Quantum Electronics **48** (9) 843–848 (2018)

QUANTUM CRYPTOGRAPHY

https://doi.org/10.1070/QEL16739

Role of intensity fluctuations in quantum cryptography with coherent states

D.A. Kronberg, Yu.V. Kurochkin

Abstract. **A new type of attack in quantum cryptography with coherent states is considered. This attack calls for only a possibility of changing (within some limits) the intensity of the states reaching a receiver. The critical quantum bit error rate (QBER) of the B92 protocol with a strong reference state is calculated for different limitations on intensity.**

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

1. Introduction

The purpose of quantum cryptography is to distribute a secret key between distant users (referred to as Alice and Bob) without any suggestions about the computational or technological possibilities of an eavesdropper (Eve). In particular, Eve can solve rapidly NP-complete problems; therefore, legitimate users have no right to apply the important assumption of classical asymmetric cryptography. The main limitation imposed by quantum mechanics is that one cannot extract all information from a set of nonorthogonal quantum states. Alice and Bob use nonorthogonal quantum states to encode key bits in quantum key distribution protocols; these protocols are developed so that Eve cannot gain all information about a key without introducing an error into signal states.

Quantum cryptography protocols based on coherent states are of great interest, because they do not call for single-photon sources and can relatively easily be implemented in practice. In these cryptographic schemes, attenuated laser pulses transmitted through fibre communication links serve as information states.

The attenuation of coherent pulses in fibre communication links provides an eavesdropper with new opportunities, in addition to conventional attacks (during which the eavesdropper tries to gain information from an ensemble of nonorthogonal states). One can select two main types of attacks on coherent protocols: the so-called beam-splitting attack and the unambiguous state discrimination (USD) attack.

In the case of a beam-splitting attack, Eve takes a part of each state to its quantum memory using a beam splitter and sends the remaining part to Bob through an ideal channel without attenuation. After applying this attack, Bob receives a state of exactly the same intensity as he expects, as a result of which the beam-splitting attack cannot be detected. However, Eve gains only partial information, limited by the Holevo value for her states [1]. After rejecting the positions with an unambiguous measurement result, Bob has complete information about the key. The aim of Eve is to have the same information about the key as Bob; therefore, to compensate for the incompleteness of her information, she can introduce an error into the channel between Alice and Bob. The larger the amount of information Eve can derive from her states, the smaller the error that must be introduced. Therefore, the critical quantum bit error rate (QBER) of coherent-state protocols against the beam-splitting attack depends on the channel length (it decreases at large lengths) and on the initial intensity (the higher the intensity, the lower the critical QBER value).

When carrying out a USD attack [2], Eve performs an unambigous measurement on each state; sometimes this measurement provides complete information and sometimes yields an inconclusive result. If Eve was lucky enough to obtain all information, she sends Bob states of higher intensity; in the case of an inconclusive result, she blocks the message.

The USD attack, which does not introduce an error, is very powerful; however, it calls for a possibility of blocking some part of messages and increasing the intensity of the other part. In general, after this attack, Eve sends receiver a mixture of high-intensity and vacuum states rather than the initial states. Coherent-state protocols tend to block this possibility, i.e., to detect the sending of vacuum states. The widespread methods used to this end are as follows:

(i) Sending not only information states but also decoy states of different intensity. This approach allows one to detect an eavesdropper from the changed statistics of states of different types [3].

(ii) Sending control states along with information ones, which hinders the USD and supplies legitimate users with a new visibility parameter for detecting the eavesdropper. A well-known protocol based on this scheme is the coherent one-way (COW) protocol [4].

(iii) Sending sequences of coherent states with information encoded through the phase difference between neighbouring states, as in the differential phase-shift protocol [5]. In this case, blocking one state also introduces an error.

(iv) Using a strong reference state, which must be detected by Bob. Information is encoded into the phase difference between the reference and weak information pulses. This scheme was proposed when describing the original B92 proto-

D.A. Kronberg V.A. Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia; e-mail: dmitry.kronberg@gmail.com;
Yu.V. Kurochkin Russian Quantum Center, Skolkovo, 143025 Moscow, Russia

Received 24 May 2018; revision received 3 July 2018
Kvantovaya Elektronika **48** (9) 843–848 (2018)
Translated by Yu.P. Sin'kov

col [6]. Here, the blocking of an information pulse by Eve causes an error at the receiving side.

As a result, a USD attack can be applied only when the intensity of states received by Bob may change from zero (when sending vacuum states, i.e., blocking a message) to infinity, and this attack may introduce no error. A beam-splitting attack does not change intensity at the receiving side and can be applied to any coherent-state protocol in the case of a communication line with attenuation, but it has a relatively large critical QBER value. A question arises of how Eve can use the possibility of changing the intensity of states in a more general case, where the intensity should be in some specified range.

Recently a new concept of attack on the COW protocol was proposed, which was referred to as active beam-splitting attack [7]. It does not require an unambiguous measurement, because in this version the measurement is applied to only a part of the initial state, while the rest part can be send to Bob without any changes. Therefore, the attack of this type can be used in situations where the USD attack is poorly applicable; for example, in the case of the COW protocol. Our purpose was to generalise this attack to other protocols.

In this study, we propose an attack of new type, which can be considered in some cases as a generalisation of the USD, beam-splitting, and active beam-splitting attacks. The proposed attack requires to change the intensity of the states received by Bob; the wider the range of variation in this intensity, the more efficient the attack is (i.e., the smaller the critical QBER). We will consider the application of this attack to the B92 protocol with a strong reference state, whose security was proven in [8].

2. B92 protocol and description of the main types of attack

A coherent state $|\alpha\rangle$ is expressed in terms of the complex number α as

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

where $|n\rangle$ is a Fock state. The average number of photons $\mu = |\alpha|^2$ is referred to as the coherent state intensity. The intensity at the output of a channel of length l can be written as

$$\mu' = \mu 10^{-\frac{\delta l}{10}}, \tag{2}$$

where $\delta \approx 0.2$ dB km^{-1} is the optical fibre attenuation coefficient. The B92 protocol with a strong reference state uses two nonorthogonal coherent states, corresponding to signals 0 and 1:

$$\begin{aligned} &0\colon |A\rangle \otimes |\alpha\rangle, \\ &1\colon |A\rangle \otimes |-\alpha\rangle, \end{aligned} \tag{3}$$

where $|A| \gg |\alpha|$. These are sequences from the reference and information states, each of which is localised in the corresponding time slot; the bit value is encoded in the phase difference. Bob uses a beam splitter with a transmittance α/A to split off a part of the reference state of the same intensity as the information state. The rest part of the reference state is also measured (to provide detection of blocking of the entire two-mode state). After this procedure the state is transformed into the following one:

$$\begin{aligned} &0\colon |\alpha\rangle \otimes |\alpha\rangle, \\ &1\colon |\alpha\rangle \otimes |-\alpha\rangle. \end{aligned} \tag{4}$$

Bob uses a Mach–Zehnder interferometer to transform the states into

$$\begin{aligned} &0\colon |0\rangle \otimes |\sqrt{2}\,\alpha\rangle, \\ &1\colon |\sqrt{2}\,\alpha\rangle \otimes |0\rangle, \end{aligned} \tag{5}$$

where $|0\rangle$ is a vacuum state. Then the measurement in each mode is described by observable

$$M_0 = |0\rangle\langle 0|, \quad M_1 = \sum_{i=1}^{+\infty} |i\rangle\langle i|, \tag{6}$$

where result 0 means the absence of detector click, and result 1 indicates detection of state. The probability of detecting a state of intensity μ is $1 - \mathrm{e}^{-\mu}$; it is low for low-intensity states.

Result 1 in the first time slot indicates that the bit value is 0, and result 1 in the second time slot indicates a value of 1; if result 1 is obtained nowhere, Bob fixes an inconclusive result. The longer the communication line, the lower the output state intensity and the higher the probability of the inconclusive result. After the communication session, Alice and Bob use a public authentic channel to reject positions with inconclusive results.

Below we describe the two main attacks on this protocol. Since the reference-state phase can easily be measured, we assume that Eve knows it. Therefore, Eve's main task is to extract information from the two states $|\alpha\rangle$ and $|-\alpha\rangle$ so as to make the mutual information of Eve and Alice be equal to that of Alice and Bob and reduce to minimum the error introduced during this procedure. Eve will use attenuation in the channel in both attacks.

It follows from Stinespring's theorem (see, e.g., [1]) that any transformation of a quantum system (i.e., quantum channel) can be described as a unitary interaction between the system and environment. When performing an attack on quantum cryptography protocols, Eve may possess all the environment. The USD attack can be described by the transformation

$$\begin{aligned} &|\alpha\rangle \to |\psi_0\rangle = \sqrt{1 - \mathrm{e}^{-2\mu}}\,|\beta\rangle|e_0\rangle + \mathrm{e}^{-\mu}|0\rangle|f\rangle, \\ &|-\alpha\rangle \to |\psi_1\rangle = \sqrt{1 - \mathrm{e}^{-2\mu}}\,|-\beta\rangle|e_1\rangle + \mathrm{e}^{-\mu}|0\rangle|f\rangle, \end{aligned} \tag{7}$$

where $|\pm\beta\rangle$ are Bob's new coherent states of high intensity and $|e_0\rangle$, $|e_1\rangle$ and $|f\rangle$ are Eve's mutually orthogonal states. One can easily make sure that the unitarity condition is satisfied: $\langle\psi_0|\psi_1\rangle = \mathrm{e}^{-2\mu} = \langle\alpha|-\alpha\rangle$. The probability of successful state discrimanation is $1 - \mathrm{e}^{-2\mu}$, and Bob receives the states

$$\begin{aligned} &\rho_0^{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}|\psi_0\rangle\langle\psi_0| = (1 - \mathrm{e}^{-2\mu})|\beta\rangle\langle\beta| + \mathrm{e}^{-2\mu}|0\rangle\langle 0|, \\ &\rho_1^{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}|\psi_1\rangle\langle\psi_1| = (1 - \mathrm{e}^{-2\mu})|-\beta\rangle\langle-\beta| + \mathrm{e}^{-2\mu}|0\rangle\langle 0|. \end{aligned} \tag{8}$$

The expected probability of Bob's conclusive result when measuring states (5) after the channel with attenuation and Mach–Zehnder interferometer is

$$1 - e^{-2\mu'}, \tag{9}$$

where μ' is found from (2). For large $|\beta|^2$ values this probability is lower than the probability of obtaining a conclusive result when measuring states (8):

$$(1 - e^{-2\mu})(1 - e^{-2|\beta|^2}). \tag{10}$$

Therefore, when carrying out this attack, Eve can set the intensity of the states $|\pm\beta\rangle$ received by Bob such as to make probabilities (9) and (10) coincide. However, due to the presence of a strong reference state, this attack is impossible for the B92 protocol: Bob can detect it because of the reference state loss. For other protocols, this attack can potentially be detected from the change in the intensity of Bob's states: from zero to $|\beta|^2$. Below we will consider Eve's strategy in the case where some limitations are imposed on Bob's states.

In the case of a beam-splitting attack, Eve divides each state into two parts: her part with intensity $|\varepsilon|^2$ and Bob's part with intensity μ'. If an error is introduced into Bob's part with a probability q, the transformation can be written as

$$\begin{aligned} |\alpha\rangle \to |\varphi_0\rangle &= (\sqrt{1-q}\,|\sqrt{\mu'}\rangle|g_0\rangle + \sqrt{q}\,|-\sqrt{\mu'}\rangle|g_1\rangle)|\varepsilon\rangle, \\ |-\alpha\rangle \to |\varphi_1\rangle &= (\sqrt{q}\,|\sqrt{\mu'}\rangle|g_1\rangle + \sqrt{1-q}\,|-\sqrt{\mu'}\rangle|g_0\rangle)|-\varepsilon\rangle, \end{aligned} \tag{11}$$

where $|g_0\rangle$ and $|g_1\rangle$ are mutually orthogonal states, corresponding to Eve's information on whether an error was introduced in this position or not (they do not give any information about the bit value to Eve) and $|\pm\sqrt{\mu'}\rangle$ are the coherent states received by Bob [they have an intensity μ', calculated from (2)]. One can easily make sure that the unitarity condition is satisfied if the intensity of Eve's states $|\pm\varepsilon\rangle$ is equal to $\mu - \mu'$, a situation provided by beam splitter.

In this case, Bob's partial states are

$$\begin{aligned} \rho_0^{\mathrm{B}} &= \mathrm{Tr_E}\,|\varphi_0\rangle\langle\varphi_0| = (1-q)\,|\sqrt{\mu'}\rangle\langle\sqrt{\mu'}| + q\,|-\sqrt{\mu'}\rangle\langle-\sqrt{\mu'}|, \\ \rho_1^{\mathrm{B}} &= \mathrm{Tr_E}\,|\varphi_1\rangle\langle\varphi_1| = q\,|\sqrt{\mu'}\rangle\langle\sqrt{\mu'}| + (1-q)\,|-\sqrt{\mu'}\rangle\langle-\sqrt{\mu'}|, \end{aligned} \tag{12}$$

their intensity is equal exactly to the expected value (2). Eve must introduce an error to make her information on Alice's states the same as Bob's information. Eve's information is given by the Holevo value χ of the states $|\pm\varepsilon\rangle$; therefore, the necessary error probability can be found from

$$1 - h_2(q) = \chi(\{|\varepsilon\rangle, |-\varepsilon\rangle\}) = h_2\left[\frac{1 - e^{-2(\mu-\mu')}}{2}\right], \tag{13}$$

where $h_2(q) = -q\log q - (1-q)\log(1-q)$ is the binary Shannon entropy. At a channel length tending to infinity (and, correspondingly, high attenuation), the limiting critical QBER value is set as

$$1 - h_2(q) = \chi(\{|\alpha\rangle, |-\alpha\rangle\}) = h_2\left(\frac{1 - e^{-2\mu}}{2}\right). \tag{14}$$

Note that the above-considered strategy of the beam-splitting attack is not optimal, because Eve can introduce an error more efficiently when trying to gain additional information from the ensemble of nonorthogonal states $|\pm\alpha\rangle$. Nevertheless, in the case of high attenuation, this more complicated attack scenario does not yield any essential advantage. In this study, we consider a concept of attack with introducing error in a simpler way: by adding noise.

A comparison of these two main types of attack shows that a USD attack can be used only when the protocol makes it possible to change intensity from zero to infinity, whereas a beam-splitting attack can be applied to any coherent-state protocol for a communication line with loss; however, its critical QBER value always exceeds zero [moreover, exceeds the limiting critical value set by (14)]. The USD attack benefits from the possibility of taking a solution dependent on the success of measurement.

3. Intensity fluctuation attack

Let us now assume that Bob can verify the intensity of received states. For the B92 protocol with intense reference state, this may indicate, for example, that Bob measures the reference state intensity and checks whether it lies in a certain range. Since the intensities of the reference and information states should be interrelated, Eve cannot change one of them without introducing an additional error. Therefore, when measuring the reference state intensity, Alice and Bob can also check the information state intensity. The main question of the work is as follows: if the information state intensity may change from $\mu_{\min} < \mu'$ to $\mu_{\max} > \mu'$, how can Eve use this fact?

Before describing the main attack, let us consider the operation of soft filtering, which was introduced in [9, 10]. It extracts (in a fairly general form) information from nonorthogonal states. Unambiguous measurement is a particular case of this operation. Soft filtering acts on a set of two coherent states $|\pm\alpha\rangle$ as

$$\begin{aligned} |\alpha\rangle \to |\psi_0\rangle &= \sqrt{p}\,|\beta\rangle|e\rangle + \sqrt{1-p}\,|0\rangle|f\rangle, \\ |-\alpha\rangle \to |\psi_1\rangle &= \sqrt{p}\,|-\beta\rangle|e\rangle + \sqrt{1-p}\,|0\rangle|f\rangle. \end{aligned} \tag{15}$$

In contrast to the unambiguous measurement (7), the output states $|\pm\beta\rangle$ may be nonorthogonal, while Eve's states, corresponding to a successful result, coincide: $|e_0\rangle = |e_1\rangle = |e\rangle$. We denote their intensity as μ_{B}; then the unitarity condition $\langle\alpha|-\alpha\rangle = \langle\psi_0|\psi_1\rangle$ can be written as

$$e^{-2\mu} = pe^{-2\mu_{\mathrm{B}}} + 1 - p, \tag{16}$$

therefore, the probability of success is

$$p = \frac{1 - e^{-2\mu}}{1 - e^{-2\mu_{\mathrm{B}}}}. \tag{17}$$

If the output states are orthogonal, the probability of success is exactly the same as for the unambiguous measurement (9). In this case, the $|e_0\rangle$ and $|e_1\rangle$ states can also be made orthogonal, because this procedure does not affect the unitarity condition. However, if the output states are nonorthogonal, the probability of success increases (and reaches unity if the output intensity is the same as the input one).

Soft filtering (for brevity, it will be referred to as filtering below) makes states more distinguishable with some probability p or yields an inconclusive result with a probability $1-p$.

If filtering was successful, one can extract a larger amount of information from the 'more informative' states $|\pm\beta\rangle$. Therefore, filtering is a fairly general case of extracting information.

Let us now describe the main attack. It can be schematically represented as follows:

(i) Eve takes a part of each state using a beam splitter.

(ii) Eve performs soft filtering for its part of the state.

(iii) Depending on the success of filtering, Eve sends either a high-intensity state with a small error to Bob (case of successful filtering) or a low-intensity state with a high probability of error (case of unsuccessful filtering).

This attack is applied to a protocol based on states (4) of intensity μ; it uses two parameters: part t of the state on which filtering acts and the gain a. First Eve takes (using a beam splitter) a part of state of intensity $t\mu$ to extract information; the other part of intensity, $(1-t)\mu$, remains the same at this step. The output intensity for filtering is $at\mu$; therefore, the probability of success is

$$p = \frac{1-\mathrm{e}^{-2t\mu}}{1-\mathrm{e}^{-2at\mu}}.$$

In the case of success, Eve can extract a large amount of information about the bit value; it is desirable for her to send a state of high-intensity μ_1 to Bob in order to give him a good chance to obtain a conclusive result. Since the maximum intensity of Bob's states is limited by $\mu_{\max}$, the μ_1 value should not exceed $\min\{\mu_{\max},(1-t)\mu\}$ (below we will consider a modified attack allowing for states with intensity higher than $(1-t)\mu$). In this case, Eve also takes the remaining part of the state and obtains states of intensity $at\mu + (1-t)\mu - \mu_1$; therefore, her information about the key is

$$I_{\mathrm{AE}}^{\mathrm{succ}} = h_2\left(\frac{1-\mathrm{e}^{-2[at\mu+(1-t)\mu-\mu_1]}}{2}\right).$$

In the case of unsuccessful filtering, when Eve may obtain a small amount of information about the bit value, she uses a beam splitter again to take a part of the remaining state of intensity $(1-t)\mu$. Then she sends Bob a state of low intensity $\mu_2 \geqslant \mu_{\min}$. In this case, Eve's information is

$$I_{\mathrm{AE}}^{\mathrm{fail}} = h_2\left(\frac{1-\mathrm{e}^{-2[(1-t)\mu-\mu_2]}}{2}\right).$$

The intensities μ_1 and μ_2 should also satisfy the condition that the expected number of conclusive results remains invariable. This yields in sum the following three relations:

$$\begin{aligned} &\mu_1 \leqslant \min\{\mu_{\max},(1-t)\mu\},\ \ \mu_2 \geqslant \mu_{\min},\\ &p(1-\mathrm{e}^{-2\mu_1}) + (1-p)(1-\mathrm{e}^{-2\mu_2}) = 1-\mathrm{e}^{-2\mu'}. \end{aligned} \tag{18}$$

Depending on the filtering result, Eve introduces an error into Bob's states: q_1 and q_2 values for successful and unsuccessful filtering, respectively. As in the case of beam-splitting attack, the purpose of this error is to make Bob's information on the key equal to Eve's information. The error probabilities are set as

$$\begin{aligned} I_{\mathrm{AE}}^{\mathrm{succ}} &= 1-h_2(q_1),\\ I_{\mathrm{AE}}^{\mathrm{fail}} &= 1-h_2(q_2). \end{aligned} \tag{19}$$

Bob's states after this attack are

$$\begin{aligned} \rho_0^{\mathrm{B}} &= p[(1-q_1)\,|\sqrt{\mu_1}\rangle\langle\sqrt{\mu_1}\,| + q_1\,|-\sqrt{\mu_1}\rangle\langle-\sqrt{\mu_1}\,|]\\ &+ (1-p)[(1-q_2)\,|\sqrt{\mu_2}\rangle\langle\sqrt{\mu_2}\,| + q_2\,|-\sqrt{\mu_2}\rangle\langle-\sqrt{\mu_2}\,|],\\ \rho_1^{\mathrm{B}} &= p[q_1\,|\sqrt{\mu_1}\rangle\langle\sqrt{\mu_1}\,| + (1-q_1)\,|-\sqrt{\mu_1}\rangle\langle-\sqrt{\mu_1}\,|]\\ &+ (1-p)(q_2\,|\sqrt{\mu_2}\rangle\langle\sqrt{\mu_2}\,| + (1-q_2)\,|-\sqrt{\mu_2}\rangle\langle-\sqrt{\mu_2}\,|), \end{aligned} \tag{20}$$

and the average error expected by him can be written as

$$q = q_1 p(1-\mathrm{e}^{-2\mu_1}) + q_2(1-p)(1-\mathrm{e}^{-2\mu_2}). \tag{21}$$

Eve's purpose is to choose optimal attack parameters t and a in order to make her information equal to Bob's information with a minimally possible average error (21); this is a conventional computational problem.

4. Results for different limitations

Let us now analyse how the critical QBER value changes for limitations of different types. We will see that, the more stringent the limitations are (i.e., the smaller the deviation of Bob's intensity from the expected value is), the larger the critical QBER is and the closer it approaches the critical QBER value for the beam-splitting attack, which is suitable for situations where intensity fluctuations are impossible.

We will consider a protocol with the initial intensity of Alice's states $\mu_{\mathrm{A}} = 0.2$ photons per pulse; the reference state intensity is of no importance. For simplicity, we will introduce a parameter s and consider the following $\mu_{\min}$ and $\mu_{\max}$ values [where μ' is set, as previously, by formula (2)]:

$$\mu_{\min} = (1-s)\mu', \qquad \mu_{\max} = \frac{\mu'}{1-s}.$$

The case $s = 0$ corresponds to severe limitations, when only a beam-splitting attack is possible. In the case $s = 1$, the intensity may take values from zero to infinity, and an attack by unambiguous measurement can be implemented.

Limitations of three main types can be selected:

(i) Both intensities are limited; i.e., Bob's intensity μ_{B} should be between $\mu_{\min}$ and $\mu_{\max}$.

(ii) Limitation from below; i.e., Bob's intensity μ_{B} should to be no smaller than $\mu_{\min}$.

(iii) Limitation from above; i.e., Bob's intensity μ_{B} should not exceed $\mu_{\max}$.

The critical QBER for two values of parameter s under limitations of these three main types is shown in Fig. 1 as a function of the length of a channel with an attenuation parameter $\delta = 0.2$ dB km^{-1}. These error values are compared with the error for a beam-splitting attack (corresponding to $s = 0$).

It can be seen that, if only the upper limitation $\mu_{\mathrm{B}} \leqslant \mu'/(1-s)$ is imposed, an attack may provide Eve (at some s values) with all information without introducing any error if the channel is sufficiently long. In this case, Eve performs an unambiguous measurement for each state of intensity $\mu_{\mathrm{A}} - \mu'/(1-s)$. She blocks the state in the case of failure; otherwise, she sends Bob a state of maximally possible inten-

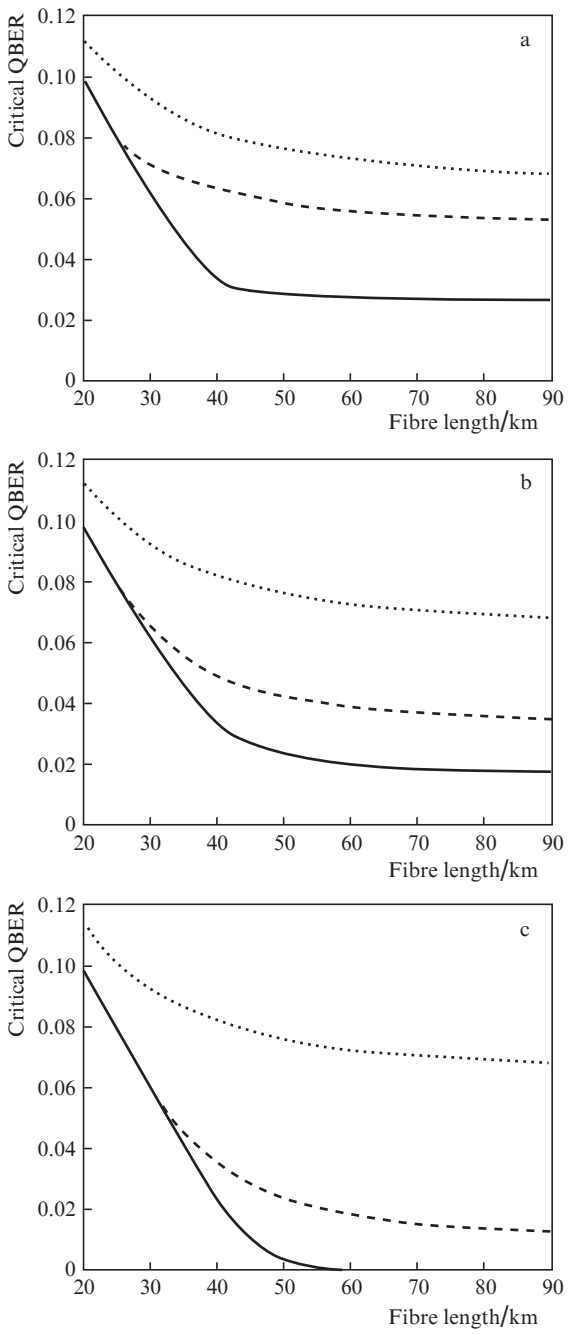

Figure 1. Dependence of the critical QBER on the fibre length in the cases where Bob's intensity should satisfy the conditions (a) $(1-s)\times\mu' \leqslant \mu_B \leqslant \mu'/(1-s)$, (b) $\mu_B \geqslant (1-s)\mu'$, and (c) $\mu_B \leqslant \mu'/(1-s)$ at $s =$ (dashed line) 0.5 and (solid line) 0.75. The dotted line corresponds to $s = 0$.

sity $\mu'/(1-s)$. The condition for the absence of error during attack can be written as

$$\left\{1-\exp\left[-2\left(\mu_A-\frac{\mu'}{1-s}\right)\right]\right\}$$

$$\times\left[1-\exp\left(-2\frac{\mu'}{1-s}\right)\right]=1-e^{-2\mu'},$$

If the channel length tends to infinity, this condition takes a simple form:

$$s > e^{-2\mu_A}. \quad (22)$$

It is noteworthy that, if this condition is not satisfied or there is a limitation from below ($\mu_B \geqslant \mu_{min}$ for any $\mu_{min} > 0$), the attack cannot have a zero error. Indeed, in this case Eve cannot block states and, for any message, she must send Bob a state, which can be detected with a nonzero probability. The maximum information that Eve can extract from states is limited by the Holevo value, and the minimum error that Eve can introduce into low-intensity states is given by (14). Since Bob obtains a conclusive result with a nonzero probability, he obtains a nonzero error as well.

5. Discussion of results and conclusions

A beam-splitting attack is possible for any quantum key distribution scheme based on coherent states under attenuation conditions, because Eve's actions ideally model attenuation. We considered an attack that may occur if Eve can also slightly change the intensity of Bob's states. In general, in this attack, Eve benefits from the possibility of making decisions: Eve attempts to extract information and decides if she has to send a state of high or low intensity.

An attack can be improved by applying other error introduction methods, especially in the case of a channel with low attenuation. We considered simple introduction of noise; however, Eve can gain a larger amount of information by measuring some states.

Another possible modification of attack in the absence of limitation from above is the use of states with an intensity exceeding that of the states used initially by Alice. This is possible in the case of successful filtering. From this point of view, the constructed attack is a generalisation of attacks of two types: unambiguous measurement and beam-splitting attack.

The above-described improvements and applications of this attack to other known protocols are a subject of future studies.

This type of attack shows that Bob must monitor intensity to resist eavesdropping. If Alice and Bob can verify that the state intensity is limited from below (i.e., that Eve does not block states) or that the maximum intensity is lower than the value given by (22), this attack cannot give Eve all information without introducing an error.

Moreover, we suggest that the conditions of this type may be sufficient to provide security of coherent-state protocols against any attack, on the assumption that Bob receives coherent states and can check their intensity. Therefore, an urgent problem is to develop protocols allowing for intensity monitoring at the receiving side.

Acknowledgements. This study was supported by the Russian Science Foundation (Project No. 17-11-01388) and performed at the Steklov Mathematical Institute of the Russian Academy of Sciences.

References

1. Holevo A.S. *Quantum Systems, Channels, Information* (Berlin, Boston: De Gryuter, 2012; Moscow: MTsNMO, 2010).
2. Dusek M., Jahma M., Lutkenhaus N. *Phys. Rev. A*, **62**, 022306 (1999).
3. Lo H.-K., Ma X., Chen K. *Phys. Rev. Lett.*, **94**, 230504 (2005).
4. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett.*, **87**, 194108 (2005).

5. Inoue K., Waks E., Yamamoto Y. *Phys. Rev. Lett*., **89**, 037902 (2002).
6. Bennett C.H. *Phys. Rev. Lett*., **68**, 3121 (1992).
7. Kronberg D.A., Kiktenko E.O., Fedorov A.K., Kurochkin Yu.V. *Quantum Electron*., **47** (2), 163 (2017) [*Kvantovaya Elektron*., **47** (2), 163 (2017)].
8. Tamaki K., Lutkenhaus N., Koashi M., Batuwantudawe J. *Phys. Rev. A*, **80**, 032302 (2009).
9. Kronberg D.A., Molotkov S.N. *JETP Lett.*, **100**, 279 (2014) [*Pis'ma Zh. Eksp. Teor, Fiz*., **100**, 305 (2014)].
10. Kronberg D.A. *Laser Phys.*, **24**, 025202 (2014).