Digitalization of the agro-industrial complex: analysis of existing vulnerabilities in quantum cryptography systems

Larisa Cherkesova[1], *Denis* Korochencev[1,*], *Elena* Revyakina[1], *Nikolay* Boldyrihin[1], and *Evgeniya* Roshchina[1]

[1]Don State Technical University, 1, Gagarin sq., 344003, Rostov-on-Don, Russia

Abstract. This article deals with vulnerabilities of quantum cryptography systems and quantum key distribution. Solutions that exclude the possibility of quantum attacks on existing quantum key distribution systems are proposed.

1 Introduction

The quantum cryptography systems have long been considered invulnerable, since they do not use traditional mathematical methods to ensure the information secrecy, but emphasize the information transmission using quantum mechanics objects. In fact, quantum communication lines can protect, for example, from attacks such as "man-in-the-middle attack" [1].

However, despite the relative security of the quantum communication line itself, the direction of a successful attack by cybercriminals may turn out to be information transferring software, as well as other vulnerabilities of specific software and hardware implementations of quantum key distribution systems [2].

As in classical key distribution systems, it is advisable to use symmetric ciphers, such as AES–128–GCM or CHACHA20 – POLY1305, to transmit information [3-5].

In case of domestic using symmetric ciphers in quantum technologies, the possibility of Russian encryption algorithms such as Kuznechik (GOST 34.12–2015) or Magma (GOST 28147–89) is not excluded, which does not contradict, but contributes to development of domestic state policy of import substitution.

What is the reason for using symmetric ciphers in quantum encryption? The reason for this is the rather low data encryption speed when using asymmetric encryption systems, or the low speed of the quantum key distribution system.

Suppose that an attacker connects to a quantum communication line (see Fig. 1) at the time the photo is transmitted, and tries to measure its state. A particle instantly changes its state in a random way - this is a consequence of the observer effect. The sender and the recipient learn about the attempt to compromise (unauthorized access) and begin the transfer again [6].

*Corresponding author: mytelefon@mail.ru

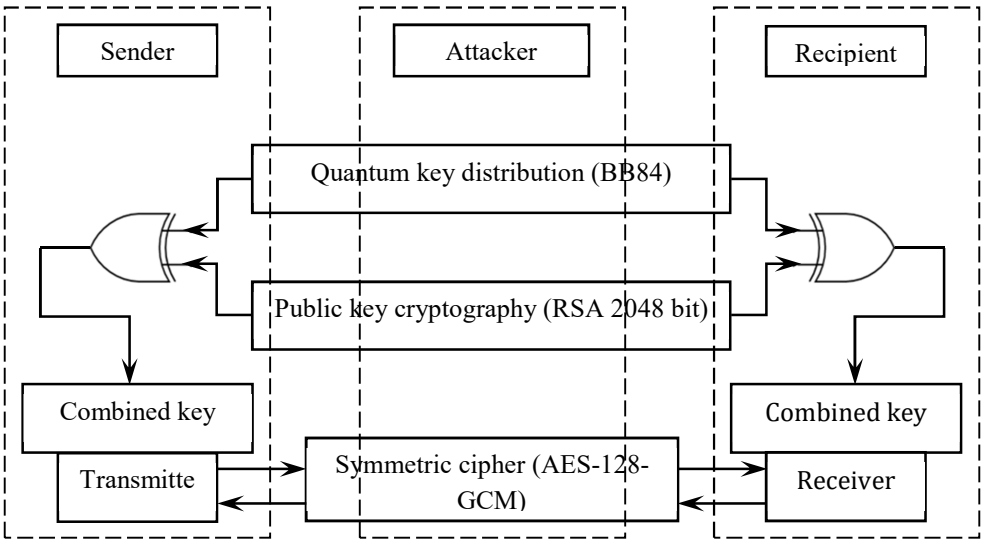

Fig. 1. Data transmission scheme using a quantum key distribution system.

This figure represents how a quantum communication system works under ideal conditions. But in practice, there are no technically perfect systems, so the information transmitted through a quantum channel can be vulnerable to a number of attacks [7].

2 Coherent and incoherent attacks

Coherence is a coordinated time course of several oscillatory and / or wave processes, which manifests itself when they are added. Oscillations are coherent if the phase difference remains constant in time, and when the oscillations are added, it determines the amplitude of the total oscillation [8 – 11].

The simplest attack may be a coherent attack based on the interception and re-sending of photons. An attacker reads data in a random basis and sends it further over the communication line. If the basis is guessed, then the attacker successfully intercepts a bit of information (see table. 1). The quantum protocol BB84 [2] is immune to this type of attack with a sufficiently large key size, since the probability of a successful attack is

$$P = \frac{1}{2^n} \tag{1}$$

where *n*- the number of bits of the key.

If the sender and receiver publicly compare some bits (these bits are no longer a secret, and cannot be used in the key), then when comparing n bits, the probability of detecting an attacker is

$$P = 1 - \left(\frac{3}{4}\right)^n. \tag{2}$$

When sending 384 bits of information, of which only 128 random bits are the key, the probability of an attacker being detected is infinitely close to one.

Table 1. The example of an attempt to use an intercept and re-send attack.

Random Sender Bit	**0**	**1**	**0**	**0**
Random sender basis	+	×	×	×
Sender Photon Polarization	↑	↘ □	↗ □	↗ □
The attacker random basis	+	+	+	×
Intruder Photon Polarization	↑	→	→	↗ □
Random recipient basis	+	×	×	×
Recipient Photon Polarization	↑	↗ □	↗ □	↗ □
Key Error	no	yes	no	no
Key leak	yes	no	no	yes

An attacker can confuse a sample of any dimension with a whole group of transmitted single photons in any (unitary) way. The ultimate variant of this attack is occurred when an attacker can confuse his sample with the entire sequence of photons transmitted by the sender [12].

Further, the attacker stores his large sample until all open communications between the subscribers of the quantum communication line have ended, and then he makes the most general sample measurement of his choice [13].

A subclass of coherent attacks is collective attacks, in which each photon from the transmitter is individually confused with a separate quantum breakdown, as in incoherent attacks. However, the measurement will not be carried out individually for each sample, but on all samples immediately and simultaneously, considered as a single large quantum system [12].

In incoherent attacks, the attacker processes each photon received from the re-sensor separately. The simplest option is the above attack of interception - sending a photon. Since during this attack photons are not passed further along the communication line, but new photons are sent, this strategy is called opaque. Incoherent is also the attack of entangling quantum samples with photons sent through the channel. In this case, each photon is confused with a separate breakdown independently of the others, and the interacting photon is sent to the receiver. Now, an attacker can store samples in quantum memory, and measure their state separately after an open exchange of messages ends. Eavesdropping to open messages allows one to find out the basis of the sender, and thereby choose the optimal measuring procedures to get more information about the key. This attack is translucent, since the states of the photons with which the attacker confuses his samples change. The level of errors introduced by an attacker can be decreased by reducing the amount of key information received by him [14].

3 Detector Attacks

Consider the blinding attack of a single-photon detector of a receiver, developed by the research group of V. Makarov at the Norwegian University of Natural and Technical Sciences [14]. An attacker reads the information sent by the transmitter and sends it further through the communication channel, but uses a very powerful pulse (see Fig. 2). An imperfect detector perceives that impulse as a normal signal, as a result of which the observer effect is lost. In this case, the attacker goes unnoticed, and gets the opportunity to read all the information transmitted through the quantum communication channel.

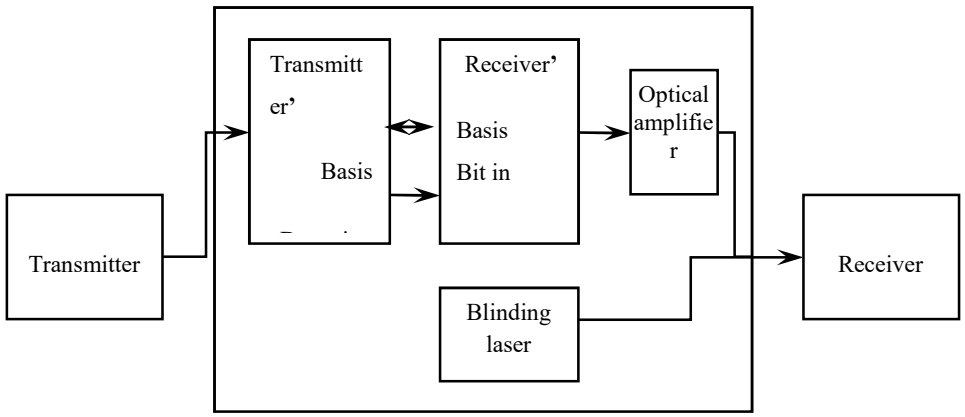

Fig. 2. Blind Detector Attack Scheme.

One can protect himself from this vulnerability by installing a single photon source in front of the detectors, which is triggered at random times. This will make sure that the detector does not read light signals like a normal detector, but operates in a quantum mode [15, 16].

Another example of a successful attack is the photon separation attack. In the BB84 protocol, laser pulses are used to send a quantum state [17, 18]. In most implementations, for each pulse, a very small number of photons is transmitted (mainly from 0 to 2). They are distributed over the momenta in accordance with the Poisson distribution. Zero photons are transmitted per pulse, sometimes it is one, less often two or more (see Fig. 3). In the event that more than one photon is transmitted in one pulse, the attacker can separate them, and the assigned photon will be confused with the sample [19]. In this case, the remaining unchanged part of the information is sent to the recipient, and the interceptor receives the exact value of the transmitted bit without introducing errors into the sifted key. This allows an attacker to remain undetected and secretive while reading information [20].

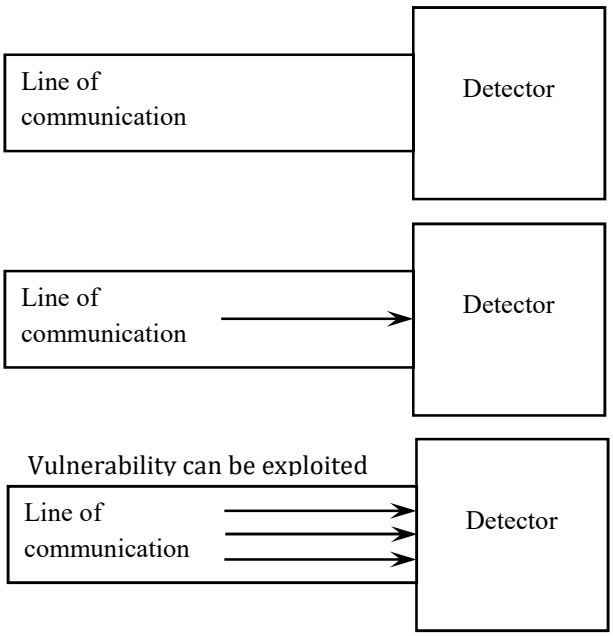

Fig. 3. Photon Separation Attack Conditions.

There are several solutions to this problem. The best solution would be to use ideal photon sources. They are under active development and are already successfully used [21]. Another solution is to modify the BB84 protocol. For example, in the SARG04 protocol, the sender does not announce the basis of its bit [22]. As a result, the attacker will need to store much more copies of the measurements in order to determine the photons state.

In practice, weak coherent pulses emitted by laser LEDs are still used - multiphoton sources. Since most of the pulses carry only one photon, the attacker must pass them in order to go unnoticed. With a small number of pulses with more than one photon, the amount of information intercepted is very small. Most likely, the interceptor will be forced to turn to another strategy, for example, to block pulses with only one photon. This strategy can allow an attacker to go unnoticed by recovering all the key information [23].

4 Quantum channel replacement

Consider also the possibility of an attacker to replace a lossy quantum channel used by subscribers by a lossless channel. Of course, this replacement should go unnoticed. In this case, the attacker gets the opportunity to block most of the pulses (provided that the source channel had a large percentage of losses) so that the receiver receives approximately the expected number of pulses. Thus, an attacker can obtain all information about the key by successfully reading all the transmitted data without introducing any errors. It follows that in practice only quantum channels with a high transmission coefficient should be used in order to avoid the successful application of this attack.

At the Max Planck Institute, the Trojan Horse quantum attack was developed. It consists in sending a sufficiently bright ray of light to the recipient and analysis of the returned ray [24]. Being aimed at the SARG04 protocol, this attack restores the key by reading the

random basis of the recipient with a probability of over 90%. The SARG04 protocol is more resistant to the photon separation attack than BB84 [25], but is vulnerable to the Trojan Horse attack and requires the installation of a monitor-detector, which randomly redirects some of the incoming signals to the receiver's detector. Also, an effective solution may be the constant monitoring of the receiver's avalanche LEDs in real time.

5 Conclusion

In reality, there are no technically perfect systems. This also applies to quantum communication systems. Therefore, the information transmitted through a quantum channel can undoubtedly be vulnerable to a number of quantum attacks: coherent and incoherent, attacks on the detector, attacks on the separation of photons, etc. At present, about 20 attacks on quantum communication lines are known [26].

Thus, we can conclude that the latest developments and innovations in the field of quantum cryptography, despite their apparent perfection, impeccability and invulnerability, have a lot of vulnerabilities, holes and gaps in their structure, and can not guarantee 100% protection at all transmitted information from attacks by attackers of various categories.

Considering the fact that quantum technologies today have not yet received wide distribution, it can be argued that quantum cryptography in the future will not be able to provide absolute information security. With the development of quantum communication channels, undoubtedly, new types of quantum attacks will be developed that can be carried out by sufficiently skilled hackers who have at their disposal the appropriate software and hardware.

At the same time, at this stage, quantum cryptography is still the most reliable encryption method. Its development is the most promising, high-tech and unique direction of cyber security.

References

1. N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs, New Journal of Physics **16(12)**, 123030 (2014)
2. C.H. Bennett, G. Brassard, *Proc. IEEE Intern. Confer. Computers, Systems and Signal Processing*, 175-179 (2014) doi.org/10.1016/j.tcs.2014.05.025
3. A. Pljonkin, K. Rumjantsev, *Proc. 15th International Conference on Electronics, Information, and Communication*, 7562955 (2016) doi: 10.1109/elinfocom.2016
4. T. Ferreira da Silva, G.B. Xavier, G.P. Temporão, J. Pierre von der Weid, Optics express **20(17)**, 18911-18924 (2012)
5. K. Rumyantsev, H.H. Shakir, *Proc. IEEE East –West Design & Test Symposium*, 171–175 (2019)
6. V. Kurochkin, Y. Kurochkin, Photonics **5**, 54–66 (2012)
7. V. Hahanov, W. Gharibi, S. Chumachenko, International Journal of Design, Analysis & Tools for Integrated Circuits & Systems **6**, 23 (2017)
8. W. Gharibi, D. Devadze, V. Hahanov, *Proc. IEEE East –West Design & Test Symposium*, 48 – 52 (2019)
9. V. Hahanov, A.V. Hacimahmud, E. Litvinova, *Proc. IEEE East –West Design & Test Symposium*, 1-7 (2018)
10. V. Hahanov, E. Litvinova, S. Chumachenko, *Proc. of 5th Prague Embedded Systems Workshop*, 45-51 (2017)

11. V. Hahanov, W. Gharibi, M. Liubarskyi, *Proc. of Int' Conf. Modeling, Sim. and Vis. Methods in The 2018 World Congress in Computer Science, Computer Engineering & Applied Computing*, 10-16 (2018)
12. V. Hahanov, S. Chumachenko, I. Hahanov, *Proc. of IEEE East-West Design and Test Symposium*, 445–450 (2017)
13. V. Hahanov, W. Gharibi, S. Chumachenko, International Journal of Design, Analysis & Tools for Integrated Circuits & Systems **6**, 23–27 (2017)
14. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nature Photonics **4(10)**, 686-689 (2010) doi:10.1038/nphoton.2010.214
15. K. Rumiantsev, E. Rudinsky, *Proc. of the 10th International Conference on Security of Information and Networks*, 140 – 150 (2017) doi 10.1145/3136825.3136888.
16. K. Rumyantsev, E. Rudinsky, Proceedings of the 2nd International Conference on Multimedia and Image Processing, 346–349 (2017) doi: 10.1109/ICMIP.2017.68
17. K. Rumyantsev, E. Rudinsky, Izvestiya SFU. Technical science **5**, 75–89 (2017)
18. A. Pljonkin, K. Rumjantsev, *Proc. of the International Conference on Computational Techniques in Information and Communication Technology*, 531 – 534 (2016)
19. K. Rumyantsev, A. Plyonkin, Radio and communications technology **2**, 125 – 134 (2015)
20. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, 0978051-1976667 (Cambridge University Press, 2010)
21. K. Rumyantsev, Telecommunications **2**, 32 – 40 (2017)
22. K. Rumyantsev, Telecommunications **3**, 36–44 (2017)
23. K. Rumyantsev, A. Plyonkin, Engineering sciences **8(169)**, 6 – 19 (2015)
24. I. Gerhardt, Q. Liu, A. Lamas–Linares, C. Kurtsiefer, J. Skaar, Nature Communication **2(1)**, 349 (2011)
25. A. Pljonkin, K. Rumjantsev, *Proc. of the IEEE Photonics Society Workshop on Recent Advances in Photonics*, 7805988 (2015)
26. R.J. Lipton, K.W. Regan, Quantum Algorithms via Linear Algebra, MIT Press eBook **47(3)**, 2993749-2993752 (2014)