Quantum Electronics **50** (5) 454–460 (2020)

https://doi.org/10.1070/QEL17286

Possibilities of using practical limitations of an eavesdropper in quantum cryptography

A.S. Avanesov, D.A. Kronberg

Abstract. **An important advantage of quantum cryptography over classical cryptography consists in the fact that the security of the transmitted keys is not related to the assumptions about the eavesdropper capabilities and is guaranteed by the laws of nature. Nevertheless, in some situations it makes sense to consider some reasonable assumptions about the eavesdropper capabilities, which can increase the secret key distribution rate. Methods are proposed for legitimate users to employ some practical limitations, and attacks are constructed that the eavesdropper can apply under the conditions of these limitations.**

Keywords: *quantum cryptography, coherent states, pseudo-random generators.*

1. Introduction

The most important property of quantum cryptography, first proposed in [1], consists in the fact that it does not use the assumptions about computational capabilities of an eavesdropper, but relies on a fundamental prohibition on extracting complete information from nonorthogonal quantum states.

Nevertheless, quantum cryptography still uses a number of assumptions, including the presence of random number generators at legitimate users' disposal and the correct operation of transmitting and receiving devices. If an eavesdropper relies on equipment imperfections that are unknown to legitimate users (including those caused by eavesdropper actions such as laser damage), the security of quantum cryptography can be totally compromised [2–6]. This can also occur when the eavesdropper intervenes in the operation of random number generators, as a result of which the eavesdropper receives information about the generated sequences. In addition, the unconditional security of the transmitted data is possible only when use is made of a one-time pad key [7], which, due to existing restrictions on the key generation rate, is not always effectively implemented in practice. In most cases, to receive secret messages, distributed keys are used in classic encryption algorithms, such as AES.

On the one hand, quantum cryptography exhibits a trend to reduce the number of assumptions. Thus, quite popular is the concept of quantum cryptography, the cryptographic security of which does not use assumptions about the properties of measuring devices [8], including those at the eavesdropper disposal, since a significant part of the works on cracking quantum cryptography systems is devoted to attacks on measuring devices. The next step is the concept of quantum cryptography, whose security does not depend on any devices [9–11]. In this case, the only requirement consists in the fact that legitimate users have device-independent random number generators, the hardware independence of which is now being transformed from a concept to a practical application [12]. However, taking into account such capabilities of the eavedropper or imperfect components of the protocol elements leads to a decrease in the key generation rate.

Of interest is an opposite approach, i.e. a study of a possible increase in the key generation rate in quantum cryptography with the conscious use of a number of new assumptions. This approach opens up new possibilities for legitimate users, including the use of a pseudo-random generator for matching bases [13], which requires a rather weak assumption about the impossibility of a quick solution of some computational problems. It is important that, under this assumption, the key is secure for unlimited time, which preserves an important advantage of quantum cryptography over classical cryptography. It should be noted that the proposed approach does not necessarily deteriorates the quantum key distribution system, but rather is associated with the choice of security parameters: as more stringent, related to traditional quantum cryptography, and so providing a higher key distribution rate with less security.

In this paper, we consider new methods for using computational constraints, as well as the possibility of applying other limitations of an eavesdropper, i.e. nonideal communication lines and limitations on the quality of quantum memory; in addition, we describe eavesdropper actions under conditions of these limitations.

2. Limitations on the quality of a communication line

Traditionally, the security of quantum key distribution protocols is studied by assuming that an eavesdropper (usually called Eve) has access to an ideal (lossless) transmission line. The legitimate users themselves (Alice and Bob, where Alice sends messages to Bob) can use only available present day

A.S. Avanesov Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia; Moscow Institute of Physics and Technology (National Research University), Institutskii per. 9, 141701 Dolgoprudnyi, Moscow region, Russia; e-mail: avanesov@phystech.edu;
D.A. Kronberg Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia; Russian Quantum Center, Skolkovskoe sh. 45, 121353 Moscow, Russia; Moscow Institute of Physics and Technology (National Research University), Institutskii per. 9, 141701 Dolgoprudnyi, Moscow region, Russia; e-mail: dmitry.kronberg@gmail.com

Received 28 February 2020
Kvantovaya Elektronika **50** (5) 454–460 (2020)
Translated by I.A. Ulitkin

technologies. In particular, there are losses in the communication channel between Alice and Bob. At the initial intensity $\mu_{\rm A}$ of the signal transmitted between legitimate users, the output intensity $\mu_{\rm B}$ is expressed as:

$$\mu_{\rm B} = 10^{-\kappa_{\rm B}L/10}\mu_{\rm A},$$

where $\kappa_{\rm B}$ is the attenuation parameter of the transmission line, and L is its length. In a beam-splitting attack scenario [14], Eve takes part of each state to her quantum memory, replacing the channel between Alice and Bob with her lossless channel, and then measures that part in an optimal way after the bases are announced. Eve's ability to take part of the signal depends on how small the loss is in the communication line, which she uses to replace the channel between Alice and Bob: it is traditionally assumed that Eve can use an ideal (lossless) channel.

Nevertheless, as was noted in [15], losses in a fibre-optic communication line are physical rather than technological, while alternative data transfer technologies (teleportation and switching to a different wavelength) do not currently appear feasible. Therefore, it is reasonable to assume that the channel at Eve's disposal also has losses. We denote the corresponding attenuation parameter as $\kappa_{\rm E}$; in this case, the part f of the state that Eve can take away should be such that on the Bob side there is no excessive drop in the intensity of the incoming signal, i.e., the condition

$$10^{-\kappa_{\rm B}L/10}\mu_{\rm A} = 10^{-\kappa_{\rm E}L/10}(1-f)\mu_{\rm A}$$

is met. As a result, Eve will take measurements over intensity states:

$$\mu_{\rm E} = f\mu_{\rm A} = (1 - 10^{-(\kappa_{\rm B}-\kappa_{\rm E})L/10})\mu_{\rm A}.$$

In the limit of a communication line of long length L, the intensity $\mu_{\rm E}$ will tend to $\mu_{\rm A}$ in any channel, where the losses are smaller than those in a channel between Alice and Bob. Consequently, while the limitations on optical fibre are apparently unavoidable even for a technologically advanced eavesdropper, they do not give much advantage to legitimate users. Since the most popular cases of quantum key distribution correspond to large losses, the assumption that Eve does not have an ideal channel does not significantly improve the situation for legitimate users, and the traditional assumption that the eavesdropper has an ideal channel seems reasonable.

3. Limitations on computational capabilities

In classical cryptographic systems, the computational capabilities of the eavesdropper are traditionally believed to be limited. Thus, the RSA algorithm, most popular asymmetric encryption algorithm, is based on the difficulty of factoring an unknown prime number, and the Diffie–Hellman scheme of remote key distribution assumes the complexity of the discrete logarithm problem [7].

A more accurate assumption of classical cryptography is that the eavesdropper has not found effective algorithms for problems to be quickly solved and does not have computational capabilities to solve them by currently known algorithms in a time period during which the secret is still relevant.

In this context, an important threat to classical cryptography is the appearance of a quantum computer at the eavesdropper's disposal, which will not only make it impossible to use a number of important technologies of classical cryptography, but will also allow all data encrypted using such algorithms to be deciphered by this time [16]. This leads to an increase in interest in post-quantum cryptography: the development of algorithms whose cryptographic security does not depend on the presence of a quantum computer at the eavesdropper's disposal [17].

A relevant topic is the use of classical cryptography methods to increase the key generation rate in quantum cryptography, while preserving the key advantage of the latter, i.e. guaranteed cryptographic security of the stored key. The role of classical technologies in this case is to counteract a number of real-time attacks.

In our work [13] we considered the possibility of using pseudo-random generators to increase the key generation rate due to the coincidence of bases in all messages. This proposal relies on a number of previously proposed ideas [18–20]. A large number of bases make it possible to overcome an important real-time attack such as an unambiguous state discrimination (USD) attack [21].

Let us consider other possibilities of using pseudorandom generators by the example of coherent-state key distribution protocols; these are COW, DPS, and B92 protocols with a strong reference pulse. They do not use basis reconciliation; therefore, a pseudorandom sequence will be used not to select bases, but to counter a number of attacks by setting a pseudorandom phase.

Let us start with the COW protocol [22], the operation scheme of which is shown in Fig. 1. In the original version of the protocol, Alice encodes each bit transmitted to Bob with a sequence of two states: bit 0 corresponds to the pair $|\alpha\rangle|0\rangle$, and bit 1, to the pair $|0\rangle|\alpha\rangle$. Here $|0\rangle$ is the vacuum state, and $|\alpha\rangle$ is the coherent state given by the complex number $\alpha = \sqrt{\mu} \times \exp({\rm i}\varphi)$, where μ is the intensity of the state and φ is its phase. In addition to sequences carrying information, control sequences of the form $|\alpha\rangle|\alpha\rangle$ are also sent. Bob divides each state into two parts. One part is sent to detector $\rm D_B$, where the signal arrival time is recorded, the other is sent to the interferometer, which has a delay on one arm and with which Bob observes interference between two consecutive non-vacuum signals. In this case, the triggering of detector D2 indicates a loss of coherence and is interpreted as the presence of Eve. The protocol assumes that the phase φ of each state is the same and known to the eavesdropper.

All detectors considered in this section are single-photon and described by an observable

$$\left\{M_0 = |0\rangle\langle 0|,\, M_1 = \sum_{n=1}^{+\infty}|n\rangle\langle n|\right\}.$$

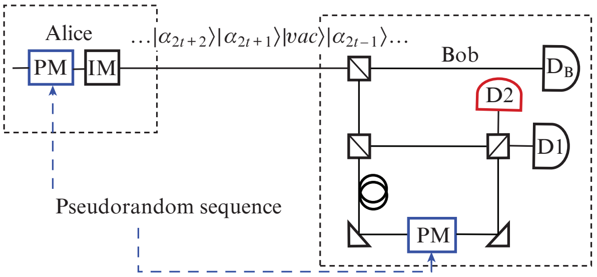
Alice
$\dots|\alpha_{2t+2}\rangle|\alpha_{2t+1}\rangle|vac\rangle|\alpha_{2t-1}\rangle\dots$
PM
IM
Bob
$\rm D_B$
D2
D1
Pseudorandom sequence
PM

Figure 1. Scheme of the COW protocol using a pseudorandom number generator: (PM) phase modulator; (IM) intensity modulator.

The probability of their triggering on a coherent state of intensity μ is $1 - \exp(-\mu)$.

As a modification, we can consider a scheme in which Alice chooses the phase of each state φ_t in accordance with a pseudorandom sequence. In this case, Bob uses the same pseudorandom sequence and a phase modulator on one of the arms of the interferometer to match the phase and obtain an interference pattern.

Now, Eve knows neither the intensity of each state (0 or μ) nor its phase φ_t (in the case of sending a non-vacuum state). If Eve fails to calculate the initial key of the pseudorandom sequence during the communication session, then she cannot know the phase of the transmitted signals, which does not allow her to perform attacks distinguishing between a vacuum and a non-vacuum state [23, 24].

Let us show how ignorance of the state phase prevents the eavesdropper from detecting vacuum states. In a known phase, a measurement that detects vacuum states is described by an observable (decomposition of the identity)

$$M_0 = I - |\alpha\rangle\langle\alpha|, \quad M_? = |\alpha\rangle\langle\alpha|,$$

$$p(0|0) = 1 - |\langle 0|\alpha\rangle|^2 = 1 - \exp(-\mu).$$

At the same time, the problem of distinguishing the vacuum state $|0\rangle$ from a set of N states of the form

$$\{|\alpha_k\rangle\}_{k=1}^{N} = \{|\sqrt{\mu}\exp(\mathrm{i}2\pi k/N)\rangle\}_{k=1}^{N}$$

is more complex. The vacuum state detection operator M_0^N must have the property

$$\langle\alpha_k|M_0^N|\alpha_k\rangle = 0\ \forall k;$$

therefore, due to the symmetry of the states $\{|\alpha_k\rangle\}_{k=1}^{N}$, it has the form $M_0^N = \lambda I - G$, where $G = N^{-1}\sum_{k=1}^{N}|\alpha_k\rangle\langle\alpha_k|$ is the Gramian operator of a set of vectors $\{|\alpha_k\rangle\}_{k=1}^{N}$, and $\lambda = \langle\alpha_k|G|\alpha_k\rangle \leqslant \lambda_{\max}(G)$ is a quantity that does not depend on a particular vector and does not exceed the maximum eigenvalue of G. For the probability of detecting a vacuum, we have

$$p(0|0) = \langle 0|M_0^N|0\rangle = \lambda - \langle 0|G|0\rangle \leqslant \lambda_{\max}(G) - \exp(-\mu).$$

The greater the N, the smaller this value, that is, the more states unknown to the eavesdropper are used by legitimate users.

This modification makes it possible to increase the secret key generation rate by increasing the intensity of the states sent by Alice. The assumption consists in the fact that Eve cannot calculate the pseudorandom sequence during the communication session and perform an attack with the detection of vacuum states.

Similarly, the choice of the phase of the transmitted state using a pseudorandom number generator can also be used in the DPS protocol [25] (Fig. 2). In the original scheme of this protocol, Alice sends to Bob a train of l time-coherent states of the form $|\pm\alpha\rangle$. Logical bits are encoded by the relative phase between two consecutive signals. The phase difference 0 corresponds to bit 0, and the phase difference π corresponds to bit 1. In this case, Bob uses an interferometer with a delay in one arm to observe the interference of two successive coherent states. The triggering of detector D0 corresponds to the reception of states with the same phase (bit 0), and the triggering of detector D1 corresponds to the reception of states with the opposite phase (bit 1).

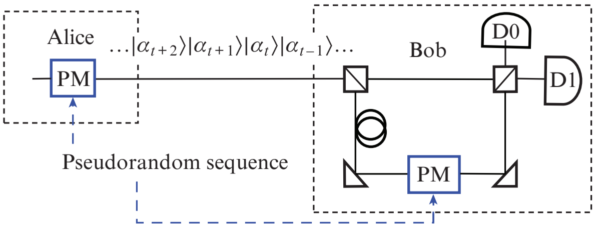
Alice
$\ldots|\alpha_{t+2}\rangle|\alpha_{t+1}\rangle|\alpha_t\rangle|\alpha_{t-1}\rangle\ldots$
Bob
PM
D0
D1
Pseudorandom sequence
PM

Figure 2. Scheme of the DPS protocol using a pseudorandom number generator.

Now let us again assume that Alice is preparing a train of states of the form $|\pm\alpha\exp(\mathrm{i}\varphi_t)\rangle$, with the quantity φ_t for each element of the train being generated pseudorandomly. Bob knows the initial key of the pseudorandom sequence, and so he can use a phase modulator to match the phases between two consecutive train signals, the interference of which he measures.

With the unknown phase of each state, Eve can no longer in particular use a scheme similar to that used on the receiving side to redirect only part of the trains, as is the case during a USD attack. Also difficult to perform is an active beam-splitting attack [26], when Eve tries to increase the intensity of each state of the train to obtain more information about the key and blocks the entire train if many of these attempts fail.

Similarly to the COW protocol modification, this modification allows the key generation rate to be increased due to the use of higher intensity signals, since some of the effective attacks are not applicable.

The third protocol, allowing modification according to a similar scenario, is the B92 protocol with a strong reference pulse [27, 28]. The scheme of the protocol is shown in Fig. 3. Alice is assumed to send to Bob two states in each message: a signal state $|\alpha_t\rangle$, and an auxiliary high intensity state $|a\alpha\rangle$ (i.e. $|a| \gg 1$), with $|\alpha_t\rangle = |\alpha\rangle = |\sqrt{\mu}\rangle$ corresponding to bit 0 and $|\alpha_t\rangle = |-\sqrt{\mu}\rangle$ corresponding to bit 1. At the receiver's side, the auxiliary pulse is divided into two parts using a beam splitter, the parameters of which are selected so that one of the parts represents a state $|\alpha\rangle = |\sqrt{\mu}\rangle$ (Fig. 3), and the other is sent to detector D, the triggering of which makes it possible to estimate the intensity of the transmitted control state. Next, the first part of the auxiliary pulse $|\alpha\rangle$ interferes with the signal state $|\alpha_t\rangle$. The triggering of detector D0 is interpreted by Bob as the transmitted bit 0, and the triggering of detector D1 is interpreted as bit 1.

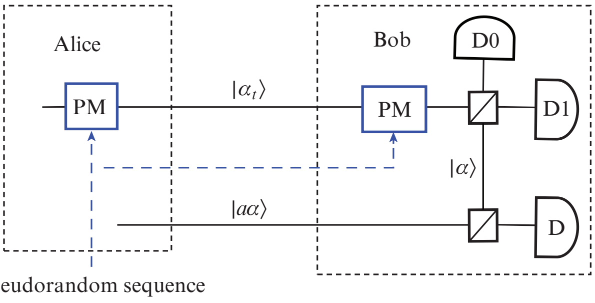

Figure 3. Protocol modification scheme with a strong reference pulse using a pseudorandom number generator.

The use of a pseudorandom number generator, as in the cases of COW and DPS protocols, makes it possible to modify the protocol in question by using a larger number of phases when generating signal states, with the phase being selected pseudorandomly and being matched between Alice and Bob. A phase unknown to the eavesdropper will make it impossible to convert the probabilistic enhancement of the information state that occurs in attacks presented in [24, 26, 29].

4. Limitations on the quality of quantum memory

The presence of ideal quantum memory allows Eve to use part of the signal sent by Alice and store it until Alice announces the bases in which the transmitted states were prepared, or until the code words used to correct the error between legitimate users are announced. However, in reality, quantum memory has limitations, and the states in it can either be lost or change over time in comparison with the initial states, which worsens their distinguishability after extraction from quantum memory.

The simplest implementation of quantum memory can be a bundle of optical fibre. Due to the attenuation processes, the intensity of the extracted signal will decrease. Thus, for an optical fibre with an attenuation parameter of 0.15 dB km^{-1}, a decrease in intensity is 50% for a storage time of 100 μs (taking into account the lower speed of light propagation in optical fibre). The characteristics of this implementation of quantum memory are the starting points in the development of its other types and the evaluation of their performance. For example, Cho et al. [30] implemented a memory scheme, which demonstrated better behaviour than a fibre-based scheme, in the sense that the intensity of the extracted signal was halved over a time exceeding 100 μs. The same work presents the characteristics of existing implementations of quantum memory.

Note that the consideration of the problem taking into account the non-ideality of Eve's quantum memory is not entirely correct under the assumption that Eve has a lossless communication channel. Indeed, in this case, the eavesdropper can delay the signal for an arbitrary time by selecting the channel length. Since transmission is lossless, the extracted state will not experience attenuation. Thus, the assumption that the storage time of quantum states is limited automatically requires taking into account the attenuation in the communication channels available to the eavesdropper.

Legitimate users can simply use the eavesdropper's limitations on quantum memory, because, as noted in [15], they can simply delay the time of announcing bases for the time during which Eve's states in quantum memory will finally lose touch with Alice's states. Such a delay in the conditions of continuous transfer of quantum states in a quantum key distribution system has practically no effect on the rate of their generation and requires only an increase in the volume of classical memory for storing a raw key, since its classical processing can only begin when it is necessary to obtain a new secret key.

Thus, using the assumption that the eavesdropper's quantum memory is not ideal, Alice and Bob, when choosing an adequate delay time, can assume that by the time classical information is announced, the eavesdropper no longer has states in quantum memory and cannot make the necessary measurement that extracts the maximum possible information. Bechmann-Pasquinucci [31] considered a situation of the absence of quantum memory at the eavesdropper's disposal and showed that in this case the intercept/resend strategy represents an optimal attack. We use a weaker assumption that the eavesdropper has quantum memory and can make collective measurements, but is not able to store states in quantum memory until classical information is announced.

An important consequence of this limitation is that the eavesdropper's information should be estimated from the one-shot capacity, rather than from the Holevo value of its states [32]. In fact, the classical mutual information between the sender and the receiver of quantum states generally demonstrates superadditivity, when the receiver can extract more information as a result of collective measurements over the entire transmitted sequence; in this case, the recipient information is limited by the Holevo value [32]. Nevertheless, this effect is achieved only with the proper selection of code words on the transmitter's side and measurement in accordance with this coding: for example, Theorem 2 in [33] states that if the measured ensemble of states splits into the product of ensembles related to subsystems, then mutual information, even in the case of collective measurement of such an ensemble, is given by the sum of the capacities when measuring each subsystem separately, which corresponds to the additive case. The information disclosed by legitimate users when correcting errors is actually a set of code words. If the set of code words at the time of measurement is unknown, the eavesdropper deals with measuring any possible string of initial states. In this case mutual information between the transmitter and receiver is strictly additive and in terms of one message is equal to the one-shot capacity. This capacity is defined as maximum mutual information in individual measurements of quantum states:

$$C_1 = \max_{\{p_i\},\Gamma} I_1(\{p_i\},\Gamma),$$

where $I_1(\{p_i\},\Gamma)$ is the mutual information with the probabilities of states at the transmitter's side, $\{p_i\}$, and the application of the observable Γ at the receiver's side. Finding the optimal observable Γ for an arbitrary ensemble of states is a nontrivial task; however, we can present the values of two nonorthogonal pure states, such as coherent states $|\pm\alpha\rangle$ for which the Holevo value χ and one-shot capacity C_1 are known [32]:

$$C_1 = 1 - h_2\left(\frac{1-\sqrt{1-|\langle-\alpha|\alpha\rangle|^2}}{2}\right) = 1 - h_2\left(\frac{1-\sqrt{1-\exp(-4\mu)}}{2}\right),$$

$$\chi(|\pm\alpha\rangle) = h_2\left(\frac{1-|\langle-\alpha|\alpha\rangle|}{2}\right) = h_2\left(\frac{1-\exp(-2\mu)}{2}\right),$$

where $\mu = |\alpha|^2$ is the intensity, and $h_2(x) = -(1-x)\log_2(1-x) - x\log_2 x$ is the Shannon binary entropy. Thus, if there were no errors in the channel, and the eavesdropper was able to use the states $\mu = 0.2$ photons per pulse, the secret key length when evaluating the eavesdropper information by the Holevo value [34] is $1 - \chi \approx 0.354$ bits of forward communication, and when evaluating the information in terms of the one-shot capacity, it is $1 - C_1 \approx 0.555$ bits of forward communication, which is significantly more profitable for legitimate users. With a 0.5 intensity of states assigned to the eavesdropper, these values will be approximately 0.1 and 0.219 bits of forward communication, which means more than a doubled gain. Once again we note: here we only use the assumption that Eve takes measurements without knowing the set of code words, although she has the opportunity to have quantum memory and make collective measurements, but she will not benefit from their use.

It also follows from the assumption that Eve has limited quantum memory that she will measure states without knowing the basis in which they were prepared. This circumstance imposes additional restrictions on the amount of information obtained by Eve through measurements.

In general, legitimate users can use higher-intensity states to increase the key generation rate. However, Alice and Bob still cannot make the forwarded states arbitrarily distinguishable, even when they use a large number of bases. Indeed, in the case of the transmission of high-intensity signals, Eve can make use of part of the state and perform a measurement, storing its classical result in memory. After the procedure for basis matching between legitimate users, Eve uses the results of her measurements and new information to determine the transmitted bit. As an illustration, we consider the configuration of symmetric coherent states from [13] and an attack, where part of the state is used by the eavesdropper to be homodyned, that is, the quadrature $\hat{X}_\phi = \hat{a}\exp(\mathrm{i}\phi) + \hat{a}^\dagger \times \exp(-\mathrm{i}\phi)$ is measured. We set $\phi = 0$, then the probability density function of the outcomes x of such a measurement in the case of a coherent state $|\alpha\rangle$ has the form

$$P(x|\alpha) = \sqrt{\frac{2}{\pi}}\exp[-2(x - \mathrm{Re}\alpha)^2].$$

Consider a configuration in which the phase shift between the basis states is δπ. Let b be the basis number, k be the transmitted bit, and M be the number of bases. Then Alice sends the states of the form

$$|\alpha_{b,k}\rangle = |\sqrt{\mu}\exp(\mathrm{i}\varphi_{b,k})\rangle,$$

where μ is the intensity and $\varphi_{b,k} = \pi(b/M + k)$ is the phase.

Thus, the density distribution of the outcomes of Eve's measurement, when Alice selects the basis b and bit k, has the form

$$P(x|k,b) = \sqrt{\frac{2}{\pi}}\exp\left\{-2\left[x - \sqrt{\mu}\cos\left(\frac{\pi b}{M} + \pi k\right)\right]\right\}.$$

Using Bayes' theorem, we can obtain an *a posterior* probability that Alice sent bit k given the results of Eve's measurement and basis announcement. Bits are selected with equal probability, that is, $P(k|b) = 1/2$ for all values of k and b. The parameter k can take two values: 0 or 1. We have

$$P(0|x,b) = \frac{1}{1 + \exp[-8x\sqrt{\mu}\cos(\pi b/M)]}.$$

For conditional mutual information between Alice and Eve we obtain

$$I(\mathrm{A:B}|x,b) = 1 - h_2(P(0|x,b)),$$

where $h_2(q) = -q\log_2(q) - (1-q)\log_2(1-q)$. Integrating over x and summing over b, we obtain the amount of mutual information

$$I(\mathrm{A:E}) = 1 - \frac{1}{M}\int_{-\infty}^{+\infty}\mathrm{d}x\sum_{b=0}^{M-1}P(x|b)h_2(P(0|x,b))$$
$$= 1 - \int_{-\infty}^{+\infty}\mathrm{d}x\mathcal{L}(x),$$

where

$$\mathcal{L}(x) = \frac{1}{M}\sqrt{\frac{1}{2\pi}}\sum_{b=0}^{M-1}\{\exp[-2(x + f(b))^2]$$
$$\times\log_2[1 + \exp[8f(b)x]] + \exp[-2(x - f(b))^2]$$
$$\times\log_2[1 + \exp[-8f(b)x]]\};$$

$$f(b) = \sqrt{\mu}\cos(\pi b/M).$$

With such a measurement, the result x itself, without knowing the basis b, does not contain information about the signal k, but this information can be obtained after the basis is announced, and a large number of bases M, although it reduces the probability of a reliable discrimination of all states [35], almost does not complicate the described measurement. A conclusion can be drawn that even if the eavesdropper does not have quantum memory and does not know the basis at the moment of signal transmission, the state within the basis, generally speaking, cannot be made arbitrarily distinguishable.

Note that in the case of legitimate users using an odd number of bases, mutual information is close to unity at high intensities, that is, $I(\mathrm{A:E}) \sim 1$. However, in the case of using an even number of bases this is not so: $I(\mathrm{A:E}) \sim 1 - M^{-1}$. A decrease in information is due to the fact that in the considered attack scheme, Eve will have problems with distinguishing between the states $|\pm\mathrm{i}\alpha\rangle$, whose projections on the homodyning axis coincide. To make the extracted information close to unity, the eavesdropper should rotate the homodyning axis in the phase plane by an angle $\varphi = -\pi/(2M)$ so that there are no states of the same basis with matching projections relative to it. For $\varphi = -\pi/(2M)$, the quantity $f(b)$ is modified as $f(b) \to \sqrt{\mu}\cos[\pi b/M + \pi/(2M)]$ and for all $b \in \{0,..,M-1\}$ the function $f(b)$ becomes nonzero. As a result, at high intensities $I(\mathrm{A:E}) \sim 1$. The dependence of $I(\mathrm{A:E})$ on the values of μ is shown in Fig. 4.

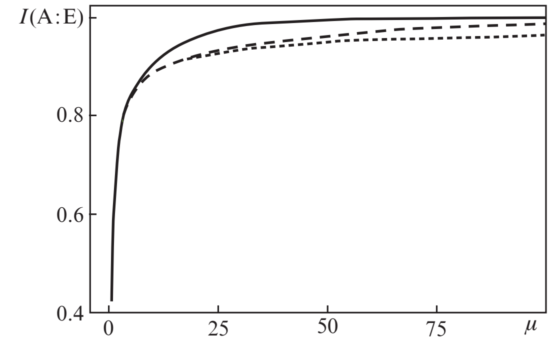

Figure 4. Dependences of the mutual information function $I(\mathrm{A:E})$ on the intensity of the states transmitted by Alice during homodyning along the axis $\varphi = -\pi/(2M)$. We consider a symmetric coherent-state protocol with a phase shift of vectors inside the basis $\delta = \pi$. The solid curve corresponds to the number of bases $M = 8$, the dashed curve corresponds to $M = 16$, and the dotted curve corresponds to $M = 64$.

In connection with a desire to use a large number of bases (randomly or pseudorandomly selected) to counter an eavesdropper that does not have quantum memory, the following theoretical problem can be formulated: to find an ensemble of states R divided into a set of bases B so that, when the basis is known and the observable $\Gamma_{\rm B}$ depending on it is applied, the information about the key K would be great; if the basis is not known, any measurement of Γ independent B would give little information about the key, even when the basis becomes known:

$$I(K, \Gamma|B) \ll I(K, \Gamma_{\rm B}|B).$$

The presence of such an ensemble of states would mean the possibility of using it in quantum cryptography: Bob could select (randomly or pseudorandomly) a basis, after which, with a random choice of bases, users would discard messages with unmatched values and measure the value of $I(K, \Gamma_{\rm B}|B)$ as mutual information; at the same time, the eavesdropper is limited to measurements that are independent of the choice of basis, although its mutual information is calculated with subsequent knowledge of the basis.

As shown above, the configuration of symmetric coherent states of high intensity is poorly suited for this purpose, since the eavesdropper can perform a measurement and, after the bases are revealed, obtain much information about the key from the measurement results.

This problem is similar to the classical problem of constructing a trapdoor function [7], that is, the function $F_k(x)$, for which it is easy to calculate $y = F_k(x)$ if x is known, and it is also easy to calculate x, if y and k are known; at the same time, there are no efficient algorithms for calculating x by y without knowing k. Such functions are used in a number of classical algorithms, in particular RSA; however, the question of their existence remains open, and for the constructed functions the statement that x over y is really difficult to calculate is only an assumption based on the fact that for a number of problems it was not possible for a long time to find effective solution algorithms.

For ensembles of quantum states, the role of such a 'trapdoor' is played by the knowledge of the basis. The problem of constructing a 'trapdoor ensemble' is nontrivial, since constructing an optimal observable in itself is a difficult task for highly dimensional spaces, while the problem requires optimality of the observable, taking into account the subsequent receipt of additional information.

Note that the formulated problem can also be generalised to the case when the eavesdropper can block some states. Such measurements [21], as a rule, provide the eavesdropper with more information, which improves his/her capabilities. It is important that the decision to block states should be made without knowing the secret, and the measurement constructed above, in principle, allows this, since the information about the key depends on the value of x obtained during the measurement: for large values of x, there is more information. This makes it possible to generalise the attack in the case when the eavesdropper blocks part of the state. Typically, quantum cryptography protocols use methods of protection against blocking part of the states, which include the above mentioned distributed encoding, sending a strong reference pulse, and using decoy states [36].

5. Conclusions

The considered limitations of the eavesdropper capabilities, primarily his/her computational resources and the storage time of quantum states, allow legitimate users to match bases using a pseudorandom number generator and increase the signal intensities used in the protocol. This leads to an increase in the key generation rate. Coherent-state protocols are considered as examples.

The assumption about Eve's computational capabilities allows the use of a larger number of bases, which makes the protocols considered in the work more secure to some attacks. At the same time, matching bases using a pseudorandom number generator allows one not to reduce the key generation rate.

The assumption that the storage time of the quantum state is limited makes it possible to use states of higher intensity, which also increases the key generation rate. However, protocols that use states of too high intensity are vulnerable. Using the example of a protocol on geometrically uniform coherent states, Eve's information about the key was calculated, which she can obtain by homodyning and then using the information revealed by Alice during basis reconciliation (when considering the problem of the limitations of quantum memory, it was assumed that the bases were chosen randomly).

The main conclusion of the work is that quantum cryptography systems should have a built-in possibility of increasing the key generation rate under some realistic assumptions about the capabilities of the eavesdropper so that, along with a fully protected mode, there is a possibility of faster generation of the key, which has practical security, in particular against real-time attacks, while retaining the main advantage of quantum cryptography: unchanged key security after its generation. Such a scheme seems more secure than a system with slow generation of a completely secret key using the methods of 'pure' quantum cryptography, after which the key is used in a classical symmetric system to encrypt a large amount of data. This issue is relevant until quantum cryptography systems have been developed that can provide a key generation rate sufficient for encryption in one-time pad mode.

In this regard, the following problems acquire sense: a rigorous justification of the formula for the key generation rate under practical constraints, as well as the development of a configuration of quantum states for which the maximum mutual information for a basis-independent measurement will be limited by a small quantity, while the measurement with a well-known basis makes it possible to extract a large amount of information, including after discarding inconclusive outcomes.

Acknowledgements. The authors express their gratitude to A.S. Trushechkin for numerous discussions.

The study was supported by the Russian Science Foundation (Project No. 18-71-00074).

References

1. Bennett Ch.H., Brassard G., in *Proc. Int. Conf. Comput., Syst. Sign. Proces.* (Bangalore, India, 1984) pp 175–179.
2. Qi B., Fung C.H.F., Lo H.K., Ma X. arXiv preprint quant-ph/0512080 (2005).
3. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. *Phys. Rev. A*, **73** (2), 022320 (2006).

4. Makarov V., Anisimov A., Skaar J. *Phys. Rev. A*, **74** (2), 022313 (2006).
5. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nature Photon*., **4** (10), 686 (2010).
6. Bugge A.N., Sauge S., Ghazali A.M.M., Skaar J., Lydersen L., Makarov V. *Phys. Rev. Lett*., **112** (7), 070503 (2014).
7. Yashchenko V.V., Varnavskii N.P., Nesterenko Yu.V., et al. *Vvedenie v kriptografiyu* (Introduction to Cryptography) (Moscow: MTsNMO, 2012).
8. Lo H.K., Curty M., Qi B. *Phys. Rev. Lett*., **108** (13), 130503 (2012).
9. Acín A., Massar S., Pironio S. *New J. Phys*., **8** (8), 126 (2006).
10. Acín A., Brunner N., Gisin N., Massar S., Pironio S., Scarani V. *Phys. Rev. Lett*., **98** (23), 230501 (2007).
11. Vazirani U., Vidick T. *Commun. ACM*, **62** (4), 133 (2019).
12. Liu Y., Zhao Q., Li M.H., Guan J.Y., Zhang Y., Bai B., Li H. *Nature*, **562** (7728), 548 (2018).
13. Avanesov A.S., Kronberg D.A. *Quantum Electron*., **49** (10), 974 (2019) [*Kvantovaya Elektron*., **49** (10), 974 (2019)].
14. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. *J. Cryptology*, **5** (1), 3 (1992).
15. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74**, 145 (2002).
16. Shor P.W., in *Proc. 35th Ann. Symp. Foundati. Comput. Sci*. (Santa Fe, 1994) p. 124.
17. Bernstein D.J., Buchmann J., Dahmen E. (Eds) *Post-Quantum Cryptography* (Berlin, Heidelberg: Springer, 2009).
18. Hirota O., Sohma M., et al. *Phys. Rev. A*, **72** (2), 022335 (2005).
19. Kurochkin Y. *Quantum Inform*., **5833**, 213 (2004).
20. Trushechkin A.S., Tregubov P.A., Kiktenko E.O., Kurochkin Y.V. Fedorov A.K. *Phys. Rev. A*, **97** (1), 012311 (2018).
21. Dušek M., Jahma M., Lütkenhaus N. *Phys. Rev. A*, **62** (2), 022306 (2000).
22. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett*., **87** (19), 194108 (2005).
23. Branciard C., Gisin N., Lütkenhaus N., Scarani V. *Appl. Phys. Lett*., **87**, 194108 (2005).
24. Kronberg D.A., Nikolaeva A.S., Kurochkin Y.V., Fedorov A.K. *Phys. Rev. A*, **101** (3), 032334 (2020).
25. Inoue K., Waks E., Yamamoto Y. *Phys. Rev. Lett*., **89** (3), 037902 (2002).
26. Avanesov A.S., Kronberg D.A., Pechen A.N. *P-Adic Num. Ultrametr. Anal. Appl.*, **10** (3), 222 (2018).
27. Bennett C.H. *Phys. Rev. Lett*., **68** (21), 3121 (1992).
28. Tamaki K., Lütkenhaus N., Koashi M., Batuwantudawe J. *Phys. Rev. A*, **80** (3), 032302 (2009).
29. Kronberg D.A., Kurochkin Yu.V. *Quantum Electron*., **48** (9), 843 (2018) [*Kvantovaya Elektron*., **48** (9), 843 (2018)].
30. Cho Y.-W., Campbell G.T., Everett J.L., Bernu J., Higginbottom D.B., Cao M.T., Geng J., Robins N.P., Lam P.K., Buchler B.C. *Optica*, **3** (1), 100 (2016).
31. Bechmann-Pasquinucci H. *Phys. Rev. A*, **73** (4), 044305 (2006).
32. Holevo A.S. *Quantum Systems, Channels, Information* (Berlin, Boston: De Gryuter, 2012; Moscow: MTsNMO, 2010).
33. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Rev. A*, **58** (1), 146 (1998).
34. Devetak I., Winter A. *Proc. Royal Soc. A*, **461**(2053), 207 (2005).
35. Chefles A., Barnett S.M. *Phys. Lett. A*, **250** (4-6), 223 (1998).
36. Lo H. K., Ma X., Chen K. *Phys. Rev. Lett*., **94** (23), 230504 (2005).