Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 56 – 60 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

REVIEW OF MODERN QUANTUM KEY DISTRIBUTION PROTOCOLS

Sergiy Gnatyuk[1], Tetiana Okhrimenko[1], Sergiy Dorozhynskyy[1], Andriy Fesenko[2]
[1]National Aviation University, Kyiv, Ukraine
[2]Taras Shevchenko Kyiv National University, Kyiv, Ukraine

ABSTRACT: Modern quantum technologies of information security consist of following direction: quantum key distribution, quantum secure direct communication, quantum steganography, quantum secret sharing, quantum stream cipher quantum digital signature etc. In practice quantum key distribution is the most real technology for existed ICT and infrastructures. From this viewpoint, in the paper up-to-date quantum key distribution protocols were carried out as well as analysis of their strengths and weaknesses, prospects and difficulties of implementation in ICT was fulfilled. Also the modern commercial quantum key distribution systems were analyzed in accordance to used protocols of key distribution and encryption.

KEYWORDS: Quantum Cryptography, Quantum Key Distribution, Protocol, Data Confidentiality, Encryption, Commercial Systems, Information Communication Technologies.

I. Introduction

One of the most effective ways to ensure data confidentiality and integrity in information communication technologies (ICT) and systems is cryptographic methods and systems. The purpose of them is to provide key distribution, authentication, legitimate users authorisation, and encryption. Key distribution is one of the most important problems of cryptography. This problem can be solved with the help of quantum key distribution (QKD), that provides information-theoretic security and it can also be used as a scheme for increase in key length [1].

In recent years, QKD has attracted considerable interest [2]. The overwhelming majority of theoretic and practical research projects in quantum cryptography are related to the development of QKD protocols. The number of different quantum technologies is increasing, but there is no comprehensive information about classification of these technologies in scientific literature (there are only a few works concerning different classifications of QKD protocols. This makes it difficult to estimate the level of the latest achievements and does not allow using quantum technologies with full efficiency. The main purpose of this paper is the review of up-to-date QKD protocols, analysis of their strengths and weaknesses, prospects and difficulties of implementation in ICT.

II. QKD Protocols Review

Up-to-date QKD includes the following protocols [3-5]:

- using single (non-entangled) qubits (two-level quantum systems) and qudits (d-level quantum systems, $d>2$);
- using phase coding;
- using entangled states;
- decoy states protocols and others.

Let's analyse various QKD protocols based on different quantum technologies:

1) BB84 Protocol. The main task of QKD protocols is encryption key generation and distribution between two users connecting via quantum and classical channels. In 1984 Ch. Bennett from IBM and G. Brassard from Montreal University introduced the first QKD protocol, which has become an alternative solution for the problem of key distribution. This protocol is called BB84 and it refers to QKD protocols using single qubits. The states of these qubits are the polarisation states of

single photons. The BB84 protocol uses four polarisation states of photons (0°, 45°, 90°, 135°). These states refer to two mutually unbiased bases. Error searching and correcting is performed using classical public channel, which need not be confidential but only authenticated. For the detection of intruder actions in the BB84 protocol, an error control procedure is used, and for providing unconditionally security a privacy amplification procedure is used. The efficiency of the BB84 protocol equals 50%. Efficiency means the ratio of the photons number which is used for key generation to the general number of transmitted photons.

2) Six-State Protocol requires the usage of four states, which are the same as in the BB84 protocol, and two additional directions of polarization: right circular and left circular. Such changes decrease the amount of information, which can be intercepted. But on the other hand, the efficiency of the protocol decreases to 33%.

3) 4+2 Protocol is intermediate between the BB84 and B92 protocol. There are four different states used in this protocol for encryption: "0" and "1" in two bases. States in each base are selected non-orthogonal. Moreover, states in different bases must also be pairwise non-orthogonal. This protocol has a higher information security level than the BB84 protocol, when weak coherent pulses, but not a single photon source, are used by sender. But the efficiency of the 4+2 protocol is lower than efficiency of BB84 protocol.

4) Goldenberg-Vaidman Protocol. In this protocol, encryption of "0" and "1" is performed using two orthogonal states. Each of these two states is the superposition of two localised normalised wave packets. For protection against intercept-resend attack, packets are sent at random times.

5) Koashi-Imoto Protocol. A modified type of Goldenberg-Vaidman protocol is called the Koashi-Imoto protocol. This protocol does not use a random time for sending packets, but it uses an interferometer's non-symmetrisation (the light is broken in equal proportions between both long and short interferometer arms).

6) B92 Protocol. Another type of QKD protocol is a protocol using phase coding: for example, the B92 protocol using strong reference pulses. An eavesdropper can obtain more information about the encryption key in the B92 protocol than in the BB84 protocol for the given error level, however. Thus, the security of the B92 protocol is lower than the security of the BB84 protocol. The efficiency of the B92 protocol is 25%.

7) Ekert Protocol (E91) refers to QKD protocols using entangled states. Entangled pairs of qubits that are in a singlet state $\left|\psi^-\right\rangle = 1/\sqrt{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$ are used in this protocol. Qubit interception between Alice to Bob does not give Eve any information because no coded information is there. Information appears only after legitimate users make measurements and communicate via classical public authenticated channel. But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol. Kaszlikowski et al. carried out the generalisation of the Ekert scheme for three-level quantum systems and Durt et al. carried out the generalisation for *d*-level quantum systems: this increases the information capacity of the protocol a lot. Thus, from all contemporary QKD protocols using qudits, the most effective and secure against non-coherent attack is the protocol using single qudits and two bases (BB84 for qubits).

The aforementioned protocols with qubits are vulnerable to photon number splitting attack. This attack cannot be applied when the photon source emits exactly one photon. But there are still no such photon sources. Therefore, sources with Poisson distribution of photon number are used in practice. The part of pulses of this source has more than one photon. That is why Eve can intercept one photon from pulse (which contains two or more photons) and store it in quantum memory until Alice transfers Bob the sequence of bases used. Then Eve can measure stored states in correct basis and get the cryptographic key while remaining invisible. It should be noted that there are more advanced strategies of photon number splitting attack which allow Bob to get the correct statistics of the photon number in pulses if Bob is controlling these statistics.

In practice for realisation of BB84 and six-state protocols weak coherent pulses with average photon number about 0.1 are used. This allows avoiding small probability of two- and multi-photon pulses, but this also considerably reduces the key rate.

8) SARG04 protocol does not differ much from the original BB84 protocol. The main difference does not refer to the "quantum" part of the protocol; it refers to the "classical" procedure of key sifting, which goes after quantum transfer. Such improvement allows increasing security against photon number splitting attack. The SARG04 protocol in practice has a higher key rate than the BB84 protocol.

9) Decoy states protocol. Another way of protecting against photon number splitting attack is the use of decoy states QKD protocols, which are also advanced types of BB84 protocol. In such protocols, besides information signals Alice's source also emits additional pulses (decoys) in which the average photon number differs from the average photon number in the information signal. Eve's attack will modify the statistical characteristics of the decoy states and/or signal state and will be detected. As practical experiments have shown for these protocols (as for the SARG04 protocol), the key rate and practical length of the channel is bigger than for BB84 protocols. Nevertheless, it is necessary to notice that using these protocols, as well as the others considered above, it is also impossible without users pre-authentication to construct the complete high-grade solution of the problem of key distribution.

III. Advantages and Disadvantages of QKD Protocols

After the analysis of the first and scale quantum method, we must sum up and highlight the following advantages of QKD protocols:

- These protocols always allow eavesdropping to be detected because Eve's connection brings much more error level (compared with natural error level) to the quantum channel. The laws of quantum mechanics allow eavesdropping to be detected and the dependence between error level and intercepted information to be set. This allows applying privacy amplification procedure, which decreases the quantity of information about the key, which can be intercepted by Eve. Thus, QKD protocols have unconditional (information-theoretic) security.
- The information-theoretic security of QKD allows using an absolutely secret key for further encryption using well-known classical symmetrical algorithms. Thus, the entire information security level increases. It is also possible to synthesize QKD protocols with Vernam cipher (One-Time Pad) which in complex with unconditionally secured authenticated schemes gives a totally secured system for transferring information.

The disadvantages of QKD protocols are:

- A system based only on QKD protocols cannot serve as a complete solution for key distribution in open networks (additional tools for authentication are needed).
- The limitation of quantum channel length which is caused by the fact that there is no possibility of amplification without quantum properties being lost. However, the technology of quantum repeaters could overcome this limitation in the near future.
- Need for using weak coherent pulses instead of single photon pulses. This decreases the efficiency of protocol in practice. But this technology limitation might be defeated in the nearest future.
- The data transfer rate decreases rapidly with the increase in the channel length.
- Photon registration problem which leads to key rate decreasing in practice.
- Photon depolarization in the quantum channel. This leads to errors during data transfer. Now the typical error level equals a few percent, which is much greater than the error level in classical telecommunication systems.
- Difficulty of the practical realisation of QKD protocols for *d*-level quantum systems.

IV. Commercial QKD Systems

The world's first commercial quantum cryptography solution was QPN Security Gateway (QPN-8505) proposed by MagiQ Technologies (USA). This system is a cost-effective information security solution for governmental and financial organisations. It proposes VPN protection using

QKD (up to 100 256-bit keys per second, up to 140 km) and integrated encryption. The QPN-8505 system uses BB84, 3DES and AES protocols.

The Swiss company ID Quantique offers systems called Clavis and Cerberis. Clavis uses a proprietary auto-compensating optical platform, which features outstanding stability and interference contrast, guaranteeing low quantum bit error rate. Secure key exchange becomes possible up to 100 km. This optical platform is well documented in scientific publications and has been extensively tested and characterized. Cerberis is a server with automatic creation and secret key exchange over a fibre channel (FC-1G, FC-2G and FC-4G). This system can transmit cryptographic keys up to 50 km and carries out 12 parallel cryptographic calculations. The latter substantially improves the system's performance. The Cerberis system uses AES (256-bits) for encryption and BB84 and SARG04 protocols for quantum key distribution. Main features of Cerberis system are:

- Future-proof security.
- Scalability: encryptors can be added when network grows.
- Versatility: encryptors for different protocols can be mixed.
- Cost-effectiveness: one quantum key server can distribute keys to several encryptors.

Toshiba Research Europe Ltd (Great Britain) recently presented another QKD system named Quantum Key Server. This system delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages. The system provides world-leading performance. In particular, it allows key distribution over standard telecom fibre links exceeding 100 km in length and bit rates sufficient to generate 1 Megabit per second of key material over a distance of 50 km – sufficiently long for metropolitan coverage. Toshiba's system uses a simple "one-way" architecture, in which the photons travel from sender to receiver. This design has been rigorously proven as secure from most types of eavesdropping attack. Toshiba has pioneered active stabilisation technology that allows the system to distribute key material continuously, even in the most challenging operating conditions, without any user intervention. This avoids the need for recalibration of the system due to temperature-induced changes in the fibre lengths. Initiation of the system is also managed automatically, allowing simple turn-key operation. It has been shown to work successfully in several network field trials. The system can be used for a wide range of cryptographic applications, e.g., encryption or authentication of sensitive documents, messages or transactions. A programming interface gives the user access to the key material.

Another British company, QinetiQ, realised the world's first network using quantum cryptography – Quantum Net (Qnet). The maximum length of telecommunication lines in this network is 120 km. Moreover, it is a very important fact that Qnet is the first QKD system using more than two servers. This system has six servers integrated to the Internet.

V. Conclusions

Today the most developed direction of quantum cryptography is QKD protocols. In research institutes, laboratories and centres, quantum cryptographic systems for secret key distribution for distant legitimate users are being developed. This paper presents a systematization of modern QKD protocols. Analysis of the advantages and disadvantages of various QKD protocols is made. Their advantage is a high level of security and some properties, which classical means of information security do not have. One of these properties is the ability always to detect eavesdropping.

Modern commercial QKD systems were analyzed in accordance to used protocols of key distribution and encryption. QKD systems can be combined with any classical cryptographic (encryption) scheme [6-7], which provides information-theoretic security, and the entire cryptographic scheme will have information-theoretic security also.

Quantum technologies therefore represent an important step towards improving the security of ICT against cyberattacks. But many theoretical and practical problems must be solved for wide practical use of QKD in ICT and information infrastructures.

REFERENCES

1. Nielsen M.A., Chuang I.L. (2010) Quantum computation an quantum information, Cambrige, Cambrige University Press, 708 p.

2. Advanced Technologies of Quantum Key Distribution, Monograph [edited by Sergiy Gnatyuk], London, Great Britain : InTech, 227 p. (2018).

3. S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015), Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.

4. Zh. Hu, S. Gnatyuk, T. Okhrimenko (Zhmurko), V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.

5. Qoussini A.E., Daradkeh Y.I., Al Tabib S.M., Gnatyuk S., Okhrimenko T., Kinzeryavyy V. Improved model of quantum deterministic protocol implementation in channel with noise, Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2019), 2019, pp. 572-578.

6. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings, Vol. 2104, pp. 657-668, 2018.

7. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing, Vol. 1126, pp. 93-104, 2020.