splitter (see below) into two channels:

$$|e^{i\varphi_{0,1}}\alpha[T(L)]_q\rangle \otimes |\alpha[T(L)]_{cl}\rangle$$
$$\rightarrow \begin{pmatrix} |e^{i\varphi_{0,1}}\frac{\alpha[T(L)]_q}{\sqrt{2}}\rangle \otimes |\frac{\alpha[T(L)]_{cl}}{\sqrt{2}}\rangle \\ |e^{i\varphi_{0,1}}\frac{\alpha[T(L)]_q}{\sqrt{2}}\rangle \otimes |\frac{\alpha[T(L)]_{cl}}{\sqrt{2}}\rangle \end{pmatrix}.$$

(v) The intensity in a time window corresponding to the classical coherent state in the second channel (see item (iv)) is measured by a calibrated classical photodetector and a sync pulse for the gating of avalanche detectors is simultaneously generated (see below).

(vi) Since the ratio of the amplitudes of the classical and quantum coherent states $\zeta = \frac{|\alpha_{cl}|^2}{|\alpha_q|^2}$ is known publicly and is an open parameter of the protocol, the online measurement of the intensity of a classical coherent state $|\alpha_{cl}[T(L)]/\sqrt{2}|^2$ makes it possible to weaken it by a factor of $\frac{|\alpha_{cl}[T(L)]|^2}{|\alpha_q[T(L)]|^2}$ in the time window corresponding to the classical state in the first channel (see item (iv)). In this case, the intense state undergoes the transition $|\frac{\alpha_{cl}[T(L)]}{\sqrt{2}}\rangle \rightarrow |\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle$. As a result,

a pair of states identical to the phase factor arises: $|e^{i\varphi_{0,1}}\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle \otimes |\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle$.

(vii) Decoding is performed on the receiver side: a compensating phase is randomly imposed on the state $|e^{i\varphi_{0,1}}\frac{\alpha_q[T(L)]}{\sqrt{2}}\rangle$. After that, a pair is guided to a Mach–Zehnder interferometer at whose output two states interfere with each other (constructively and destructively at two outputs) and are detected in the central time window by single-photon avalanche detectors. *It is fundamentally important that interference occurs between the initial quantum coherent state and the state that originates from the intense coherent state weakened to the same level.*

(viii) The numbers of sent and detected classical pulses are verified through an open channel. When these numbers do not coincide with each other, the entire series is rejected. When these numbers coincide with each other, the protocol is continued as other quantum key distribution protocols.

Thus, unambiguous measurements in this protocol are really excluded. Since information on the key is encoded in the phase of weakened coherent states, the eavesdropper should distinguish one of the nonorthogonal states $|e^{\varphi_0}\alpha_q\rangle$ and $|e^{\varphi_1}\alpha_q\rangle$ (it is assumed in favor of the eavesdropper that the phase α_q is known, e.g., from the classical state). In the case of an inconclusive outcome of the distinguishing of information quantum states, the eavesdropper cannot block the intense classical state (otherwise, the whole series is rejected). For this reason, instead of the weakened information quantum state, the eavesdropper has to send a certain state randomly rather than the true state, e.g., $|e^{i\varphi_0}\alpha_q\rangle$, which results in an error at interference with the weakened classical pulse. Thus, the eavesdropper never can know the entire key without the generation of errors on the receiver side. If the classical pulse with which interference occurs on the interferometer were not presented, the eavesdropper could block messages in which an inconclusive outcome (?) is obtained in unambiguous measurements. In the presence of a classical reference state, unambiguous measurements generate errors on the receiver side. Consequently, the situation that occurs in other protocols discussed above where, beginning with certain losses, the eavesdropper knows the whole key, does not generate errors on the receiver side, and is not detected is excluded.

FIBER-OPTIC IMPLEMENTATION OF THE PROTOCOL

Figure 1 shows the implementation of the protocol. A laser forms a time-localized intense pulse of a coherent state $|\alpha\rangle$ ($|\alpha|^2 \gg 1$). A Mach–Zehnder interferometer with different lengths of the arms transforms one state into two time-shifted states. The lower arm of the interferometer is equipped with a constant attenuator, which weakens the state passing in the lower arm to the quasi-single-photon level $|\alpha_q\rangle$ ($|\alpha|^2 < 1$). At the output of the interferometer, a pair of coherent states including the intense classical and quantum states appears, $|\alpha_q\rangle \otimes |\alpha_{cl}\rangle$. Then, the pair of states passes through a phase modulator. When a quantum state passes through the phase modulator, a voltage pulse is supplied to it, resulting in the appearance of an additional phase in the quantum coherent state $|e^{i\varphi_{0,1}}\alpha_q\rangle \otimes |\alpha_{cl}\rangle$. After that, the states are guided to the communication channel. Evolution in the channel is the same for both states. The pair of states is separated on the receiver side by the beam splitter into two channels. In the second channel in the time window corresponding to the intense state, the classical state is recorded by the calibrated detector. The intensity of the classical state is estimated on-line from the flowing photocurrent. According to the intensity, a voltage pulse is generated on the intensity modulator and weakens the classical state in the first channel to the quasi-single-photon level. After that, the pair of states is guided to the phase modulator, which changes the relative phase, and is then guided to the interferometer, where the states are shifted with respect to each other and undergo constructive and destructive interference. The constant (more precisely, slow) controllable attenuator in the Mach–Zehnder interferometer on the receiver side has two functions. First, it ensures a certain constant attenuation in the short arm. This is necessary because fast intensity modulators (MI in Fig. 1) ensure the attenuation coefficient no more than 60 dB. The fast attenuator (MI), together with the constant attenuator, should ensure the required attenuation coefficient. Second, if losses in the channel do not vary during the transmission of a series, the required attenuation coefficient can be ensured only by the constant attenuator.

ANALYSIS OF THE STABILITY OF THE PROTOCOL WITH RESPECT TO UNAMBIGUOUS MEASUREMENTS

Three types of attacks are possible: (i) unitary attack, (ii) attack with a beam splitter, and (iii) attack with unambiguous measurements. Stability with respect to the first two attacks is guaranteed by the nonorthogonality of states. The full analysis is too lengthy. At present, it is sufficient to demonstrate that the protocol in the communication channel with arbitrary unknown losses is stable with respect to the unambiguous measurement attack.

Since the eavesdropper cannot block the classical reference state and the probability of an inconclusive

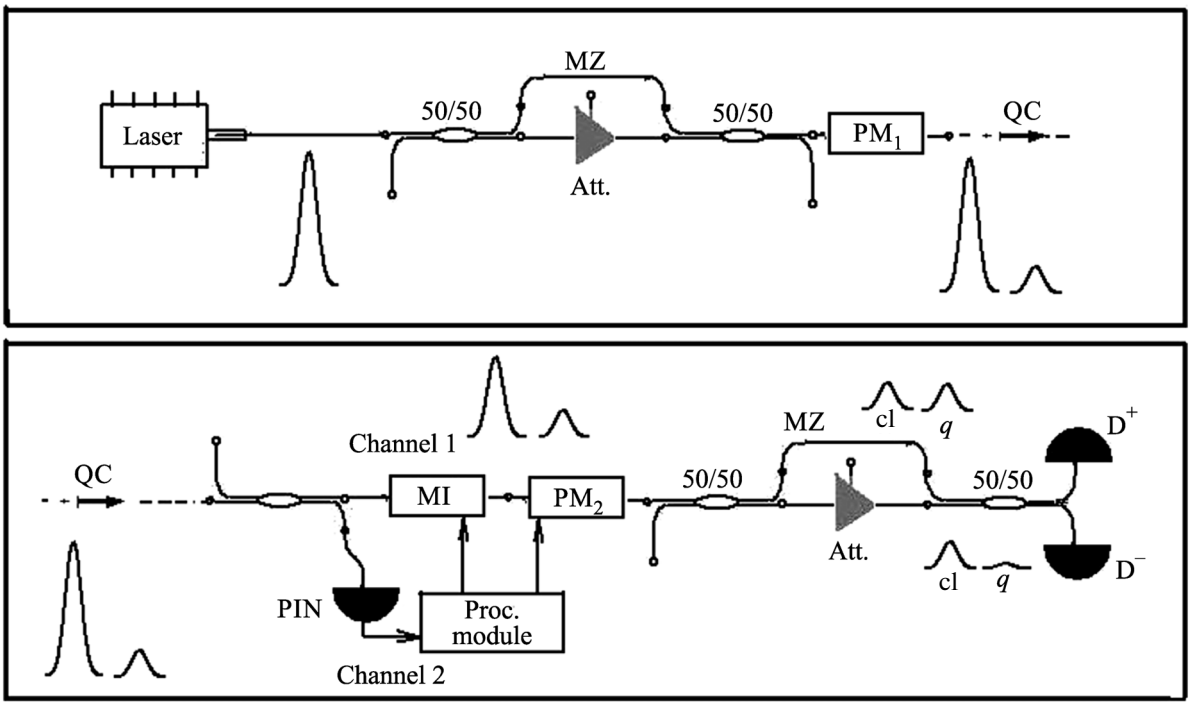

Fig. 1. Functional scheme of the fiber part of the system: (Laser) source of coherent states; (50/50) symmetric beam splitter; (MZ) Mach–Zehnder interferometers with different lengths of arms; (MI) fast intensity modulator; ($PM_{1,2}$) phase modulators, (q and cl) states originating from the intense classical and weakened coherent states, respectively; (Att.) slow controllable attenuator; (proc. module) control electronic module for the generation of a sync pulse and the estimation of the intensity of the classical coherent state; (PIN) calibrated detector; ($D^{\pm}$) single-photon avalanche detectors, and (QC) quantum communication channel.

outcome in measurements of an information quantum state is (see Eq. (4))

$$\Pr(?) = \left|\langle e^{i\varphi_0}\alpha_q \left| e^{i\varphi_1}\alpha_Q\rangle\right|, \tag{5}$$

the conditional entropy in the asymptotic limit of long transmitted sequences per message is given by the expression

$$H(X|Y_E) = (1-p) + p\Pr(?), \tag{6}$$

where $0 \le p \le 1$ is the fraction of messages where the eavesdropper uses unambiguous measurements, X is the transmitted bit string, and Y_E is the bit string of the eavesdropper. In other words, since messages with inconclusive outcome (?) cannot be blocked, in the fraction of messages p, the eavesdropper has to send quantum states randomly instead of true quantum states; as a result, the probability of an error in these messages is 1/2. The conditional Shannon entropy between the legitimate users per message is

$$\begin{aligned} H(X|Y) &= h(Q), \\ h(Q) &= -Q\log Q - (1-Q)\log(1-Q), \\ Q &= \frac{1}{2}p\Pr(?), \end{aligned} \tag{7}$$

where Q is the error generated on the receiver side by unambiguous measurements and Y is the bit string on the receiver side. The length of the secret key is given by the expression (see, e.g., [7])

$$\begin{aligned} R(p, Q) &\ge H(X|Y_E) - H(X|Y) \\ &= (1-p) + p\Pr(?) - h(Q). \end{aligned} \tag{8}$$

In the case of ideal photodetectors without dark noise, the error Q is due only to unambiguous measurements and is $Q = \frac{1}{2}p\Pr(?)$. Formula (8) has an intuitively transparent interpretation. The quantity $H(X|Y_E)$ is the number of information bits that are missed for the eavesdropper to know the transmitted bit sting X entirely if he has only the string Y_E. Similar, $H(X|Y)$ is the number of information bits that are missed for the receiver to know the transmitted bit sting X entirely if he has only the string Y. The difference between these conditional information amounts is a secret key that is unknown to the eavesdropper. Since Pr(?) is a parameter of the protocol and is determined only by the structure of information states, whereas the parameter p is controlled by the eavesdropper, it is convenient to

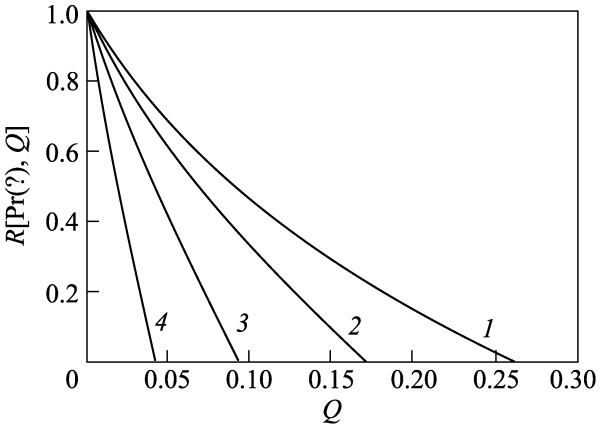

Fig. 2. Length of the secret key R[Pr(?), Q] per position versus the error observed on the receiver side for the parameter Pr(?) = (*1*) 0.75, (*2*) 0.5, (*3*) 0.25, and (*4*) 0.1.

rewrite Eq. (8) in terms of the observed error and Pr(?). Taking into account that $p = 2Q/\Pr(?)$, we have

$$R[\Pr(?), Q] \geq 1 - h(Q) - 2Q\left(\frac{1}{\Pr(?)} - 1\right). \qquad (9)$$

Figure 2 shows the dependences of the length of the secret key on the observed error Q at various Pr(?) values.

CONCLUSIONS

To summarize, the transfer of a classical sync pulse from the technical part of the system to the cryptographic part, together with the on-line measurement of its intensity and subsequent attenuation to the level of the quantum information state, makes it possible to completely exclude unambiguous measurements by the eavesdropper, which are responsible for the loss of security in other protocols in the presence of losses in the communication channel. It is noteworthy that this scheme lifts the requirement on losses, which were considered as a priori known in the preceding variant [18]. In this scheme, losses in the communication channel are not assumed a priori known and can vary during key distribution even in each individual message. Furthermore, each message in this protocol is independent of the preceding message; as a result, the analysis of the stability of the protocol is quite simple and can be performed completely.

I am grateful to D.A. Kronberg and S.P. Kulik for stimulating discussions, as well as to my colleagues at the Academy of Cryptography of the Russian Federation for permanent support.

REFERENCES

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
2. A. Chefles, arXiv/quant-ph: 9807022; A. Chefles and S. M. Barnett, arXiv/quant-ph: 9807023.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, US Patent No. 5307410 (1994).
4. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer Systems and Signal Processing, Bangalore, India, December 1984*, p. 175.
5. D. Mayers, J. ACM **48**, 351 (2001).
6. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
7. R. Renner, PhD Thesis (ETH Zürich, 2005).
8. S. N. Molotkov, JETP Lett. **95**, 332 (2012).
9. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).
10. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nature Photon. **1**, 343 (2007).
11. K. Wen, K. Tamaki, and Y. Yamamoto, arXiv/quant-ph:0806.2684.
12. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, arXiv:quant-ph/0506097.
13. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, arXiv:quant-ph/0609090.
14. C. Branciard, N. Gisin, and V. Scarani, arXiv:quant-ph/0710.4884.v2.
15. D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, arXiv:quant-ph/08095264.
16. S. N. Molotkov, J. Exp. Theor. Phys. **112**, 370 (2012); JETP Lett. **94**, 469 (2011); JETP Lett. **96**, 342 (2012).
17. I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, arXiv:quant-ph/1403.3122; Laser Phys. Lett. **11**, 065203 (2014).
18. S. N. Molotkov, JETP Lett. **93**, 747 (2011).

Translated by R. Tyapaev