Quantum Electronics **51** (10) 928–937 (2021)

QUANTUM CRYPTOGRAPHY

https://doi.org/10.1070/QEL17625

Vulnerabilities of quantum cryptography on geometrically uniform coherent states

D.A. Kronberg

Abstract. **It is shown that the quantum cryptography protocol on geometrically uniform coherent states, which uses the restriction for unambiguous discrimination of a set of symmetric coherent states and allows resisting an unambiguous state discrimination attack (USD attack), is not secure to a number of other attacks. The key length formula from the work of S.N. Molotkov [*JETP Lett.*, 101 (8), 579 (2015)] and the key generation rate for a number of constructive attacks of the eavesdropper are compared and it is shown that the key generation rate in this work is significantly overestimated. This leads to the fact that the distributed key is not secret.**

Keywords: *quantum cryptography, coherent states, quantum information theory.*

1. Introduction

The goal of quantum cryptography [1–3], or, more precisely, quantum key distribution, is the distribution of a shared key between two remote users, the key secrecy being not based on any assumptions about the limited capabilities of the eavesdropper. Thus, the distributed key must be secure against *any* actions (attacks) of an eavesdropper that do not contradict the laws of quantum mechanics. For a number of protocols of quantum key distribution, security proof have been obtained [4–7]; however, for some protocols, the construction of the security proof against all possible attacks is an unsolved and very challenging task.

A number of attacks in quantum cryptography are best known because they most clearly demonstrate the capabilities of an eavesdropper due to certain technological restrictions imposed on legitimate users. In this regard, when proposing a new quantum cryptography protocol, it is reasonable to test its security against the most well-known attacks. However, this resistance does not mean that the protocol will remain secure against all other attacks.

The quantum cryptography protocol on geometrically uniform coherent states [8–10] is aimed at counteracting an unambiguous state discrimination attack (USD attack) [11], also called unambiguous measurement attack (UM attack). In this attack, which is possible for linearly independent states in a lossy line, the eavesdropper obtains full information from them with a certain probability of success. In the case of failure, the eavesdropper blocks the states, and in the case of success, the eavesdropper sends them to the receiving side, increasing their intensity. The protocol uses a configuration of symmetric coherent states, for which the upper bound for the unambiguous discrimination probability is known [12]. This makes it possible to ensure the impossibility of a USD attack at practically important distances due to the use of a sufficiently large number of states. Molotkov [9] presented a formula for generating a secret key, which, among other things, is related to the USD success probability.

However, being secure against a USD attack does not mean being resilient against any other attack for a lossy line. The key disadvantage of a USD attack from an eavesdropper's point of view is that it does not use information about the bases that legitimate users announce when communicating over a public channel. Given the use of a large number of states, this information is quite valuable and can be used to construct a number of other attacks. This paper proposes attacks that exploit this information. Conditions are presented under which the considered attacks demonstrate an overestimation of the key generation rate presented in [9], which leads to the nonsecrecy of the distributed keys.

Chefles and Barnett [12] note that the formulae for working with symmetric coherent states cannot be reduced to a simple form; therefore, the main results of the work, presented in the plots of the key generation rate and critical intensities, were obtained numerically. For each constructed attack, physical ideas describing its fundamental feasibility and the reasons for its effectiveness will be considered.

The paper is organised as follows. Section 2 briefly describes the quantum cryptography protocol on geometrically uniform coherent states. Section 3 is devoted to the derivation of the formula for the key generation rate presented in [9]. Section 4 discusses the most conceptually simple attack in quantum cryptography – the beam splitting attack. It is shown that even against such an attack, the key generation rate is overestimated. The eavesdropping scheme using an active beam splitter is also described, which will be used in further sections. Sections 5–7 discuss other attacks: modified photon-number splitting attack, state amplification attack, and key bit discrimination attack. For some attacks, the key generation rates are presented, and for others, the critical value of the intensity depending on the length of the communication line. The Conclusions presents the main results of the work.

D.A. Kronberg Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia;
e-mail: dmitry.kronberg@gmail.com

Received 17 June 2021
Kvantovaya Elektronika **51** (10) 928–937 (2021)
Translated by I.A. Ulitkin

2. Protocol on geometrically uniform states

The idea of using symmetric coherent states in quantum cryptography is found in Refs [13–16], as well as in later works [8–10, 17, 18], and some protocols have been implemented in practice [19–21]. Here is a description of the protocol from Refs [8–10].

Recall that the coherent state $|\alpha\rangle$ is written as

$$|\alpha\rangle = \exp(-|\alpha|^2/2)\sum_{n=0}^{+\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

where $|n\rangle$ is the Fock basis. The protocol uses N symmetric coherent states of the form [12]

$$|\alpha_j\rangle = |\alpha\exp(\mathrm{i}2\pi j/N)\rangle, \quad j = 0,\ldots,N-1,$$

that is, for all such states, the intensities $\mu = |\alpha|^2$ coincide, and the phase takes values $\{2\pi j/N\}_{j=0}^{N-1}$ from a set with equal intervals. Since N is an even number, the states are divided by $M = N/2$ bases. The phase shifts θ inside each basis coincide and, therefore, the states of one basis b, corresponding to sending 0 and 1, have the form

$$\begin{aligned}|\alpha_b^0\rangle &= |\alpha\exp[\mathrm{i}2\pi k(b)/N]\rangle,\\ |\alpha_b^1\rangle &= |\alpha\exp\{\mathrm{i}[2\pi k(b)/N+\theta]\}\rangle,\end{aligned} \tag{1}$$

where the initial value of $k(b)$ for each basis is determined by the configuration of states.

In what follows, we will use the notations traditional for quantum cryptography, as well as we will call Alice and Bob legitimate users, and the eavesdropper will be called Eve.

At the first step, Alice randomly chooses a basis $b \in \{0,\ldots,M-1\}$ and a bit $k \in \{0,1\}$ in each position, and then sends the corresponding state $|\alpha_b^k\rangle$ to Bob. More precisely, Alice sends a reference state $|\alpha\rangle$, the phase of which is known and is always the same [8], and an information state; therefore, her states have the form

$$|\psi_b^k\rangle = |\alpha\rangle\otimes|\alpha_b^k\rangle. \tag{2}$$

Bob receives a state after the signal has passed a communication line of length L. Coherent states in fibre-optic communication lines are converted in a self-similar way, and Bob's state in the absence of an eavesdropper will differ from Alice's state only by the intensity μ, which is converted into

$$\tilde{\mu} = \mu\times 10^{-\kappa L/10}, \tag{3}$$

where κ is the attenuation coefficient in the communication line, which is approximately 0.2 dB km^{-1} for optical fibre (hereafter, we will use this value).

Bob randomly chooses a basis and performs an unambiguous discrimination between the states of this basis [22]. The theoretical probability of success with unambiguous discrimination of states $\{|\tilde{\alpha}_b^0\rangle, |\tilde{\alpha}_b^1\rangle\}$, where $\tilde{\alpha} = \sqrt{\tilde{\mu}}$ [the reference state $|\alpha\rangle$ in (2) is needed to make a measurement, but it does not change scalar relations and the probability of success] [23], is

$$p_{\mathrm{succ}}^{\max} = 1 - |\langle\tilde{\alpha}_n^0|\tilde{\alpha}_n^1\rangle| = 1 - \exp[-(1-\cos\theta)\tilde{\mu}]. \tag{4}$$

In practice, however, the scheme may be less effective and give a lower probability of success. The scheme proposed in [9] with one detector and a phase modulator for selecting a bit within the basis gives the success probability (for more details, see [17])

$$p_{\mathrm{succ}} = \tfrac{1}{2}\{1 - \exp[-\tfrac{1}{2}(1-\cos\theta)\tilde{\mu}]\}. \tag{5}$$

In what follows, for the success probability with unambiguous state discrimination, we will use formula (5), although formula (4) gives similar results. Let us assume that the equipment of legitimate users works perfectly: In particular, the detectors on the receiving side have a unit efficiency and a zero dark count rate.

After Alice transmits states in all positions, and Bob makes measurements, they proceed to the stage of *basis reconciliation*: Through a public channel, they reveal the bases used to prepare and measure states in each position, and discard messages in case of mismatch (the probability of basis matching is $1/M = 2/N$). Messages where Bob's measurement gave an inconclusive outcome are also discarded. As a result, *a raw key* is obtained.

At the next stage – *error correction*, Alice and Bob correct errors in the raw key, also communicating over a public channel; as a result, part of the information about the key is revealed. Before that, they evaluate the error by revealing a part of the raw key and then discarding the revealed positions (note that there are more efficient methods for evaluating the error, see, for example, [24, 25]). Information leakage to the eavesdropper at this stage is denoted as leak, and it is also taken into account when calculating the length of the final key. After error correction, Alice and Bob have matching keys (except for a very small probability of incorrect operation of the error correction module, which we will neglect in our work).

At the last stage – *privacy amplification*, legitimate users compress their key to discard the eavesdropper's information. At this stage, it is important that the correct upper estimate of the eavesdropper's information is used in the formula for the length of the final key: In this case, the eavesdropeer's information about the final key will be close to zero. An error in evaluating the eavesdropper's information and overestimating the key length can lead to the fact that part of the final key will be known to the eavesdropper, which is unacceptable. Section 3 describes the formula for the length of the secret key from paper [9].

Vtyurina et al. [20] and Borisova et al. [21] mention the practical implementation of the protocol; in particular, Borisova et al. [21] present the most relevant sets of parameters from a practical point of view: an intensity, $\mu = 0.3-0.5$ photons per pulse, an attenuation of 18 dB in the channel (which in our the model corresponds to a 90-km-long fibre-optic communication line, although in practical systems such attenuation is possible at other communication line lengths), and a quantum bit error rate of 3%–6%.

3. Formula for the secret key generation rate

The formula for the secret key generation rate is a major theoretical element of the quantum cryptography protocol. In fact, the security proof is reduced to the proof of the fact [6, 7] that if we choose the length of the final key according to the formula, then the key will be secret in accordance with the

secrecy parameter (for more details about the secrecy parameter, see [26]).

As the basic formula for the secret key length (or, which is the same, the secret key generation rate), Molotkov [9] uses the Devetak–Winter formula [27]

$$R_{\text{key}} = I(\text{A}:\text{B}) - I(\text{A}:\text{E}) = H(X|\text{E}) - \text{leak}, \tag{6}$$

where I is the mutual information between the users (A stands for Alice; B, for Bob; and E, for Eve); and $H(X|\text{E})$ is the conditional entropy that characterises Eve's lack of information about the key X if she has quantum states obtained with the best attack.

From formula (6) it follows that the length of the secret key in terms of one message is determined by the difference between the mutual information of legitimate users and the eavesdropper's information about the key. Evaluation of the eavesdropper's information is nontrivial: As follows from [9], it should depend only on the parameters observed on the receiving side, as well as on the state configuration that is known to legitimate users. Let p_{click} be the probability of the detector click at the receiver side; then $p_{\text{loss}} = 1 - p_{\text{click}}$ is the observed probability of loss. The observed parameters also include Q, that is, the quantum bit error rate in the raw keys of legitimate users.

The USD attack is considered the most powerful attack in the case of attenuation. Let us denote the probability of success with unambiguous discrimination of initial states by p_{USD}; for this probability an upper bound was given in [12]. If p_{loss} is greater than the probability of failure of unambiguous discrimination of initial states, $1 - p_{\text{USD}}$, then the eavesdropper knows the entire key, since it can carry out a USD attack. If the level of losses is less than the probability of failure of unambiguous discrimination, then it is assumed that the optimal strategy for the eavesdropper is to apply unambiguous state discrimination to the fraction of messages, δ. In fact, Eve in each position with probability δ applies unambiguous state discrimination, and in the rest of the messages, the fraction of which is $1 - \delta$, performs optimal individual measurements. Moreover, when evaluating Eve's information extracted from such a measurement, it is assumed that at the time of measurement, Eve knows the basis, but does not know the set of codewords, as a result of which her information is estimated through C_1, that is, the one-shot capacity for two vectors in one basis [28, 29]. For two pure equiprobable states $\{|\alpha_b^0\rangle, |\alpha_b^1\rangle\}$,

$$C_1 = 1 - h_2\left(\frac{1 - \sqrt{1 - |\langle\alpha_b^0|\alpha_b^1\rangle|^2}}{2}\right),$$

where $h_2(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$ is the Shannon binary entropy.

It is also important that both for the positions in which unambiguous discrimination was applied, and for the positions in which Eve did not apply this discrimination, she resends the states with high intensity instead of the original ones to Bob. This is done in order to compensate for the insertion loss as much as possible: In this case, unambiguous discrimination can be applied to a larger fraction of the states.

In this case, the total length of the raw key (the eavesdropper's information is not taken into account here) is

$$R_{\text{raw key}} = 1 - \delta + \delta p_{\text{USD}} = 1 - p_{\text{loss}},$$

from which we can conclude that the fraction of the messages δ, to which unambiguous discrimination is applied, is $p_{\text{loss}} \times (1 - p_{\text{USD}})^{-1}$.

The length of the secret key, taking into account Eve's information, is expressed as follows. From the entire raw key of length $1 - p_{\text{loss}}$ Eve knows the leak information obtained from the public channel during error correction (this value depends both on the observed error Q and on the error correction method used by legitimate users). She also knows all the information about the δp_{USD} part for which unambiguous discrimination was successful, and the C_1 information about the $1 - \delta$ part, to which unambiguous discrimination was not applied, but which got into the key. We have

$$R_{\text{key}} = (1 - p_{\text{loss}})(1 - \text{leak}) - (1 - \delta)C_1 - \delta p_{\text{USD}}, \tag{7}$$

which coincides with formula (11) in [9] {see also [30], where this formula is given under number (7) with duplication of argumentation}.

It is emphasised that this formula includes a conservative upper bound for Eve's information, and it depends only on the values observed and calculated based on the parameters of the protocol.

Let us briefly list the main mistakes made in the derivation of formula (7):

1. The application of unambiguous discrimination to a part of the messages is not an optimal strategy; more effective attacks will be proposed below.

2. It is incorrect to evaluate the information of the eavesdropper through the one-shot capacity, C_1, since in other attacks it can make measurements knowing the set of codewords.

In the following sections, these theses are clarified, and attacks are demonstrated in which the eavesdropper has more information, that is, in which the key generation rate should be lower. In fact, this means that if we use formula (7), then part of the key turns out to be known to the eavesdropper, which, of course, is unacceptable.

Figure 1 shows the dependence of the secret key generation rate on the distance between legitimate users, as well as this rate per one bit of the raw key:

$$R_{\text{key/bit}} = \frac{R_{\text{key}}}{R_{\text{raw key}}}$$

$$= \frac{(1 - p_{\text{loss}})(1 - \text{leak}) - (1 - \delta)C_1 - \delta p_{\text{USD}}}{1 - p_{\text{loss}}}. \tag{8}$$

The dependence obtained by formula (8) is more evident on a linear scale; therefore, in the future we will often compare the key lengths for this particular case. Note that formulae (7) and (8) do not contain the probability of basis matching $1/M$; however, when choosing the optimal parameters of the protocol, these probabilities, of course, must be taken into account.

4. Beam splitting attack, schematic of an active beam splitter

This section shows that formula (7) turns out to be inaccurate even when the eavesdropper uses the conceptually simplest attack for a lossy line: the beam splitting attack. This attack boils down to the fact that Eve simulates losses in the channel using a beam splitter, taking away part of the state, and then

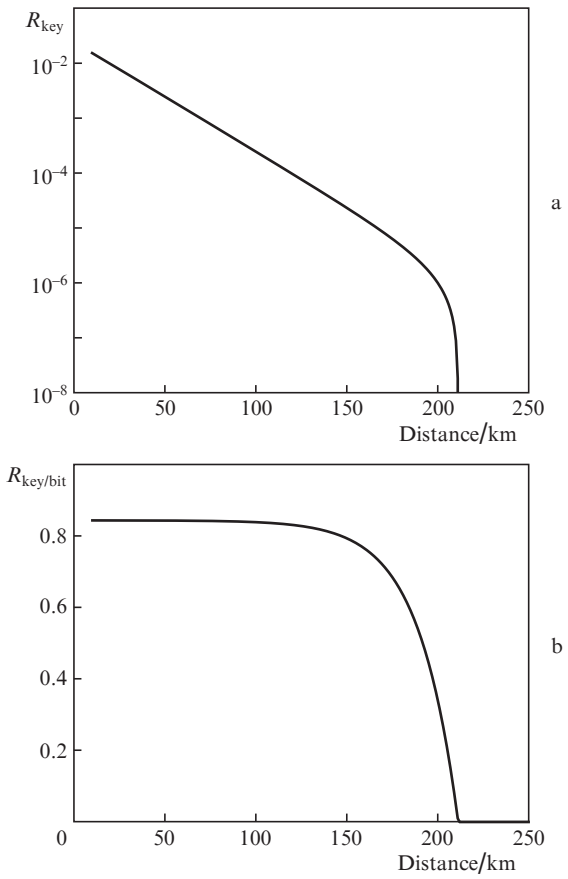

Figure 1. Dependences of the secret key generation rate on the distance between legitimate users for the protocol on geometrically uniform states with $N = 8$ states, divided into $M = 4$ bases (intensity $\mu = 0.4$ photons per pulse, phase shift within the basis $\theta = \pi/4$) according to formula (7) (a) and in terms of one bit of the raw key according to formula (8) (b). The attenuation in the communication line is $\kappa = 0.2$ dB km^{-1} and the error is zero.

measures this part, knowing the basis. This section also describes the scheme of an active beam splitter, which will be needed below to build more effective attacks.

The action of the beam splitter on the coherent state $|\alpha\rangle$, where the vacuum state is at the second input, can be described as

$$|\alpha\rangle_A \to |t\alpha\rangle_B |r\alpha\rangle_E, \tag{9}$$

where r and t are the reflectance and transmittance, respectively; and $|r|^2 + |t|^2 = 1$. In order for Bob to obtain the state with the intensity $\tilde{\mu}$, determined from (3), Eve needs to use the coefficient $t = \sqrt{\tilde{\mu}/\mu}$.

Next, Eve sends the states $t = \sqrt{\tilde{\mu}/\mu}$ over a lossless channel to Bob, and Bob receives exactly what he expects. Eve stores the states $|r\alpha\rangle_E$ in her quantum memory and measures them after the bases are anounced and after the disclosure of the rest of the information (such as the set of codewords for error correction). Eve's information $I_{BS}(A:E)$ in this case is given by the Holevo value [28, 31] of the states $\{|r\alpha_b^0\rangle_E, |r\alpha_b^1\rangle_E\}$ within the basis:

$$I_{BS}(A:E) = h_2\left(\frac{1 - |{}_E\langle r\alpha_b^0 | r\alpha_b^1\rangle_E|}{2}\right) =$$

$$= h_2\left\{\frac{1 - \exp[-(1 - \cos\theta)(\mu - \tilde{\mu})]}{2}\right\}.$$

The eavesdropper's information yields the key generation rate per one message

$$R_{key/bit,\,BS} = 1 - I_{BS}(A:E)$$

$$= 1 - h_2\left\{\frac{1 - \exp[-(1 - \cos\theta)(\mu - \tilde{\mu})]}{2}\right\}. \tag{10}$$

With a long communication line, $\tilde{\mu} \to 0$ and Eve's information tends to the Holevo value of the initial states; therefore, with such an attack, the eavesdropper does not receive full information even at very large channel losses.

Figure 2 shows the secret key generation rates per one bit of the raw key for formula (8) and for a beam splitting attack according to (10). One can see that at communication line of 12–172 km in length, the beam splitting attack works efficiently and the key generation rate turns out to be lower than that obtained by formula (8). The error that led to the overestimation of the key generation rate in (8) was already mentioned above: This is the use of the one-shot capacity C_1 instead of the Holevo value to estimate the eavesdropper's information. Such use is justified when an eavesdropper faces the need to measure states without a set of codewords [29] (see also [32]); however, in the case of a beam splitting attack, this is not necessary, and the eavesdropper can wait for the announcement of codewords. Thus, with a 90-km-long communication line (a loss of 18 dB, as in [21]), the key generation rate is overestimated by about 20%, which means that the eavesdropper knows more than 17% of the key.

It should be noted that if in (8) we replace the one-shot capacity C_1 by the Holevo value of states within the basis, then the beam splitting attack will no longer lead to a loss of secrecy, since the key obtained by the formula

$$R'_{key/bit} = \frac{(1 - p_{loss})(1 - leak) - (1 - \delta)\chi - \delta p_{USD}}{1 - p_{loss}}, \tag{11}$$

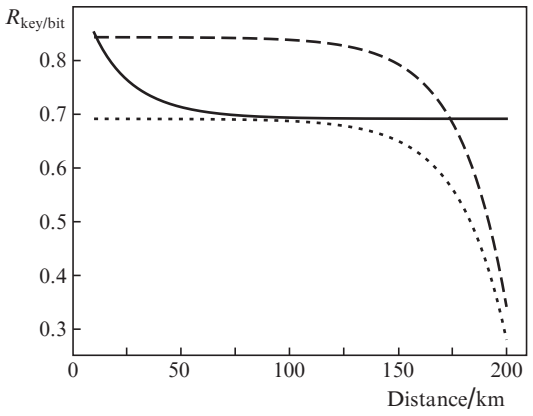

Figure 2. Dependences of the secret key generation rate on the distance between legitimate users in the case of a beam splitting attack, obtained by formula (10) (solid line), by formula (8) (dashed line), and also by formula (11) (dotted line). Protocol parameters are as follows: $N = 8$ states ($M = 4$ bases), intensity $\mu = 0.4$ photons per pulse, and phase shift within the basis $\theta = \pi/4$. The attenuation in the communication line is $\kappa = 0.2$ dB km^{-1}, and the error is zero.

where the Holevo value χ of equiprobable states $\{|\alpha_b^0\rangle, |\alpha_b^1\rangle\}$ is

$$\chi(\{|\alpha_b^0\rangle, |\alpha_b^1\rangle\}) = h_2\Big(\frac{1-|\langle\alpha_b^0|\alpha_b^1\rangle|}{2}\Big),$$

turns out to be shorter than the secret key obtained by formula (10) (Fig. 2). In what follows, however, more effective attacks will be described, for which formula (11) also turns out to be incorrect.

Let us describe here the scheme of an active beam splitter (Fig. 3), which has already been used for a number of attacks [33, 34] and will be used in our work. The essence of this eavesdropping technology is that Eve does not just keep the states assigned by the beam splitter in her quantum memory, but applies a transformation and, depending on its result, blocks the remaining state or sends it to the receiving side. This scheme allows for greater flexibility: Eve can send states to Bob only in those positions in which she is sure that she can get a lot of information from her states and block states in other cases. Another important advantage of such a scheme is that Eve performs the transformation over a part of the state that Bob does not get, and so she can introduce any changes there, and this will not lead to an error on the receiving side.

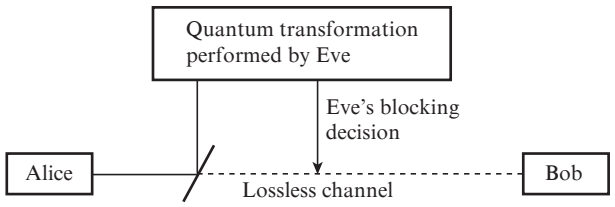

Figure 3. Scheme of an active beam splitting attack.

The condition for the applicability of an active beam splitting attack is that Bob's detector should be triggered with the same probability as in the absence of an attack. If Eve sends states with intensity $|t|^2\mu$ to the receiving side, then this imposes the following requirement on the probability of success $p_{\text{succ}}^{\text{E}}$ of her transformation (that is, on the probability of sending states):

$$\tfrac{1}{2}\{1-\exp[-\tfrac{1}{2}(1-\cos\theta)\tilde{\mu}]\} = \tfrac{1}{2}p_{\text{succ}}^{\text{E}}\{1-\exp[-\tfrac{1}{2}(1-\cos\theta)\,|t|^2\mu]\}. \quad (12)$$

The left-hand side of this expression corresponds to the expected probability (5) of obtaining a conclusive outcome within the basis in the absence of an eavesdropper. The right-hand side corresponds to the fact that the eavesdropper with the probability $p_{\text{succ}}^{\text{E}}$ sends pulses with the intensity $|t|^2\mu$ to the receiving side, and a conclusive outcome is obtained for these pulses on the receiving side.

Note that the scheme of an active beam splitter presented here has a drawback: In case of failure, the remaining state is blocked, while it is more efficient to apply a transformation over the entire state, so that in case of success, it also has a state for sending to Bob, and in case of failure, it always gives one and the same state at the output. Then, unitarity conditions will increase the overall probability of success (see, for example, [35]). Nevertheless, such a technique will complicate the mathematical description of the above attacks and make their physical interpretation less clear. However, since attack optimisation is not the goal of this work, we will consider below a conceptually simple active beam splitter scheme described here.

5. Variant of a photon-number splitting attack

This section will describe an attack that most clearly demonstrates the inaccuracy of formula (7) for the secret key length.

A photon-number splitting attack (PNS) was developed for the BB84 protocol and is described in detail in [15]. The essence of this attack is that if legitimate users use coherent states with phase randomisation

$$\rho_\mu = \int_0^{2\pi} |\sqrt{\mu}\exp(\mathrm{i}\phi)\rangle\langle\sqrt{\mu}\exp(\mathrm{i}\phi)|\frac{\mathrm{d}\phi}{2\pi} = \exp(-\mu)\sum_{n=0}^{+\infty}\frac{\mu^n}{n!}|n\rangle\langle n|,$$

then the eavesdropper can perform a nondemolishing measurement of the number of photons in a pulse, and then, if there are more than one photon, take some of them into its quantum memory. After revealing the bases, the eavesdropper performs a measurement in the required basis and receives all the information.

It is important to note here that the reasoning that led to formulae (7) and (8) for the secret key length does not depend in any way on the phase shift θ between states within the basis used in the protocol on geometrically uniform states. Therefore, if this reasoning is correct, the formulae should be valid for any value of θ. Moreover, it is not difficult to carry out numerical optimisation of the key length according to these formulae for an arbitrary length of the communication line, taking into account the probability of the basis mismatch, and to see that the optimal value of the phase shift is $\theta = \pi$. This also follows from such considerations: In formula (7), the key length depends on the scalar product between the vectors within the basis and on the probability of unambiguous state discrimination. If we fix the number of states and the scalar product within the basis, then the minimum probability of success for unambiguous state discrimination will be achieved on states with low intensity and with a phase shift π within the basis. In this case, the probability of a conclusive outcome on the receiving side, as can be seen from (4) and (5), depends only on the scalar product. Therefore, the optimal phase shift within the basis, according to (7), is the shift π. All the argumentation that led to formula (7) turns out to be valid for this case as well: Eve still has a limited probability of success for unambiguous state discrimination (which depends only on the intensity μ and the number N of coherent states rather than on θ); in addition, Eve's information is limited due to the nonorthogonality of states within the basis (although it was shown above that the use of the Holevo value instead of the one-shot capacity would be more justified). The phase shift θ will affect the value of C_1, but otherwise the formula for the key generation rate should remain correct.

Let us show that the use of the phase shift $\theta = \pi$ leads to a catastrophic loss of secrecy.

At first glance, the PNS attack is not applicable to a protocol that uses pure states without phase randomisation, since measuring the number of photons will result in the loss of phase information. However, we will show that the scheme of an active beam splitter described in Section 4 allows us to

bypass this problem. Let Eve leave some of the states with the intensity $|t|^2\mu$ to Bob, and assign herself the states with the intensity $|r|^2\mu$. Eve can perform any transformations allowed by quantum mechanics over her states. In particular, Eve can perform a general phase randomisation for a pair of the reference and information states $|r\alpha\rangle|r\alpha\exp(i\gamma)\rangle$ [see (2)], after which it will have the form [15]

$$\rho_\gamma^{\mathrm{E}} = \int_0^{2\pi} |r\alpha\exp(i\phi)\rangle\langle r\alpha\exp(i\phi)| \otimes |r\alpha\exp[i(\phi+\gamma)]\rangle\langle r\alpha\exp[i(\phi+\gamma)]| \frac{d\phi}{2\pi} = \exp(-2|r|^2\mu)\sum_{n=0}^{+\infty}\frac{(2|r|^2\mu)^n}{n!}|\psi_n(\gamma)\rangle\langle\psi_n(\gamma)|. \quad (13)$$

It is a mixture of states

$$|\psi_n(\gamma)\rangle = \sum_{m=0}^{n}\sqrt{\frac{C_n^m}{2^n}}\exp(im\gamma)\,|n-m\rangle|m\rangle \quad (14)$$

with a certain number of photons n, which the eavesdropper can measure without disturbing the states $|\psi_n(\gamma)\rangle$. In fact, the eavesdropper measures the total number of photons in two modes – reference and information modes, rather than the number of photons in each of them. If there is at least one photon, the eavesdropper stores it in his quantum memory, and sends the state of intensity $|t|^2\mu$ left after the beam splitter to Bob. If the number of photons is zero, the eavesdropper blocks the pulse heading towards Bob. After the basis is announced, the eavesdropper faces the task of extracting information from single-photon states $\{|\psi_1(2\pi k(b)/N)\rangle, |\psi_1(2\pi k(b)/N+\theta)\rangle\}$ within one known basis [see (1)], which, as it is easy to see, are mutually orthogonal for the phase shift $\theta = \pi$:

$$|\psi_1(2\pi k(b)/N)\rangle = \frac{1}{\sqrt{2}}(|1\rangle|0\rangle + \exp[i2\pi k(b)/N]\,|0\rangle|1\rangle).$$

$$|\psi_1(2\pi k(b)/N+\pi)\rangle = \frac{1}{\sqrt{2}}(|1\rangle|0\rangle + \exp[i2\pi k(b)/N+\pi]\,|0\rangle|1\rangle).$$

Thus, in the presence of at least one photon in its state (13), which happens with the probability $p_{\mathrm{succ}}^{\mathrm{E}} = 1-\exp(-2|r|^2\mu)$, the eavesdropper has all the information. The condition for the applicability of attack (12), as noted above, consists in the fact that the losses introduced by the eavesdropper are equal to the expected ones.

It is important to note here that condition (12) is independent of the total number of states N, that is, an increase in the number of states prevents the application of the USD attack, but does not interfere with the modification of the PNS attack described here. The effectiveness of the proposed attack arises due to the fact that the eavesdropper does not try to perform complex actions, such as discrimination of all N states. She only maps these states to mutually orthogonal pairs in each basis, which occurs during phase randomisation and blocking of messages in which the number of photons is zero. This operation has a significantly higher probability of success, which is independent of the number of states. It should also be noted that the described attack, in contrast to the USD attack, essentially uses information about the basis that is announced later, as a result of which it has a high efficiency. The fact that such an attack was not taken into account in the derivation of the secret key generation formula may have been caused by a gross error in [10, 30], where the PNS attack was called a special case of the USD attack. This is not the case, and in this section it is shown that the PNS attack is more powerful due to the use of subsequently announced information about the bases, which makes it unnecessary for the eavesdropper to discriminate all N states at the time of the attack.

Figure 4 shows the optimal intensity for each length of the communication line with a phase shift $\theta = \pi$ within the basis (with the optimal choice of the number of bases M) according to formula (7), taking into account the probability of basis matching, as well as the critical intensity at which the protocol ceases to be secret in the case of the PNS attack described here. It can be seen that, starting from a length of 45 km, with the signal intensity optimal from the point of view of (7), Eve receives all the information about the key.

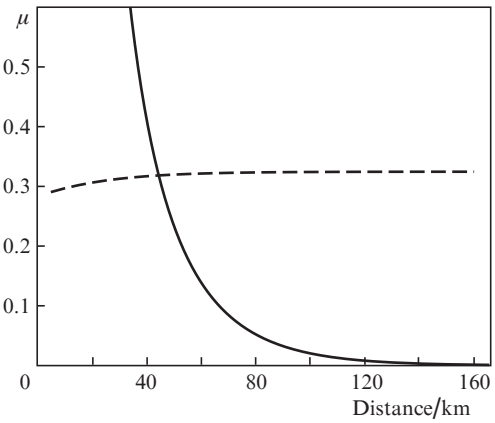

Figure 4. Dependences of the critical intensity μ, at which the eavesdropper knows the entire key, on the communication line length, if the eavesdropper uses a modified PNS attack (solid curve), as well as the optimal intensity according to (7) (dashed curve). The phase shift within the basis is $\theta = \pi$, the attenuation in the communication line is $\kappa = 0.2$ dB km^{-1}, and the error is zero.

The main conclusion of this Section is that for the phase-shift $\theta = \pi$, formula (7) turns out to be grossly incorrect. For other phase shifts, the attack considered here turns out to be less effective, since when only one photon is diverted, the eavesdropper has incomplete information due to the nonorthogonality of one-photon states of form (14). However, the eavesdropper can keep more than one photon, which can also increase the effectiveness of the proposed attack. A complete analysis of the constructed attack is beyond the scope of this work, the purpose of which is to demonstrate the most striking examples of the incorrectness of formula (7). In the subsequent sections, we consider the values $\theta = \pi/M$ corresponding to [9] and the attacks for them.

6. State amplification attack

In this Section, we will consider an attack that demonstrates significant key overestimation in practical conditions [21].

According to formula (7), if the probability of loss in the channel is less than the probability of failure with unambiguous discrimination of input states, Eve can no longer apply unambiguous discrimination to each position. Therefore, the USD attack is impossible at communication line lengths less

than the critical one, when Alice and Bob expect small losses. However, it is assumed in (7) that, at such small lengths, the optimal strategy for the eavesdropper is to apply unambiguous discrimination to the fraction δ of messages, and for the remainder, to use other eavesdropping strategies.

In papers [34, 36, 37], a different approach is proposed to the actions of an eavesdropper at the lengths of the communication line, in which a USD attack is impossible. Eve may not apply unambiguous discrimination in a probabilistic way, but make it only 'partially', that is, increase the distinguishability of input states without making them completely orthogonal (see also [38]). This operation has a higher probability of success, and therefore it is acceptable even in conditions of small losses in the channel. In this Section, we will offer a modified version of the attack from [37], which is simpler and more effective.

Let A be a matrix whose columns are the coefficients of each vector $\{|\alpha_j\rangle\}_j$ expanded in some orthonormal basis. Due to the linear independence of states, there is an inverse matrix A^{-1}. It is easy to see that the vectors $\{A^{-1}|\alpha_j\rangle\}_j$ are mutually orthogonal and have unit length. Next, we consider the set $\{|\beta_j\rangle\}_j$ of also symmetric coherent states with intensity μ_{B}, and the corresponding matrix of coefficients B. Obviously,

$$|\beta_j\rangle = BA^{-1}|\alpha_j\rangle;$$

thus, the BA^{-1} transformation, in the case when $\mu_{\mathrm{B}} > \mu$, increases the intensity of each state, while preserving their other properties. The Kraus operators for a quantum channel corresponding to success and failure can be defined as follows:

$$M_{\mathrm{succ}} = \frac{BA^{-1}}{\sqrt{\lambda}}, \quad M_{\mathrm{fail}} = \sqrt{1 - M_{\mathrm{succ}}^{\dagger} M_{\mathrm{succ}}}, \tag{15}$$

where λ is the maximum eigenvalue of the matrix $(BA^{-1})^{\dagger}BA^{-1}$. This quantum transformation, if successful, increases the intensity of all coherent states.

The attack based on the constructed transformation is simple: Eve performs transformation (15) and blocks the states in case of failure, and in case of success, she assigns part of them to her quantum memory, and sends part of them to Bob through a lossless channel. The attack has only two parameters: the intensity μ_{B} of states at the output of transformation (15), as well as the intensity of the state that Eve retains in case of success. It is not difficult to find numerically the values of these parameters for each channel length, which would yield maximum information to the eavesdropper. The eavesdropper's information about the key is given, as in the case of a beam splitting attack, by the Holevo value of its states within the basis.

Figure 5 shows the dependences of the key length on the length of the communication line for a protocol with $N = 8$ states with an intensity $\mu = 0.4$, divided into $M = 4$ bases. One can see that, for example, for a 165-km-long communication line, formula (8) overestimates the key length by about 64%; this means that approximately 39% of the keys are known to the eavesdropper. It is also shown that, in contrast to the beam splitting attack, even if the C_1 value in (8) is replaced by the Holevo value of the states, the secret key length will still be overestimated.

In addition, it makes sense to describe the results of applying the attack for the practical parameters presented in [21]: For example, on the city line of PJSC Rostelecom (attenuation of 18 dB, initial intensity of 0.5 photons per pulse, and observed error of 6%) overestimation of the key length exceeds 88%, that is the eavesdropper knows more than 46% of the key. Such a large overestimate is due to the fact that in the presence of an error, the eavsedropper receives relatively large information from the public channel during the error correction procedure, and the difference between the key lengths becomes even more significant. Note that here we considered the worst case for the eavesdropper, when, with the observed error Q, she receives only $h_2(Q)$ information, which corresponds to the use of codes with ideal efficiency. With practically available error correction methods, the eavesdropper has more information [9, 30], and the key length is even more overestimated.

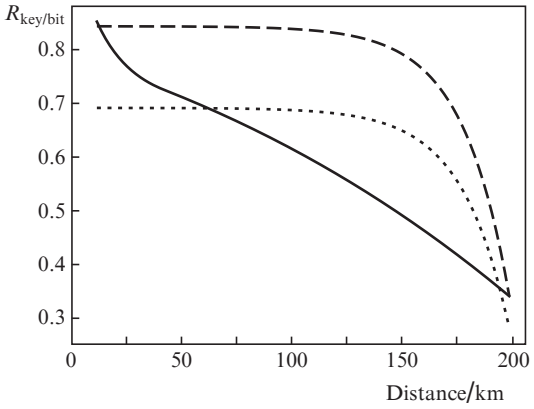

Figure 5. Dependence of the secret key generation rate on the distance between legitimate users in a state amplification attack (solid line), as well as dependences obtained by formulas (8) (dashed line) and (11) (dotted line). Protocol parameters are as follows: $N = 8$ states ($M = 4$ bases), intensity $\mu = 0.4$ photons per pulse, and phase shift within the basis $\theta = \pi/4$. The attenuation in the communication line is $\kappa = 0.2$ dB km^{-1}, and the error is zero.

Thus, the transformation of soft filtering [35, 36, 39], the next version of which was demonstrated here, is more effective for attacking and obtaining information with a given probability of success than the probabilistic application of unambiguous state discrimination, which was used to derive (7).

Note in addition that the attack proposed in [37], if applied to the same input parameters, also demonstrates an overestimation of the key length in formula (7).

7. Key bit discrimination attack

In this Section, we will consider an attack that shows that increasing the number of bases does not necessarily significantly help legitimate users to protect themselves from an eavesdropper in the case of attenuation. In this attack, the eavesdropper does not try to discriminate between all transmitted states, as she does in the USD attack and (in a milder form) in the state amplification attack described in Section 6. This action is quite 'expensive' for an eavesdropper, since it has a low probability of success with a large number of states. However, it is important to note that when carrying out an attack, the ultimate goal of an eavesdropper is to know the bits of the key, rather than which state is sent over the channel. Here we consider a generalisation of unambiguous state discrimination, which has a significantly higher probability of success, but identifies not a state, but only its belonging to a

class of states. This allows the discrimination between 0 and 1 in a raw key with a significantly increased probability of success, which finally gives all the information to the eavesdropper.

Let us first consider in more detail the measurement corresponding to unambiguous discrimination of states $\{|\alpha_j\rangle\}_j$. Each element of the observable, corresponding to a successful outcome k, can be written in the form [40]

$$M_k = c\,|\psi_k^{\perp}\rangle\langle\psi_k^{\perp}| = c(I - P_k), \tag{16}$$

where $|\psi_k^{\perp}\rangle$ is a vector orthogonal to all vectors $\{|\alpha_j\rangle\}_{j,j\neq k}$ and P_k is a projector onto the subspace spanned by the vectors $\{|\alpha_j\rangle\}_{j,j\neq k}$. The coefficient c is determined by the requirement that the failure operator $M_?$ is nonnegative:

$$\lambda_{\min}(M_?) = \lambda_{\min}\left(1 - \sum_{k=1}^{N} M_k\right) = 0. \tag{17}$$

It is easy to see that the error probability for such a measurement is zero:

$$p(k|j) = \mathrm{Tr} M_k\,|\alpha_j\rangle\langle\alpha_j| = c\,|\langle\alpha_j|\psi_k^{\perp}\rangle|^2 = c\,|\langle\alpha_j|\psi_k^{\perp}\rangle|^2\delta_{jk},$$

while the success probability is determined by requirement (17) and the resulting value of the coefficient c (the same for all operators M_k in the symmetric case).

In a similar way, we can define an observable with three elements, $\{M_0, M_1, M_?\}$, which does not completely identify the vector, but only gives information about its belonging to a set of vectors corresponding to 0 or 1 in the raw key:

$$M_0 = c(I - P_1),\ \ M_1 = c(I - P_0),\ \ M_? = I - M_0 - M_1, \tag{18}$$

where P_i is a projector onto the subspace spanned by the vectors $\{|\alpha_b^i\rangle\}_b$, corresponding to 0 or 1 in the raw key. It is easy to make sure that outcome 0 of such a measurement occurs only on states corresponding to zeros in the raw key, and outcome 1, only on states corresponding to ones. In this case, the probability of failure can be much lower than for transformation (16), since measurement (18) yields, generally speaking, less information about the state itself. But for an attack in quantum cryptography, it turns out to be very useful because of the higher probability of success, which is easy to calculate using a specific orthonormal basis in the space spanned by symmetric coherent states and the expansion coefficients from [12].

In fact, this transformation corresponds to unambiguous discrimination of two states,

$$\frac{1}{M}\sum_b |\alpha_b^0\rangle\langle\alpha_b^0|, \quad \frac{1}{M}\sum_b |\alpha_b^1\rangle\langle\alpha_b^1|,$$

which correspond to sending bits 0 and 1 of keys, respectively, when the basis b is unknown. Methods for unambiguous discrimination of mixed states are well known [41, 42].

Let us consider right away a small modification of the measurement that makes the corresponding attack more effective. Because Eve subsequently receives information about the basis, she does not need to discriminate between exactly the zeros and ones of the raw key. It is enough for Eve to discriminate only between two groups of states, where the states of each basis belong to different groups. For example, for eight states with a phase shift within the basis $\theta = \pi/4$, these can be groups of state numbers $G_a = \{0, 3, 4, 7\}$ and $G_b = \{1, 2, 5, 6\}$. Then the belonging of the state to group a will mean the vector with the index 0, if the first basis is used; vector 3, if the second basis is used, and so on: Knowledge of the group and the basis uniquely identifies the state, and hence the bit of the raw key. In this case, due to the geometry of the states, it is possible to discriminate between the G_a and G_b groups with a higher probability of success than the groups $G_0 = \{0, 2, 4, 6\}$ and $G_1 = \{1,3,5,7\}$, corresponding to bits 0 and 1 of the key.

An attack based on the proposed transformation is based on the scheme of an active beam splitter (see Section 4). Eve takes part of the state with the intensity $|r|^2\mu$ and performs over it discrimination between two groups of states. If this discrimination is successful, the remainder of the state with intensity $|t|^2\mu$ is sent to Bob; otherwise, it is blocked. In fact, the attack has only one parameter – the assigned part of the state, and with a known attenuation, an attack is possible starting from a certain critical value of the intensity. If an attack is possible, Eve receives the entire secret key.

Figure 6 shows the optimal intensities obtained by formula (7) for each link length, and the critical intensity values at which the eavesdropper knows the entire key while carrying out the attack described in this Section. The number of states and configuration are fixed. It can be seen that for the

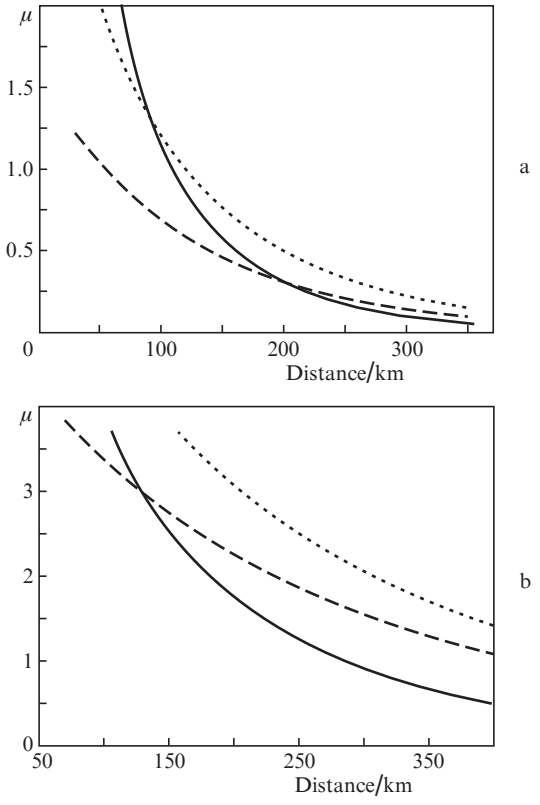

Figure 6. Dependences of the critical intensity μ, at which the eavesdropper knows the entire key, on the communication line length when the eavesdropper uses a key bit discrimination attack (solid curves) and the optimal intensity according to (7) (dashed curves), as well as the critical intensity at which the eavesdropper knows the entire key in the case of a USD attack (dotted line) with (a) $M = 4$ bases, the phase shift within the basis $\theta = \pi/4$ and (b) $M = 8$ bases, the phase shift within the basis $\theta = \pi/8$. The attenuation in the communication line is $\kappa = 0.2$ dB km^{-1}, and the error is zero.

communication line length when using four basis sets with a phase shift $\theta = \pi/4$, the critical intensity becomes more optimal starting from a distance of about 210 km, and when using eight basis sets with a phase shift $\theta = \pi/8$, this occurs starting approximately from 130 km. For comparison, the critical intensities are shown when using the USD attack, and, as expected, they turn out to be higher than the optimal ones. Thus, the protocol focuses on the USD attack and proposes measures to counter it, while when using a large number of bases, the resistance of the protocol to other attacks is not guaranteed.

It should be noted that for a number of lengths, the USD attack is more effective (as can be seen in Fig. 6a, at a length of up to 90 km). This, at first glance, unexpected fact is due to the fact that during a USD attack, Eve receives full information about the signal and can prepare the correct state with a high intensity, thereby triggering the detector in a position convenient for her. Eve is deprived of this possibility in the case of using the attack described in this Section and, therefore, for some sets of parameters, it turns out to be less effective.

It should also be noted that this attack is technically simple for the eavesdropper: It does not require Eve to have long-term quantum memory. Eve only needs to store the classic measurement result, which gives her information about the key bit after the bases are announced.

8. Conclusions

We have considered a set of attacks that demonstrate an overestimation of the secret key generation rate in a protocol on geometrically uniform coherent states. For a beam splitting attack and a state amplification attack in which Eve receives incomplete information, a comparison has been made between the length of the secret key calculated by formula (8) and the length of the secret key obtained during the attack. For a modified PNS attack and a key bit discrimination attack, in which Eve receives complete information, the critical intensity was compared for each length of the communication line with the optimal intensity for the same configuration of states obtained in accordance with (7). All attacks under certain conditions demonstrate an overestimation of the secret key length in formula (7); this means that the key distributed over the corresponding protocol is not secret. Thus, the incorrectness of the secrete key rate formula (7) has been shown.

Note that most attacks presented here have some drawbacks, the elimination of which will make the attacks more effective, but will complicate their detailed description and analysis. The aim of the work is to describe the simplest attacks that demonstrate the inaccuracy of formula (7); therefore, little attention has been paid to maximising their effectiveness. For example, attacks that introduce errors into the transmitted states are not considered at all, although this can significantly increase the amount of information known to the eavesdropper. The ideal operation of the equipment of legitimate users has been considered: full efficiency of detectors, absence of dark detectors, etc. Most likely, the optimal attack on this quantum cryptography protocol will combine the properties of several attacks presented here and will be much more complex. (See also [43], where another attack was constructed using more complex heterodyne measurements and demonstrating that increasing the number of bases does not necessarily allow counteracting the eavesdropper in the presence of a lossy channel.)

The protocol on geometrically uniform states uses a large number of states, which complicates its complete security proof, and the statements of the authors about its provable security [10, 44] are incorrect. At first glance, a complex configuration of states also complicates attacks, but our work has shown that, on the contrary, such a configuration of states opens up many new possibilities for the eavesdropper.

The main result of the work is the conclusion that the use of intuitive formulae for the secret key length, based on the assumptions about the use of certain attacks by the eavesdroper, is very risky and can lead to the compromise of the entire system: Chances are high that some of the effective actions of the eavesdropper are not taken into account when considering known attacks. A key advantage of quantum cryptography is the ability to rigorously prove its security against all eavesdropper actions (see, for example, [4–7, 45, 46]).

Acknowledgements. The work was supported by the Russian Science Foundation (Project No. 20-71-10072).

References

1. Bennett Ch.H., Brassard G. *Proc. Int. Conf. Computers, Systems & Signal Processing* (Bangalore, India, 1984) p. 175.
2. Ekert A.K. *Phys. Rev. Lett*., **67** (6), 661 (1991).
3. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74** (1), 145 (2002).
4. Mayers D. *J. ACM*, **48** (3), 351 (2001).
5. Shor P.W., Preskill J. *Phys. Rev. Lett*., **85** (2), 441 (2000).
6. Koashi M. *New J. Phys.*, **11** (4), 045018 (2009).
7. Renner R., Gisin N., Kraus B. *Phys. Rev. A*, **72** (1), 012332 (2005).
8. Molotkov S.N. *JETP Lett*., **95** (6), 332 (2012) [*Pis'ma Zh. Eksp. Teor. Fiz*., **95** (6), 361 (2012)].
9. Molotkov S.N. *JETP Lett*., **101** (8), 579 (2015) [*Pis'ma Zh. Eksp. Teor. Fiz*., **101** (8), 637 (2015)].
10. Balygin K.A., Zaitsev V.I., Klimov A.N., Klimov A.I., Kulik S.P., Molotkov S.N. *JETP Lett*., **105** (9), 606 (2017) [*Pis'ma Zh. Eksp. Teor. Fiz*., **105** (9), 570 (2017)].
11. Dušek M., Jahma M., Lütkenhaus N. *Phys. Rev. A*, **62** (2), 022306 (2000).
12. Chefles A., Barnett S.M. *Phys. Lett. A*, **250** (4–6), 223 (1998).
13. Yuen H.P. ArXiv preprint quant-ph/0311061 (2003).
14. Barbosa G.A., Corndorf E., Kumar P., Yuen H.P. *Phys. Rev. Lett*., **90** (22), 227901 (2003).
15. Acin A., Gisin N., Scarani V. *Phys. Rev. A*, **69** (1), 012309 (2004).
16. Hirota O., Sohma M., Fuse M., Kato K. *Phys. Rev. A*, **72** (2), 022335 (2005).
17. Avanesov A.S., Kronberg D.A. *Quantum Electron*., **49** (10), 974 (2019) [*Kvantovaya Elektron*., **49** (10), 974 (2019)].
18. Avanesov A.S., Kronberg D.A. *Quantum Electron*., **50** (5), 454 (2020) [*Kvantovaya Elektron*., **50** (5), 454 (2020)].
19. Futami F., Guan K., Gripp J., Kato K., Tanizawa K., Chandrasekhar S., Winzer P. *Opt. Express*, **25** (26), 33338 (2017).
20. Vtyurina A.G., Eliseev V.L., Zhilyaev A.E., Nikolaeva A.S., Sergeev V.N., Urivskii A.V. *Proceedings of TUSUR University*, **21** (2). 15 (2018).
21. Borisova A.V., Zhilyaev A.E., Alferov S.V., Eliseev V.L., Karmazikov Yu.V., Klimov A.N., Balygin K.A. *Vestnik of Russian New University. Ser. Complex Systems: Models, Analysis, Management*, (4), 100 (2019).
22. Ivanovic I.D. *Phys. Lett. A*, **123** (6), 257 (1987).
23. Peres A. *Phys. Lett. A*, **128** (1–2), 19 (1988).
24. Kronberg D.A. *Mat. Vopr. Kriptogr*., **8** (2), 77 (2017).
25. Kiktenko E.O., Malyshev A.O., Bozhedarov A.A., Pozhar N.O., Anufriev M.N., Fedorov A.K. *J. Russ. Laser Res.*, **39** (6), 558 (2018).

26. Trushechkin A.S. *Quantum Electron*., **50** (5), 426 (2020) [*Kvantovaya Elektron*., **50** (5), 426 (2020)].
27. Devetak I., Winter A. *Proc. Royal Soc. A: Mathemat., Phys. Eng. Sci*., **461** (2053), 207 (2005).
28. Holevo A.S. *Quantum Systems, Channels, Information. A Mathematical Introduction* (Berlin, New York: De Gryuter, 2012; Moscow: MTsNMO, 2010).
29. Kronberg D.A., Molotkov S.N. *JETP Lett*., **100** (4), 279 (2014) [*Pis'ma Zh. Eksp. Teor. Fiz*., **100** (4), 305 (2014)].
30. Balygin K.A., Klimov A.N., Kulik S.P., Molotkov S.N. *JETP Lett*., **104** (5), 341 (2016) [*Pis'ma Zh. Eksp. Teor. Fiz*., **104** (5), 349 (2016)].
31. Holevo A.S. *Usp. Mat. Nauk*, **53** (324), 193 (1998).
32. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Rev. A*, **58** (1), 146 (1998).
33. Kronberg D.A., Kiktenko E.O., Fedorov A.K., Kurochkin Yu.V. *Quantum Electron*., **47** (2), 163 (2017) [*Kvantovaya Elektron*., **47** (2), 163 (2017)].
34. Avanesov A.S., Kronberg D.A., Pechen A.N. *P-Adic Numbers, Ultrametric Analysis, and Applications*, **10** (3), 222 (2018).
35. Kronberg D.A., Nikolaeva A.S., Kurochkin Y.V., Fedorov A.K. *Phys. Rev. A*, **101** (3), 032334 (2020).
36. Kronberg D.A. *Laser Phys*., **24** (2), 025202 (2014).
37. Kronberg D.A. *Lobachevskii J. Mathem*., **41** (12), 2332 (2020).
38. Kronberg D.A. *Proceedings of the Steklov Mathematical Institute*, **313** (1), 113 (2021).
39. Kronberg D.A., Kurochkin Yu.V. *Quantum Electron*., **48** (9), 843 (2018) [*Kvantovaya Elektron*., **48** (9), 843 (2018)].
40. Chefles A. *Phys. Lett. A*, **239** (6), 339 (1998).
41. Feng Y., Duan R., Ying M. *Phys. Rev. A*, **70** (1), 012308 (2004).
42. Herzog U., Bergou J.A. *Phys. Rev. A*, **71** (5), 050301 (2005).
43. Avanesov A.S., Kronberg D.A. *Lobachevskii J. Mathem*., **42** (10), 2285 (2021).
44. Balygin K.A., Klimov A.N., Kulik S.P., Molotkov S.N. *JETP Lett*., **106** (2), 120 (2017) [*Pis'ma Zh. Eksp. Teor. Fiz*., **106** (2), 108 (2017)].
45. Moroder T., Curty M., Lim C.C.W., Zbinden H., Gisin N. *Phys. Rev. Lett*., **109** (26), 260501 (2012).
46. Trushechkin A.S., Kiktenko E.O., Kronberg D.A., Fedorov A.K. *Phys. Usp*., **64** (1), 88 (2021) [*Usp. Fiz. Nauk*, **191** (1), 93 (2021)].