Quantum Electronics **47** (2) 163–168 (2017)

QUANTUM CRYPTOGRAPHY https://doi.org/10.1070/QEL16240

Analysis of coherent quantum cryptography protocol vulnerability to an active beam-splitting attack

D.A. Kronberg, E.O. Kiktenko, A.K. Fedorov, Yu.V. Kurochkin

Abstract. **We consider a new type of attack on a coherent quantum key distribution protocol [coherent one-way (COW) protocol]. The main idea of the attack consists in measuring individually the intercepted states and sending the rest of them unchanged. We have calculated the optimum values of the attack parameters for an arbitrary length of a communication channel and compared this novel attack with a standard beam-splitting attack.**

Keywords: *quantum cryptography, quantum information theory.*

1. Introduction

Progress in manipulating individual quantum systems plays a key role in implementing quantum technologies. In turn, quantum technologies have a great potential for the development of modern computing [1–3] and communication devices [4]. In particular, the use of quantum systems as basic structural elements for computers allows the performance to be dramatically improved in a number of applications [3], for example, in a search of an unstructured database [5], and also in integer factorisation and discrete logarithm problems [6]. The latter ones are of particular importance for public-key cryptography [7, 8], which is based on the complexity of their solutions for classical computers. With the advent of quantum computing devices, such problems can be solved more quickly, jeopardising the existing methods of information protection using cryptographic means. Besides, the absence of effective nonquantum algorithms for solving such problems is still unproved.

The advent of quantum computers limits the range of possible cryptographic solutions to two possible methods. The first one consists in using problems, for which there are neither classical nor quantum efficient algorithms, as a basis of novel public-key systems. The totality of these methods lays the foundation of post-quantum cryptography [9]. However, as the proof of the absence of an effective algorithm is an extremely challenging task, such methods will apparently be potentially vulnerable for a long time.

Another possible solution is to use private-key cryptography. On the one hand, such systems (under certain conditions) are completely secure [10]. If legitimate users (Alice and Bob) have identical random private keys that are used only once, the key size being equal to or greater than the size of the message, Shannon's theorem [10] shows that messages encrypted with a private key generated by a one-time pad [11] cannot be, in principle, decrypted by an eavesdropper (Eve). However, the key distribution, satisfying these requirements, is challenging.

To solve the key distribution problem, one can make use of the resource of quantum systems [4]. When transmitting information via individual quantum objects (for example, single photons), confidentiality will be guaranteed by the principles of quantum physics [12, 13]. First, an arbitrary quantum state cannot be copied in accordance with the no-cloning theorem [14]. Second, a pair of states, to which noncommuting Hermitian operators correspond, cannot be discriminated with unit probability. Finally, any measurement perturbs or destroys the quantum state. Thus, in distributing a key with the help of single photons, one obtains a scheme which can reliably detect the fact of interference in the key generation process. Therefore, the method of quantum key distribution will potentially allow one to build a new architecture of information and telecommunication systems, in which the security of the transmitted information will be guaranteed by the fundamental laws of physics. However, imperfections in the technical implementation of quantum key distribution systems, such as absorption of photons in optical fibre, effectiveness of single-photon detectors and actions of the eavesdropper using these imperfections, can lead to possible attacks. In particular, if the quantum channel is longer than a certain critical value, the distributed keys cannot be secured [13].

It is worth noting that attacks on quantum key distribution systems can be divided into two classes. The first class is an attack on key distribution protocols. The quantum key distribution protocol commonly represents a general scheme of preparation and measurement of quantum states, as well as the procedure for obtaining the results of measurements of quantum states of a key on Alice's and Bob's side. The first quantum key distribution protocol is the BB84 protocol. In considering the attacks of this class, it is traditionally assumed [12, 13] that the eavesdropper has all the technological

D.A. Kronberg Steklov Mathematical Institute of Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia; M.V. Lomonosov Moscow State University, Vorob'evy Gory, 119991 Moscow, Russia; e-mail: dmitry.kronberg@gmail.com;
E.O. Kiktenko LLC 'DEFAN', ul. Novaya 100, Skolkovo, 143025 Moscow, Russia; N.E. Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Bld. 1, 105005 Moscow, Russia;
A.K. Fedorov Russian Quantum Centre, ul. Novaya 100A, Skolkovo, 143025 Moscow, Russia; LLC 'Acronis', Altuf'evskoe sh. 44, 127566 Moscow, Russia; Laboratoire de Physique Théorique et Modèles Statistiques, Centre National de la Recherche Scientifique, Université Paris-Sud, Université Paris-Saclay, Orsay 91405, France;
Yu.V. Kurochkin Russian Quantum Centre, ul. Novaya 100A, Skolkovo, 143025 Moscow, Russia

Received 19 October 2016; revision received 12 December 2016
Kvantovaya Elektronika **47** (2) 163–168 (2017)
Translated by I.A. Ulitkin

resources that do not contradict the laws of physics [12], such as a quantum computer, quantum memory and ideal channels that transmit quantum states. Of course, the practical implementation of the considered attacks depends essentially on the required technological resources. The second class involves an attack on the technical implementation of quantum cryptographic systems (so-called "quantum hacking") [15–17]. For example, these are attacks on certain types of single photon detectors [17].

Quantum key distribution devices are available on the market. However, their implementation meets a number of technological difficulties. One of the most promising methods of working with quantum systems, which is employed in quantum cryptography, is the use of attenuated coherent states instead of single photons, and therefore of coherent quantum key distribution protocols, for example the coherent one-way (COW) protocol [18–20]. These protocols go back to a classical communication means with the use of fibre-optic systems [20]. The most significant advantage of the COW protocol is the simplicity of its implementation [13, 18–20], associated with a fairly simple optical layout. This protocol is easy to implement experimentally and has been used in the European integrated project to build a SECOQC quantum key distribution network [21]. However, despite the prevalence of this method and its unquestionable practical importance, analysis of the possibility of attacks, allowing an eavesdropper to gain information about the key, still remains an urgent task [18–26].

Note also that the quantum key distribution systems are not, in the full sense, communication systems. The quantum resource in the form of single photons is used to generate a random sequence of bits (key) that is identical for legitimate users rather than to transmit information. The typical speed of key generation in these systems is on the order of 10 kbit s^{-1} at distances of 50–80 km. Some limitation of such systems is the fact that legitimate users require a dedicated forward link channel (i.e., 'point-to-point' network topology) to generate the key. Once the key is distributed, it can be used for encryption in the regime of one-time pads or as a source of entropy. Endpoint information rate in this case depends on the communication system transmitting the encrypted information.

In this paper, we consider a new type of attack on the COW quantum key distribution protocol. The basic idea of the attack is to individually measure part of intercepted states and to send the rest of them unchanged. The proposed attack belongs to the first class (attacks on the protocol). One of its advantages, however, is the fact that the implementation of this attack does not require the use of quantum memory or complex elements and is limited by a common assumption that the eavesdropper has a lossless channel. In other respects, the proposed attack has a relatively simple optical layout to implement, thus allowing one to achieve benefits in comparison with the known beam-splitting attack under certain restrictions on the parameters of the key distribution system.

2. Coherent quantum key distribution protocol (COW)

In the COW quantum key distribution protocol, Alice and Bob use two information states [18–20], in which the value of the bit (0 or 1) is encoded by a coherent state $|\alpha\rangle$ in one time slot and by a vacuum state in the other. Consequently, the states corresponding to 0 and 1 can be presented as follows:

$$|\psi_0\rangle = |\alpha\rangle\otimes|0\rangle,\ |\psi_1\rangle = |0\rangle\otimes|\alpha\rangle, \tag{1}$$

where the intensity of the coherent state $|\alpha\rangle$ is denoted by $\mu = |\alpha|^2$.

One of the simplest scenarios of an attack on the COW protocol is the 'intercept–resend' attack. In this attack, Eve tries to measure the state in each time slot and to subsequently resend the obtained state (with an increase in intensity to compensate for the loss). In order to detect an eavesdropper using an attack like this, Alice and Bob, in addition to the information states, employ decoy states of form

$$|\psi_c\rangle = |\alpha\rangle\otimes|\alpha\rangle. \tag{2}$$

Decoy states are used to detect an attempt aimed at distinguishing between information states. When attacking, the interceptor will occasionally send information states instead of decoy states that would allow him to be detected. The fraction of the decoy states denoted by f is usually about 10% [13, 18–20].

3. Beam-splitting attack on the COW protocol

Real fibre-optic communication lines are subject to attenuation, which leads to the fact that Bob receives states of lower intensity. The intensity of the state obtained by Bob has the form:

$$\mu_B = 10^{-\delta l/10}\mu, \tag{3}$$

where l is the channel length in kilometres, and δ is the attenuation coefficient (a typical attenuation coefficient of fibre-optical lines in the spectral range of 1.5 μm is 0.2 dB km^{-1}).

In analysing attacks on the quantum key distribution protocol, it is assumed that Eve has unlimited technological resources. Therefore, one of the possible attack scenarios is the use of a beam splitter in combination with an ideal communication channel. Since states are transformed in a self-similar way on a beam splitter and in a fibre-optic line with attenuation, Eve may take part of each state on the beam splitter and send the remaining part to Bob via a channel replaced by an ideal one (lossless channel).

The maximum signal intensity, which can be intercepted by Eve, has the form

$$\mu_E^{\max} = \mu - \mu_B = (1 - 10^{-\delta l/10})\mu. \tag{4}$$

From Bob's point of view, this transfer of the states using a beam splitter does not differ from the attenuation in a channel and cannot be detected. Eve's strategy with withdrawn states may vary for different attacks.

Consider a scenario of a beam-splitting attack, in which Eve stores withdrawn states so that to retrieve information from them [25]. The configuration of the states and the measurement at the receiver side are such that in the absence of Eve (as well as in the withdrawing part of states and resending the remaining part via an ideal channel), Bob has a zero quantum bit error rate (QBER), and his mutual information with Alice after discarding inconsistent outcomes is equal to unity. Since Eve has less information, she introduces errors in this attack so that her information was equal to Bob's information. Thus, Eve's information states in this attack have the form

$$|\psi_0^E\rangle = |\sqrt{\mu_E^{\max}}\rangle\otimes|0\rangle,\ |\psi_1^E\rangle = |0\rangle\otimes|\sqrt{\mu_E^{\max}}\rangle. \tag{5}$$

The information that Eve can retrieve from these states in the case of a collective measurement is given by the Holevo quantity (χ value) [27]:

$$I_{AE} = \chi(\{|\psi_0^E\rangle, |\psi_1^E\rangle\}). \quad (6)$$

In this case, it is easy to find a critical value of QBER, which Eve should add in order to make her information coincident with Bob's information. The critical value of QBER is expressed through the binary entropy of the introduced error as follows:

$$I_{AB} = 1 - h_2(\text{QBER}), \quad (7)$$

where h_2(QBER) is the binary entropy function.

The strong point of the beam-splitting attack is that it uses collective measurements over the entire transmitted sequence. This makes it possible to achieve the χ value due to quantum superadditivity and to obtain a theoretical maximum of information from quantum states. However, a disadvantage of such an attack consists in the fact that in long-haul communication lines, the critical error of the protocol does not tend to zero because Eve's information is limited by the χ quantity of the initial states. At the same time, since Bob receives fewer states with increasing channel length, a natural requirement to the attack is that it enjoyed an opportunity, for example, to block some of the states, from which it was impossible to extract enough information.

4. Active beam-splitting attack on the COW protocol

In this paper, we propose an alternative scenario of an attack on the COW protocol. Its difference from the beam-splitting attack consists in the following. First, in the attack in question Eve withdraws a smaller part of the states than in the beam-splitting attack. Second, the eavesdropper performs individual measurements of each state. In the case of an inconclusive result of measurements (i.e., in detecting vacuum states in both positions), Eve is able to block the state since the information about it is inaccessible. At the same time, in the general case, Eve is unable to block all such states due to the fact that in this case the intensity at the receiver side is lower than the expected intensity, which will detect the presence of Eve. Therefore, to estimate the efficiency of this attack we consider the idea similar to that in the beam-splitting attack: if the channel length does not allow Eve to block all states, from which she fails to retrieve information, she introduces an error in the transmitted states in order to make Bob's information comparable with Eve's information. We call this attack the active beam-splitting attack because its use depends on Eve's ability to extract information from withdrawn states.

Let us describe Eve's actions in detail with allowance for all the parameters. Eve withdraws part of states with the intensity μ_E and then measures each time slot of the state. Her measurement in each time slot is described by the observable quantity:

$$M_0 = |0\rangle\langle 0|, \quad M_1 = \sum_{i=1}^{\infty} |i\rangle\langle i|. \quad (8)$$

The probability of obtaining result 1 in the measurement of the state of intensity μ_E has the form

$$p_{\text{conc}}^{\text{inf}} = 1 - \exp(-\mu_E). \quad (9)$$

This expression gives the probability of obtaining a conclusive result in the measurement of the information state (1) but with a lower intensity. When transmitting the decoy state, the probability of the conclusive result is as follows:

$$p_{\text{conc}}^{\text{cont}} = 2\exp(-\mu_E)(1 - \exp(-\mu_E)) + (1 - \exp(-\mu_E))^2. \quad (10)$$

Thus, the total probability of the conclusive result by Eve taking into account the fraction of the decoy states is expressed as:

$$p_{\text{conc}}^{E} = (1-f)\, p_{\text{conc}}^{\text{inf}} + f p_{\text{conc}}^{\text{cont}}. \quad (11)$$

It should be noted that the use of the decoy states does not allow one to detect Eve since she still sends part of the initial state unaffected by measurements. A possible error arising when the decoy state is not differentiated from the information state does not lead to a decrease in Eve's information, because decoy states are discarded by legitimate users.

In the case of an inconclusive result of Eve's measurement, the probability of which is equal to $1 - p_{\text{conc}}^{E}$, Eve tends to block the states transmitted to Bob. In the general case, Eve is able to implement this not universally but for a small fraction of states so that the blocking is undetectable at the receiver side due to large attenuation. Let us calculate this fraction of the states, which can be blocked.

Bob expects states with intensity (3). For these states the probability to obtain a conclusive result for information states is equal to $1 - \exp(-\mu_B)$. In reality, by using a beam splitter Eve can keep higher intensity states for Bob in order to block 'inconvenient' states, and therefore the intensity of Bob's states is $\mu'_B = \mu - \mu_E$. Consequently, the permissible fraction of states b blocked by Eve can be obtained from the relation

$$(1 - b)(1 - \exp(-\mu'_B)) = 1 - \exp(-\mu_B). \quad (12)$$

This fraction of blocked states can be determined for a given channel length and Eve's attack parameters, in particular, the intensity of withdrawn states. This intensity varies from zero to the maximal intensity $\mu_E^{\max}$ found from expression (4). For each channel length Eve should choose a fraction of withdrawn states maximising her information.

Eve's information can be calculated as follows. The information is equal to unity for the cases, where Eve has conclusive results. At the same time, for an arbitrary channel length Eve cannot block all states, where she does not extract complete information. Then, she still has to send the states to Bob. For the probability of the conclusive result and the probability of state blocking b, determined from Eqn (12), we have

$$I_{AE} = p_{\text{conc}}^{\text{inf}}/(1 - b). \quad (13)$$

One can see that if Eve is able to block all states with the inconclusive result of the measurement (i.e., if $b = 1 - p_{\text{conc}}^{\text{inf}}$), then her information is equal to unity. The values of the parameter b, exceeding the probability of the inconclusive result of the measurement, is useless to consider, whereas at lower values, Eve's information decreases and in the absence of state blocking it reaches a minimum that is equal to the probability of the conclusive measurement result, which represents the capacity of the channel with attenuation.

We consider the issue about the choice of the optimal value of the intensity of Eve's withdrawn state μ_E ensuring a maximum of the intercepted information I_{AE}. Using expression (9) for the probability p_{conc}^{inf} and identity (12) determining the permissible fraction of the states b blocked by Eve, we rewrite expression (13) in the form

$$I_{AE} = \frac{(1 - \exp(-\mu + \mu_E))(1 - \exp(-\mu_E))}{1 - \exp(-\mu_B)}. \quad (14)$$

It is clear that I_{AE} is a convex function of the argument μ_E, which reaches a maximum at $\mu_E = \mu/2$. However, because the intensity μ_E is bounded by the quantity μ_E^{max}, the information maximum of the intercepted intensity is achieved at

$$\mu_E = \min(\mu_E^{max}, \mu/2). \quad (15)$$

Note that in the case $\mu_E = \mu_E^{max}$, we have $\mu_E^{max} = \mu_E'$ and $b = 1$. Thus, at $\mu_E^{max} \leqslant \mu/2$, Eve should send all states to Bob rather than block them.

The critical length l_0 at which it is reasonable for Eve to block the states is given by the identity

$$(1 - 10^{-\delta l_0/10}) = 1/2 \quad (16)$$

and is calculated as

$$l_0 = 10 \log_{10} 2/\delta \approx 3/\delta. \quad (17)$$

For a typical value $\delta = 0.2$ dB km^{-1}, we then obtain $l_0 \approx 15$ km.

5. Discussion

Thus, let us briefly describe the scenario of the attack in question and the method for searching for the critical error of the protocol. For a given channel length Eve calculates the maximum intensity of the states, which she can withdraw. Then she considers the possibility of withdrawing the states of different intensity – from zero to maximum. For each of them one can explicitly calculate Eve's information and the fraction of the states which Eve can block. The greater the intensity of the states received by Bob, the more states can be blocked. Eve chooses the intensity at which her information is maximal. If she can block all states with the inconclusive result of measurements, Eve is able to attack without introducing an additional error, which makes the protocol insecure. If the fraction of states that can be blocked proves to be smaller, Eve introduces an error in the channel between Alice and Bob in order to level the difference between Bob's and her information. The minimum value of the error, at which their information is compared, is a critical QBER value of the protocol against this attack. Figure 1 shows a critical QBER of a standard beam-splitting attack and an active beam-splitting attack in question for three values of the intensity.

A question may arise as to which intensity of the initial states is optimal for legitimate users under the assumption that an eavesdropper uses this particular attack. On the one hand, it is clear that in order to increase the critical QBER, they should use the lowest intensity of the initial states. On the other hand, the low intensity of the initial states leads to a low key generation rate because of a too large fraction of the states that are lost during transmission to the receiver side.

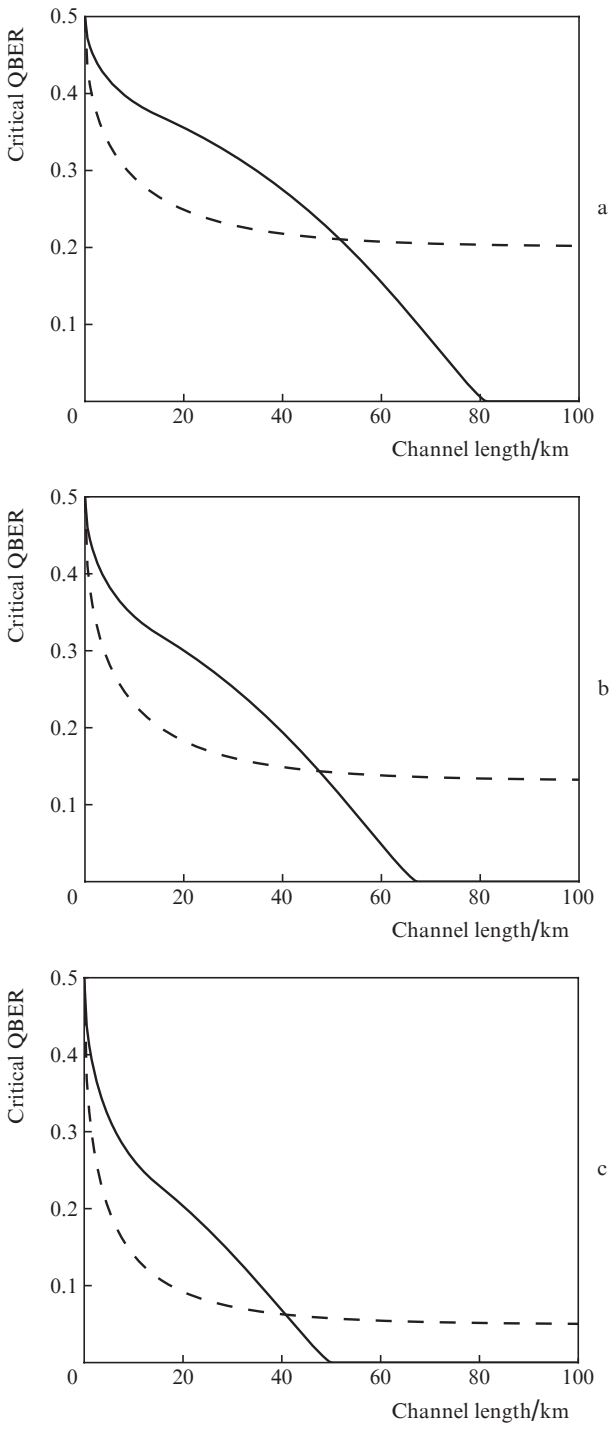

Figure 1. Comparison of the critical QBER value for the standard beam-splitting attack (dashed line) and the active beam-splitting attack (solid line) for the intensity μ = (a) 0.1, (b) 0.2 and (c) 0.5.

We will seek for the optical intensity in the following way. Let Eve withdraw the maximum fraction of the states (permissible by the attack) without introducing however any errors in the channel between Alice and Bob (because the magnitude of the error is no longer a factor). The length of the secret key between Alice and Bob, recalculated with regard to one state, is given by the difference of information between Alice and Bob, I_{AB}, and between Alice and Eve, I_{AE}. The former one is equal to the capacity of the communication channel with attenuation, equal to the probability of the inconclu-

sive result $\exp(-\mu_B)$, while the latter one can be calculated by Eqn (13) and then multiplied by the probability of the conclusive result of Bob. An optimal value of the intensity for this channel length is thus the value at which the difference

$$I_{AB} - I_{AE} = 1 - \exp(-\mu_B) - (1 - \exp(-\mu_B))\,\frac{p_{\text{conc}}^{\text{inf}}}{1-b} \qquad (18)$$

is maximal. Figure 2 shows an optimal intensity for difference channel lengths and a critical QBER for the chosen optimal intensity. For comparison we present a critical error of the beam-splitting attack. However, we should note that the initial intensity is optimized under the assumption that the eavesdropper will use the active beam-splitting attack only.

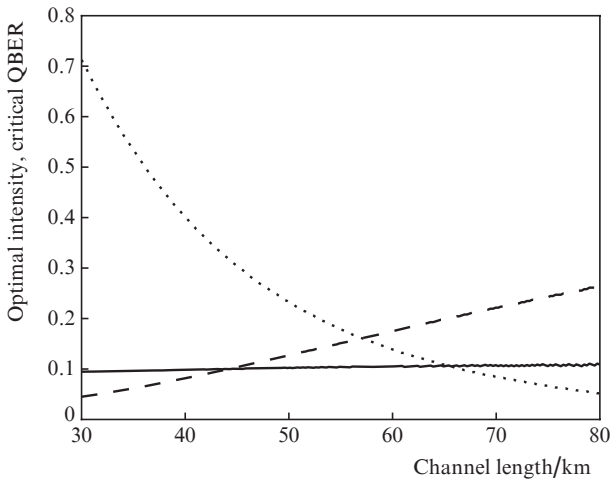

Figure 2. Optimal intensity for different channel lengths (dotted curve) as well as the critical QBER at the optimal choice of the intensity by Eve (solid line), and the critical QBER of the beam-splitting attack at the given length and given choice of intensity (dashed line).

A disadvantage of this attack is the fact that Eve is unable to amplify the signal transmitted to Bob for those states which yielded conclusive results. Another drawback is that Eve should perform all the measurements at once, which eliminates the possibility of achieving superadditive information. On the other hand, unlike a standard beam-splitting attack, this attack, starting with a critical length of the communication channel, is possible without introducing errors. Nevertheless, an attack with an unambiguous measurement [26] is more effective because there is a possibility of amplifying the intensity of the states from which information is extracted. The advantages of the attack in question include a fairly simple technical implementation.

Thus, the active beam-splitting attack under study is first of all interesting due to the fact that it can be potentially implemented at a given technological level rather than due to the fact that it is optimal from the point of view of the eavesdropper limited only by the laws of physics. The development of the idea of an unchanged forwarding state is urgent in the context of other quantum-cryptography protocols utilising coherent states [13].

Note also that despite the fact that the attack under study does not lead to a change in the type of state (the decoy state cannot be transformed into the signal one and vice versa), it leads to a distortion of the statistics of the decoy states being received. This phenomenon is related both to a change in the intensity of the states transmitted to Bob (from μ_B to μ'_B) and to the fact that the probability of state blocking is determined by the probability of obtaining a conclusive result by Eve. In turn, in the case of the decoy state this probability turns higher than in the case of the signal state and the total probability of obtaining a decoy state by Bob increases. As a result, the attack under study can be potentially detected by taking into account the statistics of registration of decoy states in the classical key post-processing. However, the protocol designers consider only a requirement of the absence of changes in the type of state, which means that accounting for such statistics will require a significant change in the protocol in terms of evaluation of the interceptor information.

An interesting and relevant is the problem of the COW protocol modification to take the proposed attack into account. However, this issue requires further analysis, which is beyond the scope of this paper.

6. Conclusions

We have considered a new type of attack on a coherent quantum key distribution protocol (COW protocol) using an active beam splitter. We have calculated optimum values of the attack parameters for any length of the communication channel, as well as have compared it with a standard beam-splitting attack.

The advantages of the considered attack include a fairly simple technical implementation. It should be noted that the proposed attack is actually relevant for channels of any length. However, it has particular relevance for quantum-cryptography systems operating in urban environments and using short (30–50 km) urban fibre-optic communication lines with fairly heavy losses. In recent experiments on quantum key distribution in urban environments, the losses in a 30-km-long channel amounted to about 11 dB at a key generation rate of 0.5 kbit s^{-1} after post-processing [28].

Acknowledgements. The authors thank A.S. Trushechkin and O.V. Lychkovskiy for helpful discussions, and the reviewers for valuable comments.

This work was supported by the Ministry of Education of the Russian Federation in the framework of the Federal Target Programme 'Research and development on priority directions of the scientific-technological complex of Russia for 2014–2020' (Agreement No. 14.579.21.0105, ID RFMEFI 57915X0105).

References

1. Feynman R.P. *Intern. J. Theor. Phys.*, **21** (6), 467 (1982).
2. Feynman R.P. *Opt. News*, **11** (2), 11 (1985).
3. Deutsch D. *Proc. R. Soc. London, Ser. A*, **400**, 97 (1985).
4. Bennett C.H., Brassard G. *IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE, 1984) p. 175.
5. Grover L.K. *Proc. 28th Ann. ACM Symp. on the Theory of Computing* (New York: ACM Press, 1996) p. 212.
6. Shor P.W. *SIAM J. Comput.*, **26**, 1484 (1997).
7. Diffie W., Hellman M.E. *IEEE Trans. Inf. Theory*, **22** (28), 644 (1976).
8. Rivest R.L., Shamir A., Adleman L. *Commun. ACM*, **21** (2), 120 (1978).
9. Bernstein D.J. *Introduction To Post-Quantum Cryptography* (Berlin: Springer-Verlag, 2009).
10. Shannon C. *Bell System Techn. J.*, **4** (28), 656 (1949).
11. Vernam G.S. *J. Am. Inst. Electr. Eng.*, **45**, 109 (1958).

12. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys.*, **74**, 145 (2002).
13. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dusek M., Lutkenhaus N., Peev M. *Rev. Mod. Phys.*, **81** (3), 1301 (2009).
14. Wootters W.K., Zurek W.H. *Nature*, **299**, 802 (1982).
15. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nat. Photonics*, **4**, 686 (2010).
16. Gerhardt I., Liu Q., Lamas-Linares A., Skaar J., Kurtsiefer C., Makarov V. *Nat. Commun.*, **2**, 349 (2011).
17. Jain N., Anisimova E., Khan I., Makarov V., Marquardt Ch., Leuchs G. *New J. Phys.*, **16**, 123030 (2014).
18. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett.*, **87**, 194108 (2005).
19. Stucki D., Barreiro C., Fasel S., Gautier J.-D., Gay O., Gisin N., Thew R., Thoma Y., Trinkler P., Vannel F., Zbinden H. *Opt. Express*, **17**, 13326 (2009).
20. Stucki D., Walenta N., Vannel F., Thew R.T., Gisin N., Zbinden H., Gray S., Towery C.R., Ten S. *New J. Phys.*, **11**, 075003 (2009).
21. Alléaume R., Branciard C., Bouda J., Debuisschert T., Dianati M., Gisin N., Godfrey M., Grangier P., Langer T., Lutkenhaus N., Monyk C., Painchault P., Peev M., Poppe A., Pornin Y., Rarity J., Renner R., Ribordy G., Riguidel M., Salvail L., Shields A., Weinfurter H., Zeilinger A. *Theor. Comput. Sci.*, **560**, 62 (2014).
22. Branciard C., Gisin N., Lutkenhaus N., Scarani V. *Quantum Inf. Comput.*, **7**, 639 (2007).
23. Branciard C., Gisin N., Scarani V. *New J. Phys.*, **10**, 013031 (2008).
24. Curty M., Zhang L.L., Lo H.-K., Lutkenhaus N. *Quantum Inf. Comput.*, **7**, 665 (2007).
25. Kronberg D.A., Molotkov S.N. *Zh. Eksp. Teor. Fiz.*, **145**, 5 (2014) [*JETP*, **118**, 1 (2014)].
26. Molotkov S.N. *Pis'ma Zh. Eksp. Teor. Fiz.*, **93**, 194 (2011) [*JETP Lett.*, **93**, 178 (2011)].
27. Holevo A.S. *Quantum Systems, Channels, Information* (Berlin–Boston: De Gruyter, 2012; Moscow: MTsNMO, 2010).
28. Kiktenko E.O., Trushechkin A.S., Kurochkin Y.V., Fedorov A.K. *J. Phys.: Conf. Ser.*, **741**, 012081 (2016).