IRSTI 50.07.03

D. Turanov[1], A. Selbayev[2]
[1,2]Suleyman Demirel University, Kaskelen, Kazakhstan

THREAT FOR QKD WITH A TRANSFER OF A MODIFIED CONDITION

Abstract. Quantum key distribution makes it possible to generate a secret key between authenticated users. The security of the process, it is possible to achieve, by using the states of quantum mechanics. To date, the quantum system is in experimental states, although several commercial projects have already been implemented. And in particular, single-photon avalanche photo-detectors. The technical level of devices does not yet allow creating the ideal condition for an ultra-secure system. In this article we will present the attack method and the protocols that are able to detect these attempts.

Keywords: BB84, BB92, photo-detectors, single-photon, cryptosystem, ultra-secure system, QKD, photo-diode.

***

Аннотация. Квантовое распределение ключей позволяет генерировать секретный ключ между аутентифицированными пользователями. Безопасность процесса можно достичь, используя состояния квантовой механики. На сегодняшний день квантовая система находится в экспериментальном состоянии, хотя несколько коммерческих проектов уже реализованы. И, в частности, однофотонные лавинные фотоприемники. Технический уровень устройств пока не позволяет создать идеальные условия для сверхзащищенной системы. В этой статье мы представим метод атаки и протоколы, которые могут обнаружить эти попытки.

Ключевые слова: BB84, BB92, фотодетекторы, однофотонный, криптосистема, сверхзащищенная система, QKD, фотодиод.

***

Аңдатпа. Кванттық кілттерді үлестіру түпнұсқалығы расталған пайдаланушылар арасында құпия кілт жасайды. Процестің қауіпсіздігі кванттық механиканың жағдайын қолдана отырып қол жеткізуге болады. Қазіргі уақытта кванттық жүйе эксперименталды күйде, бірақ бірнеше коммерциялық жобалар іске асырылған. Атап айтқанда, бір фотонды

көшкіні фотоаппарат. Құрылғылардың техникалық деңгейі әлі де ультра қауіпсіз жүйенің мінсіз жағдайын жасауға мүмкіндік бермейді. Бұл мақалада біз осы әрекеттерді анықтай алатын шабуыл әдісі мен хаттамаларды ұсынамыз.

Түйін сөздер: BB84, BB92, фото-детекторлар, бір фотонды, криптожүйе, ультра-қауіпсіз жүйе, QKD, фото-диод.

Introduction

The quantum world is complex from the point of view of the laws of ordinary mechanics, since these laws are limited in the expanses of quantum physics. One of the main limitations of these laws is the immeasurability of quantum states. The limitations of the laws and is the main fundamental link, which makes quantum cryptography one of the most secure systems. There are many ways to take advantage of quantum physics in systems. One of the most realized uses of quantum technologies is the creation of a randomly generated secret key for encryption. There is a vulnerability of the system, due to the imperfection of the devices used. For example, one of the fundamental conditions for the application of quantum technologies in cryptography is the creation of a pure single-photon source. This difficulty will have to be solved in the future when more advanced devices appear. Today, multi-photon devices are used, which, as the study shows, leave unauthorized access.

The quantum key distribution protocol usually means authentication, pre-process preparation, transfer, examination of states, handling errors (eliminating or enhancing secrecy using the compression method), analyzing and verifying the obtained keys. The data transmitted by the system must be absolutely protected from third parties and, if necessary, disclose the audition. When unauthorized access to the transmitted data occurs, the system should detect this attempt using the ratios of valid and resulting error. In other situations, the system is considered unprotected when unauthorized access by a third party goes unnoticed and the key is known to it. For several years, research has been conducted in which the capabilities of quantum cryptography have been demonstrated [1, 2].

Currently, in quantum systems, attenuated laser radiation is used as a source of a single-photon state (which is not purely single-photon), single-photon avalanche photo detectors (which has dark noise), efficiency (whose properties are not rare), communication channels (fiber optic and open space), which are subject to loss and noise. This in turn leads to the emergence of the possibility of a photon-splitting system attack (PNS, Photon Number Splitter attack [7]) and an attack with measurements with a certain outcome

(Unambiguous Measurements [8, 9]). We included these factors in the analysis of the security of protocols [6].

Unauthorized access to a key using photo-detector blinding [10] is one of the new threats to quantum key distribution. In this threat, a third party uses the possibility of affecting a communication channel in which it sends a modified (falsified) state. This allows a third party to control the counts or their absence at the receiving side, and impose their own counting, which does not lead to an error at the recipient (receiving side). As a result, the third party remains unnoticed and informed about the key. This new method of threat significantly reduces the secrecy of the system. Most of the protocols, with no additional parameters, were potentially not resistant to this threat (BB84 [3], SARG04 [13], Six-State QKD [14], DPS (Differential Phase Shift) [5,15], COW (Coherent One Way) [16], E91 [17], Decoy State QKD [18].

One way to solve this problem is to create a strictly single-photon source, which at the present time has proved difficult to implement. Until this difficulty is resolved, the threat will always exist. To date, the search for solutions to these problems. From the basic solutions, it is proposed to complicate and add additional parameters to existing protocols. The proposed solution does not solve the problem, but only complicates access by a third party. The methods of the third party in turn become cleverer.

The best way to create an over-secure system is to create a protocol in which security is achieved through internally-structured methods, rather than an improvement and addition in technical terms [11].

1. Threat with photon modification.

Below we provide information about this new threat on the host device, while not trying to look at all this in terms of technical vision, since all this is in the articles [10, 12, 19].

The more devices are not perfect, the some ways to use these imperfections. One of these ways to influence the receiving side:

1. On avalanche photo-detectors, there is a difference in the sensitivity of temporal dependencies. This allows a third party to modify (falsify) the state and blind the devices of the receiving party.
2. Using the state of the lower threshold of intensity, in order to include only one device, in situations where the bases of the third party and the recipient will be the same. Otherwise, everything happens without counting.

Basically, the possibility of third-party unauthorized access arises from the work of semiconductors (the so-called avalanche photo-detectors InGaAs:P). A blocking voltage is applied to the avalanche photo-diode. At the moment of

arrival of the photon, a gate voltage pulse (typical duration of the order of several nanoseconds and an amplitude of several volts) is applied, which opens the photo-diode. The absorption of a photon leads to the formation of an avalanche of carriers and a voltage pulse, which is recorded.

1. The first blinding attack is based on the following property. If the radiation intensity is increased slightly above the quasi-single-photon mode, this will lead to an increase in the current flowing through the photo-diode at the time of registration. Due to the fact that a photo-diode without illumination is not active (locked), the dynamic increase in current above a certain value will lead to an effective decrease in the bias voltage during the action of the strobe and to lock the diode and, accordingly, decrease, up to its absence, the avalanche current ("no click"). Thus, the photo-diode is effectively blinded.

2. The second attack is connected with the transfer of the photo-diode from the counting mode to the linear classical photo-detection mode, when the current is a function of the radiation intensity (usually proportional to it). If we further increase the radiation intensity, then after blinding the photo-diode (see paragraph 1 above) and the absence of the registration current, starting with a certain threshold intensity value, a signal will appear again on the photo-diode through the photodiode a current proportional to the radiation intensity will flow [4].

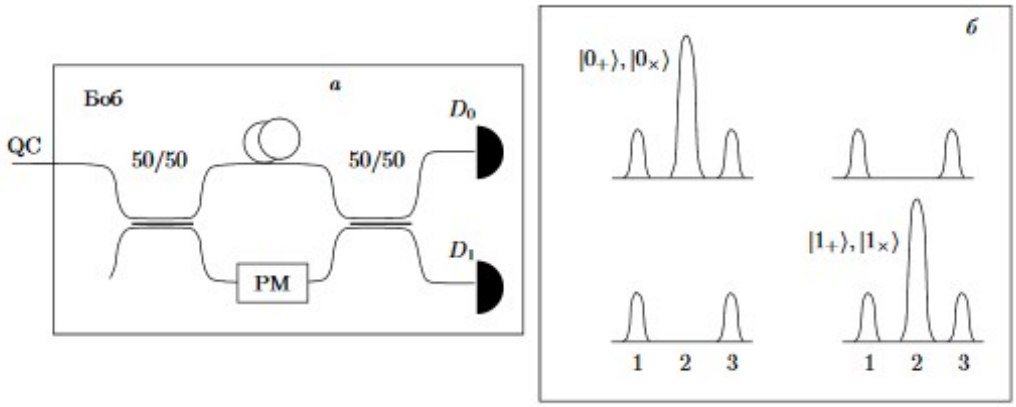

Fig.1 a) Schematic diagram of the receiving part of the fiber optic quantum cryptography system implementing the BB84 protocol. QC - quantum canal, Pm - phase-modulator.

b) Photo-count statistics in two detectors for different information states.

2.1. The use of the difference in the sensitivity.

The first protocol in quantum cryptography BB84 [3] is in any way well suited to explain the main points of opposition to the threats to which some protocols are exposed and their strong and weak aspects [3, 10, 12, 19].

States in basis + from quantum channel:

$$|0_+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle),\ |1_+\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \quad (1)$$

and in the basis of ×,

$$|0_\times\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i\,|0\rangle),\ |1_\times\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i\,|2\rangle), \quad (2)$$

where $|1\rangle$ and $|2\rangle$ states localized in the time windows 1 and 2. The distance between the localized states is equal to the difference in travel along the upper and lower arms of the unbalanced interferometer (Fig. 1)

In the process of entering the receiving device, taking into account the selected phase, the quantum state in basis + have the form

$$\begin{aligned} &|0_+\rangle \rightarrow \frac{1}{\sqrt{8}}, , \\ D_0: \\ &|1_+\rangle \rightarrow \frac{1}{\sqrt{8}}, \\ &|0_+\rangle \rightarrow \frac{1}{\sqrt{8}}, , \\ D_1: \\ &|1_+\rangle \rightarrow \frac{1}{\sqrt{8}}, \end{aligned} \quad (3)$$

in basis of × (value = π / 2)

$$\begin{aligned} &|0_\times\rangle \rightarrow \frac{1}{\sqrt{8}}, \left(1 + \left(1 + e^{i\varphi_B(x)}\right) \vee 2 + 3\right), \\ &D_0: \\ &|1_\times\rangle \rightarrow \frac{1}{\sqrt{8}}, \left(1 + \left(-1 + e^{i\varphi_B(x)}\right) \vee 2 + 3\right) \\ &|0_\times\rangle \rightarrow \frac{1}{\sqrt{8}}, \left(-1 + \left(-1 - e^{i\varphi_B(x)}\right) \vee 2 + 3\right), \\ &D_1: \\ &|1_\times\rangle \rightarrow \frac{1}{\sqrt{8}}, \left(-1 + \left(1 - e^{i\varphi_B(x)}\right) \vee 2 + 3\right) \end{aligned} \quad (4)$$

If the bases on the receiving and transmitting sides of the state coincide, corresponding to 0 in both bases, they will give readings in time window 2 (Fig. 1) only in the D_0 detector. Accordingly, the states corresponding to 1 in both bases will give counts only in the D1 detector [2].

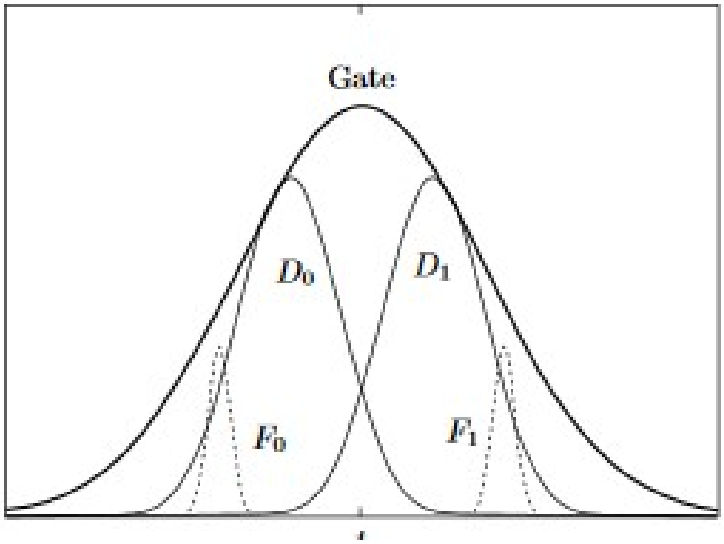

Fig. 2. An example of temporal dependences of the sensitivity of avalanche photo-detectors (D_0, D_1), gating pulse (Gate) and falsified quantum states (F_0,F_1).

However, the avalanche photodiodes D_0 and D_1 have different temporal characteristics of sensitivity (Fig. 2). The threat comes down to the following. The third party breaks the quantum communication channel (optical fiber) and carries out measurements similar to those on the receiving side in a randomly chosen basis.

There are two options. Immediately, we note that the third party sends its modified state in the basis opposite to the one in which it carried out its measurements (see details in [12, 19]).

1) With the coincidence of the bases of the third party and the authenticated participants. (for example, "+"). Assuming that after the analysis, the third party received a "0", i.e. the correct result, but the third party does not know about it until the end of the process between the sender and the recipient, and therefore she prepares the falsified state "1" in the opposite basis "x", but more localized (narrow) and slightly shifted in time so that it does not fell into the sensitivity curve of the photo-detector D_1 (Fig. 2). And the third party re-sends:

$$|1_{F_0\times}\rangle = \frac{1}{\sqrt{2}}(|1_{F_0}\rangle - i\,|2_{F_0}\rangle), \quad (5)$$

After passing through the interferometer and phase modulator with the phase in the basis + (F), the states in front of the entrance to the photo-detectors are:

$$D_0: \quad \frac{1}{\sqrt{8}}(|1_{F_0}\rangle - (i+1)|2_{F_0}\rangle + |3_{F_0}\rangle),$$
$$D_1: \quad \frac{1}{\sqrt{8}}(-|1_{F_0}\rangle - (i-1)|2_{F_0}\rangle + |3_{F_0}\rangle), \tag{6}$$

The falsified state does not fall in time in the sensitivity curve of the photo-detector D_1, and will not give an erroneous reading of the detector D_1 in the central time window 2 (Figure 1,2). As a result, it turns out an error-free reading in the D_0 detector. It does not matter that the number of counts in the detector D_0 and the ratio of the false state and the correct one decrease.

I would like to mention that the error ratio is influenced not only by device perfection and the appearance of unauthorized access, but also due to the loss in the channel itself, which no longer depends on the technological component of the system.

2) *If there is no coincidence of the bases of the third party and the authenticated participants.* In this case, which would not be the outcome, the probability of a chance of getting the correct result for a third party is 50%. Given that if a third party does not apply the correct basis for the analysis, it will spoil not only the result, but also the state itself.

2*a*) suppose that the third party guessed the basis of the analysis. Then the third party re-sends the modified state in the wrong state, which remains unnoticed in time in the sensitivity curve of the receiving device D_0 (formula 6). This will not result in a readout in the D_1 host device. And the ratio of errors will be in the normal range.

2*b*) suppose that the third party did not guess the basis. The same as in the first case, everything repeats, except that the action remains noticed and will be shifted in time, but does not involve the rest of D_0:

$$|0_{F_0\times}\rangle = \frac{1}{\sqrt{2}}(|1_{F_1}\rangle - i\,|2_{F_1}\rangle), \tag{7}$$

The correct state transforms the count after the sensitivity of the D_0 detector falls into the curve, but this does not happen because the modified state is shifted in time. And this leads to the fact that on D_0, produces a count and errors in D_1. All this is caused by the interference of the state, which constructively extends over the different arms of the interferometer for D_0, and is extinguished on the D_1 state, along the upper and lower arms.

And this whole process not only allows the third party to remain unnoticed in relation to the recipient (reducing the error to a valid one), but also in the end to intercept real information about the registered keys, which the recipient will not suspect.

In the real world, of course, it is difficult to carry out this threat, but it is quite provable and feasible. When it comes to analyzing the strength limit of any cryptographic system, it is taken into account that the third party will have the most advanced equipment and will have an ideal condition for implementing unauthorized interception and access to an encrypted and secure channel.

2.2. Threat to key with transfer from one mode to another.

This threat consists of stages in which a third party re-sends the state of the sender (intercepted in the quantum channel). In this case, the third party after analyzing in a random basis and increases the intensity so as to transfer the detector to the classic mode. This thin line between the modes is retained by the method of insufficient intensity, which is used so as not to lose the blinding mode [10, 12, 19], [20]).

There are moments:

1. With the coincidence of third party bases and authenticated participants. This leads to a complete constructive interference, the reason for this is to capture the detector full intensity, and that leads to the count in time.
2. If there is no coincidence of the bases of the third party and the authenticated participants. In this case, the detector is transferred to the blinding mode, the cause of which is not enough intensity in time.

The intensity with which the detector exits the blinding mode registers the signal as a linear device, and is equal to I_{th}, and the intensity with which the detector is blinded (lies in the "no click" zone) is equal to I_{bl}, (I_{bl}, <I_{th},).

The intensity of the falsified state is equal to I_{facked}. The intensity in the side time windows (see Fig. 2) does not depend on the choice of third party bases and authenticated participants and is equal to I_{facked}/8 (see Fig. 2 and formulas (3) - (7)). In this case, two situations are possible:

a) The intensity of I_{facked} is such that in the side time windows, where the intensity does not depend on constructive or destructive interference, it is equal to I_{facked},/8. At the same time, I_{facked},/8 is obviously less than the threshold intensity I_{th}, at which the detector works as linear, but more than the intensity I_{bl}, which causes the blinding effect: I_{bl}<I_{facked} = <I_{th}. There will be no counts in the side time windows (Fig. 1).

b) The intensity I_{facked} in the side time windows is equal to I_{facked}/8, less than the threshold intensity I_{th}, and the intensity I_{bl} causing the blinding effect: I_{facked}/8 <I_{bl},I_{th}. In this case, counts in side time windows (Fig. 1) will take place. The detector is not blinded and works as a single-photon counting mode.

The whole point of the threat from the third party comes down to what she is trying to guess, but at the same time minimizes the ratio of permissible and received errors as a result of the distribution process, if attempts to guess will be in vain, and she will reveal herself about her presence.

3. Conclusion

Many QKD protocols as already mentioned in this article are not protected from certain threats due to imperfections of the devices used. Such threats, which were described above, allow unauthorized access to data, and at the same time remain unnoticed. These vulnerabilities referring to imperfections of the device have been proven in many research studies.

Considering that a lot of effort is being made to counter the vulnerabilities of the received devices, with the improvement and addition of additional devices, this is not an output for quantum cryptography. Since unauthorized access can be implemented with improved devices and capabilities in an ideal environment with application against the vulnerability of imperfections, which is not acceptable for this system. Indeed, in essence, quantum cryptography, even when used in an ideal environment and with devices that provide for all the needs of the system, must remain unattainable for unauthorized access.

The security of the entire system can be achieved only by relying on the protocol component itself, and not on the technical limitations of a third party. Indeed, in our time, these restrictions remain only a temporary obstacle to unauthorized access.

References

1 Wootters, W.K., Zurek, W.H. A Single quantum cannot be cloned. *Nature*, 299 (1982): pp. 802-803.

2 Weisner, S. Conjugate Coding. *ACM SIGACT News* (New York), (1983): pp. 78-88.

3 Bennett, C.H., Brassard, G. *Quantum Cryptography: Public-Key Distribution and Tossing.* Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, (1984): pp. 175-179.

4 Bennet, C.H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters,* 68, (1992): pp. 3121-3124.

5 Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. Quantum Cryptography. *Physical Review Letters*, 74 (2002): pp. 145-190.

6 Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lutkenhaus, N., Peev, M. The security of practical quantum key distribution. *Physical Review Letters,* 6 (2009): pp. 1301.
7 Brassard, G., Lutkenhaus, N., Mor, T., Sanders, B., Limitations on practical quantum cryptography. *Physical Review Letters,* 85 (2000) pp. 1330.
8 Dieks, D. Overlap and distinguishability of quantum states. *Physical Review Letters,* 126 (1988): pp. 303.
9 Chefles, A. Quantum state discrimination. *Journal Contemporary Physics*, 6 (2010): pp. 401-424.
10 Lydersen, L. Wiechers, C. Wittmann, C. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics,* 4 (2010): pp. 686.
11 Kolokov, A., Katamadze, G., Kulik, C. On the passive probing of fiber optic quantum communication channels. *Journal of Experimental and Theoretical Physics,* 137 (2010): pp. 637.
12 Makarov, V., Anisimov, A., Sauge, S. Controlling an actively quenched single photon detector with bright light, September 19, 2008. URL: arXiv:quant-ph/0809.3408.
13 Scarani, V., Acin, A., Ribordy, G., Gisin, N., Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters,* 057901-1 (2004): pp. 92.
14 Bruss, D. Optimal eavesdropping in quantum cryptography with six states, May 7, 1998. URL: arXiv:quant-ph/9805019.
15 Inoue, K., Waks, E., Yamamoto, Y. Differential Phase shift quantum key distribution. *Physical Review Letters,* 037902 (2002): pp. 89.
16 Gisin, N., Ribordy, G., Zbindeu, H., Stucki, D., Brunner, N., Scarani, V. Towards practical and fast Quantum Cryptography, November 3, 2004. URL: arXiv:quant-ph/0411022.
17 Ekert, A. Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 6 (1991): pp. 661-663.
18 Won-Young, H., Observation of a Broad structure. *Physical Review Letters,* 057901-1 (2003): pp. 95.
19 Lydersen, L., Wiehers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V., Thermal blinding of gated detectors in quantum cryptography, September 14, 2010. URL: arXiv:quant-ph/1009.2663.
20 Yuan, Z.L., Dynes, J.F., Shields, A.J. Avoiding the blinding attack in QKD. *Nature Photonics,* 4 (2010): pp. 800-801.