QUANTUM CRYPTOGRAPHY https://doi.org/10.1070/QEL17054

Coherent-state quantum cryptography using pseudorandom number generators

A.S. Avanesov, D.A. Kronberg

Abstract. **Quantum key distribution plays an important role in modern cryptography, since the security of the transmitted keys is guaranteed by fundamental laws of nature. A method using pseudorandom number generators well known from classical cryptography is considered. It is shown that their use in quantum cryptography makes it possible to increase the key generation rate under very weak assumptions about the capabilities of the eavesdropper. A practical scheme of a coherent-state quantum key distribution protocol using pseudorandom sequences is proposed. The cryptographic strength of the proposed protocol against a beam-splitting attack is considered.**

Keywords: *quantum cryptography, quantum information, coherent states, pseudorandom number generators.*

1. Introduction

Quantum cryptography, which was proposed more than 30 years ago [1], has been rapidly developing in recent years. There are a number of commercial schemes for quantum key distribution, including quantum key transfer between cities [2] and from a satellite to the ground [3].

The key advantage of quantum key distribution over the classical one is that the security of the keys is guaranteed by the fundamental laws of nature and cannot be reduced to assumptions about the limited capabilities of the eavesdropper. Classical cryptography is mainly based on the assumption that some computational tasks cannot be solved quickly. However, this assumption has not yet been proven, which entails the potential vulnerability of classical cryptographic schemes, both due to the improvement of the computational capabilities of the eavesdropper and to the development of new algorithms. Thus, in 1998, the EFF's DES cracker was built, capable of performing a brute force search of the DES cipher's key in a matter of days, which was due to a rapid increase in the processing power of computing devices in two decades after the adoption of the DES standard in 1977.

In addition, Shor [4] showed already in 1994 that the implementation of a quantum computer can make a number of important classical schemes completely unsecure, including losing all secrecy of information encrypted by this time. This leads to the idea that information, for which security is important for a long time, should now be encrypted using the schemes that will be fault-tolerant despite the appearance of a quantum computer at the eavesdropper's disposal in the foreseeable future [5]. Classical cryptography schemes that are resistant to the appearance of a quantum computer are called post-quantum cryptography [6].

In this context, an important advantage of quantum cryptography is that it allows one to keep the transmitted keys secure for an infinitely long time, and the eavesdropper has no way to obtain additional information about the key when solving computational problems or when he has new technological means. It should be noted that the implementation of quantum cryptography protocols, as a rule, has its drawbacks, which leads to the possibility of performing attacks relying on imperfection of the equipment or on targeted damage to individual elements of legitimate user schemes by the eavesdropper [7, 8]. However, all attacks of these kinds are related to real-time attacks and do not provide an opportunity to obtain a secret key after the end of its generation session.

An important goal of scientific and experimental groups working on quantum key distribution is the high-speed and long-distance transmission of keys. At the same time, practical encryption schemes, even based on quantum cryptography for key generation, can in some cases use elements of classical cryptography, such as AES schemes, to increase the speed, which makes the system no longer completely secure, since the key length is less than the length of the encrypted message. This approach may be appropriate for applications where the use of a perfectly secure one-time pad is practically not justified due to the rapid use of the key. For such applications, the urgent task is to increase the key generation rate in quantum cryptography protocols using a number of classical cryptography technologies, albeit at the cost of abandoning full theoretical security.

An important concept of classical cryptography, which can also be used in quantum technologies, is a pseudorandom number generator [9], i.e., a function that from a given initial key of length K (sometimes called a pseudorandom sequence seed) constructs a string of longer length $q(K)$ (a pseudorandom sequence). This string cannot be easily (from a computa-

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, 1213353 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 30 April 2019; revision received 28 June 2019
Kvantovaya Elektronika **49** (10) 974–981 (2019)
Translated by I.A. Ulitkin

tional point of view) distinguished from a random one, i.e., it is difficult to calculate the seed from the output string and predict the following symbols of the pseudorandom sequence [10]. Such a generator can be obtained from classical encryption systems, such as AES, if one runs them in output feedback mode (OFB) [11].

An example of the application of pseudorandom number generators in quantum cryptography is the Y-00 protocol [12–14], which uses coherent states that are well distinguishable if the pseudorandom sequence is known and are poorly distinguishable without this knowledge. This protocol will be further discussed in detail. Pseudorandom sequences were also proposed to be used when choosing bases in single-photon protocols of quantum cryptography [15], which allows the key generation rate to be increased while maintaining unconditional security. It was shown that a quantum stream cipher based on a pseudorandom sequence is no longer able to ensure theoretical security [16]. In addition, 'quantum Enigma' [17] deserves mentioning – a method that allows one to transmit a secret message of arbitrary length in the presence of a key of limited length between legitimate users. However, this method requires legitimate users to be able to perform transformations over quantum states in large-dimensional spaces, which complicates its practical use.

In this paper, we propose a scheme that uses pseudorandom number generators as an integral part and therefore requires assumptions regarding the computational capabilities of the eavesdropper. We will use the assumption that the eavesdropper cannot calculate the seed of the pseudorandom sequence during the communication session, which, as a rule, is no longer than several minutes. At the same time, when fulfilling this weak assumption, the security of the distributed keys is maintained for an unlimited time, which confirms the important advantage of quantum cryptography over classical cryptography.

The work is organised as follows. Section 2 is devoted to the protocols of quantum cryptography with symmetric coherent states. It introduces a general scheme of such protocols, summarising the two currently proposed protocols, and proposes an optical measurement scheme. Section 3 describes the main protocol with a pseudorandom choice of bases. Section 4 considers the beam-splitting attack and discusses why this attack is close to optimal for the proposed protocol. Section 5 is devoted to possible modifications of the protocol in various practical conditions. The Conclusions provide the main results of the work.

2. Use of symmetric coherent states in quantum cryptography

Attenuated laser radiation is one of the most accessible sources of quantum states in practice and, therefore, much attention is paid to the protocols of coherent-state quantum cryptography. The coherent state defined by the complex number α is written as

$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \qquad (1)$$

where $|n\rangle$ is the nth photon state. The parameter α is related to the light beam intensity as

$$\mu = |\alpha|^2. \qquad (2)$$

The scheme with four geometrically uniform coherent states [18] is one of the first proposed protocols of coherent-state quantum cryptography. This configuration of states is close to the BB84 protocol, because the knowledge of the basis increases the probability of distinguishing the states. However, since coherent states are nonorthogonal, states in one basis are also not orthogonal, and the protocol is similar to the B92 protocol using two nonorthogonal states [19], which is why it is also called the 4 + 2 protocol.

This protocol uses $|\alpha\rangle$, $|\mathrm{i}\alpha\rangle$, $|-\alpha\rangle$ and $|-\mathrm{i}\alpha\rangle$ states forming two bases $\{|\alpha\rangle, |-\alpha\rangle\}$ and $\{|\mathrm{i}\alpha\rangle, |-\mathrm{i}\alpha\rangle\}$. In describing quantum key distribution protocols, the active agents, between whom the keys are distributed, are customarily called Alice and Bob. The communication channel between them can be intercepted by an eavesdropper called Eve. We denote the used basis by the parameter $b \in \{0, 1\}$, and the sent bit of the message by k. Then Alice sends a state $|(-1)^k \mathrm{i}^b \alpha\rangle$ in each message. Bob uses a Mach–Zehnder interferometer for measurements. Changing the phase on the lower arm of the interferometer, Bob takes a measurement in a randomly selected basis. With a probability of 1/2, he correctly guesses the basis, and then with a probability of $1 - \mathrm{e}^{-\mu}$, one of the detectors is triggered. Then, as in the BB84 protocol, Alice and Bob communicate over an open channel and discard the messages where their bases did not coincide, after which they carry out error correction and privacy amplification to obtain a matching key, about which the eavesdropper has little information.

Using this protocol and in the absence of attenuation in the communication channel, Eve does not know the selected basis at the time of the state transfer and introduces an error when trying to obtain information from the signal (in the simplest case, when trying to guess the basis and perform a measurement, but this is not the best strategy). However, due to the nonorthogonality of the states within the basis and the attenuation in the communication channel, Bob does not expect detectors to be triggered in all positions, which gives Eve new opportunities for eavesdropping. In particular, she can block part of the message for which she could not receive all the information. This leads to an unambiguous state discrimination (USD) attack [20]. In such an attack, the eavesdropper performs an unambiguous measurement, which gives either complete information about the transmitted state or an inconclusive result. In the latter case, the eavesdropper blocks the message; otherwise, the eavesdropper sends a state without errors, if necessary with increased intensity. With sufficiently large losses in the communication channel, this attack strategy allows the eavesdropper to obtain complete information about the key without being detected.

The states of the 4 + 2 protocol have symmetry, namely, they can be obtained by the action of the transformation U: $|\alpha_{\mathrm{i}+1}\rangle = U|\alpha_{\mathrm{i}}\rangle$, $U^N = I$. An important result for symmetric (sometimes also called geometrically uniform) coherent states is an estimate of the probability of their unambiguous discrimination [21, 22], which limits the use of the USD attack – for a fixed intensity, the more states the legitimate users use, the more difficult they are unambiguously discriminated. The 4 + 2 protocol uses only two bases, which makes the use of the USD attack quite simple. Then the natural suggestion is to use more bases, because Eve will have more difficulties to distinguish them. However, this will also interfer with the legitimate users, since the key generation rate will decrease with increasing number of bases due to their frequent mismatch between Alice and Bob.

We should also mention the protocol with geometrically uniform coherent states [23], in which the transmitted message is encoded into $2M$ coherent states forming M bases, with a phase shift between the basis states $\delta = \pi/M$. Let us also mention the protocol [24, 25], which uses a similar set of symmetric coherent states with a phase shift π within the basis, but employing a different (compared to the 4 + 2 protocols and the aforementioned protocol with geometrically uniform states) side-frequency measurement scheme on Bob's side.

Our proposal is that the use of a large number of bases M allows us to select them in a pseudorandom manner, i.e., in accordance with the pseudorandom sequence specified by the common seed shared between Alice and Bob. We can also use an arbitrary phase shift between states within the basis, instead of $\delta = \pi$ in the 4 + 2 protocol and $\delta = \pi/M$ in the protocol with geometrically uniform states. Thus, it is possible to construct a whole family of quantum key distribution schemes, special cases of which will be two of the above protocols.

Let us consider the case of arbitrary values of δ and M and describe the actions of legitimate users. Two cases are discussed separately, because different measurement schemes are used for them.

1. Let $\delta = \pi$, then we choose bases of the form $\{|e^{i\pi b/M}\alpha\rangle, |-e^{i\pi b/M}\alpha\rangle\}$, $b = 0,..., M-1$...

2. If $\delta \neq \pi$, then we additionally require that $\delta \neq 2\pi k/M$, where $k \in Z$. The corresponding bases will be chosen in the form $\{|e^{i2\pi b/M}\alpha\rangle, |e^{i\delta}e^{i2\pi b/M}\alpha\rangle\}$, $b = 0,..., M-1$.

Figure 1 shows the images of the states transmitted in the protocol in the phase plane for eight bases; two options are considered: $\delta = 3\pi/8$ and $\delta = \pi$.

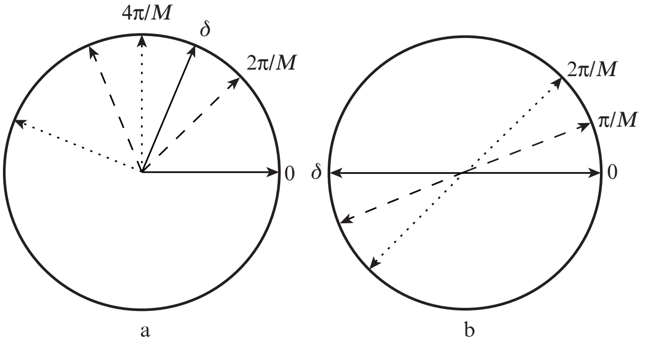

Figure 1. Examples of states transmitted by Alice for $M = 8$. The states of the first three bases ($b \in \{0, 1, 2\}$) are shown for (a) $\delta = 3\pi/8$ and (b) $\delta = \pi$. The same types of lines indicate the states of one basis.

A step-by-step description of the protocol is as follows.

1. Alice and Bob choose an integer M corresponding to the number of bases, and a phase shift δ.

2. Next, the following actions are repeated N times:

a) Alice randomly selects the basis $b \in \{0, 1,..., M-1\}$ and the value of the bit $k \in \{0, 1\}$;

b) Alice sends the state $|\alpha_k^{(b)}\rangle = |\alpha e^{i\theta_b}e^{ik\delta}\rangle$, where

$$\theta_b = \frac{\pi b}{M}(1 + [\delta \neq \pi]) \tag{3}$$

(here $[\delta \neq \pi]$ is an indicator that $\delta \neq \pi$); and

c) Bob randomly selects the basis $b' \in \{0, 1,..., M-1\}$ and performs an unambiguous measurement, discriminating between the states $|\alpha_0^{(b)}\rangle$ and $|\alpha_0^{(b')}\rangle$. As a result, Bob obtains either an inconclusive result, or the number k' corresponding to the state $|\alpha_{k'}^{(b')}\rangle$.

3. Alice and Bob reveal the bases b and b' through the open channel. Messages with noncoinciding b and b' are discarded. In addition, all the messages with the inconclusive result on Bob's side are discarded.

4. Alice and Bob reveal part of their sequences k and k' to assess the probability of error. If the error turns out to be more critical, the protocol execution is interrupted, and error correction is performed through the open channel.

5. Alice and Bob carry out a procedure for privacy amplification, as a result of which they receive a bit string of shorter length, about which Eve's information is small.

The measurement scheme on Bob's side is shown in Fig. 2. Alice sends a reference signal $|\alpha\rangle$ in every message and then, an information state $|\alpha_k^{(b)}\rangle$ with a fixed delay relative to the reference signal. The Mach–Zehnder interferometer is used on the receiver side. To observe the interference of the part of the reference signal passing along the lower path and the part of the information state travelling along the upper path, a delay on the lower path is equal to that while sending states. In addition, on the lower path, Bob, using a phase modulator, 'twists' the phase of the reference state in accordance with b' and k' to obtain information about Alice's transmitted bit.

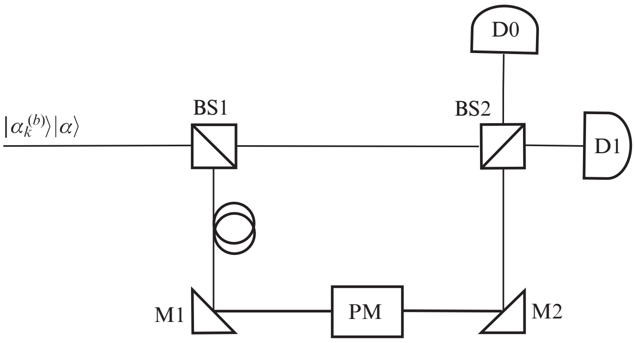

Figure 2. Measurement scheme on Bob's side: (BS1, BS2) beam splitters; (M1, M2) mirrors; (D0, D1) detectors. Part of the reference signal $|\alpha\rangle$ passes along the lower path through the delay line and on changes its phase the phase modulator PM in accordance with the parameters $b' \in \{0,...,M-1\}$ and $l \in \{0,1\}$ chosen by Bob. The resulting state $|-i\alpha_l^{(b')}/\sqrt{2}\rangle$, after passing through BS2, interferes with part of the signal state $|i\alpha_k^{(b)}/\sqrt{2}\rangle$ that has passed through the upper path. The possible options are: if $\delta = \pi$, then l is always set equal to zero, b' is chosen randomly, and the triggering of the detectors D0 and D1 correspond to $k' = 0$ and $k' = 1$; at $\delta \neq \pi$, the parameters b' and l are randomly selected, the readings of the detector D0 are ignored, and if the detector D1 is triggered, the value $k' = l \oplus 1$ is assigned to the parameter k'.

The beam splitter BS1 at the interferometer input divides the state $|\alpha\rangle$ in two parts: $|\alpha/\sqrt{2}\rangle$ on the upper path and $|i\alpha/\sqrt{2}\rangle$ on the lower path. Two mirrors M1 and M2 on the lower path change the total phase by 2π, and the phase modulator PM transforms the input signal state $|\alpha\rangle$ into $|e^{i\theta}\alpha\rangle$; the choice of θ is made by Bob.

When $\delta = \pi$, the transformation of the reference signal between the beginning and end of the lower path has the form

$$\left|\frac{i\alpha}{\sqrt{2}}\right\rangle \to \left|\frac{ie^{i\theta_{b'}}\alpha}{\sqrt{2}}\right\rangle. \tag{4}$$

Then both beams pass through the beam splitter BS2. Consider the time moment when part of the information state that has passed along the upper path is received by the detectors. Suppose that the basis is correctly guessed, i.e., $b' = b$. Then, after the beam splitter BS2, the state $|{}^1/_2 e^{i\pi b/M}(e^{i\pi k} + 1)\alpha\rangle$ arrives at the input of the detector D0, and the state $|{}^1/_2 e^{i\pi b/M}(e^{i\pi k} - 1)\alpha\rangle$ arrives at the input of the detector D1. When the state $|\alpha_0^{(b)}\rangle$ is sent, there is a nonzero probability of the detector D0 being triggered, which indicates that the classic bit 0 was sent, i.e. $k' = 0$. The second detector should not be triggered, and this event is considered to be an error. If Alice sent the state $|\alpha_1^{(b)}\rangle$, and the basis is correctly guessed, then the detector D1 is triggered with some nonzero probability and $k' = 1$. The triggering of both detectors is treated as an error. As a result, the probability that Bob guessed the basis and one of his detectors was triggered takes the form

$$p = \frac{1 - e^{-\mu}}{M}. \tag{5}$$

Let us now consider the option $\delta \neq \pi$. In this case, Bob not only tries to guess the basis, but also adjusts the scheme for each information state, i.e., selects a random bit l and uses the phase modulator to perform the transformation

$$\left|\frac{i\alpha}{\sqrt{2}}\right\rangle \to \left|\frac{ie^{i\theta_{b'}}e^{i\delta l}\alpha}{\sqrt{2}}\right\rangle = \left|\frac{i\alpha_l^{(b')}}{\sqrt{2}}\right\rangle. \tag{6}$$

Suppose again that the basis was correctly guessed, i.e., $b' = b$, and consider the moment of arrival of part of the information state along the upper path. After the beam splitter BS2, the state $|{}^1/_2 e^{i\pi b/M}(e^{i\delta k} - e^{i\delta l})\alpha\rangle$ arrives at the input of the detector D1. The detector D1 can only be triggered if $l \oplus 1 = k$, and so Bob assumes $k' = l \oplus 1$. In other cases, Bob obtained an inconclusive result. We will ignore the possible triggering of the detector D0; it can be removed from the scheme. For the probability of a conclusive result, we obtain the expression

$$p = \frac{1 - \exp[-|(\alpha - e^{i\delta}\alpha)/2|^2]}{2M} = \frac{1 - \exp(-\mu \sin^2(\delta/2))}{2M}. \tag{7}$$

The key generation rate is a value proportional to the probability p of successfully receiving information about the sent state.

3. Choice of a basis using a pseudorandom number generator

Note that for a fixed δ, the conclusive result probability is inversely proportional to the number of bases used in the protocol. This, in turn, limits the key generation rate.

The basis b in the above-described protocol was randomly selected. It makes sense to consider the possibility of using a pseudorandom sequence generator to select the values of the parameter b. In other words, Alice and Bob initially have some common secret, a seed of a pseudorandom sequence. Using this information, they can deterministically obtain identical sequences of bases b. In this case, the schemes given below will no longer be unconditionally secure protocols of quantum key distribution; however, if certain assumptions are fulfilled, we can talk about their security. An important protocol that uses a pseudorandom sequence to select bases is the Y-00 protocol [12, 13]. This protocol uses the above-discussed configuration of states for a large number of bases ($M \gg 1$) with a phase shift between the basis states $\delta = \pi$. The protocol also uses the high intensity of the transmitted coherent states ($\mu \gg 1$), which makes it possible to employ homodyne detection that, at a high intensity and with Bob's knowledge of the basis, yields a small error.

The Y-00 protocol has a high key generation rate with relatively simple implementation [14]; however, it provides only practical security when the eavesdropper is limited by the current technological level and cannot, for example, store states in quantum memory for a long time and perform collective measurements over quantum states in a space of large dimension.

We propose generating the numbers of bases b in a pseudorandom manner, as in the Y-00 protocol, but we assume that Bob uses a single-photon detector. This allows weak coherent states to be used in transmission. Note that for small μ, the basis states become less distinguishable, which makes it difficult to eavesdrop even in the absence of assumptions about the technological capabilities of the eavesdropper: Even after calculating the seeed of the pseudorandom sequence, Eve cannot obtain enough information about the key due to the indistinguishability of the measured states. However, if Eve calculates the seed of the pseudorandom sequence before the transfer of quantum states is completed, then the protocol we are describing is vulnerable to a USD attack, because Eve can make an error-free measurement in each position in the basis known to her, after which, according to the USD attack scenario, she blocks the state with an inconclusive result or increases its intensity when receiving all the information. As a result, the protocol is secure under the assumption that the calculation time of the seed of the pseudorandom sequence is longer than the communication session between Alice and Bob, and this weak computational assumption is the only assumption about the eavesdropper capabilities in the proposed scheme.

It will be shown below that the protocol is still secure when the seed of the pseudorandom sequence is calculated after the communication session, because Eve is no longer able to block the messages from which she was unable to extract information. Since, in addition to the seed, there is no information that can help Eve obtain the secret key, the key security does not change over time, which is an important advantage of the quantum key distribution. Between communication sessions, Alice and Bob change the seed of the pseudorandom number generator, taking part of the secret key distributed between them, and therefore calculating the seed of previous sessions is not relevant when intercepting the key distributed during the next communication sessions.

Finally, we can consider a whole family of protocols, each representative of which is determined by the selected values of the parameters μ, δ and M. Since the bases are selected in accordance with a pseudorandom sequence, in the protocols we propose, the conclusive result probability for Bob will not depend on the number of bases used and according to (6) and (7) is equal to $1 - e^{-\mu}$ and $(1 - e^{-\mu \sin^2(\delta/2)})/2$ for $\delta = \pi$ and $\delta \neq \pi$, respectively.

Thus, an increase in the parameter M does not affect the key generation rate. Using a large number of bases makes the protocol more secure to a USD attack.

4. Beam-splitting attack

For the protocol (μ, M, δ), we will consider one of the basic attacks on coherent-state protocols under the conditions of communication channel attenuation – a beam-splitting attack. With such an attack, for every state $|\alpha_k^{(b)}|$ sent by Alice, Eve uses a beam splitter, which divides the beam into two (Fig. 3). One part ($|t\alpha_k^{(b)}|$) is sent to Bob, and the other ($|r\alpha_k^{(b)}|$, where $|t|^2 + |r|^2 = 1$) is used for the optimal collective measurement to obtain maximum information about the value of the bit k. Note that Eve has the ability to store states in quantum memory and take measurements on the deferred part of the state after she computes the pseudorandom sequence. This means that at the moment of measurement the basis will be known to the eavesdropper and she will need to distinguish between the states $|r\alpha_0^{(b)}|$ and $|r\alpha_1^{(b)}|$.

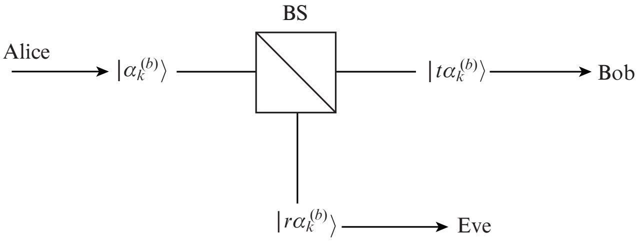

Figure 3. Beam-splitting attack: (BS) beam splitter; $|t|^2$ and $|r|^2$ are the transmission and reflection coefficients, respectively.

The greatest information that can be extracted is limited by the Holevo value [26], which has the following form for two equally probable pure states:

$$\chi(|r\alpha_0^{(b)}\rangle, |r\alpha_1^{(b)}\rangle) = H\left(\frac{|r\alpha_0^{(b)}\rangle\langle r\alpha_0^{(b)}| + |r\alpha_1^{(b)}\rangle\langle r\alpha_1^{(b)}|}{2}\right)$$

$$= h_2\left(\frac{1 - |\langle r\alpha | \mathrm{e}^{\mathrm{i}\delta} r\alpha\rangle|}{2}\right), \tag{8}$$

where $H(\hat{\rho}) = \mathrm{Tr}(\hat{\rho}\log\hat{\rho})$ is the von Neumann entropy, and $h_2(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy.

The expected signal intensity at the receiver in the attenuating communication channel is $\mu 10^{-\kappa L/10}$, where L is the channel length and $\kappa > 0$ is the attenuation parameter. Below, we will assume $\kappa = 0.2$ dB km^{-1}, which corresponds to the parameters of optical fibre. By assumption, Eve can replace the channel between Alice and Bob with a perfect lossless channel, and then, in order for the expected intensity signals to arrive at the receiver, the parameters of Eve's beam splitter should be determined by the relations

$$|r|^2 = 1 - 10^{-\frac{\kappa L}{10}},\ |t|^2 = 10^{-\frac{\kappa L}{10}}. \tag{9}$$

We denote the initial scalar product of Alice's states within the basis by ε. Then

$$\varepsilon = |\langle\alpha | \mathrm{e}^{\mathrm{i}\delta}\alpha\rangle| = |\mathrm{e}^{\mu(\mathrm{e}^{\mathrm{i}\delta} - 1)}| = \mathrm{e}^{-2\mu\sin^2(\delta/2)}, \tag{10}$$

and using this quantity we express the probability of a conclusive result on Bob's side (this probability depends on the length of the communication line L, rather than on whether the attack was performed or not, because Eve simulates the attenuation in the channel by the beam splitter):

$$p(\varepsilon, L) = \frac{1 - \varepsilon^{|t|^2/2}}{2^s} = \frac{1 - \varepsilon^{1/_2 10^{-\kappa L/10}}}{2^s}, \tag{11}$$

where, in accordance with the measurement schemes described in the previous section, $s = 0$, if $\delta = \pi$, otherwise $s = 1$.

For the information that Eve can extract from her states, we obtain

$$\chi(\varepsilon, L) = \chi(|r\alpha_0^{(b)}\rangle, |r\alpha_1^{(b)}\rangle)$$

$$= h_2\left(\frac{1 - \varepsilon^{|r|^2}}{2}\right) = h_2\left(\frac{1 - \varepsilon^{1 - 10^{-\kappa L/10}}}{2}\right). \tag{12}$$

Thus, both the largest information extracted by Eve during measurement and the conclusive result probability on Bob's side depend only on the initial scalar product of states within the basis $\varepsilon = |\langle\alpha|\mathrm{e}^{\mathrm{i}\delta}\alpha\rangle|$ and the communication channel length L.

For the secret key generation rate [27], taking into account the conclusive result probability, Bob has

$$R(\varepsilon, L) = p(\varepsilon, L)[1 - h_2(q) - \chi(\varepsilon, L)], \tag{13}$$

where q is the average observed probability of an error in the channel between Alice and Bob (quantum bit error rate, QBER). The critical error Q, at which the key generation rate vanishes, is determined by the expression

$$h_2(Q) = 1 - \chi(\varepsilon, L). \tag{14}$$

Solving the following equation

$$\frac{\partial R(\varepsilon, L)}{\partial \varepsilon} = 0, \tag{15}$$

we can find the dependence of the optimal scalar product $\varepsilon_{\mathrm{opt}}(L)$ of Alice's states within the basis, giving the highest key generation rate, on the communication channel length L. In the case of a zero error level ($q = 0$), this dependence is shown in Fig. 4.

The given value of ε can be obtained by varying the parameters μ and δ. In other words, for optimal protocol operation, it is necessary to choose such values of the phase shift and intensity of transmitted signals so that the relation

$$\mu\sin^2\frac{\delta}{2} = -\frac{1}{2}\ln(\varepsilon_{\mathrm{opt}}) \tag{16}$$

is fulfilled.

Suppose that one of the parameters, δ or μ, should remain unchanged regardless of the current length L of the communication channel. Let us assume that we use light signals of only certain intensity. Then the optimal value of ε can be obtained

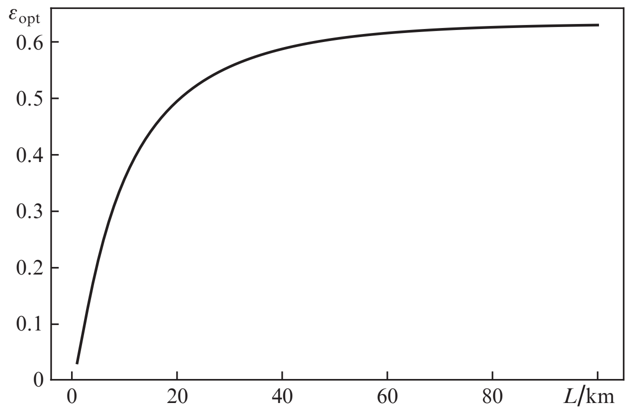

Figure 4. Dependence of the optimal scalar product of basis vectors $\varepsilon_{\rm opt}$ on the communication channel length L at $q = 0$.

by changing the value of the phase shift between the basis states δ. It also means that on Bob's side, a single-detector measurement scheme is used. If it is technically possible to change the signal intensity, then it is more preferable to use a scheme with two detectors, setting $\delta = \pi$. In this case, the intensity value of the signals used must coincide with the optimal value of the parameter for a given length of the communication line, i.e.

$$\mu(L) = -\frac{1}{2}\ln(\varepsilon_{\rm opt}(L)). \tag{17}$$

The obtained dependence of the key generation rate on L for both cases is presented in Fig. 5.

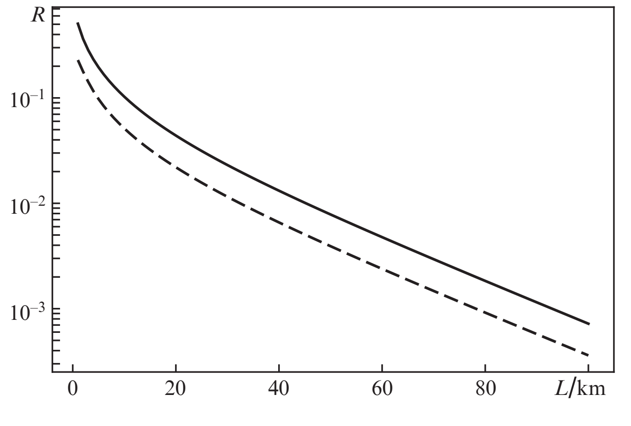

Figure 5. Dependence of the key generation rate R on the communication channel length L at $q = 0$ and the optimal choice of ε. Two cases were considered: (solid curve) the intensity μ depends on the length of the communication channel, $\delta = \pi$; and (dashed curve) the phase shift δ depends on the length of the communication channel, and $\mu = 1.0$.

With a large number of M bases used and large losses in the channel (which corresponds to key transmission over a long distance), the beam-splitting attack is close to an optimal one. Indeed, since, according to our assumption, Eve does not know the basis at the time of signal transmission (because she cannot calculate the seed of the pseudorandom sequence), she cannot use the USD measurement, which gives complete information about the transmitted states, and an attempt to perform such a measurement without knowing the basis will have a very low success probability, as shown in [21]. Further, due to the fact that the attenuation in the communication channel is large, Eve sends after the beam splitter a very low intensity state to Bob, from which she cannot extract much information (since the Holevo value for these states is very small); therefore, an attempt to apply a coherent attack introducing an error will not lead to any noticeable increase in amount of information on the eavesdropper's side.

5. Possible protocol modifications

The above-described beam-splitting attack requires the eavesdropper to be able to store states in quantum memory for the entire time during which the seed of the pseudorandom sequence is calculated, and the only restriction imposed on the eavesdropper is the inability to calculate the seed of the pseudorandom sequence during the communication session. We can also consider another practical limitation on the eavesdropper: decoherence of its quantum memory. In this case, its information about the states will be less than $\chi(\varepsilon, L)$ in (12), which means an increase in the key generation rate under yet another assumption about the eavesdropper's capabilities – nonideality of the quantum memory. Thus, the optimal value of the scalar product of states within the basis on Alice's side can become less than the value calculated under the assumption of Eve's ideal quantum memory, which also means an increase in the secret key length due to Bob's greater number of conclusive results due to the greater distinguishability of the states. Therefore, using the assumption of a technical limitation on Eve's quantum memory, it is possible to increase the key generation rate in the proposed scheme.

Let us discuss one more modification of the constructed protocol family. Thus, the scheme with parameters (μ, δ and M) turned out to be secret under the assumption that the eavesdropper cannot calculate the pseudorandom sequence during the transmission of signals and measurements of $\tau_{\rm session}$ at the receiver'. If we denote the time for calculating the seed of the pseudorandom sequence by $\tau_{\rm calc}$, we obtain that security is ensured if the inequality

$$\tau_{\rm calc} > \tau_{\rm session} \tag{18}$$

holds.

If the last condition is not met, the protocol is vulnerable to a USD attack. To avoid loss of security, it is necessary to increase the $\tau_{\rm calc}$ time. An obvious opportunity to do this is to return to truly random basis generation. In this case, Eve, in principle, cannot in a deterministic way find out in what basis the signals are transmitted. Thus, we return to the original quantum key distribution protocols in which the generation rate is inversely proportional to the number of the used bases.

To avoid a large drop in the key generation rate, we consider an intermediate version between truly random and pseudorandom basis choices. The number of bits required to encode the basis in one message is [log (M)]. We will select a certain number of bits $m <$ [log (M)] at random, and the rest using a pseudorandom sequence. In this case, Eve will need to carry out an additional enumeration of 2^m options in the calculations, which, in turn, increases $\tau_{\rm calc}$. Thus, we select m so that condition (18) is satisfied. Then for the probability of a conclusive result, we have

$$p = \frac{1 - \mathrm{e}^{-\mu}}{2^m}, \ \delta = \pi, \tag{19}$$

$$p = \frac{1 - \mathrm{e}^{-\mu \sin^2(\delta/2)}}{2^{m+1}}, \ \delta \neq \pi. \tag{20}$$

Taking into account the new parameter m, we expand the family of the introduced protocols. Now each representative will have its own set of signal intensities, bases, phase shifts between the states of one basis and random bits encoded in the basis b. With the introduced designations, we will use the notation (μ, M, δ, m) for the corresponding protocol. The measurements on Bob's side will also be described by the scheme depicted in Fig. 2.

6. Conclusions

A family of protocols is proposed that combine the use of random and pseudorandom choice of bases and can be considered as a generalisation of the previously proposed 4 + 2 protocols and the protocol on geometrically uniform states, as well as the Y-00 protocol. The security of this family with respect to two basic attacks – a USD attack and a beam-splitting attack– is shown under a weak computational assumption of the eavesdropper's capabilities. However, at the moment it is premature to talk about the security of the constructed family of protocols against an arbitrary attack, because even for a completely random choice of bases the tolerance of the protocol against attacks of general form has not been proved. Thus, there are more effective attacks on coherent-state quantum cryptography protocols, generalising the beam-splitting attack [28–30], although for the constructed family of protocols the benefit from their use is small due to the large number of bases. On the whole, the proof of the security of the constructed family of protocols against an arbitrary attack remains an open problem.

It is important to note that this family of protocols allows one to keep the main advantage of quantum cryptography, namely, the security of the key for unlimited time, which distinguishes this scheme from the schemes of classical cryptography and the Y-00 protocol.

The proposed family of protocols makes it possible to adjust the key generation rate under various assumptions about the capabilities of the eavesdropper. Thus, under the assumption of a restriction on quantum memory, this may be a scheme with more distinguishable states within the basis, which provides a higher key generation rate by reducing the conclusive result probability at the receiver. In situations where more stringent requirements are applied to the security of the key, the scheme makes it possible to use less distinguishable states within the basis and increase the share of true randomness in the choice of the basis, which means approximation to the schemes of truly quantum key distribution. Such regulation can be carried out only by changing the software part (without changing the hardware implementation), while it is possible to quickly switch between key generation regimes.

Two schemes for practical implementation are proposed: with two detectors and with one detector at the receiver's side, which reduces the cost of the scheme but decreases the key generation rate. Switching between different rates and security regimes in the second scheme does not require a change in intensity, which can be attributed to its advantages.

This work can be considered as an addition of the classical technology of pseudorandom generators to two existing protocols of quantum key distribution. However, according to a similar principle, this approach can be applied to other quantum cryptography protocols to increase the key generation rate and maintain stability against the USD attack. However, this is an issue of future research.

Acknowledgements. The authors are grateful to A.S. Trushechkin, D.V. Sych, I.V. Chizhov and Kentaro Kato for numerous discussions.

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

References

1. Bennett Ch.H., Brassard G. *Proc. Int. Conf. Comput., Syst. Signal Process. (Bangalore, India)* (New York: IEEE, 1984) pp 175–179.
2. Boaron A., Boso G., Rusca D., et al. *Phys. Rev. Lett.*, **121**, 190502 (2018).
3. Liao S.-K., Yong H.-L., Liu C., et al. *Nat. Photonics*, **11**, 509 (2017).
4. Shor P.W. *Proc. 35th Ann. Symp. Found. Comput. Sci.* (Los Alamos, 1994) pp 124–134.
5. Mosca M. *IEEE Secur. Priv.*, **16**, 38 (2018).
6. Bernstein D.J. *Post-Quantum Cryptography* (Berlin, Heidelberg: Springer, 2009) pp 1–14.
7. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nat. Photonics*, **4** (10), 686 (2010).
8. Bugge A.N., Sauge S., Ghazali A.M.M., Skaar J., Lydersen L., Makarov V. *Phys. Rev. Lett.*, **112** (7), 070503 (2014).
9. Blum M., Micali S. *SIAM J. Comput.*, **13** (4), 850 (1984).
10. Yashchenko V.V., Varnavskii N.P., Nesterenko Yu.V., et al. *Vvedenie v kriptografiyu* (Introduction to Cryptography) (Moscow: MTsNMO, 2012).
11. Smart N. *Cryptography: An Introduction* (New York: McGraw Hill, 2004; Moscow: Tekhnosfera, 2005).
12. Yuen H.P. arXiv:quant-ph/0311061 (2003).
13. Hirota O., Sohma M., Fuse M., Kato K. *Phys. Rev. A*, **72**, 02335 (2005).
14. Futami F., Guan K., Gripp J., Kato K., Tanizawa K., Chandrasekhar S., Winzer P.J. *Opt. Express*, **25** (26), 33338 (2017).
15. Trushechkin A.S., Tregubov P.A., Kiktenko E.O., Kurochkin Y.V., Fedorov A.K. *Phys. Rev. A*, **97**, 012311 (2018).
16. Tregubov P.A., Trushechkin A.S. *Itogi Nauki i Tekhniki, Seriya Sovremennaya Matematika i Ee Prilozheniya. Tematicheskie Obzory*, **151**, 91 (2018).
17. Guha S., Hayden P., Krovi H., Lloyd S., Lupo C., Shapiro J.H., Takeoka M., Wilde M.M. *Phys. Rev. X*, **4** (1), 011016 (2014).
18. Huttner B., Imoto N., Gisin N., Mor T. *Phys. Rev. A*, **51**, 1863 (1994).
19. Bennet C.H. *Phys. Rev. Lett.*, **68**, 3121 (1992).
20. Dušek M., Jahma M., Lütkenhaus N. *Phys. Rev. A*, **62** (2), 022306 (2000).
21. Chefles A., Barnett S.M. *Phys. Lett. A*, **250**, 223 (1998).
22. Chefles A. *Phys. Lett. A*, **239**, 339 (1998).
23. Molotkov S.N. *JETP Lett.*, **95**, 332 (2012) [*Pis'ma Zh. Eskp. Teor. Fiz.*, **95**, 361 (2012)].
24. Miroshnichenko G.P., Kozubov A.V., Gaidash A.A., Gleim A.V., Horoshko D.B. *Opt. Express*, **26** (9), 11292 (2018).

25. Kozubov A., Gaidash A., Miroshnichenko G. arXiv:1903.04371 (2019).
26. Holevo A.S. *IEEE Trans. Inform. Theory*, **44** (1), 269 (1998).
27. Devetak I., Winter A. *Proc. Roy. Soc. A: Math., Phys., Eng. Sci.*, **461** (2053), 207 (2005).
28. Kronberg D.A., Kiktenko E.O., Fedorov A.K., Kurochkin Yu.V. *Quantum Electron.*, **47** (2), 163 (2017). [*Kvantovaya Elektron.*, **47** (2), 163 (2017)].
29. Kronberg D.A., Kurochkin Yu.V. *Quantum Electron.*, **48** (9), 843 (2017) [*Kvantovaya Elektron.*, **48** (9), 843 (2017)].
30. Avanesov A.S., Kronberg D.A., Pechen A.N. *Ultrametr. Anal. Appl.*, **10** (3), 222 (2018).