UDC 003.26:621.39:530.145 (045)

COMPARATIVE ANALYSIS OF QUANTUM KEY DISTRIBUTION SYSTEMS

S. O. Gnatyuk

National Aviation University

E-mail: s.gnatyuk@nau.edu.ua

Quantum cryptography has attracted considerable interest among specialists in information security. The overwhelming majority of research projects in quantum cryptography are related to the development of quantum key distribution protocols. Absence of generalized classification & systematization makes it difficult to estimate the level of the latest achievements and does not allow using quantum technologies with full efficiency. From this viewpoint the analysis of existed quantum key distribution systems, basic protocols, strengths & weaknesses, its implementation prospects was carried out in the paper. It gives a possibility to formalize some actual problems of quantum key distribution systems and outline the ways of its solving.

Keywords: information security, quantum cryptography, quantum key distribution, comparative analysis, protocol, commercial quantum key distribution system.

Квантова криптографія викликає значний інтерес серед фахівців у галузі інформаційної безпеки. Переважна більшість дослідницьких проектів у галузі квантової криптографії пов'язані з розробкою протоколів квантового розподілу ключів. Відсутність узагальненої класифікації та систематизації ускладнює процес оцінки рівня останніх досягнень і не дозволяє ефективно використовувати квантові технології. З цієї точки зору у статті виконано аналіз існуючих систем квантового розподілу ключів, базових протоколів, переваг та недоліків, перспектив їх впровадження. Це дозволяє формалізувати деякі актуальні проблеми систем квантового розподілу ключів і окреслити шляхи їх вирішення.

Ключові слова: інформаційна безпека, квантова криптографія, квантовий розподіл ключів, порівняльний аналіз, протокол, комерційна система квантового розподілу ключів.

Problem Definition & Analysis of Publication

In recent years, quantum cryptography (QC) has attracted considerable interest among specialists in information security (IS).

Quantum key distribution (QKD) [1–4] plays a dominant role in QC. The overwhelming majority of theoretic and practical research projects in QC 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, for example [3]).

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 the paper** is an analysis of existed QKD systems from viewpoint of used protocols, strengths & weaknesses, its implementation prospects.

The first of all quantum technologies of IS consist of [1]: Quantum Key Distribution; Quantum Secure Direct Communication; Quantum Steganography; Quantum Secret Sharing; Quantum Stream Cipher; Quantum Digital Signature, etc.

The theoretical basis of quantum cryptography is stated in set of books and review papers (see e.g. [1, 5–7]).

QKD Protocols

QKD includes the following protocols: protocols using single (non-entangled) qubits (two-level quantum systems) and qudits (d-level quantum systems, $d > 2$) [5; 7]; protocols using phase coding [1–3]; protocols using entangled states [6]; decoy states protocols [1; 2] and some other protocols [1–3].

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 [1], which has become an alternative solution for the problem of key distribution. This protocol is called BB84 [1] 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^o, 45^o, 90^o, 135^o). 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 are used for key generation to the general number of transmitted photons.

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 [1–3]. Such changes decrease the amount of information, which can be intercepted. But on the other hand, the efficiency of the protocol decreases to 33 %.

Next, the 4 + 2 *protocol* is intermediate between the BB84 and B92 protocol [1]. 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 IS level than the BB84 protocol, when weak coherent pulses, but not a single photon source, are used by sender [5]. But the efficiency of the 4 + 2 protocol is lower than efficiency of BB84 protocol.

In the *Goldenberg-Vaidman protocol* [1–3], 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. A modified type of Goldenberg–Vaidman protocol is called the *Koashi-Imoto protocol* [2]. 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).

Six-state protocol and BB84 protocol were generalised in case of using *d*-level quantum systems — qudits instead qubits [1; 6]. This allows increasing the information capacity of protocols. We can transfer information using *d*-level quantum systems (which correspond to the usage of trits, quarts, etc.). It is important to notice that QKD protocols are intended for classical information (key) transfer via quantum channel.

The generalisation of BB84 protocol for qudits is called protocol using single qudits and two bases due to use of two mutually unbiased bases for the eavesdropping detection. Similarly, the generalisation of six-state protocol is called protocol using qudits and $d + 1$ bases. These protocols' security against intercept-resend attack and non-coherent attack was investigated in a number of articles [2; 3].

Another type of QKD protocols are *protocols using phase coding*: for example, the *B92 protocol* [2] 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 %.

The *Ekert protocol* (E91) [1] refers to QKD protocols using entangled states. Entangled pairs of qubits that are in a singlet state [6] 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 [2]. But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol [1].

Kaszlikowski et al. carried out the generalisation of the Ekert scheme for three-level quantum systems [1] and Durt et al. carried out the generalisation of the Ekert scheme for *d*-level quantum systems [6]: this increases the information capacity of the protocol a lot. Also the security of the protocol using entangled qudits is investigated. In the paper [2] security comparison of protocol using entangled qudits and protocols using single qudits against non-coherent attack is made. It was found that the security of these two kinds of protocols is almost identical. But the efficiency of the protocol using entangled qudits increases more slowly with the increasing dimension of qudits than the efficiency of the protocol using single qudits and two bases. 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.

The *SARG04 protocol* does not differ much from the original BB84 protocol [1–3]. 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 im-

provement allows increasing security against photon number splitting attack. The SARG04 protocol in practice has a higher key rate than the BB84 protocol [2].

Another way of protecting against photon number splitting attack is the use of *decoy states QKD protocols* [2], 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 [1]. 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.

Advantages of QKD protocols:

1) 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;

2) the information-theoretic security of QKD allows using an absolutely secret key for further encryption using well-known classical symmetrical algorithms. Thus, the entire IS 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:

1) 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);

2) 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;

3) 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;

4) the data transfer rate decreases rapidly with the increase in the channel length;

5) photon registration problem which leads to key rate decreasing in practice;

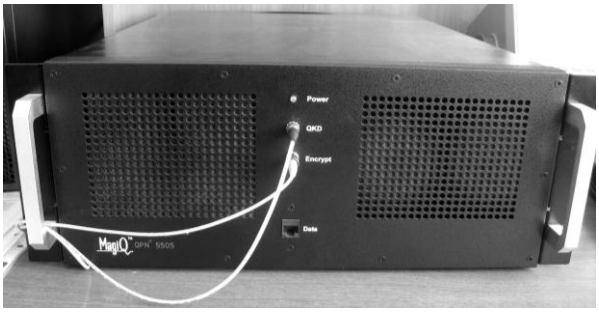
6) photon depolarization in the quantum channel. This leads to errors during data transfer. Now the typical error level equals a few percent, which is much greater than the error level in classical telecommunication systems;

7) difficulty of the practical realisation of QKD protocols for *d*-level quantum systems;

8) the high price of commercial QKD systems.

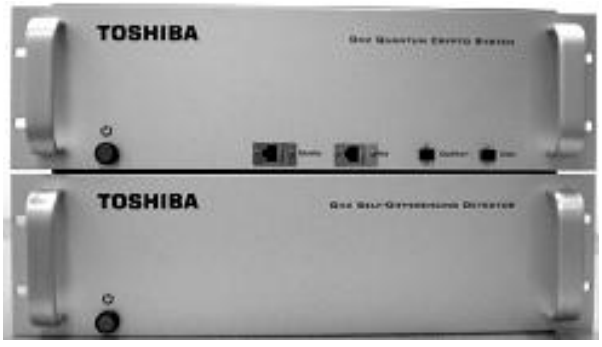
Commercial QKD Systems

The world's first commercial quantum cryptography (in particular QKD) solution was *QPN Security Gateway (QPN-8505)* [8] proposed by *MagiQ Technologies (USA).* This system (fig. 1, *a*) is a cost-effective IS 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 & AES protocols.



a

b



c

Fig. 1. Most popular commercial QKD systems

The Swiss company *Id Quantique* [9] offers a systems called Clavis^2 (fig. 1, *b*) and *Cerberis*. Clavis^2 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 QKD. Main features: 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* [10]. This system (fig. 1, *c*) 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 Mbit 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)* [1]. 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.

Conclusion

Quantum cryptography has attracted considerable interest among specialists in information security. The overwhelming majority of research projects in quantum cryptography are related to the development of quantum key distribution protocols. Absence of generalized classification & systematization makes it difficult to estimate the level of the latest achievements and does not allow using quantum technologies with full efficiency. From this viewpoint the analysis of existed quantum key distribution systems, basic protocols, strengths & weaknesses, its implementation prospects was carried out in the paper. It gives a possibility to formalize some actual problems of quantum key distribution systems and outline the ways of its solving.

Accordingly, QKD protocols research is the most developed direction of quantum information security technology today. Such QKD systems can be combined with any classical cryptographic scheme, which provides information-theoretic security, and the entire cryptographic scheme will have information-theoretic security also.

QKD protocols can generally provide higher information security level than appropriate classical schemes. A comparative analysis of the advantages and imperfections of concrete QKD protocols was made in the paper.

In research institutes, laboratories and centres, quantum cryptographic systems for secret key distribution for distant legitimate users are being developed. Also, in the paper the analysis of existed QKD systems, strengths & weaknesses, its implementation prospects to existed network architecture was carried out. It gives a possibility to formalize some actual problems of QKD systems and outline the ways of its solving in future.

REFERENCES

1. *Quantum* secure telecommunication systems / [Oleksandr Korchenko, Petro Vorobiyenko, Maksym Lutskiy, Yevhen Vasiliu, Sergiy Gnatyuk] // Telecommunications Networks: Current Status and Future Trends / edited by *Jesus Hamilton Ortiz.* — Rijeka, Croatia : InTech, 2012. — P. 211–236.

2. *Korchenko O.* Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Ye. Vasiliu, S. Gnatyuk // Aviation. Vilnius: Technika, 2010. — V. 14. — № 2. — P. 58–69.

3. *Korchenko O.* Modern directions of quantum cryptography / O. Korchenko, E. Vasiliu, S. Gnatyuk // «AVIATION IN THE XXI-st CENTURY» — «Safety in Aviation and Space Technologies»: IV World Congress: Proceedings, September 21-23, Kyiv, NAU, 2010. — P. 17.1–17.4.

4. *Korchenko O. G.* Modern quantum technologies of information security / O. G. Korchenko, E. V. Vasiliu, S. O. Gnatyuk // arXiv: 1005.5553v2 [cs.CR].

5. *Wooters W. K.* A single quantum cannot be cloned / *W. K. Wooters, W. H. Zurek* // Nature. — 1982. — V. 299. — P. 802.

6. *Boström K.* Deterministic secure direct communication using entanglement / K. Boström, T. Felbinger // Physical Review Letters, 2002. — Vol. 89. — № 18, 187902.

7. *Cerf N.* Security of quantum key distribution using d-level systems / N. Cerf, M. Bourennane, A. Karlsson, N. Gisin // Physical Review Letters. — 2002. — V. 88, № 12. — 127902.

8. *QPN-8505 Security Gateway* [Electronic resource] : Data Sheet / MagiQ Technologies, Inc. — Electronic data. — Somerville, Massachusetts, USA : MagiQ Technologies, Inc., [11.01.2013]. — Mode of access: World Wide Web. — URL. — [Електронний ресурс]. — Режим доступу: http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf. — Description based on screen.

9. *Cerberis Encryption Solution* [Electronic resource] : Layer 2 Encryption with Quantum Key Distribution / ID Quantique SA. — Electronic data. — Geneva, Switzerland: ID Quantique SA, [11.01.2013]. — Mode of access: World Wide Web. — URL. — [Електронний ресурс]. — Режим доступу: http://www.idquantique.com/products/cerberis.htm. — Description based on screen.

10. *Quantum Key Distribution System* [Electronic resource] : Toshiba Research Europe Ltd., Cambridge Research Laboratory. — Electronic data. — Tokyo, Japan : Toshiba Corporation, [11.01.2013]. — Mode of access: World Wide Web. — URL. — [Електронний ресурс]. — Режим доступу: http://www.toshiba-europe.com/research/crl/qig/quantum keyserver. html. — Description based on screen.

Стаття надійшла до редакції 07.03.12.