Aviation

ISSN: 1648-7788 (Print) 1822-4180 (Online) Journal homepage: http://www.tandfonline.com/loi/tavi20

Modern quantum technologies of information security against cyber-terrorist attacks

Oleksandr Korchenko , Yevhen Vasiliu & Sergiy Gnatyuk

To cite this article: Oleksandr Korchenko , Yevhen Vasiliu & Sergiy Gnatyuk (2010) Modern quantum technologies of information security against cyber-terrorist attacks, Aviation, 14:2, 58-69, DOI: 10.3846/aviation.2010.10

To link to this article: https://doi.org/10.3846/aviation.2010.10

Published online: 09 Jun 2011.

AVIATION
2010
14(2): 58–69

MODERN QUANTUM TECHNOLOGIES OF INFORMATION SECURITY AGAINST CYBER-TERRORIST ATTACKS

Oleksandr Korchenko[1], Yevhen Vasiliu[2], Sergiy Gnatyuk[3]

[1,3]Department of Information Security Technologies, National Aviation University,
Kosmonavta Komarova Ave 1, 03680 Kiev, Ukraine
[2]Department of Information Technologies and Control Systems,
Odesa National Academy of Telecommunications n.a. O.S. Popov, Koval`ska Str 1, 65029 Odesa, Ukraine
E-mails: [1]icaocentre@nau.edu.ua, [2]vasiliu@ua.fm, [3]aspirans@nau.edu.ua

Received 3 January 2010, accepted 20 May 2010

Oleksandr KORCHENKO, Prof Dr Habil
Date and place of birth: 1961, Kiev, Ukraine.
Education: Kiev Institute of Civil Aviation Engineers (National Aviation University since 2000), 1983.
Affiliation and functions: Dr Habil from National Aviation University since 2004, professor at National Aviation University since 2005, head of Information Technologies Security's Department of National Aviation University since 2004.
Research interests: information and aviation security.
Publications: over 140 books and articles, 8 patents.

Yevhen VASILIU, PhD
Date and place of birth: 1966, Yalta, Crimea, Ukraine.
Education: Odessa State University n.a. I. Mechnikov, 1990.
Affiliation and functions: PhD in theoretical physics since 1999, docent at Odesa National Academy of Telecommunications n.a. O. Popov since 2004.
Research interests: quantum information, quantum cryptography.
Publications: over 50 books and articles.

Sergiy GNATYUK, MSc
Date and place of birth: 1985, Netishyn, Khmelnytskyi Oblast, Ukraine.
Education: National Aviation University, 2007.
Affiliation and functions: post-graduate student at National Aviation University since 2007.
Research interests: information security, quantum cryptography.
Publications: 5 articles, 2 patents.

Abstract. In this paper, the systematisation and classification of modern quantum technologies of information security against cyber-terrorist attack are carried out. The characteristic of the basic directions of quantum cryptography from the viewpoint of the quantum technologies used is given. A qualitative analysis of the advantages and disadvantages of concrete quantum protocols is made. The current status of the problem of practical quantum cryptography use in telecommunication networks is considered. In particular, a short review of existing commercial systems of quantum key distribution is given.

Keywords: information security, quantum technologies, quantum key distribution, quantum secure direct communication, quantum secret sharing, quantum stream cipher, quantum digital signature, quantum steganography.

ISSN1648-7788 print / ISSN 1822-4180 online
http://www.aviation.vgtu.lt
DOI: 10.3846/aviation.2010.10

1. Introduction

Today there is virtually no area where information technology (IT) is not used in some way. Computers support banking systems, control the work of nuclear reactors, and control aircraft, satellites and spacecraft. The high level of automation therefore depends on the security level of IT. The latest achievements in communication systems are now applied in aviation. These achievements are public switched telephone network (PSTN), circuit switched public data network (CSPDN), packet switched public data network (PSPDN), local area network (LAN), and integrated services digital network (ISDN) (Бабак *и др*. 2004). These technologies provide data transmission systems of various types: surface-to-surface, surface-to-air, air-to-air, and space telecommunication. Cyber-terrorist attacks (CTA) (Гнатюк *и др*. 2009) can cause economic damage to aircraft companies and can also reduce flight security or cause casualties. Protection against such attacks is therefore an important scientific and technical problem.

One of the most effective ways of ensuring confidentiality and data integrity during transmission is cryptographic system. The purpose of such systems 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: classical information-theoretic schemes (requires channel with noise; efficiency is very low, 1–5 %), classical public-key cryptography schemes (Diffie-Hellman scheme, digital envelope scheme; it has computational security), classical computationally secure symmetric-key cryptographic schemes (requires a pre-installed key on both sides and can be used only as scheme for increase in key size but not as key distribution scheme), quantum key distribution (provides information-theoretic security; it can also be used as a scheme for increase in key length), Trusted Couriers Key Distribution (it has a high price and is dependent on the human factor) (SECOQC…).

In recent years, quantum cryptography (QC) has attracted considerable interest. Quantum key distribution (QKD) plays a dominant role in QC (Bennett *et al.* 1984; Bennett *et al.* 1995; Bennett 1992; Bennett *et al.* 1992; Bouwmeester *et al*. 2000; Branciard *et al*. 2005; Brassard *et al.* 2000; Bruss 1998; Cerf *et al*. 2002; Desurvire 2009; Durt *et al*. 2004б; Ekert 1991; Fuichs *et al.* 1997; Gisin *et al.* 2002; Goldenberg *et al.* 1995; Huttner *et al.* 1995; Inamori *et al.* 2001; Kaszlikowski *et al.* 2003; Koashi *et al.* 1997; Lutkenhaus *et al.* 2002; Nielsen *et al.* 2000; Peng *et al.* 2007; Rosenberg *et al.* 2007; Scarani *et al*. 2004; Scarani *et al.* 2009; Vasiliu *et al.* 2009; Zhao *et al.* 2006; Василиу *и др*. 2006; *Энциклопедия…* 2008).. 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 of information security (QTIS) is increasing, but there is no information about classification of these technologies in scientific literature (there are only a few works concerning classification of QKD protocols, for example (Gisin *et al*. 2002; Scarani *et al*. 2009). This makes it difficult to estimate the level of the latest achievements and does not allow using QTIS with full efficiency. *The purpose of this article* is the systematisation and classification of up-to-date quantum technologies of data (transmitted via telecommunication channels) security against CTA, analysis of their strengths and weaknesses, and prospects and difficulties of implementation. Quantum technologies of information security consist of quantum key distribution, quantum secure direct communication (Boström *et al.* 2002; Boström *et al.* 2008; Cai *et al*. 2004a; Cai *et al*. 2004b; Chuan *et al*. 2005; Wang *et al.* 2005; Zhang *et al.* 2005b; Василиу *и др*. 2006a; Василиу *и др*. 2009b; Василиу *и др*. 2009c), quantum secret sharing (Deng *et al*. 2005; Hillery *et al*. 1999; Li *et al*.; Qin *et al.* 2007; Yan *et al.* 2008; Zhang *et al*. 2005a), quantum stream cipher (Barbosa *et al.* 2003; Corndorf *et al.* 2005; Hirota *et al.* 2000; Hirota *et al*. 2005; Nair *et al*.), quantum digital signature (Gottesman *et al*.; Wang *et al*. 2006; Xiao-Jun *et al*.), quantum steganography (Conti *et al.* 2004; Curty *et al.* 2000; Imai *et al*. 2006), etc.

2. Quantum key distribution

QKD includes the following protocols: *protocols using single (non-entangled) qubits (two-level quantum systems) and qudits* (*d*-level quantum systems, $d>2$) (Bennett *et al.* 1984; Bennett *et al.*1995; Bouwmeester *et al*. 2000; Branciard *et al*. 2005; Brassard *et al.* 2000; Bruss 1998, Cerf *et al*. 2002; Fushs *et al*. 1997; Gisin *et al.* 2002; Goldenberg *et al*. 1995; Huttner *et al*. 1995; Koashi *et al*. 1997; Lutkenhaus *et al*. 2002; Peng *et al*. 2007; Rosenberg *et al.* 2007; Scarani *et al*. 2004; Scarani *et al.* 2009; SECOQC …, Vasiliu *et al*. 2009, Zhao *et al*. 2006; *Энциклопедия…* 2008; *protocols using phase coding* (Bennett 1992; Gisin *et al*. 2002) and *rotocols using entangled states* (Durt *et al.* 2004; Ekert 1991; Inamori *et al.* 2001; Kaszlikowski *et al.* 2003).

The main task of QKD protocols is encryption key generation and distribution between two users connecting via quantum and classical channels (Gisin *et al*. 2002). In 1984 Ch. Bennet 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 (Bennett *et al.* 1984; Bouwmeester *et al*. 2000; Desurvire 2009; Scarani *et al*. 2009; SECOQC…). 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 (Nielsen *et al*. 2000). 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 (Bennet *et al.* 1995). The efficiency of the BB84 protocol equals 50 %. Efficiency

means the ratio of the photons number that is 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 (Bruss 1998). 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 (Huttner *et al.* 1995). There are four different states used in this protocol for encryption: 0 and 1 in two bases. States in each bases 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 (Huttner *et al.* 1995). But the efficiency of the 4+2 protocol is lower than efficiency of BB84 protocol. In the Goldenberg-Vaidman protocol, encryption of 0 and 1 is performed using two orthogonal states (Goldenberg *et al.* 1995). 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 (Koashi *et al.* 1997). 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).

The measure of QKD protocols security is Shannon's mutual information between legitimate users (Alice and Bob) and eavesdropper (Eve): $I_{AE}(D)$ and $I_{BE}(D)$, where D is error level that is created by eavesdropping. For most attacks on QKD protocols $I_{AE}(D) = I_{BE}(D)$, we will therefore use $I_{AE}(D)$. The lower $I_{AE}(D)$ in the extended range of D is, the more secure the protocol is.

Six-state protocol and BB84 protocol were generalised in case of using d-level quantum systems-qudits instead qubits (Cerf *et al.* 2002). 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.) unlike the classical transmission systems, which use bits. It is important to notice that QKD protocols are intended for classical information (key) transfer via quantum channel.

Similarly, the generalisation of the 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 (e.g. Cerf *et al.* 2002). In E. V. Vasiliu *et al.* paper comparative analysis of the efficiency and security of different protocols using qudits (on the basis of known formulas for mutual information) are carried out (Vasiliu *et al.* 2009).

In figure 1 dependences of $I_{AB}(D)$, $I_{AE}^{(d+1)}(D)$ and $I_{AE}^{(2)}(D)$ are presented, where $I_{AB}(D)$ is mutual information between Alice and Bob, $I_{AE}^{(d+1)}(D)$ and $I_{AE}^{(2)}(D)$ is mutual information between Alice and Eve for protocols using d+1 and two bases accordingly.

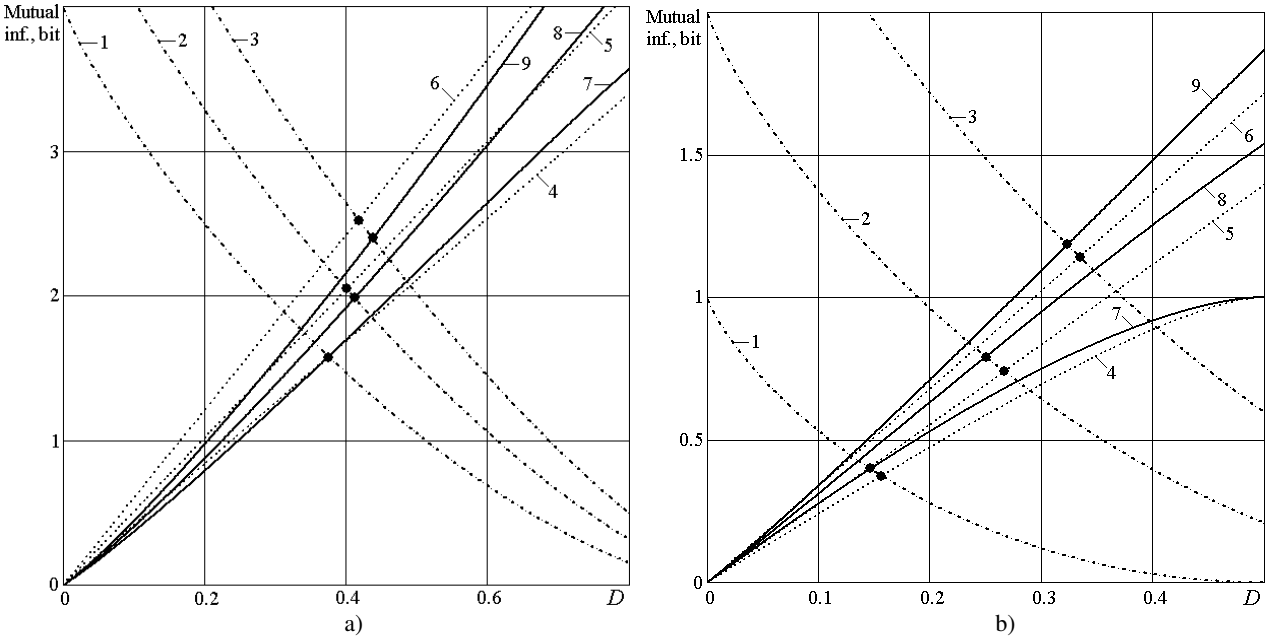

Fig 1. Mutual information for non-coherent attack. 1, 2, 3 – $I_{AB}(D)$ for d = 2, 4, 8 (a) and d = 16, 32, 64 (b); 4, 5, 6 – $I_{AE}^{(d+1)}(D)$ for d = 2, 4, 8 (a) and d = 16, 32, 64 (b); 7, 8, 9 – $I_{AE}^{(2)}(D)$ (6) for d = 2, 4, 8 (a) and d = 16, 32, 64 (b)

In figure 1 we can see that at low qudit dimension (up to d ~ 16) the protocol's security against non-coherent attack is higher when d+1 bases are used (when d = 2 it corresponds as noted above to greater security of six-state protocol than BB84 protocol). But the protocol's security is higher when two bases are used in the case of large d, while the difference in Eve's information (using d+1 or two bases) is not large in the work region of the

protocol, i.e. in the region of Alice's and Bob's low error level. We can conclude that the number of bases used has little influence on the security of the protocol against non-coherent attack (at least for the qudit dimension up to d = 64). The Crossing points of curves $I_{AB}(D)$ and $I_{AE}(D)$ correspond to boundary values D, up to which one's legitimate users can establish a secret key by means of a privacy amplification procedure (even when eavesdropping occurs) (Bennet *et al.* 1995).

Article E. V. Vasiliu *et al.* shows that the security of a protocol with qudits using two bases against intercept-resend attack is practically equal to the security of this protocol against non-coherent attack at any d (Vasiliu *et al.* 2009). At the same time, the security of the protocol using d+1 bases against this attack is much higher. Intercept-resend attack is the weakest of all possible attacks on QKD protocols, but on the other hand, the efficiency of the protocol using d+1 bases rapidly decreases as d increases. A protocol with quits using two bases therefore has higher security and efficiency than a protocol with using d+1 bases.

Another type of QKD protocol is a protocol using phase coding (Gisin *et al.* 2002). For example, the B92 protocol using strong reference pulses (Bennett *et al*. 1992). 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 (Fuchs *et al*. 1997). The efficiency of the B92 protocol is 25 %.

The Ekert protocol (E91) refers to QKD protocols using entangled states. Entangled pairs of qubits that are in a single state $|\psi^-\rangle = 1/\sqrt{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$ are used in this protocol (Ekert 1991; Gisin *et al.* 2002; Inamori *et al*. 2001). 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 (Ekert 1991). But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol (Inamori *et al*. 2001).

In article of D. Kaszlikowski *et al.* generalisation of the Ekert scheme for three-level quantum systems introduced and in the article of T. Durt, *et al*. generalisation of the Ekert scheme for d-level quantum systems is proposed: this increases the information capacity of the protocol a lot (Durt *et al.* 2004). Also in in the article of T. Durt *et al*. the security of the protocol using entangled qudits is investigated. In article of E. V. Vasiliu *et al*., based on the results of T. Durt *et al.*, the security comparison of protocol using entangled qudits and protocols using single qudits against non-coherent attack has been made (Durt *et al.* 2004; Vasiliu *et al*. 2001; Cerf *et al.* 2002). 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 that allow Bob to get the correct statistics of the photon number in pulses if Bob is controlling these statistics (Lutkenhaus *et al*. 2002).

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 (Branciard *et al.* 2005; Scarani *et al.* 2004; Scarani *et al.* 2009). 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 (Branciard *et al*. 2005).

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 (Brassard *et al*. 2000; Peng *et al.* 2007; Rosenberg *et al.* 2007; Scarani *et al.* 2009; Zhao *et al.* 2006). 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 (Peng *et al.* 2007; Rosenberg *et al.* 2007; Zhao *et al.* 2006). 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.

As a conclusion, after the analysis of the first and scale QTIS method, we must sum up and highlight the following 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 that 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 information security level increases. It is also possible to synthesize QKD protocols with Vernam cipher (one-time pad) that in complex with unconditionally secured authenticated schemes gives a totally secured system for transferring information.

The disadvantages of quantum key distribution 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; 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. When the channel length is 100 km, the data transfer rate equals few bps; 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 communication systems; 7) difficulty of the practical realisation of QKD protocols for *d*-level quantum systems; 8) the high price of commercial QKD systems.

3. Quantum secure direct communication

The next method of information security based on quantum technologies is the usages of quantum secure direct communication (QSDC) protocols (Boström *et al.* 2002; Boström *et al.* 2008; Bruss 1998; Cai *et al.* 2004b; Chuan *et al.* 2005; Wang *et al.* 2005; Zhang *et al.* 2005b; Василиу *и др*. 2006a; Василиу *и др*. 2006b; Василиу *и др.* 2006c). The main feature of QSDC protocols is that there are no cryptographic transformations; thus, there is no key distribution problem in QSDC. In these protocols, a secret message is coded by qubits' (qudits') quantum states, which are sent via quantum channel. QSDC protocols can be divided into several types: *ping-pong protocol (and its enhanced variants)*, *protocols using block transfer of entangled qubits*, *protocols using single qubits* and *protocols using entangled qudits* (Boström *et al.* 2002; Cai *et al.* 2004b; Василиу *и др*. 2006b; Василиу *и др*. 2006c; Chuan *et al.* 2005; Wang *et al.* 2005; Cai *et al.* 2004a). There are QSDC protocols for two parties and for multi-parties, e.g. broadcasting or when one user sends message to another under the control of a trusted third party.

Most contemporary protocols require a transfer of qubits by blocks (Chuan *et al.* 2005; Wang *et al.* 2005). This allows eavesdropping to be detected in the quantum channel before transfer of information. Thus, transfer will be terminated and Eve will not obtain any secret information. But for storing such blocks of qubits there is a need for a large amount of quantum memory. The technology of quantum memory is actively being researched, but it is still far from usage in common standard telecommunication equipment. So from the viewpoint of technical realisation, protocols using single qubits or their non-large groups (for one cycle of protocol) have an advantage. There are few such protocols and they have only asymptotic security, i.e. the attack will be detected with high probability, but Eve can obtain some part of information before detection. Thus, the problem of privacy amplification appears. In other words, new preprocessing methods of transferring information are needed. Such methods should make intercepted information negligible.

One of the quanta secure direct communication protocols is the ping-pong protocol (Boström *et al.* 2002; Cai *et al.* 2004b; Wang *et al.* 2005; Василиу *и др*. 2006b; Василиу *и др*. 2006c), which does not require qubit transfer by blocks. In the first variant of this protocol, entangled pairs of qubits and two coding operations that allow the transmission of one bit of classical information for one cycle of the protocol is used. The usage of quantum superdense coding allows transmitting two bits for a cycle (Cai *et al.* 2004b). The subsequent increase in the informational capacity of the protocol is possible by the usage instead of entangled pairs of qubits their triplets, quadruplets etc. in Greenberger-Horne-Zeilinger (GHZ) states (Василиу *и др*. 2006c). The informational capacity of the ping-pong protocol with GHZ-states is equal to *n* bits on a cycle where *n* is the number of entangled qubits. Another way of increasing the informational capacity of ping-pong protocol is using entangled states of qudits. Thus, the corresponding protocol based on Bell's states of three-level quantum system (qutrit) pairs and superdense coding for qutrits is introduced in the papers of Ch. Wang *et al*. and E. B. Василиу *и др.* (Wang *et al.* 2005; Василиу *и др.* 2009).

The advantages of QSDC protocols are a lack of secret key distribution, the possibility of data transfer between more than two parties, and the possibility of attack detection providing a high level of IS (up to information-theoretic security) for the protocols using block transfer. The main disadvantages are difficulty in practical realisation of protocols using entangled states (and especially protocols using entangled states for *d*-level quantum systems), slow transfer rate, the need for large capacity quantum memory for all parties (for protocols using block transfer of qubits), and the asymptotic security of the ping-pong protocol. Besides, QSDC protocols similarly to QKD protocols is vulnerable to man-in-the-middle attack, although such attack can be neutralized by using authentication of all messages, which are sent via the classical channel.

Asymptotic security of the ping-pong protocol (which is one of the simplest QSDC protocols from the technical viewpoint) can be amplified by using methods of classical cryptography. Security of several types of

ping-pong protocols using qubits and qutrits against different attacks was investigated in series of works (Boström *et al.* 2002; Cai *et al.* 2004b; Zhang *et al.* 2005a; Василиу *и др*. 2006b; Василиу *и др*. 2006c). The security of the ping-pong protocol using qubits against eavesdropping attack using ancilla states is investigated (Chuian *et al.* 2005; Василиу *и др*. 2006c). In figure 2 dependences of composite probability of not detecting an attack for the ping-pong protocol with many-qubit GHZ-states are shown. It is obvious from figure 2 that the ping-pong protocol with many-qubit GHZ-states is asymptotically secure at any number n of qubits that are in entangled GHZ-states. A similar result for the ping-pong protocol using Bell states of qutrit pairs is presented by E. В. Василиу *и др*. (Василиу *и др*. 2006b).

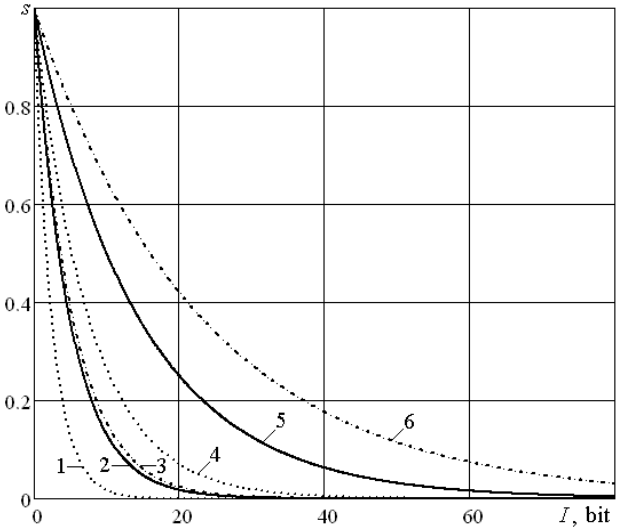

Fig 2. Composite probability of attack non-detection s for the ping-pong protocol with many-qubit GHZ-states: n=2, original protocol (1); n=2, with superdense coding (2); n=3 (3); n=5 (4); n=10 (5); n=16 (6). I is Eve's information

A non-quantum method of security amplification for the ping-pong protocol has been suggested by E. В. Василиу *и др*. (Василиу *и др*. 2006c). This method is as follows. Before the transmission, Alice divides the binary message on l block of some fixed length r; we will designate these blocks through a_i (i=1, …, l). Alice then generates for each block separately random invertible binary matrix K_i of size $r \times r$ and multiplies these matrices by appropriate blocks of the message $b_i = K_i a_i$ (multiplication is performed by modulo 2). Blocks b_i are transmitted on the quantum channel with the use of the ping-pong protocol. Even if Eve manages to intercept one (or more) from these blocks while remaining undetected, not knowing matrices K_i used, Eve cannot reconstruct source blocks a_i. To reach sufficient security level, the block length r and accordingly the size of matrices K_i should be selected so that Eve's probability of non-detection s after the transmission of one block is insignificant small. Matrices K_i are transmitted to Bob via usual (non-quantum) open authentic channel after the end of quantum transmission but only in the event that Alice and Bob are convinced of lack of eavesdropping. Bob then inverses the received matrices and having multiplied them on appropriate blocks b_i he gains the original message.

This method allows providing high security level of the ping-pong protocol (choosing suitable length of blocks for hashing). Rounded values of block length r for the ping-pong protocol with n-qubit GHZ-states at $s = 10^{-6}$ and for the case when Eve aspires to get all information and makes maximal error level for legitimate users are presented in table. The probability of detecting the attack is maximal in this case (Василиу *и др*. 2006c). The quantity of q is a probability of switching to control mode (Boström *et al.* 2002; Василиу *и др*. 2006c).

Table. Rounded values of block length r for the ping-pong protocol with n-qubit GHZ-states (bit)

n	$q = 0.5,\ d = d_{\max}$	$q = 0.25,\ d = d_{\max}$
2	69	180
3	74	186
4	88	216
5	105	254
6	123	297
7	142	341
8	161	387
9	180	434
10	200	481
11	220	529
12	240	577
13	260	625
14	279	673
15	299	721
16	319	769
17	339	817
18	359	865
19	379	913
20	399	961

Thus, after transfer of hashed block, the lengths of which are presented in table, the probability of attack non-detection will be equal to 10^{-6}; there is thus a very high probability that this attack will be detected. The main disadvantage of the ping-pong protocol, namely its asymptotic security against eavesdropping attack using ancilla states, is therefore removed.

There are some others attacks on the ping-pong protocol, e.g. attack that can be performed when the protocol is executed in quantum channel with noise (Zhang *et al.* 2005b). But there are some counteraction methods to these attacks (Boström *et al.* 2002). Thus, we can say that the ping-pong protocol (the security of which is amplified using method described above) is the most prospective QSDC protocol from the viewpoint of the existing development level of the quantum technology of information processing.

4. Other quantum methods of information security

Quantum secret sharing (QSS). Most QSS protocols use properties of entangled states (Bouwmeester *et al*. 2000; Nielsen *et al.* 2000). The first QSS protocol was proposed by Hillery, Buzek and Berthiaume in 1998 (Hillery *et al*. 1999; Qin *et al.* 2007). This protocol uses GHZ-triplets (quadruplets) similar to some QSDC protocols. The sender shares his message between two (three) parties and only cooperation allows them to read this message. Semi-quantum secret sharing protocol using GHZ-triplets (quadruplets) is proposed by Q. Li *et al.* (Li *et al.*). In this protocol, users that receive a shared message have access to the quantum channel. But they are limited by some set of operation and are called 'classical', meaning they are not able to prepare entangled states and perform any quantum operations or measurements. These users can measure qubits on a 'classical' $\{|0\rangle,|1\rangle\}$ basis, reordering the qubits (via proper delay measurements), preparing (fresh) qubits in the classical basis, and sending or returning the qubits without disturbance. The sending party can perform any quantum operations. This protocol prevails over others QSS protocols in economic terms. Its equipment is cheaper because expensive devices for preparing and measuring (in GHZ-basis) many-qubit entangled states are not required. Semi-quantum secret sharing protocol exists in two variants: randomisation-based and measurement-resend protocols. In article of Zh.-J. Zhang *et al.* QSS using single qubits that are prepared in two mutually unbiased bases and transferred by blocks is presented (Zhang *et al* 2005a.). Similar to the Hillery-Buzek-Berthiaume protocol, this allows sharing a message between two (or more) parties. The security improvement of this protocol against malicious acts of legitimate users is presented by F. G. Deng *et al*. (Deng *et al*. 2005). A similar protocol for multiparty secret sharing is presented in article of F.- L. Yan *et al.* (Yan *et al*. 2008). QSS protocols are protected against external attackers and unfair actions of the protocol's parties. Both quantum and semi-quantum schemes allow detecting eavesdropping and do not require encryption unlike the classical secret-sharing schemes. The most significant imperfection of QSS protocols is the necessity for large quantum memory that is outside the capabilities of modern technologies today.

Quantum stream cipher (QSC) provides data encryption similar to classical stream cipher, but it uses quantum noise effect and can be used in optical communication networks (Hirota *et al.* 2005). QSC is based on the Yuen-2000 protocol (Y-00, $\alpha\eta$ - scheme). Information-theoretic security of the Y-00 protocol is ensured by randomisation (based on quantum noise) and additional computational schemes In articles of E. Corndorf *et al.* and Hirota *et a.l* high encryption rate of the Y-00 protocol is demonstrated experimentally, a security analysis on the Yuen-2000 protocol against the fast correlation attack, the typical attack on stream ciphers, is presented (Corndorf *et al.* 2005; Hirota *et al*. 2000). The next advantage is better security compared with usual (classical) stream cipher. This is achieved by quantum noise effect and by the impossibility of cloning quantum states (Wooters *et al.* 1982). The complexity of practical implementation is the most important imperfection of QSC (Hirota *et al*. 2000).

Quantum digital signature (QDS) can be implemented on the basis of protocols such as QDS protocols using single qubits and QDS protocols using entangled states (authentic QDS based on quantum GHZ-correlations) (Wang *et al.* 2006; Xiao-Jun *et al.*). QDS is based on use of the quantum one-way function (Gottesman *et al*.). This function has better security than the classical one-way function, and it has information-theoretic security (its security does not depend on the power of the attacker's equipment). Quantum one-way function is defined by the following properties of quantum systems (Gottesman *et al*.): 1) qubits can exist in superposition 0 and 1 unlike classical bits; 2) we can get only a limited quantity of classical information from quantum states (according to the Holevo theorem) (Holevo 1977, Nielsen *et al.* 2000). Calculation and validation are not difficult but inverse calculation is impossible. In the systems that use QDS, user identification and integrity of information is provided similar to classical digital signature (Gottesman *et al*.). The main advantages of QDS protocols are information-theoretic security and simplified key distribution system. The main disadvantage is the possibility to generate a limited number of public key copies and the leak of some quantities of information about incoming data of quantum one-way function (unlike the ideal classical one-way function) (Gottesman *et al*.).

Quantum steganography aims to hide the fact of information transferral similar to classical steganography (Imai *et al.* 2006). In the articles of M. Curty *et al.* and H. Imai *et al.* models of quantum steganography systems are proposed, but there is no case of the practical implementation of these systems (Curty *et al.* 2000; Imai *et al.* 2006). All current models of quantum steganography systems use entangled states. For example, modified methods of entangled photon pair detection are used to hide the fact of information transfer in patent of R. S. Conti *et al.* (Conti *et al.* 2004). Theoretical research in this area has not reached the level of practical application yet, and it is very difficult to talk about the advantages and disadvantages of quantum steganography systems. Whether quantum steganography is superior to the classical one or not in practical use is still an open question (Imai *et al.* 2006).

Figure 3 represents a general scheme of quantum methods of IS for their purposes and for using QTIS.

5. Commercial QKD systems

The world`s first commercial quantum cryptography solution was QPN Security Gateway (QPN-8505) proposed by MagiQ Technologies (USA) (QPN…). This system 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

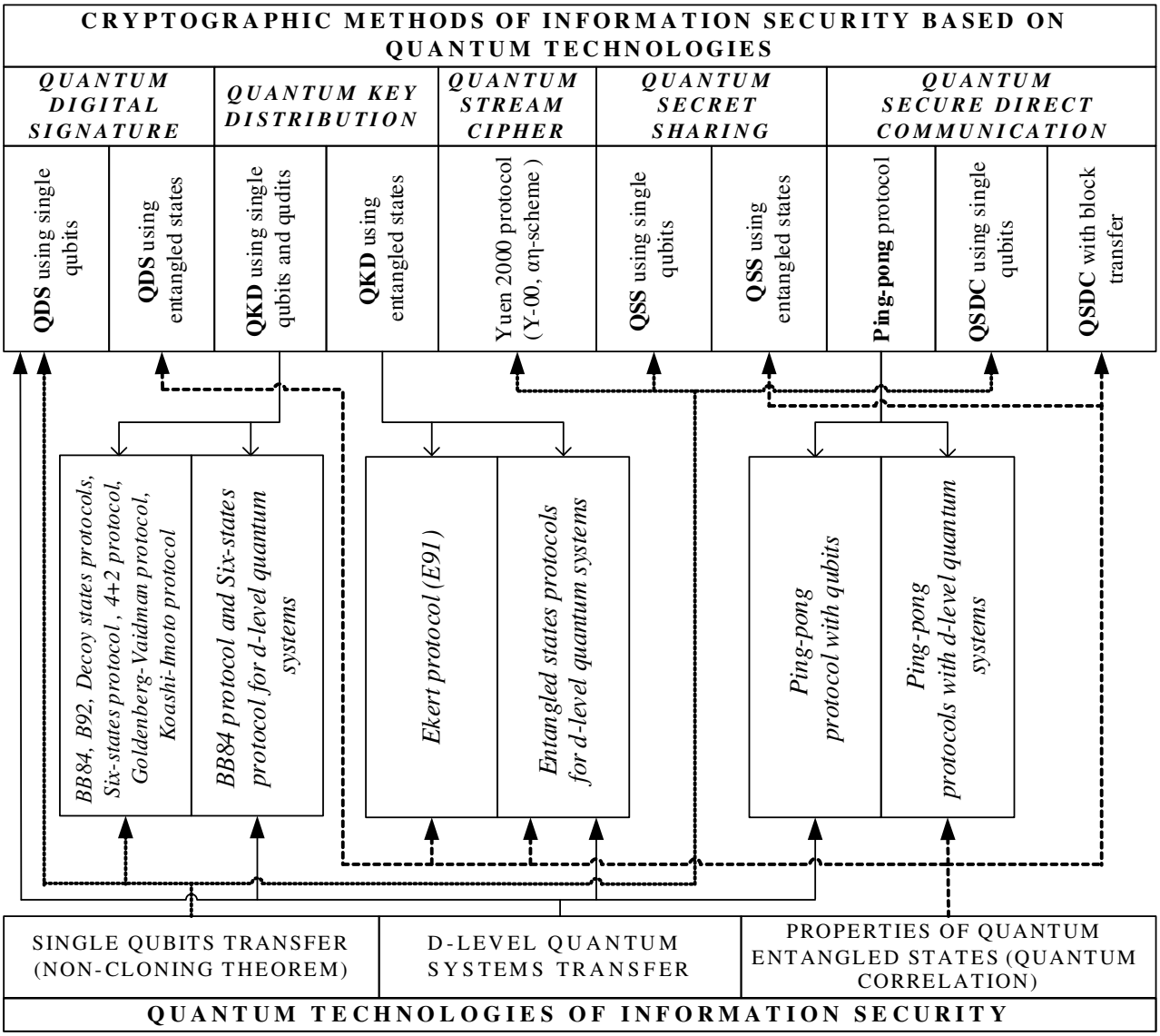

Fig 3. Classification of quantum methods of IS

km) and integrated encryption. The QPN-8505 system uses BB84, 3DES and AES protocols (NIST…1999, NIST…2001). The Swiss company Id Quantique offers a system called "Cerberis" (Cerberis…). It 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. Toshiba Research Europe Ltd (Great Britain) recently presented another QKD system named Quantum Key Server (QKS…). This system has a very simple architecture and provides up to 100 256-bit keys per second with their one-way transferring from sender to receiver. Quantum Key Server includes an integrated automatic control module that provides continuous monitoring and regulation of the system's optical characteristics. Another British company, QinetiQ, realised the world's first network using quantum cryptography – Quantum Net (Qnet) (Elliot *et al*., Hughes *et al.* 2002). The maximum length of communication lines in this network is 120 km. And 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 addition the world's leading scientists are actively taking part in the implementation of projects such as SEC OQC (Secure Communication based on Quantum Cryptography) and EQCSPOT (European Quantum Cryptography and Single Photon Technologies). (SECOQC…). There are many practical and theoretical research projects concerning the development of QTIS in research institutes, laboratories and centres (Northwestern University, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, ARS Seibersdorf Research, Los Alamos National Laboratory) (Алексеев *и др.* 2007).

Most methods and facilities of quantum cryptography are patented in different countries and have the prospect to be realised in the near future (Bennett *et al.*

1996; Dultz *et al.* 2004; Duraffourg *et al*. 2007; Elliot *et al*. 2005; Gisin *et al.* 2002; Matsumoto *et al*. 2008; Takeuchi *et al.* 2007; Tomita *et al*. 2005; Wang *et al.* 2003; Гнатюк *и др*. 2009; Молотков *и др*. 2005; Молотков *и др*. 2006).

6. Conclusions

This article presents a classification and systematisation of modern quantum technology of information security. The characteristic of the basic directions of quantum cryptography from the point of view of the quantum technologies used is given. A qualitative analysis of the advantages and imperfections of concrete quantum protocols is made. 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. Most of the technologies used in these systems are patented in different countries (mainly in the U.S.A.). 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 IS level than appropriate classical schemes.

Other quantum technologies of information security (QTIS) in practice have not yet extended beyond laboratory experiments. But there are many theoretical cryptographic schemes that provide high IS level up to the information-theoretic security. Quantum secure direct communication protocols do not have any analogues in classical cryptography. These protocols remove the secret key distribution problem because they do not use encryption. One of these is the ping-pong protocol and its improved versions. These protocols can provide high IS level of confidential data transmission using the existing level of technology with security amplification methods. Another category of QSDC is protocols with transfer qubit by blocks that have unconditional security, but these need a large quantum memory that is outside the capabilities of modern technologies today. It should be noted that QSDC protocols are not suitable for the transfer of a high-speed flow of confidential data because there is low data transfer rate in the quantum channel. But when a high IS level is more important than transfer rate, QSDC protocols should find its application.

Quantum secret sharing protocols allow detecting eavesdropping and do not require data encryption. This is their main advantage over classical secret sharing schemes. Similarly, quantum stream cipher and quantum digital signature provide higher security level than classical schemes. Quantum digital signature has information-theoretic security because it uses quantum one-way function. However, practical implementation of these QTIS is also faced with some technological difficulties.

Thus, in recent years QTIS are rapidly developing and gradually taking their place among other means of IS. Their advantage is 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. QTIS therefore represent an important step towards improving the security of communication systems against cyber-terrorist attacks. But many theoretical and practical problems must be solved for practical the use of QTIS in existing communication systems.

References

Barbosa, G. A.; Corndorf, E.; Kumar, P. *et al*. 2003. Secure Communication Using Mesoscopic Coherent States, *Physical Review Letters* 90(22): 227901.

Bennett, C. H.; Brassard, G. 1984. Quantum cryptography: public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India, 175–179.

Bennett, C. H.; Brassard, G.; Crépeau, C. *et al*. 1995. Generalized privacy amplification, *IEEE Transactions on Information Theory* 41(6): 1915–1923.

Bennett, C. H. 1992. Quantum cryptography using any two non-orthogonal states, *Physical Review Letters*. 68(21): 3121–3124.

Bennett, C. H.; Bessette, F.; Brassard, G. *et al.* 1992. Experimental Quantum Cryptography, *Journal of Cryptography*. 5(1): 3–28.

Bennett, C.H.; Charles, H. 1996 04 26. *Interferometric Quantum Cryptographic Key Distribution System.* Patent No 5307410 USA, H04B 10/142 (20060101); H04L 9/08 (20060101).

Boström, K.; Felbinger, T. 2002. Deterministic secure direct communication using entanglement, *Physical Review Letters*, 89(18): 187902.

Boström, K.; Felbinger, T. 2008. On the security of the ping-pong protocol, *Physics Letters A*. 372(22): 3953–3956.

Bouwmeester, D.; Ekert, A.; Zeilinger, A. 2000. *The Physics of Quantum Information. Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Berlin: Springer-Verlag, 314.

Branciard, C.; Gisin, N.; Kraus, B. *et al*. 2005. Security of two quantum cryptography protocols using the same four qubit states, *Physical Review A*. 72(3): 032301.

Brassard, G.; Lutkenhaus, N.; Mor, T. *et al*. 2000. Limitations on practical quantum cryptography, *Physical Review Letters* 85(6): 1330–1333.

Bruss, D. 1998. Optimal eavesdropping in quantum cryptography with six states, *Physical Review Letters*, 81(14): 3018–3021.

Cai, Q.-Y., Li, B.-W. 2004a. Deterministic secure communication without using entanglement, *Chin. Phys. Lett*. 21(4): 601–603.

Cai, Q.-Y.; Li B.-W. 2004b. Improving the capacity of the Bostrom–Felbinger protocol, *Physical Review A*. 69(5): 054301.

Cerberis [online]. Available from Internet: <http://idquantique.com/products/cerberis.htm>.

Cerf, N. J.; Bourennane, M.; Karlsson, A.; *et al*. 2002. Security of quantum key distribution using d-level systems, *Physical Review Letters*. 88(12): 127902.

Chuan, W.; Fu Guo, D.; Gui Lu, L. 2005. Multi-step quantum secure direct communication using multi-particle Greenberg-Horne-Zeilinger state, *Optics Communications* 253: 15–19.

Conti; Ralph, S.; Kenneth A. *et al.* 2004 05 21. *Quantum Steganography.* Patent No 7539308 USA, H04K 1/00 (20060101).

Corndorf, E., Liang, C., Kanter, G.S. *et al.* 2005. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks, *Physical Review A*. 71(6): 062326.

Curty, M.; Santos, D. J. 2000. Quantum steganography, in *2nd Bielefeld Workshop on Quantum Information and Complexity*, Bielefeld, Germany, 12.

Deng, F. G.; Li, X. H.; Zhou, H. Y. *et al*. 2005. Improving the security of multiparty quantum secret sharing against Trojan horse attack, *Physical Review A*. 72(4): 044302.

Desurvire, E. 2009. *Classical and Quantum Information Theory*. Cambridge: Cambridge University Press, 691.

Dultz; Wolfgang, S. *et al*. 2004 06 08. Quantum Cryptography System For a Secure Transmission of Random Keys Using a Polarization Setting Method. Patent No 6748081 USA, H04L 9/08 (20060101), C09K 19/02 (20060101), G02F 1/13 (20060101).

Duraffourg; Laurent, M. *et al*. 2007 09 04. System For Secure Optical Transmission of Binary Code. 04.09.2007. Patent No 7266304 USA, H04B 10/00 (20060101), H04K 1/00 (20060101).

Durt, T.; Kaszlikowski, D.; Chen, J.-L. *et al.* 2004. Security of quantum key distributions with entangled qudits, *Physical Review A*. 69(3): 032313.

Ekert, A. 1991. Quantum cryptography based on Bell's theorem, *Physical Review Letters*. 67(6): 661–663.

Elliot, C.; Pearson, D.; Troxel, G. Quantum Cryptography in Practice, in *arXiv:quant-ph/0307049.*

Elliot, C.; Brig, B. *et al.* 2005 05 17. *Systems and Methods for Encryption Key Archival and Auditing in a Quantum-Cryptographic Communications Network.* Patent No 6895091 USA, H04L 9/08 (20060101).

Fuchs, C.; Gisin, N.; Griffits, R. *et al*. 1997. Optimal eavesdropping in quantum cryptography. Information bound and optimal strategy, *Physical Review A*. 56(2): 1163–1172.

Gisin, N.; Ribordy, G.; Tittel, W *et al*. 2002. Quantum cryptography, *Review of Modern Physics* 74: 145–195.

Gisin, N.; Zbinden, H. *et al.* 2002 08 20. *Quantum Cryptography Device and Method.* Patent No 6438234 USA, H04L 9/08 (20060101), H04K 001/00.

Goldenberg, L.; Vaidman, L. 1995. Quantum cryptography based on orthogonal states, *Physical Review Letters* 75(7): 1239–1243.

Gottesman, D.; Chuang, I. Quantum digital signatures, in *arXiv:quant-ph/0105032v2*.

Hillery, M.; Buzek, V.; Berthiaume, A. 1999. Quantum secret sharing, *Physical Review A*. 59(3): 1829–1834.

Hirota, O.; Kurosawa, K. An immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol, in *arXiv:quant-ph/0604036v1.*

Hirota, O.; Sohma, M.; Fuse, M. *et al.* 2005. Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme, *Physical Review A*. 72(2): 022335.

Holevo, A. S. 1977. Problems in the mathematical theory of quantum communication channels, *Report of Mathematical Physics* 12(2): 273–278.

Hughes, R.; Nordholt, J.; Derkacs, D. *et al.* 2002. Practical free-space quantum key distribution over 10 km in daylight and at night, *New Journal of Physics* 4: 43.

Huttner, B.; Imoto, N.; Gisin, N.; *et al.* 1995. Quantum Cryptography with Coherent States, *Physical Review A*. 51(3): 1863–1869.

Imai, H.; Hayashi, M. *et al*. 2006. *Quantum Computation and Information. From Theory to Experiment*. Berlin: Springer-Verlag, Heidelberg, 235.

Inamori, H.; Rallan, L.; Vedral, V. 2001. Security of EPR-based quantum cryptography against incoherent symmetric attacks, *Journal of Physics A*. 34(35): 6913–6918.

Kaszlikowski, D.; Christandl, M. *et al.* 2003. Quantum cryptography based on qutrit Bell inequalities, *Physical Review A*. 67(1): 012310.

Koashi, M.; Imoto, N. 1997. Quantum cryptography based on split transmission of one-bit information in two steps, *Physical Review Letters* 79(12): 2383–2386.

Li, Q.; Chan, W. H.; Long, D-Y. Semi-quantum secret sharing using entangled states, in *arXiv:quant-ph/0906.1866v3*.

Lutkenhaus, N.; Jahma, M. 2002. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, *New Journal of Physics* 4: 44.1–44.9.

Matsumoto; Wataru, W. *et al.* 2008 12 02. *Quantum Key Delivery Method and Communication Device.* Patent No 7461323 USA, H03M 13/00 (20060101).

Nair, R.; Yuen, H. P. On the security of the Y-00 (AlphaEta) direct encryption protocol, in *arXiv:quant-ph/0702093v2.*

Nielsen, M. A.; Chuang, I. L. 2000. *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press, 676 p.

NIST. “FIPS-197: Advanced Encryption Standard.” 2001. [online]. Available from Internet: <http://csrc.nist.gov/publications/fips>.

NIST. “FIPS-46-3: Data Encryption Standard.” 1999. [online]. Available from Internet: <http://csrc.nist.gov/publications/fips>.

Peng, C.-Z.; Zhang, J.; Yang, D. *et al*. 2007. Experimental long-distance decoy-state quantum key distribution based on polarization encoding, *Physical Review Letters*. 98(1): 010505.

Qin, S.-J.; Gao, F.; Zhu, F.-Ch. 2007. Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol, *Physical Review A*. 76(6): 062324.

QKS. Toshiba Research Europe Ltd. [online]. Available from Internet: <http: //www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html>.

QPN Security Gateway (QPN – 8505) [online]. Available from Internet: <http: //www.magiqtech.com/MagiQ/Products.html>.

Rosenberg, D. *et al*. 2007. Long-distance decoy-state quantum key distribution in optical fiber, *Physical Review Letters* 98(1): 010503.

Scarani, V.; Acin, A.; Ribordy, G. *et al.* 2004. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, *Physical Review Letters* 92(5): 057901.

Scarani, V.; Bechmann-Pasquinucci, H.; Nicolas, J. *et al.* 2009. The security of practical quantum key distribution, *Review of Modern Physics*, 81: 1301–1350.

SECOQC White Paper on quantum key distribution and cryptography, in *arXiv:quant-ph/0701168v1*.

Takeuchi; Takeshi *et al.* 2007 02 20. *Quantum Cryptography Communication System And Quantum Cryptography Key Distributing Method Used In The Same*. Patent No 7178277 USA, H04K 1/00 (20060101).

Tomita, Akihisa *et al.* 2005 05 17. *Cryptographic Key Distribution Method and Apparatus Thereof*. Patent No 6895092 USA, H04L 9/08 (20060101), G06F 017/00.

Vasiliu, E. V.; Mamedov, R. S. 2009. Comparative analysis of security and efficiency of quantum key distribution protocols with qudits, in *Proceedings of International Conference on IT Promotion in Asia '2009*. Tashkent University of IT, Tashkent, 200–203.

Wang, Ch.; Deng, F.-G.; Li, Y.-S. *et al.* 2005. Quantum secure direct communication with high dimension quantum superdense coding, *Physical Review A*. 71(4): 044305.

Wang, J.; Zhang, Q.; Tang, C. 2006. Quantum signature scheme with single photons, *Optoelectronics Letters* 2(3): 209–212.

Wang; Lijun. 2003 02 18. *Quantum Cryptographic Communication Channel Based On Quantum Coherence.* Patent No 6522749 USA, H04L 9/08 (20060101).

Wooters, W. K.; Zurek, W. H. 1982. A single quantum cannot be cloned, *Nature* 299: 802.

Xiao-Jun, W.; Yun, L. Authentic digital signature based on quantum correlation, in *arXiv:quant-ph/0509129v2*.

Yan, F.-L.; Gao, T.; Li, Yu.-Ch. 2008. Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations, *Chinese Physics Letters* 25(4): 1187–1190.

Zhang, Zh.-J.; Li, Y.; Man, Zh.-X. 2005a. Multiparty quantum secret sharing, *Physical Review A*. 71(4): 044301.

Zhang, Zh.-J.; Li, Y.; Man, Zh.-X. 2005b. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss, *Physics Letters A*. 341(5–6): 385–389.

Zhao, Y.; Qi, B.; Ma, X. *et al*. 2006. Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber, in *Proceedings of IEEE International Symposium on Information Theory*: 2094–2098.

Алексеев, Д. А.; Корнейко, А. В. 2007. Практическая реальность квантово-криптографических систем распределения ключей, [Alekseev, D. A.; Korneyko, A. V. Practice reality of quantum cryptography key distribution systems], *Захист інформації* [*Information Security*], (1): 72–76. (in Russian).

Бабак, В. П.; Харченко, В. П.; Максимов, В. О. *et al.* 2004. *Безпека Авіації* [Babak, V. P.; Kharchenko, V. P.; Maksymov, V. O. *et al. Aviation Security.*]. К.: Техніка, 584 с. (in Ukrainian).

Василиу, Е. В.; Воробиенко, П. П. 2006a. Проблемы развития и перспективы использования квантово-криптографических систем [Vasiliu, E. V.; Vorobiyenko, P. P. The development problems and using prospects of quantum cryptographic systems], *Наук. праці ОНАЗ ім. О.С. Попова* [*Scientific works of the Odessa national academy of telecommunications named after O.S. Popov*] (1): 3–17. (in Russian).

Василиу, Е. В.; Мамедов, Р. С. 2009b. Анализ атаки пассивного перехвата на пинг–понг протокол с полностью перепутанными парами кутритов [Vasiliu, E. V.; Mamedov, R. S. Analysis of eavesdropping attack on the ping-pong protocol with completely entangled qutrit pairs], *Восточноевропейский журнал передовых технологий* [*Eastern-European Journal of Enter-prise Technologies*] 4/2(40): 4–11]. (in Russian).

Василиу, Е. В.; Николаенко, С. В. 2009c. Синтез основанной на пинг–понг протоколе квантовой связи безопасной системы прямой передачи сообщений [Vasiliu, E. V.; Nikolaenko, S. V. Synthesis if the secure system of direct message transfer based on the ping–pong protocol of quantum communication], *Наук. праці ОНАЗ ім. О.С. Попова [Scientific works of the Odessa National Academy of Telecommunications, named after O.S. Popov*] (1): 83–91]. (in Russian).

Гнатюк, С. О.; Кінзерявий, В. М.; Корченко, О. Г.*и др*. 2009 08 25. *Система передачі криптографічних ключів* [Gnatyuk, S. O.; Kinzeryavyy, V. M.; Korchenko, O. G. *et al*. System for cryptographic key transfer], Патент № 43779 України, МПК H04L 9/08 [Patent No 43779 UA, MPK H04L 9/08. (in Ukrainian).

Энциклопедия безопасности авиации [*Encyclopedia of Aviation Security*] 2008. Под. ред. Н. С. Кулика *и др*. [Edited by N. S. Kulik *et al*.]. Kiev, 1000 с. (in Russian).

Молотков, С.; Кулик, С. 2005 11 16. *Спосіб кодування та передачі криптографічних ключів* [Molotkov, S.; Kulik, S. *Method of Cryptographic Key Coding and Transfer*], Патент № 2302085 RU, H04L9/00 [Patent No 2302085 RU, H04L9/00. (in Russian).

Молотков, С.; Кулик, С. 2006 06 06. *Спосіб кодування та передачі криптографічних ключів* [Molotkov, S.; Kulik, S. *Method of Cryptographic Key Coding and Transfer*], Патент № 2325039 RU, H04L9/00 [Patent No 2325039 RU, H04L9/00]. (in Russian).

NFORMACIJOS SAUGUMĄ UŽTIKRINANČIOS MODERNIOSIOS KVANTINĖS TECHNOLOGIJOS, NUKREIPTOS PRIEŠ KOMPIUTERINIŲ TERORISTŲ ATAKAS

O. Korchenko, Y. Vasiliu, S. Gnatyuk

S a n t r a u k a

Šiame darbe susistemintos ir suklasifikuotos informacijos saugumą užtikrinančios moderniosios kvantinės technologijos, skirtos apsisaugoti nuo kompiuterių teroristų atakų. Remiantis kvantinėmis technologijomis, aprašyta pagrindinių kvantinės kriptografijos krypčių charakteristika. Pateikti konkrečių kvantinių protokolų kokybinės analizės privalumai ir trūkumai. Taip pat aptartas telekomunikaciniuose tinkluose naudojamos dabartinės kvantinės kriptografijos problemos statusas. Pateikta trumpa kvantinių raktų pasiskirstymo dabartinėse komercinėse sistemose apžvalga.

Reikšminiai žodžiai: informacijos saugumas, kvantinės technologijos, kvantinių raktų pasiskirstymas, kvantiniu pagrindu apsaugotas tiesioginis ryšys, slaptas kvantų paskirstymas, kvantinio srauto šifras, kvantais užkoduotas skaitmeninis parašas, kvantinė steganografija.