Classification of the Methods of Eavesdropping and Data Corruption in Quantum Cryptosystems

Igor Limar [0000-0002-8972-9935]
Engineering and Technology Institute "Bioengineering"
Odesa, Ukraine
quantum.biology@outlook.com

Yevhen Vasiliu[1][0000-0002-8582-285X], Vladyslav Kumysh[2]
[1]Educational and Scientific Institute of Radio, Television and Information Security
[2]Research and development department
O.S. Popov Odesa National Academy of Telecommunications
Odesa, Ukraine
ye.vasiliu@gmail.com, vlad.kumysh@onat.edu.ua

***Abstract*—The new extended classification of the attacks on quantum protocols and quantum cryptosystems is proposed. The classification takes into account the newest data concerning the attacks on the equipment for quantum key distribution which use the loopholes of the devices. These attacks have been named "quantum hacking". Such classification may be useful for choosing of commercially available quantum key distribution system.**

***Keywords*— quantum cryptography; quantum key distribution; quantum hacking; loophole of the device; attack classification**

I. Introduction

Only a few papers where classification of the attacks on quantum protocols and cryptosystems is described have been published for now [1-4]. The newest attacks which use the loopholes of the devices – so-called quantum hacking have arisen after the papers [1, 3, 4] were published. At the same time the several attacks described in [3, 4] were not taken into account in [2]. Therefore, the purpose of this work is to develop the extended classification of all known attacks on the protocols and the systems of quantum cryptography.

II. Developing the Classification

The non-coherent attacks, the attacks conditioned by protocols imperfection, the coherent attacks in [3] have been referred to as the "traditional" attacks. Wherein the non-coherent attacks include intercept–resend attack (IRA) and semi-transparent attacks (STA). The man-in-the-middle attack (MMA) and the denial of service attacks (DSA) have been referred to as the attacks which use imperfection of protocols. In this paper we propose to refer the attacks on specific protocols (ASP) to also as the attacks which use imperfection of protocols. The collective attacks (CA) and the joint attacks (JA) have been referred to as the coherent attacks.

When eavesdropper realizes the intercept-resend attack, he measures the quantum state of the photon which Alice sends toward Bob. Then Eve sends the other photon to Bob. The quantum state of this photon is determined by the result of the Eve's quantum measurement. When the semi-transparent attack is executed Eve uses the ancillas. The quantum entanglement arises between the single ancilla and each photon sent by Alice. Eve keeps all ancillas while photons arrive to Bob. When the open information exchange is over and the basis which Bob uses is announced Eve performs quantum measurement of the ancillas with using of this basis. The error rate which arises when semi-transparent attack is executed is lower than the error rate after intercept–resend attack execution. When collective attack is executed the quantum entanglement arises between the single ancilla and each photon sent by Alice as well, as when the semi-transparent attack is executed. When open information exchange is over, Eve performs so-called generalized quantum measurement of all ancillas simultaneously as it would be if this set of the ancillas would be the single quantum system. When eavesdropper executes the joint attack he uses only one ancilla. The quantum entanglement arises between the all photons sent by Alice and this single ancilla. To execute the man-in-the-middle attack the eavesdropper replaces all photons which Alice sends by his own and then sends these photons to Bob. Eve collects Alice's photons and in that way eavesdropper reads the private information. The denial of service attack does not let the eavesdropper to know private information. Only the violation of the information transfer from one honest user to other one is result of such attack. For example, Eve can perform the quantum measurement of the states of sent from Alice to Bob photons. After such measurement the photons are not useful for honest users.

We have referred to as the quantum hacking following attacks:

1) faked-state attack;
2) laser damage attack;
3) detection efficiency mismatch loophole;
4) time-shift attack;
5) calibration loophole;
6) wavelength-dependent attack;
7) Trojan-horse attacks;
8) beam-splitting attack and photon-number splitting attack;

9) replacing the original quantum channel by the channel with less losses.

The most well-known attacks asigned to quantum hacking are the Trojan horse attack and the faked states attack. To execute the Trojan horse attack [5, 6] the eavesdropper enters intensive pulse of light into optic fiber between honest users Alice and Bob. The photons in this pulse are called Trojan photons. The pulse of light is directed to the Alice's plant. Alice encodes her photons to transfer information to Bob. At the same time Alice encodes Eve's photons as well. Alice does not suspect that Eve is executing the attack. After Alice encodes all photons the Trojan photons are reflected from elements of Alice's plant and are directed through the optical fiber towards Bob. Eve intercepts her Trojan photons which have been arrived from Alice's plant. Since Eve knows initial states of her photons she can determine the information encoded by Alice. The faked state attack on quantum key distribution system has been described as sort of the man-in-the-middle attack in [7]. When faked states attack is executed Eve generates the pulses of the light (faked states) which are registered by honest users. At that the error rate which could tell to Alice and Bob about danger is not increased by Eve. The man-in-the-middle attack cannot be successful if Eve tries to send to Bob the photons with the same quantum states as she has detected when she has intercepted Alice's message. However, Eve can try to mislead the honest users by applying certain methods which use devices loopholes. It is necessary for Eve that honest users consider that they register initial quantum states while in fact they register the pulses of light which have been generated by Eve. In all attacks of the blinding [8], which have been developed later, the Eve's attack is successful when she forces Bob to perform quantum measurement not with basis which has been chosen randomly but with basis which has been chosen and dictated by Eve. Eve connects to the section of the optic fiber by which the apparatuses of Alice and Bob are connected. Then Eve writes and keeps her measurement basis for each quantum state which she registers. Whereupon, she provides the choosing of measurement basis by Bob for each quantum state which has been registered and sends the faked state for each of these quantum states to Bob. Bob always registers the state with such measurement basis that has been programmed by Eve. It is necessary to make the following note. On our scheme we have placed the man-in-the-middle attack in the class of the attacks which use imperfection of protocols. However, the faked state attack on quantum key distribution system also is sort of the man-in-the-middle attack. Therefore, on the scheme has been drawn the link between the man-in-the-middle attack block and the block of the faked state attack.

The next kind of attack considered in [2, 9] uses the loophole of detection efficiency mismatch (DEM). The essence of DEM loophole is as follows. In the ideal case the result of the quantum measurement in the quantum key distribution system must be determined by only relative choice of the measurement basis. This demand dictates that detectors D1 and D2, which determine the measurement basis, must be indistinguishable. However, in the real technical devices it cannot be guaranteed completely. For example, the lengths of optical fibers, which connect the detectors D1 and D2 are changing during exploitation of the system because of numerous physical influences. Thereby, in fact the moments of the time in which photons arrive to the detectors D1 and D2 are not exactly the same, though in the ideal case these moments must be coincident. By using such circumstance, the eavesdropper can control the choice of the measurement basis in the honest user's plant. In papers only two kind of attacks which use loophole of DEM have been described for now. Initially the execution of the faked states attack has been proposed. The ideal case when the sensitivity of the first of the two detectors is shifted in time relative to the sensitivity of the second detector significantly has been considered in [10]. At that, the intervals of the time when the first of the two detectors is completely blind and the other detector keep sensitivity and vice versa, are exist. The eavesdropper performs the quantum measurement of photons states which have been sent by honest user Alisa. The eavesdropper chooses measurement basis randomly. Then the eavesdropper sets his bit value for faked state and sends this faked state to honest user Bob. The pulses of the faked states are shifted in time. Moreover, the eavesdropper sets the relative phases of the pulses in such a way as that if Bob chooses the basis incompatible with Eve's basis then the whole of the pulse gets to the detector which is blinded and in the case when the measurement basis chosen by Bob is compatible with Eve's basis the pulse gets to the detector which in this moment has sensitivity. Second of two kind of attacks which use loophole of DEM has been proposed in [9]. The eavesdropper connects the special apparatus to the optic fiber between honest users Alisa and Bob. With the help of such device the eavesdropper can regulate the time of arriving of the photons to the Bob's plant. Eve forces photons to arrive either earlier or later of the interval of the time when both detectors have sensitivity. In the moment of the arriving of each photon only one detector has sensitivity. Thereby the eavesdropper influences on the results of the measurements. The results of the measurements in this case do not depend from basics which have been chosen by Bob. For prevention of the detection efficiency mismatch in the systems of quantum key distribution the equipment and software for providing the procedure of the calibration are used. For the execution of the calibration Alisa directs to the Bob's plant the group of classical (not quantum) pulses of light. Bob measures the time of the arriving of these pulses of light and tunes both detectors in such a way as to they will be indistinguishable. However, the cases when the effective attack which does not let to perform the calibration successfully has been executed, have been described in [11]. If the eavesdropper uses the faked states he can influence on results which Bob registers.

The developed extended classification of the methods of the eavesdropping and data corruption in the systems of quantum cryptography (i.e. active and passive attacks) is designated in Fig. 1.

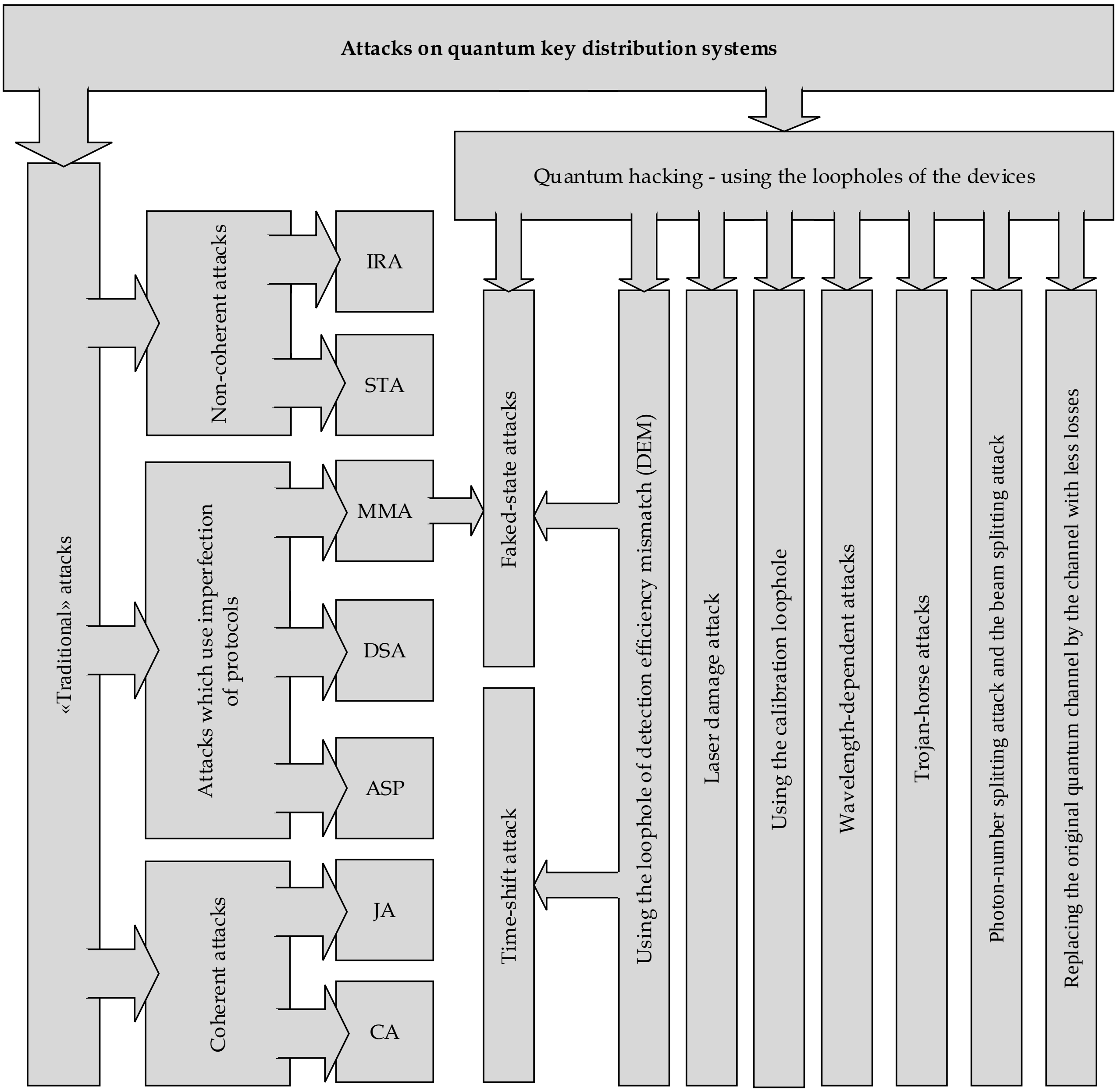
Attacks on quantum key distribution systems
«Traditional» attacks
Non-coherent attacks
IRA
STA
Attacks which use imperfection of protocols
MMA
DSA
ASP
Coherent attacks
JA
CA
Quantum hacking - using the loopholes of the devices
Faked-state attacks
Time-shift attack
Using the loophole of detection efficiency mismatch (DEM)
Laser damage attack
Using the calibration loophole
Wavelength-dependent attacks
Trojan-horse attacks
Photon-number splitting attack and the beam splitting attack
Replacing the original quantum channel by the channel with less losses

Fig. 1. The extended classification of the methods of the eavesdropping and data corruption in the systems of quantum cryptography

The so-called laser damage attack also belongs to quantum hacking [2]. The eavesdropper can direct to the honest user's plant the pulses of large power. The pulses damages avalanche photodiode of the detector and eavesdropper can use that as loophole. For example, after such damage the level of the dark noise is decreased. Initially when the honest user determines the error rate he considers the level of the dark noise. The eavesdropper can realize an attack which increases the error rate, but the full error rate will be such as before the damage of the detector. Therefore, the honest user will not observe the attack because he will consider that the part of the error rate is conditioned by the dark noise. As a matter of fact, after the damaging of the detector the dark noise does not make a contribution to the error rate. The eavesdropper can use not only the detector's loopholes but loopholes of the others elements of the plant of the honest user. For example, he can use the loophole of the beam splitter [2, 12, 13]. When the wave length which has been set by producer of the plant is used, the probability that photon will be reflected is equal to probability that photon will be let to pass. However, if the others lengths of the waves will be used, these probabilities will not be equal. Therefore, the eavesdropper can replace pulses of honest users and send his pulses with such length of the wave that let to manage the probability of the photon's passing through the beam splitter.

In addition to the attacks which have been considered in [2] it is expediently to include to the quantum hacking the two other kinds of attack called photon-number splitting attack and the beam splitting attack. The principle of executing of the attack of first kind is as follows. Because preparation of the single-photon pulses is hardly possible task, in practice, when implementing quantum cryptography protocols the weak laser pulses are used. These pulses may be well presented by coherent states with mean number of photons less than one. However, in so doing, some pulses include more than one photon. Thus, eavesdropper can split the signal and receive certain information without essential increase of the error rate in the channel [14, 15]. Such method can be executed especially effectively when quantum nondemolition (QND) measurement is applied [16]. The another kind of attacks is such that based on replacing the original quantum channel by the channel with less losses [17]. The basis method of the control of the eavesdropping which used in quantum cryptography, is the check of the error rate in the communication channel. However, the eavesdropper can to replace the original channel with certain error rate which has been organized by users by the channel with less loses. The honest users agree that error rate is such that has been pointed above. Thus, if eavesdropper has applied such method, the honest users cannot distinguish the errors which are determined by attack from errors which are determined by natural noise. That is, the honest users consider that the actual error rate is determined by only natural noise, while in fact it includes component of natural noise and component which is determined by eavesdropper attack. Thus, highest error rate which honest users have determined is much higher that actual error rate which is determined by natural noise. In this situation the eavesdropper can to increase error rate in channel without uncovering his attack. At the same time for eavesdropper it is necessary the permanent maintaining of the error rate in channel at the level which is not lower that level of error rate which has been initially determined by honest users. Eavesdropper needs this action even if during certain period he does not wiretaps the channel. If he will not apply this method the honest users will observe the anomalous low level of error rate and in that way they will uncover the attack.

III. Conclusion

The new extended classification of the attacks on quantum protocols and quantum cryptosystems have been developed. This classification includes all known kinds of the attacks including quantum hacking. Such classification may be used for choosing the commercially available quantum key distribution system.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, “The security of practical quantum key distribution,” Reviews of Modern Physics, vol. 81, issue 3, 1301, 2009.

[2] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt and G. Leuchs, “Attacks on practical quantum key distribution systems (and how to prevent them),” Contemporary Physics, vol. 57, issue 3, pp. 366–387, 2016.

[3] O.G. Korchenko, S.O. Gnatyuk, Y.V. Vasiliu and V.M. Kinzeryavyy, “Attacks in the Quantum Systems of Information Protection,” Bulletin of Engineering Academy of Ukraine, vol. 2, pp. 109-115, 2010. (on Ukrainian)

[4] O.G. Korchenko, S.O. Gnatyuk and Y.V. Vasiliu, “Modern quantum technologies of information security against cyber – terrorist attacks,” Aviation: Research Journal of Vilnius Gediminas Technical University, vol. 14, issue 2, pp. 58-69, 2010.

[5] M. Lucamarini, I. Choi, M.B. Ward, J.F. Dynes, Z.L. Yuan, and A.J. Shields, “Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution,” Physical Review X, vol. 5, issue 3, 031030, 2015.

[6] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems,” IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, issue 3, p. 168, 2015.

[7] V. Makarov and D.R. Hjelme, “Faked states attack on quantum cryptosystems,” Journal of Modern Optics, vol. 52, issue 5, pp. 691-705, 2005.

[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nature Photonics, vol. 4, issue 10, pp. 686-689, 2010.

[9] Y. Zhao, C.H.F. Fung, B. Qi, C. Chen, and H.K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” Physical Review A, vol. 78, issue 4, 042333, 2008.

[10] V. Makarov, A. Anisimov, and J. Skaar, “Effects of detector efficiency mismatch on security of quantum cryptosystems,” Physical Review A, vol. 77, issue 2, 022313, 2006.

[11] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, “Device Calibration Impacts Security of Quantum Key Distribution,” Physical Review Letters, vol. 107, issue 11, 110501, 2011.

[12] H.W. Li, S. Wang, J.Z. Huang, W. Chen, Z.Q. Yin, F.Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.C. Guo, W.S. Bao, and Z.F. Han, “Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength source,” Physical Review A, vol. 84, issue 6, 062308, 2011.

[13] J.Z. Huang, C. Weedbrook, Z.Q. Yin, S. Wang, H.W. Li, W. Chen, G.C. Guo, and Z.F. Han, “Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack,” Physical Review A, vol. 87, issue 6, 062329, 2013.

[14] M. Dusek, O. Haderka, M. Hendrych, “Generalized beam-splitting attack in quantum cryptography with dim coherent states,” Optics Communications, vol. 169, issue 1-6, pp. 103-108, 1999.

[15] G. Brassard, N. Lütkenhaus, T. Mor and B.C. Sanders, “Limitations on Practical Quantum Cryptography,” Physical Review Letters, vol. 85, issue 6, 1330, 2000.

[16] A. S. Holevo, “On the principle of quantum nondemolition measurements,” Theoretical and Mathematical Physics, vol. 65, issue 3, pp. 415-422, 1985.

[17] A. Wójcik, “Eavesdropping on the “Ping-Pong” Quantum Communication Protocol,” Physical Review Letters, vol. 90, issue 15, 157901, 2003.