Contemporary Commercial Quantum Information Security Systems

Sergiy Gnatyuk[1], Myroslav Riabyi[2], Tetiana Zhmurko[3]

[1]IT-Security Academic Department, National Aviation University, UKRAINE, Kyiv, 1, Kosmonavta Komarova ave., E-mail: s.gnatyuk@nau.edu.ua

[2]Complex Information Security Organization Academic Department, European University, UKRAINE, Kyiv, 16-V Academician Vernadskiy Blvd., E-mail: M.Ryabyy@ukr.net

[3]IT-Security Academic Department, National Aviation University, UKRAINE, Kyiv, 1, Kosmonavta Komarova ave., E-mail: TaniaZhm@gmail.com

Abstract - 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, 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.

Key words – information security, quantum key distribution, quantum cryptography, protocol, commercial quantum system.

I. Introduction

Quantum Cryptography (QC) [1] or more precisely Quantum Key Distribution (QKD) was born as an alternative to public key cryptography, which currently protects the vast majority of our information, but it is seriously threatened by the future development of a quantum computer.

QKD allows two parties – usually called Alice and Bob – to exchange an encryption key, secure in the knowledge that the key will not have been read by an eavesdropper (Eve). This guarantee is possible because the key is transmitted in terms of quantum bits (qubits) of information, which if intercepted and read are changed irrevocably, thus revealing the actions of Eve. This is possible through the use in QC unbreakable principles of quantum mechanics instead of mathematical methods, which applied in traditional cryptografy.

QKD is the only popular quantum technique that is already being used commercially. The *main aim* of this work is the analysis of existed quantum information security (IS) systems, their prospects and difficulties of implementation in modern information and communication systems.

Active research in the field of QC are carried out by scientists of the leading countries of the world (Switzerland, USA, Germany, Great Britain, France, Australia etc.) [2], and represented by products of such corporations and high-tech companies, as MagiQ Technologies, Id Quantique, Toshiba, WISeKey, QinetiQ, NEC, Nokia, IBM, Hewlett Packard, Mitsubishi, NTT and others. But there are companies who have achieved great results (MagiQ Technologies, Id Quantique, Toshiba), and presented to the market commercial systems that have practical application, thereby the detailed analysis of their products is represented below.

II. ID Quantique Products

The Swiss company ID Quantique [3] is a global leader shaping the evolution of network security through the development and commercialization of QKD and high-speed encryption products. In 2001, the company was the first to bring this new technology to the market. In 2007, it was able to announce the first public application of this technology to secure a network used for vote counting in an election in Geneva. In addition to its strong technology focus on QKD, ID Quantique has also developed expertise in the area of high-speed encryption and has a broad portofolio of solutions for layer 2 encryption. A privately held company headquartered in Geneva, Switzerland, ID Quantique is a spin-off from the University of Geneva and has close ties with leading academic institutions.

The company offers a systems called *Clavis*^{2} (fig. 1), *Vectis* and *Cerberis*. Clavis^2 (id3100/id3110 Clavis^2 QKD System from latin "clavis" – key) 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.

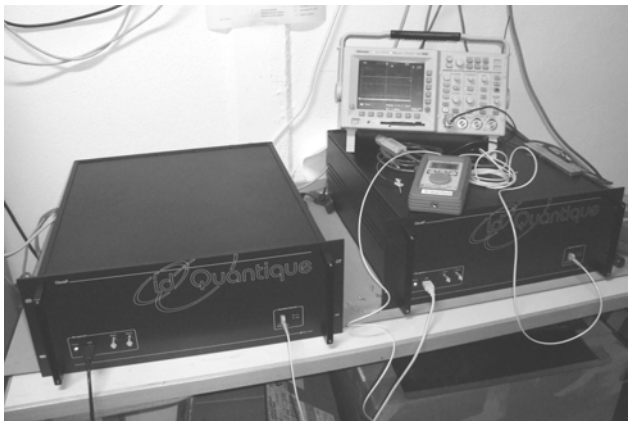

Fig. 1. Clavis^2 QKD System

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. The disadvantages of this system is the high market price and low-speed data processing, lack of dynamic control to the scattering process information data in the classical part. With the rapid development of computer technology and cheaper (last 5-10 years), another disadvantage is the low cryptographic strength.

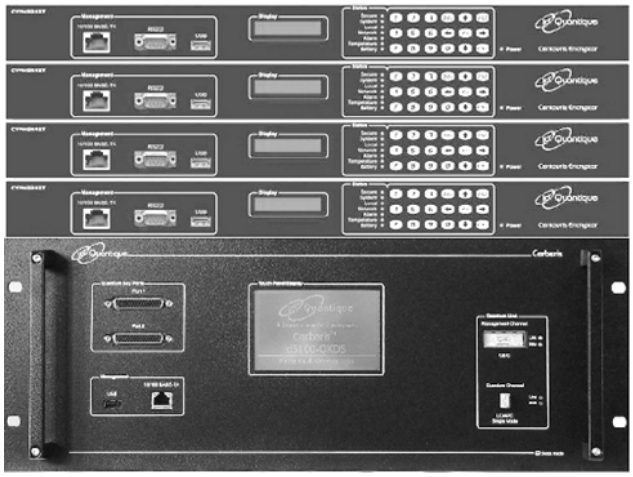

Fig. 2. Cerberis System

III. MagiQ Technologies Products

MagiQ Technologies (USA) [6] is an acclaimed research and development organization that leverages its unique blend of science, business and engineering expertise to produce advanced real world solutions The world's first commercial quantum IS system was *QPN Security Gateway (QPN-8505)* proposed by MagiQ Technologies. This system (fig. 3) is a cost-effective IS solution for governmental and financial organizations. It proposes VPN protection using QKD (up to 100 of 256-bit keys per second, up to 140 km) and integrated encryption. The QPN-8505 system uses BB84, 3DES and AES protocols.

MagiQ QPN combines traditional VPN security technology and QKD. QPN 8505 provides an always-on, industry-standard, IPSec site-to-site VPN connection. The MagiQ QPN key exchange layer is also a combination of the best traditional and quantum key exchange technologies. Thus, an eavesdropper has to be able to break through both technologies to gain acces to the data.

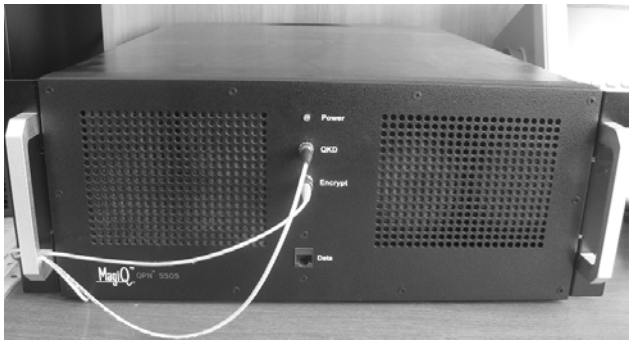

Fig. 3. QPN Security Gateway (QPN-8505)

Next product *Q-Box Workbench QKD System* is a point-to-point, single photon-based system, developed for scientists in academic, governmental and commercial organizations to conduct research related to or utilizing QKD. Specifically designed to be turned up in record time, Q-Box Workbench ships Q-Box Workbench hardware consists of two 7x19x24-inch rack-mount chassis (Alice and Bob) connected by both fiber and Ethernet cable.

IV. Toshiba Products

Toshiba Research Europe Ltd (Great Britain) [4] not long ago presented another QKD system named *Quantum Key Server*. This system (fig. 4) 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 tele-com 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 at-tack. Toshiba has pioneered active stabilisation technology that allows the system to distribute key ma-terial 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.

Fig. 4. Toshiba Quantum Key Server

Recently, Toshiba announced it has developed a method for deploying quantum cryptography on a network of up to 64 users, overcoming the point-to-point communications quantum systems are limited to now. Researchers published a paper in Nature [11] describing their multi-user architecture, which they say removes one of the main barriers to broader adoption.

Toshiba researchers designed a system to share expensive detector across multiple users, effectively creating a network hub. In its configuration, a single photon detector is at one end of the network while each end user has a photon transmitter made with off-the-shelf fiber optical components. The signals of multiple end users are combined and transmitted over a single fiber, enabled a one-to-many architecture. To do this, Toshiba researchers needed to develop a very fast photon detector that can accurately read fast-arriving signals from multiple end users. They also needed to adjust the detector to compensate for changes in temperature that can happen from having multiple users on a single fiber link, which can change its length slightly and could cause errors. The group said they demonstrated the system operating for 12 hours.

Creating a edicated quantum key distribution network with hub-and-spoke architecture is one way to make technology less expensive. In another effort, research company Battelle is working with quantum key distribution startup ID Quantique to build a hybrid encryption system that sends photons between two points and then uses traditional encryption on a local network.

Toshiba's system helps bring down the cost of quantum encryption, which could make the technology attractive to a broader set of commercial and government customers.

V. Other Companies Products

Another British company, QinetiQ, realised the world's first network using quantum cryptog-raphy – *Quantum Net* (Qnet) [7]. 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.

In 2011 was presented *the Q-KeyMaker* by Quantum Optics Lab [8], a four-user QKD network in a star configuration, i.e. with one server (Galileo) and three clients (Benjamin, Copernico and Keplero), based on decoy-state method.

Fig. 5. The Q-KeyMaker

The French company Smart Quantum [5] offers a range of systems of quantum key distribution. A separate system for quantum key distribution through the channel is called *SQKey Generator*. The integrated systems are called *SQBox Defender and SQBox FibreShield* (the latter is designed exclusively for military use).

Quintessence Labs, Inc. (Astralia) [2] presented *The Quantum Link Encryptor (QLE)* is a turn-key QKD, key manager and encryption device that can be inserted transparently into existing network architectures. QLE transparently establishes one-time pad keys through a QKD protocol between two-nodes linked by a dark fibre. LAN traffic is securely transmitted between remote locations using one-time pad cipher encryption. QLE nodes use spanning tree parallel path redundancy to ensure availability in a network infrastructure. Secure web, CLI and SNMP interfaces are provided for standards-based management of QLE nodes.

Fig. 6. The Quantum Link Encryptor QLE

VI. Main projects in QKD

In addition the world's leading scientists are actively taking part in the implementation of projects (to develop quantum IS systems) such as SECOQC (Secure Communication based on Quantum Cryptography), EQCSPOT (European Quantum Cryptography and Single Photon Technologies) and SwissQuantum [2]:

1) SECOQC is a project that aims to develop quantum cryptography network. The European Union decided in 2004 to invest € 11 million in the project as a way of circumventing espionage attempts by ECHELON (global intelligence gathering system, USA). This project combines people and organizations in Austria, Belgium, the United Kingdom, Canada, the Czech Republic, Denmark, France, Germany, Italy, Russia, Sweden and Switzerland. On October 8, 2008 SECOQC was launched in Vienna. During the SECOQC the seven most important quantum IS systems have been developed or refined. Among these QKD systems are Clavis[2] and Quantum Key Server described above and also: 1) The coherent one-way system (time-coding) designed by GAP-Universite de Geneve and idQuantique realizes the novel distributed-phase-reference coherent one-way protocol; 2) The entanglement-based QKD system developed by an Austrian-Swedish consortium. The system uses the unique quantum mechanical property of entanglement for transferring the correlated measurements into a secret key; 3) The free-space QKD system developed by the group of H. Weinfurter from the University of Munich. It employs the BB84 protocol using polarization encoded attenuated laser pulses with photons of 850 nm wavelength. Decoy states are using to ensure key security even with faint pulses. The system is applicable to day and night operation using excessive filtering in order to suppress background light; 4) The low-cost QKD system was developed by John Rarity's team of the University of Bristol. The system can be applied for secure banking including consumer protection. The design philosophy is

based on a future hand-held electronic credit card using free-space optics. A method is proposing to protect these transactions using the shared secret stored in a personal hand-held transmitter. Thereby transmitter's module is integrated within a small device such as a mobile telephone, or personal digital assistant, and receiver's module consists of a fixed device such as a bank asynchrone transfer mode.

2) The primary objective of EQCSPOT project is bringing quantum cryptography to the point of industrial application. Two secondary objectives exist to improve single photon technologies for wider applications in metrology, semiconductor characterisation, biosensing etc and to assess the practical use of future technologies for general quantum processors. The primary results will be in the tangible improvements in key distribution. The overall programme will be co-ordinated by British Defence Evaluation and Research Agency and the work will be divided into eight workparts with each workpart co-ordinated by one organisation. Three major workparts are dedicated to the development of the three main systems: NIR fibre, 1.3-1.55 μm fibre and free space key exchange. The other five are dedicated to networks, components and subsystems, software development, spin-off technologies and dissemination of results.

3) One of the key specificities of the SwissQuantum project is to aim at long-term demonstration of QKD and its applications. Although this is not the first quantum network to be deployed, it wills the first one to operate for months with real traffic. In this sense, the SwissQuantum network presents a major impetus for the QKD technology. The SwissQuantum network consists of three layers: a) Quantum Layer. This layer performs Quantum Key Exchange; b) Key Management Layer. This layer manages the quantum keys in key servers and provides secure key storage, as well as advanced functions (key transfer and routing). c) Application Layer. In this layer, various cryptographic services use the keys distributed to provide secure communications.

There are also many practical and theoretical research projects concerning the development of quantum IS systems in research institutes, laboratories and centres such as Institute for Quantum Optics and Quantum Information, Northwestern University, SmartQuantum, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, ARS Seibersdorf Research and Los Alamos National Laboratory and others.

Conclusion

This paper presents a review of modern commercial quantum IS systems, their analysis from viewpoint of prospects and difficulties of implementation in modern information and communication systems. Quantum IS systems are rapidly developing and gradually taking their place among other means of IS. Their main advantages are a high level of security and some properties, which classical means of IS do not have. One of these properties is the ability always to detect eavesdropping. Quantum IS systems therefore represent an important step towards improving the level of data security. However, many theoretical and practical problems must be solved for practical use of these systems in existing information and communication systems. Today QKD research is the most developed direction of quantum information security technology. 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. Active research in the field of QC are carried out by scientists of the leading countries of the world, however, there are still many problems requiring attention of scientists. Furthermore, a lot of things need to be done to implement quantum technology in widespread use.

References

[1] M. Nielsen, and I. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[2] Jesus Hamilton Ortiz, Ed. Telecommunications Networks: Current Status and Future Trends [Quantum secure telecommunication systems]. Rijeka, Croatia: InTech, pp. 211-236, 2012.

[3] ID Quantique SA "Cerberis Encryption Solution: Layer 2 Encryption with Quantum Key Distributio"n [Online] Available: http://www.idquantique.com/ products/cerberis.htm. [Accessed Oct. 1, 2013].

[4] Toshiba Research Europe Ltd. "Quantum Key Distribution System" [Online] Available: http://www.toshiba-europe.com/research/crl/qig/ quantum keyserver.html. [Accessed Oct. 1, 2013].

[5] O. Korchenko, E. Vasiliu, S.Gnatyuk "Modern quantum technologies of information security" Aviation. Vilnius: Technika, Vol. 14, No. 2, p. 58-69 2010. [Online]. Available: arXiv: 1005.5553v2 [Accessed Oct. 1, 2013].

[6] MagiQ Technologies, Inc. "QPN-8505 Security Gateway: Data Sheet" [Online] Available: http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf. [Accessed Oct. 1, 2013].

[7] N. Cerf, M. Bourennane, A. Karlsson, N. Gisin. "Security of quantum key distribution using d-level systems", Physical Review Letters, Vol. 88, № 12, 127902, 2002.

[8] F. A. Bovino, M. Giardina. "Practical Quantum Cryptography: The Q-KeyMaker™" [Online] Available:http://arxiv.org/ftp/arxiv/papers/1104/1104.2475.pdf [Accessed Oct. 1, 2013].

[9] C. H. Bennett, and C. Brassard, "Quantum cryptography: public key distribution and coin tossing", in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, Page 175-179, IEEE, New York (1984).

[10] O. Korchenko, E. Vasiliu, S. Gnatyuk Modern directions of quantum cryptography, in Proceedings of IV World Congress «AVIATION IN THE XXI-st CENTURY» – «Safety in Aviation and Space Technologies», September 21–23, 2010, Kyiv, Ukraine. NAU Publ., 2010. pp. 17.1-17.4.

[11] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan & A. J. Shields "A quantum access network", Nature 501, pp. 69–72, 2013. [Online] Available: http://www.nature.com/nature/journal/v501/n7465/full/nature12493.html [Accessed Oct. 1, 2013].