ISSN 0021-3640, JETP Letters, 2015, Vol. 101, No. 8, pp. 579–585. © Pleiades Publishing, Inc., 2015.
Original Russian Text © S.N. Molotkov, 2015, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2015, Vol. 101, No. 8, pp. 637–643.

On the Security of Fiber Optic Quantum Cryptography Systems without the Control of the Intensity of Quasi-Single-Photon Coherent States

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

Received February 9, 2015; in final form, March 10, 2015

Internal losses in systems of quantum cryptography can be used at attacks by an eavesdropper. As a result, the security of keys cannot be ensured for a number of protocols. This problem can be solved by using geometrically uniform coherent states with a larger number of bases. The security of keys at the number of bases $N_b/2 = 4$ and the number of states $N_b = 8$ can be guaranteed even without the control of the intensity of input states.

DOI: 10.1134/S002136401508010X

INTRODUCTION

Quantum cryptography systems serve for the distribution of secret cryptographic keys through an open quantum communication channel accessible for passive and active invasion. A classical authentic auxiliary communication channel for exchange of classical information between legitimate users at coordination of the bases (if this is required in a protocol), correction of errors in primary keys, and final compression (hashing, i.e., enhancement of security) of cleaned keys is also accessible for eavesdropping. The security of keys in quantum cryptography is guaranteed by fundamental quantum mechanical exclusions of the distinguishability of orthogonal quantum states. The security of the BB84 protocol [1] was exactly proved for the case of a strictly single-photon source of quantum states and finite lengths of transmitted sequences. The proof [2] is based on fundamental entropy uncertainty relations and does not involve assumptions on attacks of an eavesdropper against distributed keys. Real quantum states are quasi-single-photon weakened coherent states. In addition, losses in the communication channel together with quasi-single-photon states open possibilities for new attacks that are impossible in the single-photon case.

The BB84 protocol in real systems uses four coherent states including two states in each basis. The states in the + basis are $0 \to |\alpha\rangle$ and $1 \to |-\alpha\rangle$ and the states in the × basis are $0 \to |i\alpha\rangle$ and $1 \to |-i\alpha\rangle$. The complex parameters α_i ($i = 0, 1, 2, 3$) describing information states are uniformly located on a circle in the complex plane. As will be shown below, the BB84 protocol cannot guarantee the security of keys in real systems in the presence of losses in the channel and inevitable losses inside a receiver. Therefore, it is necessary to use protocols with large numbers of information states and bases.

One of such protocols is the protocol on geometrically uniform states (BB84 protocol is a particular family of such protocols). The number of bases $N_b/2 = 4$ appears to guarantee the security of keys in real systems. Information states are geometrically uniform coherent states $|\alpha_j\rangle = U^j|\alpha\rangle$ obtained by geometric shift (unitary rotation U^j, $U^N = I$), where $\alpha_j = \exp\left(i\frac{2\pi}{N_b}j\right)\alpha$ ($j = 0, 1, \ldots, N_b - 1$). The protocol involves $N_b/2 = 4$ bases. Each basis includes a pair of nonorthogonal states with $|\alpha_j\rangle$ and $|\alpha_{j+1}\rangle$ corresponding to 0 and 1.

CRITERION OF THE CORRECTNESS AND SECURITY OF KEYS

Any quantum key distribution protocol consists of the following stages:

(i) transfer of quantum states from Alice to Bob and their measurement on the receiver side (and, if it is necessary as in the BB84 protocol, the coordination of the bases—rejection or fixation of messages in which bases do not coincide or coincide); (ii) estimation of the probability of an error and correction of errors through an open classical channel; (iii) estimation of Eve's information at the observed error on the receiver side, its change after the correction of errors, and subsequent compression (privacy amplification) of cleaned keys.

The Alice–Bob–Eve situation after stage (i) is described by the joint density matrix $\rho^n_{XX'E}$, where X^n and X'^n are the bit strings of Alice and Bob (the latter string can contain errors), respectively, and $\rho^n_E = \mathrm{Tr}_{XX'}\{\rho^n_{XX'E}\}$ is the quantum system accessible for Eve. Taking into account information that Eve receives from the quantum communication channel and additional classical information at the correction of errors from the classical communication channel, Alice and Bob compress cleaned keys for Eve to obtain no information on the final secret key. A protocol should satisfy the criteria of correctness and security [3]. The correctness means that Alice's and Bob's keys after the correction of errors should be identical with a given probability $\varepsilon_{\mathrm{corr}}$,

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

where X^n and X'^n are the bit strings of Alice and Bob after the correction of errors, respectively.

A protocol is informally secret if Alice's bit string X^n does not correlate with Eve's quantum system ρ^n_E. The absence of correlations between Alice's string and Eve's quantum system means that the joint Alice–Eve density matrix (ρ^n_{XE}) is separated into the product of the density matrices of two systems, ($\rho^n_U \otimes \rho^n_E$) (ideal situation). Here, ρ^n_U is Alice's density matrix describing the uniform distribution of classical bit strings:

$$\rho^n_U = \frac{1}{2^n}\sum_{i_1, i_2, \ldots, i_n = 0, 1} |i_1\rangle\langle i_1| \otimes |i_2\rangle\langle i_2| \otimes \ldots \otimes |i_n\rangle\langle i_n|.$$

A measure of the security of keys is the trace distance between the real Alice–Eve density matrix (ρ^n_{XE}) and uncorrelated Alice–Eve density matrices ($\rho^n_U \otimes \rho^n_E$) (ideal situation). A protocol should guarantee that the trace distance Δ between these density matrices can be made smaller than a preset value $\varepsilon_{\mathrm{secr}}$:

$$\Delta = \frac{1}{2}\left\|\rho^n_{XE} - \rho^n_U \otimes \rho^n_E\right\|_1 < \varepsilon_{\mathrm{secr}}, \quad (2)$$

where the trace distance between two operators is defined as $\|\rho_1 - \rho_2\|_1 = \mathrm{Tr}\{|\rho_1 - \rho_2|\} = \mathrm{Tr}\{\sqrt{(\rho_1 - \rho_2)^2}\}$. In this case, the protocol is called $\varepsilon_{\mathrm{secr}}$-secret. Eve obtains a fraction of information from the quantum channel through attacks against quantum states. At the correction of errors, classical correcting information, which is also accessible to Eve, is transferred through the classical channel. In addition, after the correction of errors, keys are compressed through the open classical channel: Alice sends information on the hash function. These circumstances should be taken into account in Eq. (2). They can be taken into account through the leftover hash lemma [4] according to which the trace distance after the correction of errors and compression of the cleaned key by universal second order hash functions [5] becomes

$$\Delta = \frac{1}{2}\sqrt{2^{-[H^\varepsilon_{\min}(X^n|C^nE^n) - R_n]}}, \quad (3)$$

where $H^\varepsilon_{\min}(X^n|C^nE^n)$ is the smoothed conditional min-entropy and C^n includes correcting information sent by Alice to Bob through the open channel. By definition,

$$H^\varepsilon_{\min}(X^n|C^nE^n) = \sup_{\tilde\rho^n_{CE}} H_{\min}(\tilde\rho^n_{XCE}|\tilde\rho^n_{CE}),$$

where

$$H_{\min}(\tilde\rho^n_{XCE}|\tilde\rho^n_{CE}) = -\log\lambda.$$

Here, λ is the minimum number such that

$$\lambda I_X \otimes \tilde\rho^n_{CE} - \tilde\rho^n_{XCE} > 0, \quad \left\|\tilde\rho^n_{CE} - \rho^n_{CE}\right\|_1 < \varepsilon.$$

In this case, we accept that $\mathrm{Tr}(\tilde\rho^n_{CE}) = 1$. A protocol is ε-secret [3] if the length of the final secret key is

$$R_n \leq H^\varepsilon_{\min}(X^n|C^nE^n) - 2\log(1/2\varepsilon). \quad (4)$$

The following estimate can be obtained for $H^\varepsilon_{\min}(X^n|C^nE^n)$ [3]:

$$H^\varepsilon_{\min}(X^n|C^nE^n) \geq H^\varepsilon_{\min}(X^n|E^n) - \mathrm{leak}_n - 2\log(1/2\varepsilon), \quad (5)$$

where leak_n is classical information in bits transmitted through the open channel at the correction of errors, which is determined only by the correction procedure. Formula (5) has intuitively transparent interpretation. The quantity $H^\varepsilon_{\min}(X^n|C^nE^n)$ presents deficit of information required for Eve to entirely know Alice's bit string under the condition that Eve has the quantum system E and classical information $C(\rho^n_{CE})$.

In the asymptotic limit of long sequences ($n \to \infty$, i.e., automatically $\varepsilon \to 0$), the smoothed entropy tends to the conditional von Neumann entropy [3] (Shannon entropy in the classical case), $H^\varepsilon_{\min}(X^n|C^nE^n) \to H(X^n|C^nE^n)$, which has the meaning of Eve's deficit of information. The smoothed conditional entropy $H^\varepsilon_{\min}(X^n|C^nE^n)$ informally has the meaning of deficit of information required for Eve to entirely know the bit string X^n under the condition that she has the quantum system E^n together with classical information C^n transmitted through the classical channel at the correction of errors. Roughly speaking, $H^\varepsilon_{\min}(X^n|C^nE^n)$ is equal to the number of bits unknown

to Eve after all stages of the protocol. Inequality (5) allows separating Eve's information obtained from the quantum and classical communication channels.

The above interpretation is applicable if the density matrices are exactly known (e.g., in the asymptotic limit). In the real situation with finite lengths of sequences, density matrices can only be estimated with a certain accuracy with respect to the true density matrix. Only proximity to the true density matrix with accuracy ε in the sense of the trace distance can be guaranteed. The smoothed entropy $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ is the lower bound of deficit of Eve's information in the set of density matrices that are ε-close to the true density matrix.

SINGLE-PHOTON CASE

The single-photon case is a special case for the BB84 protocol. In this case, the no-cloning theorem guarantees that obtaining information on transmitted nonorthogonal states by Eve inevitably results in the perturbation of states and in the appearance of errors on the receiver side. A remarkable result was obtained [2] with the use of fundamental entropy uncertainty relations for the smoothed entropies for three-body Alice–Bob–Eve density matrix $\rho^n_{XX'E}$:

$$\frac{1}{n}[H^{\varepsilon}_{\min}(X^n|E^n) + H^{\varepsilon}_{\min}(Z^n|Z'^n)] \geq 2\log(1/c), \quad (6)$$

where

$$c = |\langle 0(X)|0(Z)\rangle| = 1/\sqrt{2}.$$

Here, $|0(X)\rangle$ and $|0(Z)\rangle$ are information states in the direct (X) and conjugate (Z) bases, respectively. The right-hand side of Eq. (6) is independent of the density matrix $\rho^n_{XX'E}$ and is determined only by the BB84 protocol itself. The quantity $H^{\varepsilon}_{\min}(Z^n|Z'^n)$ is purely classical, determines the minimum number of information bits necessary for the correction of errors in Bob's bit string Z'^n, and is related to the error Q. Furthermore, because of the symmetry of the protocol with respect to the bases X and Z, $H^{\varepsilon}_{\max}(Z^n|Z'^n) = H^{\varepsilon}_{\max}(X^n|X'^n)$. This fact and Eq. (6) make it possible to express $H^{\varepsilon}_{\min}(X^n|E^n)$ in terms of $H^{\varepsilon}_{\max}(X^n|X'^n)$: $H^{\varepsilon}_{\min}(X^n|E^n) > 1 - H^{\varepsilon}_{\max}(X^n|X'^n)$. The length of the secret key is

$$R_n \leq 1 - 2H^{\varepsilon}_{\max}(X^n|X'^n). \quad (7)$$

In the asymptotic limit $n \to \infty$, the smoothed entropy tends to the Shannon conditional entropy, $H^{\varepsilon}_{\max}(X^n|X'^n) \to nH(X^n|X')$, and $\text{leak}_n \to nH(X^n|X')$. For the binary channel with the error Q, $\text{leak}_n = nh(Q)$. In this limit, Eq. (7) gives the remarkable equation for the critical error of the BB84 protocol to which the secret key distribution is guaranteed: $1 = 2h(Q_c)$, $Q_c \approx 11\%$ [6]. *Fundamental entropy uncertainty relations* (6) *for single-photon states make it possible to relate the leakage of information to Eve to the error observed on the receiver side and to avoid the choice of the optimal attack among all possible Eve's attacks.* We note that the optimal attack can be constructed in an explicit form [7]. *Unfortunately, this remarkable fundamental result* [2] *cannot be carried over to real quantum cryptography systems. The main difficult is in the estimate of* $H^{\varepsilon}_{\min}(X^n|E^n)$*, which contains the entire information on Eve's attack.*

SECURITY IN THE QUASI-SINGLE-PHOTON CASE OF COHERENT STATES

The situation is fundamentally different if quasi-single-photon coherent states are used as information states. The set of N_b states is linearly independent, which is a necessary and sufficient condition of the existence of unambiguous measurements. Performing an unambiguous measurement, Eve breaks the channel with losses (near Alice and Bob). A certain outcome (break near Alice) can be obtained with the probability 1 – Pr(?). In this case, Eve resends correct states to Bob (from the second break). If an uncertain outcome is obtained (with the probability Pr(?)), Eve resends nothing. If the probability of losses in the channel is Pr[Loss(ch)] > Pr(?), Eve knows the entire key, does not induce errors on the receiver side, and is not detected. Thus, the key is not secret beginning with a certain length of the channel (and losses).

Such an estimate is incorrect. It is fundamentally important to take into account not only losses in the communication channel but also losses in the receiver part of systems. Below, losses are treated as total losses in a given sequence as the ratio of the numbers of the sent and detected messages, $\Pr(\text{Loss}) = N_{\text{det}}/N_{\text{send}}$. Even at Pr[Loss(ch)] < Pr(?), Eve can perform unambiguous measurements, using losses in the receiver part. The total losses are determin $\eta \approx 0.1$–0.25), average number of photons ($\mu \approx 0.1$–0.25) in the coherent state, losses in the receiver optical part, and losses in the channel. It is noteworthy that internal losses are $1 - \eta\mu \approx 1 - 10^{-2}$, which are equivalent to losses at a length of 100 km of a line based on SMF-28 fiber. It seems that Eve cannot compensate internal losses without access to the receiver part of the system. However, this is not the case. Eve can compensate losses inside the system by sending more intense states such that each resent message after unambiguous measurements is detected. For real avalanche detectors, the average number of photons immediately in the detector itself sufficient for guaranteed detection is $\mu \approx 50$–60 [8]. The resending of more intense correct states for protocols with bases results in simultaneous counts in two avalanche detectors in messages where Alice's and Bob's bases do not coincide and does not result in

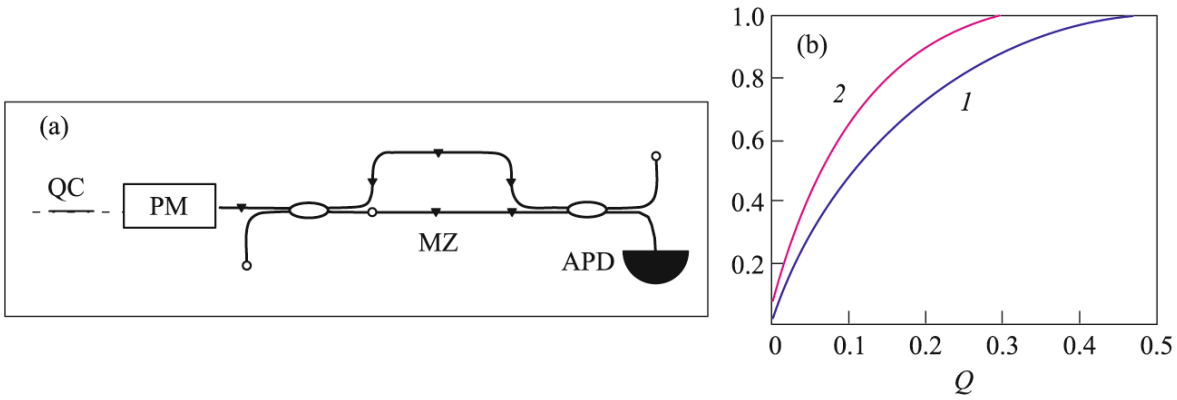

Fig. 1. (a) Layout of the receiver part of the fiber optic quantum cryptography system: (PM) phase modulator, (APD) avalanche single-photon detector, (MZ) Mach–Zehnder interferometer, (QC) quantum channel. (b) Line *1* is the binary Shannon entropy function $h(Q)$ and line *2* is the function $\mathrm{leak}_{\infty}^{\mathrm{Ham}}(Q)$ (see main text).

erroneous counts in messages where these bases coincide. A change in the rates of double counts requires the recalculation to the leakage of information to Eve. However, since avalanche detectors do not distinguish the average number of photons, a change in the count rate requires additional assumptions on the count rate from the number of photons, which is unacceptable. The decoy state protocol [9] is in fact based on such assumptions. These assumptions inevitably affect the length of the final secret key. Even if this circumstance is ignored, the number of double counts of avalanche detectors should be recalculated to take into account the leakage of information to Eve. Such a problem is very difficult and has not yet been solved appropriately.

REQUIREMENTS TO THE FORMULA FOR THE LENGTH OF THE SECRET KEY

The length of the secret key should depend only on (i) the observed error on the receiver side, (ii) the numbers of sent and detected states at coinciding bases, and (iii) the structure of a quantum state sent through the communication channel. The quantum efficiency of detectors, the probability of dark noise, and the number of double counts are the internal parameters. The length of the secret key should be independent of losses in the internal optical part and channel, because they are unknown and can vary in each message.

QUANTUM KEY DISTRIBUTION PROTOCOL WITHOUT INTENSITY CONTROL

Information states are geometrically uniform coherent states [10] weakened to a quasi-single-photon level. The average number of photons in a state is $\mu = |\alpha|^2$. The number of information states is specified by the number of bases N_b ($N_b/2 = 2, 3, 4, \ldots$). Each basis includes a pair of nonorthogonal states $|\varphi_{ib}\rangle = |\alpha_j\rangle$, corresponding to 0 and 1 ($i = 0, 1$, $b = 1, \ldots, N_b/2$ is the index of a basis). Any ith state is obtained by unitary rotation: $|\alpha_i\rangle = U^i|\alpha_0\rangle$, where $\alpha_i = \alpha\exp(i\varphi_i)$ ($i = 0, \ldots, N_b - 1$). Information states are geometrically uniform coherent states $|\alpha_j\rangle = U^j|\alpha\rangle$ obtained by unitary rotation U^j, $U^{N_b} = I$, where $\alpha_j = \exp(i\frac{2\pi}{N_b}j)\alpha$ ($j = 0, 1, \ldots, N_b - 1$). The measurement circuit of the receiver part contains one detector (Fig. 1). In this case, double counts are disregarded automatically. This scheme with one detector is resistant against active blinding and mismatch attacks against avalanche detectors and can be implemented in both one- and two-pass variants.

ATTACKS WITH UNAMBIGUOUS MEASUREMENTS

We discuss an attack with unambiguous measurements and obtain the length of the secret key in the asymptotic limit. Eve performs unambiguous measurements in the fraction δ of messages. She obtains certain and uncertain outcomes in $\delta \cdot [1 - \Pr(?)]$ and $\delta \cdot \Pr(?)$ messages, respectively. Then, Eve rejects these messages. In messages where a certain outcome was obtained, Eve resends more intense coherent states $|\alpha^*\exp(i\varphi_i)\rangle$, which are certainly detected. In the remaining $1 - \delta$ messages, she performs individual measurements, trying to distinguish states with the minimum probability of an error. Let the result of the measurement be interpreted as $|\alpha\exp(i\varphi_i)\rangle$ (possibly with an error). Then, Eve resends more intense states $|\alpha^* \exp(i\varphi_i)\rangle$ instead of the initial quasi-single-photon state in order to compensate losses in the receiver part. The structure of geometrically uniform states determines the probability of an uncertain outcome, for which the exact solution exists [11]:

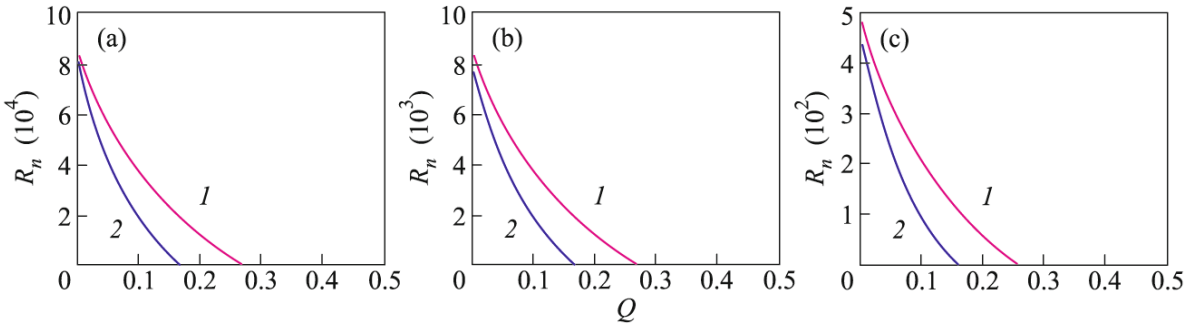

Fig. 2. Length of the secret key in the asymptotic limit at losses Pr(Loss) = (a) 0.99, (b) 0.999, and (c) 0.9999 for the protocol on geometrically uniform states, $N_b = 8$ is the number of states, and $N_b/2 = 4$ is the number of bases. Lines *1* and *2* correspond to the correction of errors by Shannon random codes and Hamming codes, respectively (see main text). The number of transmitted bits at coinciding bases is $n = 10^7$ and $\mu = 0.4$.

$$\Pr(?) = 1 - \min_r \left| \sum_{j=0}^{N_b - 1} e^{\mu\left(e^{i\frac{2\pi j}{N_b}} - 1\right)} e^{-i\frac{2\pi jr}{N_b}} \right|, \quad (8)$$
$$0 \le r \le N_b - 1.$$

LENGTH OF THE SECRET KEY IN THE ASYMPTOTIC LIMIT

We now determine the length of the secret key in the asymptotic limit $n \to \infty$. After the coordination of bases, it is

$$R_n = H(X^n|E^n) - \mathrm{leak}_n. \quad (9)$$

Let n be the number of sent messages in which bases coincide and $n[1 - \Pr(\mathrm{Loss})]$ be the number of detected messages:

$$n[1 - \Pr(\mathrm{Loss})] = n\delta[1 - \Pr(?)] + n(1 - \delta),\ n \to \infty, \quad (10)$$

where the first term is the number of messages for which a certain outcome was obtained and the second term is the number of messages for which individual measurements were performed. Here, it is important that *an unambiguous-measurement attack is possible even if the probability of total losses Pr(Loss) is smaller than the probability of an uncertain outcome Pr(?). The optimal fraction of messages in which Eve performs unambiguous measurements is* $\delta = \Pr(\mathrm{Loss})/\Pr(?) \le 1$. *The critical value is* $\delta_c = 1$ *(*$\Pr(\mathrm{Loss}) = \Pr(?)$*). In this case, Eve knows the entire key and does not induce errors on the receiver side*. As a result,

$$R_\infty = \lim_{n\to\infty} \frac{R_n}{n} = [1 - \Pr(\mathrm{Loss})](1 - \mathrm{leak}_\infty) \quad (11)$$
$$- [1 - \Pr(\mathrm{Loss},?)]C_1(N_b) - \Pr(\mathrm{Loss},?)[1 - \Pr(?)],$$

where $\Pr(\mathrm{Loss},?) = \Pr(\mathrm{Loss})/\Pr(?)$. We emphasize that *the estimate of the leakage of information* $H(X^n|E^n)$ *to Eve is not related to the estimate of the probability of error,* in contrast to single-photon case given by Eqs. (6) and (7). *For* $H(X^n|E^n)$*, the upper conservative estimate is used.* The correction of errors in the Shannon limit requires the transmission of $\mathrm{leak}_\infty^{\mathrm{Shan}}(Q) = h(Q)$ bits per position, where Q is the estimate of the probability of error, through the open channel [12]. In the real situation, constructive procedures are used to correct errors. In particular, for the procedures based on Hamming codes with the additional test of the parity and the length of a code word $(2^m - 2m - 1, m)$, $m = 3, 4, 5$, depending on the probability of error (one error per block on average), it is necessary to open $(n \to \infty)$ $\mathrm{leak}_\infty^{\mathrm{Ham}}(Q) = 1 - (0.99827\exp(-Q/0.112922) - 0.06851)$ bits [8]. Formula (11) includes only observables: the total losses Pr(Loss), the number of opened bits at correction leak_∞, the probability of an uncertain outcome Pr(?), and the classical transmission capacity of the quantum channel per one shot $C_1(N_b)$, which depend only on the structure of information states. The length of the key calculated by Eq. (11) is shown in Fig. 2.

LENGTH OF THE SECRET KEY AT FINITE LENGTHS OF TRANSMITTED SEQUENCES

We now calculate the length of the secret key in the limit of finite transmitted sequences. Here, the number n has the same meaning as above. Depending on the estimate of the error Q, a certain classical correcting code is chosen. Let $n\,\mathrm{leak}(n, Q)$ be the number of bits transmitted through the open channel at the correction of errors for a given particular sequence with the length n. After the correction of errors, it is necessary to test the identity of cleaned keys of Alice (X_A) and Bob (X_B). One of the procedures involves the comparison of the parity bits X_A and X_B with the random string X_rand with the same length through the open channel: $\mathrm{Parity}(X_\mathrm{rand} \oplus X_\mathrm{A})$, $\mathrm{Parity}(X_\mathrm{rand} \oplus X_\mathrm{B})$. The generation of the random string is open. If the parity bits after M repetitions of this procedure coincide, the probability that cleaned keys do not coincide is

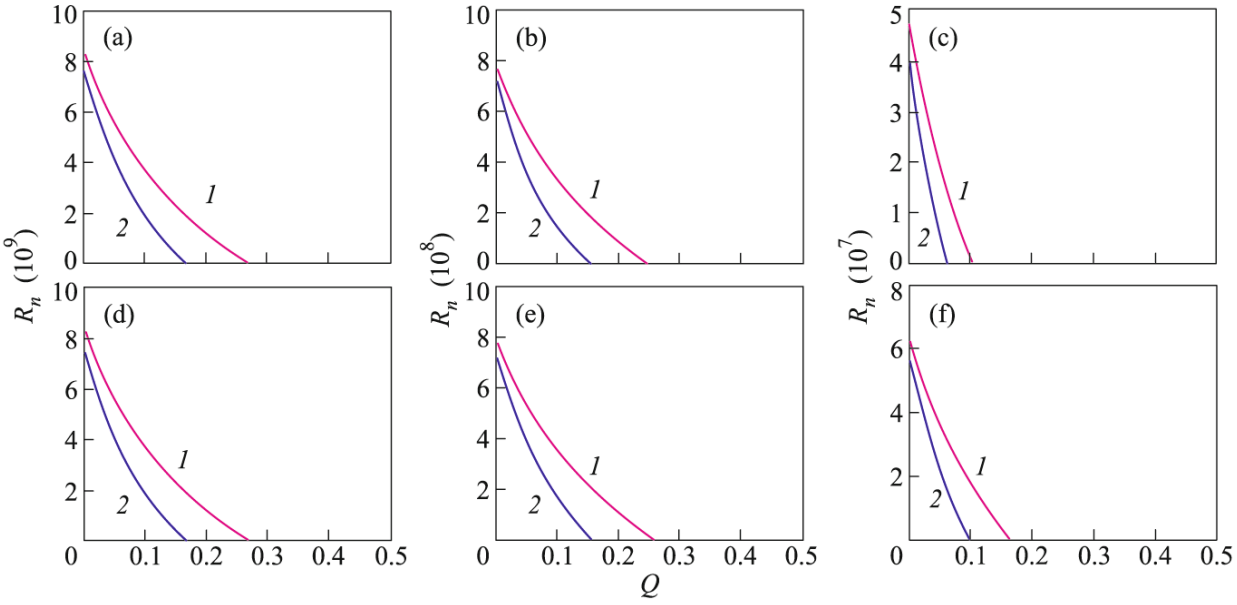

Fig. 3. Length of the secret key at a finite length of the sequence with losses Pr(Loss) = (a, d) 0.99, (b, e) 0.999, and (c, f) 0.9999 for the protocol on geometrically uniform states, $N_b = 8$ is the number of states, and $N_b/2 = 4$ is the number of bases. Lines *1* and *2* correspond to the correction of errors by Shannon random codes and Hamming codes, respectively (see main text). The number of transmitted bits at coinciding bases is $n = 10^{12}$, $\mu = 0.4$, and $\varepsilon_? = \varepsilon_c =$ (a–c) 10^{-32} and (d–f) 10^{-9}.

$\Pr[X_A \neq X_B] < (1/2)^M$. After these stages, Eve obtains $n\,\mathrm{leak}(n, Q) + M$ bits of information, which will be rejected from the key at the privacy amplification stage. If the length of the final key satisfies the inequality

$$R_n \leq H^{\varepsilon}_{\min}(\rho^n_{XE}|\rho^n_E) - n\mathrm{leak}(n, Q) - M - 2\log(1/2\varepsilon), \quad \varepsilon = \varepsilon_? + \varepsilon_c \tag{12}$$

the key is ε-secret.

It is necessary to recall that n messages refer to the case where Alice's and Bob's bases are already coordinated (identical). In view of the superadditivity of the smoothed min-entropy, we obtain (details see in [3])

$$\begin{aligned} &H^{\varepsilon_? + \varepsilon_c}_{\min}(\rho^n_{XE}|\rho^n_E) \\ &= H^{\varepsilon_? + \varepsilon_c}_{\min}(\rho^{n\delta}_{XE} \otimes \rho^{n(1-\delta)}_{XE}|\rho^{n\delta}_E \otimes \rho^{n(1-\delta)}_E) \\ &> H^{\varepsilon_?}_{\min}(\rho^{n\delta}_{XE}|\rho^{n\delta}_E) + H^{\varepsilon_c}_{\min}(\rho^{n(1-\delta)}_{XE}|\rho^{n(1-\delta)}_{XE}). \end{aligned} \tag{13}$$

The estimate of the entropy $H^{\varepsilon}_{\min}(\rho^{n\delta}_{XE}|\rho^{n\delta}_E)$ for the part of unambiguous measurements is reduced to the situation of the classical binary channel with *blocking* (do not confuse with the channel with erasing). The probability of the erasing outcome is Pr(?). As a result,

$$\begin{aligned} &(H^{\varepsilon_?}_{\min}(\rho^{\otimes n\delta}_{XE}|\rho^{\otimes n\delta}_E) > n_\delta[H(\rho_{XE}|\rho_E) - \delta_?]) \\ &= n_\delta[\mathrm{PR}(?) - \delta_?], \quad n_\delta = n\delta, \quad n_? = n\Pr(?), \end{aligned} \tag{14}$$

where $\delta_? = \log(5)\sqrt{2\log(1/2\varepsilon_?)/n_\delta}$. In the remaining part of messages $n(1-\delta)$, Eve performs individual measurements:

$$\begin{aligned} &H^{\varepsilon_c}_{\min}(\rho^{\otimes[n(1-\delta)]}_{XE}|\rho^{\otimes[n(1-\delta)]}_E) \\ &> (n - n_\delta)[H(\rho_{XE}|\rho_E) - \delta_c] \\ &= (n - n_\delta)[1 - C_1(N_b) - \delta_c], \end{aligned} \tag{15}$$

where $\delta_c = \log(5)\sqrt{2\log(1/2\varepsilon_c)/(n - n_\delta)}$. In this case, $H(\rho_{XE}|\rho_E)$ is limited by $1 - C_1(N_b)$. Here, the conservative estimate was taken in favor of Eve. The quantity $C_1(N_b)$ should be calculated for a quantum ensemble of N_b states before the opening of the bases. We assume in favor of Eve that she knows a basis and should only distinguish a pair of states inside the basis. In this case, $H(\rho_{XE}|\rho_E) \geq H(\rho_{XEB}|\rho_{EB})$ (here, ρ_{XEB} and ρ_{EB} are the density matrices in the known basis). In addition, Eq. (15) includes the transmission capacity per shot rather than the Holevo value (transmission capacity $\bar{C}(N_b)$) [13]. This is due to the duality of quantum communication channels [14, 15]. The value $\bar{C}(N_b)$ is reached on collective measurements on the known code table of the sequence of quantum states. In our case, such a table is absent and Eve should distinguish quantum states "on-line" [16]. Owing to the property of duality for quantum channels, collective measurements without a code table provide no more information than optimal individual measurements. For two states, the transmission capacity per shot is given by

the expression [13] $C_1(N_b) = (\xi^-\log\xi^- + \xi^+\log\xi^+)/2$, where $\xi^\pm = 1 \pm \sqrt{1-\varepsilon_b^2}$ and $\varepsilon_b = |\langle\alpha_i|\alpha_{i+1}\rangle|$ is the scalar product of the states in the same basis.

As a result, the length of the secret key is

$$\begin{aligned}\frac{R_n}{n} &= (1 - \Pr(\text{Loss}))[1 - \text{leak}(n, Q) - M] \\ &- [1 - \Pr(\text{Loss},?)][C_1(N_b) + \delta_c] \\ &- \Pr(\text{Loss},?)[1 - \Pr(?) + \delta_?],\end{aligned} \tag{16}$$

where $n[1 - \Pr(?)][\text{leak}(n, Q) + M]$ is the number of really opened bits for a given sequence with the length $n[1 - \Pr(?)]$ (the number of detected counts at the coinciding bases). The calculated lengths of the secret key are shown in Fig. 3.

CONCLUSIONS

Internal losses in any quantum cryptography system are about $1 - \eta\mu \approx 1 - 10^{-2}$ even at zero length of the communication channel. Eve can use these losses at attacks on the key by resending more intense states in order to compensate these losses. As a result, protocols with a small number of information states, e.g., the BB84 protocol and similar protocols, cannot ensure the security of keys because the probability of the uncertain outcome Pr(?) is small. For a protocol with eight states, the probability of the uncertain outcome is $\Pr(?) \approx (1 - 10^{-6})$–$(1 - 10^{-8})$ (at $\mu = 0.4$–0.25), which makes it possible to ensure the security at losses in the channel of 1–10^{-4}. Furthermore, in this case, it is not necessary to control the intensity of input states on the receiver side and, correspondingly, to recalculate the change in the rate of double counts taking into account the leakage of information to Eve.

I am grateful to my colleagues at the Academy of Cryptography of the Russian Federation for permanent support and to S.P. Kulik and A.N. Klimov for numerous stimulating discussions.

REFERENCES

1. C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in *Proceedings of the IEEE international Conference on Computers, Systems & Signal Processing Bangalore, India, December 1984*, p. 175.
2. M. Tomamichel, C. C. Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 634 (2011).
3. R. Renner, arXiv/quant-ph:0512258.
4. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, arXiv/quant-ph:10022436.
5. J. L. Carter and M. N. Wegman, J. Comput. Sys. Sci. **18**, 143 (1979).
6. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
7. S. N. Molotkov and A. V. Timofeev, JETP Lett. **85**, 524 (2007).
8. A. N. Klimov, private commun.
9. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
10. S. N. Molotkov, JETP Lett. **95**, 342 (2012).
11. A. Chefles, arXiv/quant-ph:9807022; A. Chefles and S. M. Barnett, arXiv/quant-ph:9807023.
12. R. G. Gallager, *Information Theory and Reliable Communication* (Wiley, New York, 1968).
13. A. S. Holevo, *Introduction to Quantum Theory of Information*, Ser. Modern Mathem. Physics, No. 5 (MTsNMO, Moscow, 2002); Usp. Mat. Nauk **53**, 193 (1998).
14. A. S. Holevo, arXiv:quant-ph/1103.2615.
15. G. M. D'Ariano, and M. F. Sacchi, arXiv:quant-ph/11031972.
16. D. A. Kronberg and S. N. Molotkov, JETP Lett. **100**, 279 (2014).

Translated by R. Tyapaev