On using intensity fluctuations for eavesdropping on coherent states quantum cryptography

D.A.Kronberg, Y.V.Kurochkin

April 24, 2017

The goal of quantum cryptography is a secret key distribution between two distant users (Alice and Bob) with no assumptions about computational or technological possibilities of an eavesdropper (Eve). The important constraint imposed by quantum mechanics is that one cannot get full information from the set of non-orthogonal quantum states. In quantum key distribution protocols, Alice and Bob use non-orthogonal quantum states to send the information, and these states are designed so that Alice and Bob could detect Eve's attack by errors in their channel.

Quantum cryptography protocols based on coherent states are of high interest since they do not need single-photon sources and are rather easy for practical implementation. In such cryptography systems, weak laser pulses are used as information states, and they are transmitted over optical fiber lines.

The attenuation of coherent pulses in practical fiber line is the thing that can give new possibilities to the eavesdropper. The two following types of attacks are the most important: beam splitting attack and unambiguous state discrimination (USD) attack. In the first one, Eve uses a beam splitter to take a part of each state to her quantum memory and sends the rest part to Bob via a perfect channel without losses. This attack can not be detected at the receiver side, but Eve gets just a partial information bordered by the Holevo value of her states [1]. In the USD attack [2] Eve performs an unambiguous measurement of each state, which sometimes gives full information and sometimes gives inconclusive result. If Eve is lucky to get full information, she sends the states of high intensity to Bob, and if she gets inconclusive result, she blocks the pulse.

The USD attack introduces no error and is therefore very powerful but it requires the possibility of blocking original signals. The protocols on coherent states try to resist this blocking. The common methods include:

1. Sending not only information states, but also control states, or decoy states of other intensity, which make an unambiguous state discrimination mores difficult or reveals the presence of an eavesdropper by changed statistics of the states of different types. The corresponding protocols include coherent-one way (COW) protocol [3] or decoy-state protocol [4].

2. Using a reference state of high intensity which must be detected by Bob. The information is encoded into the phase difference between the reference state and a weak information pulse ([5], [6]). Thus, if Eve blocks the weak information pulse, she will cause errors at the receiver side.

3. Sending tuples of coherent states with information encoded in phase difference between the successive states, like in differential phase shift (DPS) protocol [7]. The blocking of some particular states also causes error.

We consider a simple example of protocol with two coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ (with original intensity μ_A on Alice's side) and we assume that Bob can somehow check the intensity of the received

states, and legitimate user abort the protocol if this intensity is beyond some values. The main question is how Eve can use the possibility of changing the states intensity. If intensity can vary from zero to infinity, the USD attack is possible. If the value of intensity must be strictly equal to the expected value μ_B after the fiber line of the given length, only beam splitting attack is possible. Then, if the intensity can vary from $\mu_{\min} < \mu_B$ to $\mu_{\max} > \mu_B$, how can Eve use it? These limitations can include only upper or lower bounds as well.

The key idea of the proposed attack is that Eve uses a beam splitter to separate the original state in two parts: one part for extracting information and the other part for sending it to Bob. Then Eve performs an attempt of information extraction from her part. If she is lucky, and information extraction was successful, she sends the state of high intensity to Bob, otherwise she sends the state of low intensity, because Bob's conclusive result at such positions is not desirable for Eve.

This attack is a generalization of the attack on COW protocol proposed in [8], which uses the state separation on a beam splitter and unambiguous measurement of one part with sending the unchanged second part of the state in the case of success. Here, we generalize the measurement and do not necessarily block the state in the case of fail.

Our generalization of unambiguous measurement is called soft filtering. It uses the unitary transformation which with some success probability amplifies the original states to the states of target intensity μ_t or gives an inconclusive result and annihilates the states. The success probability depends on the original and target intensities: when target is close to the original one, this probability is close to one, and when target probability tends to infinity, this probability tends to the success probability of unambiguous state discrimination.

The attack is organized as follows. Eve takes the part of the state and tries to perform a soft filtering to target intensity μ_t. If there was a success, Eve's information is given by the Holevo value of her states. Then she send to Bob the rest part of the state of intensity $\mu_{\max}$ and introduces error to the line between Alice and Bob so that Bob's information becomes the same as her. The error value q_1 is given by

$$1 - h_2(q_1) = h_2(\frac{1 - e^{-2\mu_t}}{2}). \tag{1}$$

In the case of failed soft filtering Eve uses beam splitter again to take a part of the highest possible intensity μ_2 to her, sending the state of intensity $\mu_{\min}$ to Bob, and introducing the error of value q_2 which corresponds to her information similarly to (1).

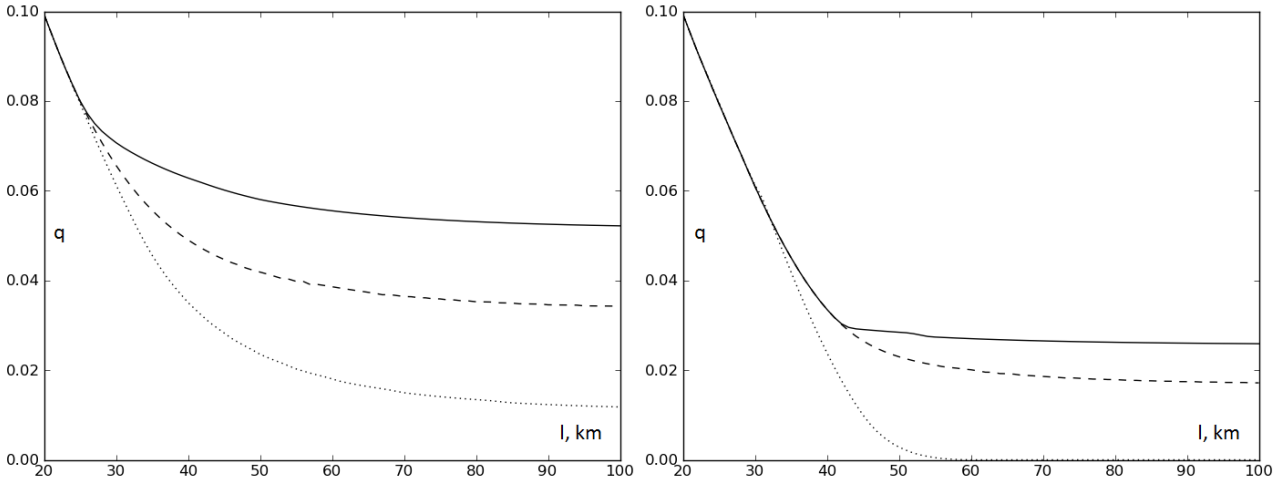
The main measure for attack efficiency is the critical error at which Eve has the same information as Bob. For the strategy described above it is given by

$$q = q_1 p(1 - e^{-2\mu_{\max}}) + q_2(1 - p)(1 - e^{-2\mu_{\min}}), \tag{2}$$

where p is the probability of successful filtering. Thus, Eve sets her parameters (the part of state for filtering and the target intensity) to the optimal values to minimize the critical error.

The figure shows the critical error of our sample protocol against the considered attack for different channel length values. The source intensity is $\mu_A = 0.2$. On the left, error is shown for $\{\mu_{\min} = \frac{1}{2}\mu_B, \mu_{\max} = 2\mu_B\}$ (both values are limited; solid line), for $\mu_{\min} = \frac{1}{2}\mu_B$ (limitation from below, dashed line), and for $\mu_{\max} = 2\mu_B$ (restriction on top value, dotted line). On the right, similarly, solid line shows error for $\{\mu_{\min} = \frac{1}{4}\mu_B, \mu_{\max} = 4\mu_B\}$, dashed line – for $\mu_{\min} = \frac{1}{4}\mu_B$, and dotted line – for $\mu_{\max} = 4\mu_B$.

This attack can be applied to a number of coherent-state protocols, this is a topic for further research. it is also important to know under which conditions the known coherent-state protocols can guarantee the secrecy of generating keys. According to this results, one can conjecture that if a protocol can guarantee non-zero intensity of states reaching Bob, then no zero-error attack is available. This conjecture is a topic for future research as well.



References

[1] Holevo A.S. Quantum Systems, Channels, Information. A Mathematical introduction, De Gruyter, BerlinBoston, 2013, ISBN: 978-3-11-027325-0.

[2] Dusek M., Jahma M., Lutkenhaus N., Unambiguous state discrimination in quantum cryptography with weak coherent states. Phys. Rev. A 62, 022306

[3] Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. Fast and simple one-way quantum key distribution. Appl. Phys. Lett., 87, 194108 (2005)

[4] Lo H.-K., Ma X., and Chen K. Decoy State Quantum Key Distribution. Phys. Rev. Lett. 94, 230504 (2005)

[5] Koashi M. Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse. Phys. Rev. Lett. 93, 120501

[6] Molotkov S.N. On a solution to the problem of ensuring the security of quantum cryptography for an infinite communication channel. Jetp Lett. 93: 747 (2011)

[7] Inoue K., Waks E., Yamamoto Y. Differential phase-shift quantum key distribution. Proc. SPIE 4917, Quantum Optics in Computing and Communications, 32 (2002)

[8] Kronberg D.A., Kiktenko E.O., Fedorov A.K., Kurochkin Yu.V. Analysis of coherent quantum cryptography protocol vulnerability to an active beam-splitting attack. Quantum Electronics, Volume 47, Number 2 (2017) arXiv:quant-ph/1611.04112