# 9

# Quantum Secure Telecommunication Systems

Oleksandr Korchenko[1], Petro Vorobiyenko[2],
Maksym Lutskiy[1], Yevhen Vasiliu[2] and Sergiy Gnatyuk[1]
*[1]National Aviation University*
*[2]Odessa National Academy of Telecommunication named after O.S. Popov*
*Ukraine*

*Our scientific field is still in its embryonic stage. It's great that we haven't been around for two thousands years. We are still at a stage where very, very important results occur in front of our eyes*
Michael Rabin

## 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 power plants, and control aircraft, satellites and spacecraft. The high level of automation therefore depends on the security level of IT.

The main features of information security are confidentiality, integrity and availability. Only providing these all gives availability for development secure telecommunication systems. *Confidentiality* is the basic feature of information security, which ensures that information is accessible only to authorized users who have an access. *Integrity* is the basic feature of information security indicating its property to resist unauthorized modification. *Availability* is the basic feature of information security that indicates accessible and usable upon demand by an authorized entity.

One of the most effective ways to ensure confidentiality and data integrity during transmission is cryptographic systems. 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 (SECOQC White Paper on Quantum Key Distribution and Cryptography, 2007; Korchenko et al., 2010a):

- *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).

In recent years, quantum cryptography (QC) has attracted considerable interest. Quantum key distribution (QKD) (Bennett, 1992; Bennett et al., 1992; Bennett et al., 1995; Bennett & Brassard, 1984; Bouwmeester et al., 2000; Gisin et al., 2002; Lütkenhaus & Shields, 2009; Scarani et al., 2009; Vasiliu & Vorobiyenko 2006; Williams, 2011) 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 (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 quantum technologies with full efficiency. The main purpose of this chapter is the systematisation and classification of up-to-date effective quantum technologies of data (transmitted via telecommunication channels) security, analysis of their strengths and weaknesses, prospects and difficulties of implementation in telecommunication systems.

The first of all *quantum technologies of information security* consist of (Korchenko et al., 2010b):

- 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. Bouwmeester et al., 2000; Gisin et al., 2002; Hayashi, 2006; Imre & Balazs, 2005; Kollmitzer & Pivk, 2010; Lomonaco, 1998; Nielsen & Chuang, 2000; Schumacher & Westmoreland, 2010; Vedral, 2006; Williams, 2011).

## 2. Main approaches to quantum secure telecommunication systems construction

### 2.1 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, 1992; Bennett et al., 1992; Bourennane et al., 2002; Bruss & Macchiavello, 2002; Cerf et al., 2002; Gnatyuk et al., 2009); protocols using phase coding (Bennett, 1992); protocols using entangled states (Ekert, 1991; Durt et al., 2004); decoy states protocols (Brassard et al., 2000; Liu et al., 2010; Peng et al., 2007; Yin et al., 2008; Zhao et al., 2006a, 2006b); and some

other protocols (Bradler, 2005; Lütkenhaus & Shields, 2009; Navascués & Acín, 2005; Pirandola et al., 2008).

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. Bennett from IBM and G. Brassard from Montreal University introduced the first QKD protocol (Bennett & Brassard, 1984), which has become an alternative solution for the problem of key distribution. This protocol is called *BB84* (Bouwmeester et al., 2000) and it refers to QKD protocols using single qubits. The states of these qubits are the polarisation states of single photons. The BB84 protocol uses four polarisation states of photons (0°, 45°, 90°, 135°). These states refer to two mutually unbiased bases. Error searching and correcting is performed using classical public channel, which need not be confidential but only authenticated. For the detection of intruder actions in the BB84 protocol, an error control procedure is used, and for providing unconditionally security a privacy amplification procedure is used (Bennett et al., 1995). 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 (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 base are selected non-orthogonal. Moreover, states in different bases must also be pairwise non-orthogonal. This protocol has a higher information security level than the BB84 protocol, when weak coherent pulses, but not a single photon source, are used by sender (Huttner et al., 1995). But the efficiency of the 4+2 protocol is lower than efficiency of BB84 protocol.

In the *Goldenberg-Vaidman protocol* (Goldenberg & Vaidman, 1995), 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* (Koashi & Imoto, 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 protocol security is Shannon's mutual information between legitimate users (Alice and Bob) and an eavesdropper (Eve): $I_{AE}(D)$ and $I_{BE}(D)$, where $D$ is error level which 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.). 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 (see e.g. Cerf et al., 2002). Vasiliu & Mamedov have carried out a comparative analysis of the efficiency and security of different protocols using qudits on the basis of known formulas for mutual information (Vasiliu & Mamedov, 2008).

In fig. 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 and $I_{AE}^{(d+1)}(D)$ and $I_{AE}^{(2)}(D)$ is mutual information between Alice and Eve for protocols using $d$+1 and two bases accordingly.

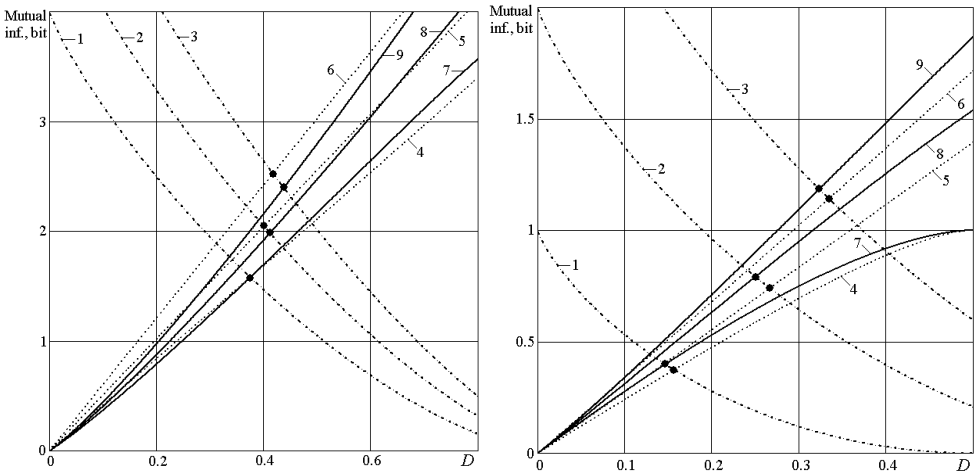


Fig. 1. Mutual information for non-coherent attack. 1, 2, 3 — $I_{AB}(D)$ for $d$ = 2, 4, 8 (a) and $d$ = 16, 32, 64 (b); 4, 5, 6 — $I_{AE}^{(d+1)}(D)$ for $d$ = 2, 4, 8 (a) and $d$ = 16, 32, 64 (b); 7, 8, 9 — $I_{AE}^{(2)}(D)$ for $d$ = 2, 4, 8 (a) and $d$ = 16, 32, 64 (b).

In fig. 1 we can see that at low qudit dimension (up to $d \sim 16$) 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. That's why 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) (Bennett et al., 1995).

It is shown (Vasiliu & Mamedov, 2008) 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 $d$. 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 qudits using two bases therefore has higher security and efficiency than a protocol using $d$+1 bases.

Another type of QKD protocol is a *protocol using phase coding*: for example, the *B92 protocol* (Bennett, 1992) using strong reference pulses (Gisin et al., 2002). 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)* (Ekert, 1991) refers to QKD protocols using entangled states. Entangled pairs of qubits that are in a singlet state $\left|\psi^-\right\rangle = 1/\sqrt{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$ are used in this protocol. Qubit interception between Alice to Bob does not give Eve any information because no coded information is there. Information appears only after legitimate users make measurements and communicate via classical public authenticated channel (Ekert, 1991). But attacks with additional quantum systems (ancillas) are nevertheless possible on this protocol (Inamori et al., 2001).

Kaszlikowski et al. carried out the generalisation of the Ekert scheme for three-level quantum systems (Kaszlikowski et al., 2003) and Durt et al. carried out the generalisation of the Ekert scheme for $d$-level quantum systems (Durt et al., 2004): this increases the information capacity of the protocol a lot. Also the security of the protocol using entangled qudits is investigated (Durt et al., 2004). In the paper (Vasiliu & Mamedov, 2008), based on the results of (Durt et al., 2004), the security comparison of protocol using entangled qudits and protocols using single qudits (Cerf et al., 2002) 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 (Lutkenhaus & Jahma, 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* (Brassard et al., 2000; Peng et al., 2007; Rosenberg et al., 2007; Zhao et al., 2006), 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 (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 quantum 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, 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 information security level increases. It is also possible to synthesize QKD protocols with Vernam cipher (one-time pad) which in complex with unconditionally secured authenticated schemes gives a totally secured system for transferring information.

The disadvantages of 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. However, the technology of quantum repeaters could overcome this limitation in the near future (Sangouard et al., 2011).
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.

### 2.2 Quantum secure direct communication

The next method of information security based on quantum technologies is the usage of *quantum secure direct communication (QSDC) protocols* (Boström & Felbinger, 2002; Chuan et al., 2005; Cai, 2004; Cai & Li, 2004a; Cai & Li, 2004b; Deng et al., 2003; Vasiliu, 2011; Wang et al., 2005a, 2005b). 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)* (Boström & Felbinger, 2002; Cai & Li, 2004b; Chamoli & Bhandari, 2009; Gao et al., 2008; Ostermeyer & Walenta, 2008;Vasiliu & Nikolaenko, 2009; Vasiliu, 2011).
- *Protocols using block transfer of entangled qubits* (Deng et al., 2003; Chuan et al., 2005; Gao et al., 2005; Li et al., 2006; Lin et al., 2008; Xiu et al., 2009; Wang et al., 2005a, 2005b).
- *Protocols using single qubits* (Cai, 2004; Cai & Li, 2004a).
- *Protocols using entangled qudits* (Wang et al., 2005b; Vasiliu, 2011).

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 developed, 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 pre-processing methods of

transferring information are needed. Such methods should make intercepted information negligible.

One of the quantum secure direct communication protocols is the ping-pong protocol (Boström & Felbinger, 2002; Cai & Li, 2004b; Vasiliu, 2011), 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 are used (Boström & Felbinger, 2002). The usage of quantum superdense coding allows transmitting two bits for a cycle (Cai & Li, 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 (Vasiliu & Nikolaenko, 2009). 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 (Wang et al., 2005; Vasiliu, 2011).

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 information security (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 papers (Boström & Felbinger, 2002; Cai, 2004; Vasiliu, 2011; Vasiliu & Nikolaenko, 2009; Zhang et al., 2005a).

The security of the ping-pong protocol using qubits against eavesdropping attack using ancilla states is investigated in (Boström & Felbinger, 2002; Chuan et al., 2005; Vasiliu & Nikolaenko, 2009).

Eve's information at attack with usage of auxiliary quantum systems (probes) on the ping-pong protocol with entangled $n$-qubit GHZ-states is defined by von Neumann entropy (Boström & Felbinger, 2002):

$$I_0 = S(\rho) \equiv -Tr\{\rho \log_2 \rho\} = -\sum_i \lambda_i \log_2 \lambda_i \tag{1}$$

where $\lambda_i$ are the density matrix eigenvalues for the composite quantum system "transmitted qubits - Eve's probe".

For the protocol with Bell pairs and quantum superdence coding the density matrix $\rho$ have size 4x4 and four nonzero eigenvalues:

$$\begin{aligned}\lambda_{1,2} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2d(1-d)},\\ \lambda_{3,4} &= \frac{1}{2}(p_3+p_4) \pm \frac{1}{2}\sqrt{(p_3+p_4)^2 - 16p_3p_4d(1-d)}.\end{aligned} \tag{2}$$

For the protocol with GHZ-triplets a density matrix size is 16x16, and a number of nonzero eigenvalues is equal to eight. At symmetrical attack their kind is (Vasiliu & Nikolaenko, 2009):

$$\begin{aligned}\lambda_{1,2} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2\cdot\frac{2}{3}d\left(1-\frac{2}{3}d\right)},\\ \lambda_{7,8} &= \frac{1}{2}(p_7+p_8) \pm \frac{1}{2}\sqrt{(p_7+p_8)^2 - 16p_7p_8\cdot\frac{2}{3}d\left(1-\frac{2}{3}d\right)}.\end{aligned} \tag{3}$$

For the protocol with *n*-qubit GHZ-states, the number of nonzero eigenvalues of density matrix is equal to $2^n$, and their kind at symmetrical attack is (Vasiliu & Nikolaenko, 2009):

$$\begin{aligned}\lambda_{1,2} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2\cdot\frac{2^{n-2}}{2^{n-1}-1}d\left(1-\frac{2^{n-2}}{2^{n-1}-1}d\right)},\\ \lambda_{2^n-1,2^n} &= \frac{1}{2}\left(p_{2^n-1}+p_{2^n}\right) \pm \frac{1}{2}\sqrt{\left(p_{2^n-1}+p_{2^n}\right)^2 - 16p_{2^n-1}p_{2^n}\cdot\frac{2^{n-2}}{2^{n-1}-1}d\left(1-\frac{2^{n-2}}{2^{n-1}-1}d\right)},\end{aligned} \tag{4}$$

where *d* is probability of attack detection by legitimate users at one-time switching to control mode; $p_i$ are frequencies of *n*-grams in the transmitted message.

The probability of that Eve will not be detected after *m* successful attacks and will gain information $I = mI_0$ is defined by the equation (Boström & Felbinger, 2002):

$$s(I,q,d) = \left(\frac{1-q}{1-q(1-d)}\right)^{I/I_0}, \tag{5}$$

where *q* is a probability of switching to control mode.

In fig. 2 dependences of $s(I,q,d)$ for several *n*, identical frequencies $p_i = 2^{-n}$, $q$ = 0.5 and $d = d_{\max}$ are shown (Vasiliu & Nikolaenko, 2009). $d_{\max}$ is maximum probability of attack detection at one-time run of control mode, defined as

$$d_{\max} = 1 - \frac{1}{2^{n-1}}. \tag{6}$$

At $d = d_{\max}$ Eve gains the complete information about transmitted bits of the message. It is obvious from fig. 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 qutrit pairs is presented (Vasiliu, 2011).

A non-quantum method of security amplification for the ping-pong protocol is suggested in (Vasiliu & Nikolaenko, 2009; Korchenko et al., 2010c). Such method has been developed on the basis of a method of privacy amplification which is utilized in quantum key distribution protocols. In case of the ping-pong protocol this method can be some kind of analogy of the Hill cipher (Overbey et al., 2005).

Before the transmission Alice divides the binary message on $l$ blocks of some fixed length $r$, we will designate these blocks as $a_i$ ($i$=1,…$l$). Then Alice 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 (multiplication is performed by modulo 2):

$$b_i = K_i a_i. \tag{7}$$

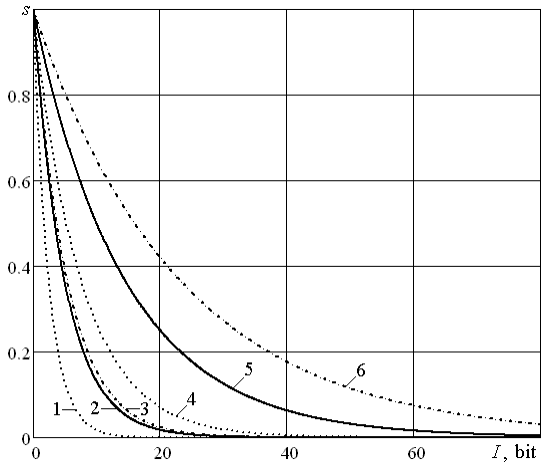


Fig. 2. Composite probability of attack non-detection $s$ for the ping-pong protocol with many-qubit GHZ-states: $n$=2, original protocol (1); $n$=2, with superdense coding (2); $n$=3 (3); $n$=5 (4); $n$=10 (5); $n$=16 (6). $I$ is Eve's information.

Blocks $b_i$ are transmitted on the quantum channel with the use of the ping-pong protocol. Even if Eve, remained undetected, manages to intercept one (or more) from these blocks and without knowledge of used matrices $K_i$ Eve won't be able to reconstruct source blocks $a_i$. To reach a sufficient security level the block length $r$ and accordingly the size of matrices $K_i$ should be selected so that Eve's undetection probability $s$ after transmission of *one* block would be 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 when Alice and Bob were convinced lack of eavesdropping. Then Bob inverses the received matrices and having multiplied them on appropriate blocks $b_i$ he gains an original message.

Let's mark that described procedure is not message enciphering, and can be named inverse hashing or hashing using two-way hash function, which role random invertible binary matrix acts.

It is necessary for each block to use individual matrix $K_i$ which will allow to prevent cryptoanalytic attacks, similar to attacks to the Hill cipher, which are possible there at a multiple usage of one matrix for enciphering of several blocks (Eve could perform similar attack if she was able before a detection of her operations in the quantum channel to intercept several blocks, that are hashing with the same matrix). As matrices in this case are not a key and they can be transmitted on the open classical channel, the transmission of the necessary number of matrices is not a problem.

Necessary length $r$ of blocks for hashing and accordingly necessary size $r \times r$ of hashing matrices should correspond to a requirement $r > I$, where $I$ is the information which is gained by Eve. Thus, it is necessary for determination of $r$ to calculate $I$ at the given values of $n$, $s$, $q$ and $d = d_{\max}$.

Let's accept $s(I, q, d) = 10^{-k}$, then:

$$I = \frac{-kI_0}{\lg\left(\frac{1-q}{1-q(1-d)}\right)}. \tag{8}$$

The calculated values of $I$ are shown in tab. 1:

| n | q = 0,5; $d = d_{\max}$ | q = 0,5; $d = d_{\max}/2$ | q = 0,25; $d = d_{\max}$ | q = 0,25; $d = d_{\max}/2$ |
|---|---|---|---|---|
| 2 | 69 | 113 | 180 | 313 |
| 3 | 74 | 122 | 186 | 330 |
| 4 | 88 | 145 | 216 | 387 |
| 5 | 105 | 173 | 254 | 458 |
| 6 | 123 | 204 | 297 | 537 |
| 7 | 142 | 236 | 341 | 620 |
| 8 | 161 | 268 | 387 | 706 |
| 9 | 180 | 302 | 434 | 793 |
| 10 | 200 | 335 | 481 | 881 |
| 11 | 220 | 369 | 529 | 970 |
| 12 | 240 | 403 | 577 | 1059 |
| 13 | 260 | 437 | 625 | 1149 |
| 14 | 279 | 471 | 673 | 1238 |
| 15 | 299 | 505 | 721 | 1328 |
| 16 | 319 | 539 | 769 | 1417 |
| 17 | 339 | 573 | 817 | 1507 |
| 18 | 359 | 607 | 865 | 1597 |
| 19 | 379 | 641 | 913 | 1686 |
| 20 | 399 | 675 | 961 | 1776 |

Table 1. Eve's information $I$ at attack on the ping - pong protocol with $n$-qubit GHZ-states at $s = 10^{-6}$ (bit).

Thus, after transfer of hashed block, the lengths of which are presented in tab. 1, 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 which can be performed when the protocol is executed in quantum channel with noise (Zhang, 2005a) or Trojan horse attack (Gisin et al., 2002). But there are some counteraction methods to these attacks (Boström & Felbinger, 2008). 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.

### 2.3 Quantum steganography

Quantum steganography aims to hide the fact of information transferral similar to classical steganography. Most 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 (Conti et al., 2004).

A simple quantum steganographic protocol (stegoprotocol) with using four qubit entangled Bell states:

$$\begin{aligned} \left|\phi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right), \ \left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2\right), \\ \left|\psi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right), \ \left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2\right), \end{aligned} \tag{9}$$

was proposed (Terhal et al., 2005). In this protocol $n$ Bell states, including all four states (9) with equal probability is divided between two legitimate users (Alice and Bob) by third part (Trent). For all states the first qubit is sent to Alice and second to Bob. The secret bit is coded in the number of $m$ singlet states $\left|\psi^{-}\right\rangle$ in the sequence of $n$ states: even $m$ represents "0" and odd represents "1". Alice and Bob perform local measurements each on own qubits and calculate the number of singlet states $\left|\psi^{-}\right\rangle$. That's why in this protocol Trent can secretly transmit information to Alice and Bob simultaneously.

Shaw & Brun proposed another one quantum stegoprotocol (Shaw & Brun, 2010). In this protocol the information qubit is hidden inside the error-correcting code. Thus, for intruder the qubits transmission via quantum channel looks like a normal quantum information transmission in the noise channel. For information qubit detection the receiver (Bob) must have a shared secret key with sender (Alice), which must be distributed before stegoprotocol starting. In the fig.3 the scheme of protocol proposed by Shaw & Brun is shown. Alice hides information qubit changing its places with qubit in her quantum codeword. She uses her secret key to determine which qubit in codeword must be replaced. Next, Alice uses key again to twirl (rotate) information qubit. This means that Alice uses one of the four single

qubit operators (Pauli operators) $I$, $\sigma_x$, $\sigma_y$ or $\sigma_z$ for this qubit by determining a concrete operation using two current key bits.

For the intruder who hasn't a key, this qubit likes qubit in maximal mixed state (the rotation can be interpreted as quantum Vernam cipher). In the next stage Alice uses random depolarization mistakes (using the same Pauli operators $\sigma_x$, $\sigma_y$ or $\sigma_z$) to some part of others qubits of codeword for simulating some level of noise in quantum channel. Next, she sent a codeword to Bob. For correct untwirl operation Bob use the shared secret key and then he uses a key again to find information qubit.

The security of this protocol depends on the security of previous key distribution procedure. When key distribution has information-theoretic security, and using information qubit twirl (equivalent to quantum Vernam cipher) all scheme can have information-theoretic security. It is known the information-theoretic security is provided by QKD protocols. But if an intruder continuously monitors the channel for a long time and he has a precise channel characteristics, in the final he discovers that Alice transmits information to Bob on quantum stegoprotocol. In addition, using quantum measurements of transmitted qubit states, an intruder can cancel information transmitting (Denial of Service attack).

Thus, in the present three basis methods of quantum steganography are proposed:

1. Hiding in the quantum noise;
2. Hiding using quantum error-correcting codes;
3. Hiding in the data formats, protocols etc.

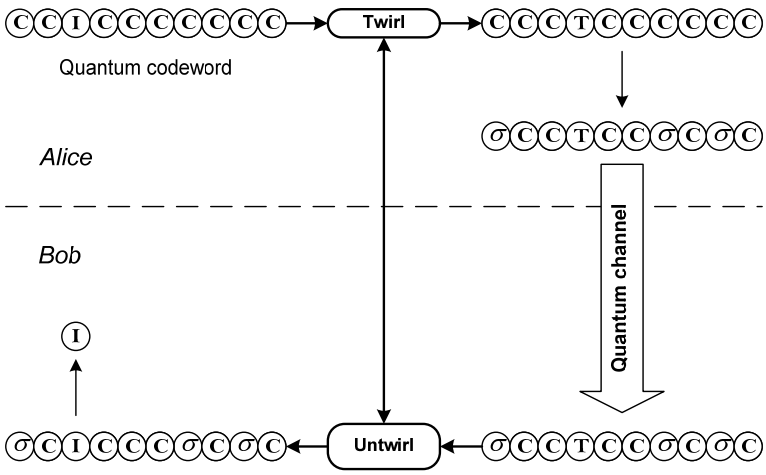


Fig. 3. The scheme of quantum stegoprotocol: $C$ – qubit of codeword, $I$ – information qubit, $T$ – twirled information qubit, $\sigma$ – qubit, to which Alice applies Pauli operator (qubit that simulate a noise).

The last method is the most promising direction of quantum steganography and also hiding using quantum error-correcting codes has some prospect in the future practice implementation.

It should be noted that theoretical research in quantum steganography 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 & Hayashi, 2006).

### 2.4 Others technologies for quantum secure telecommunication systems construction

*Quantum secret sharing (QSS).* Most QSS protocols use properties of entangled states. The first QSS protocol was proposed by *Hillery, Buzek* and *Berthiaume* in 1998 (Hillery et al., 1998; 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) was proposed by Li et al. (Li et al., 2009). 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. Zhang et al. has been presented QSS using single qubits that are prepared in two mutually unbiased bases and transferred by blocks (Zhang et al., 2005b). 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 proposed (Deng et al., 2005). A similar protocol for multiparty secret sharing also is presented (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 (Hirota et al., 2005) and can be used in optical telecommunication networks. 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 (Nair & Yuen, 2007; Yuen, 2001). In a number of papers (Corndorf et al., 2005; Hirota & Kurosawa, 2006; Nair & Yuen, 2007) the high encryption rate of the Y-00 protocol is demonstrated experimentally, and a security analysis on the Yuen-2000 protocol against the fast correlation attack, the typical attack on stream ciphers, is presented (Hirota & Kurosawa, 2006). 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 & Zurek, 1982). The complexity of practical implementation is the most important imperfection of QSC (Hirota & Kurosawa, 2006).

*Quantum digital signature (QDS)* can be implemented on the basis of protocols such as QDS protocols using single qubits (Wang et al., 2006) and QDS protocols using entangled states (authentic QDS based on quantum GHZ-correlations) (Wen & Liu, 2005). QDS is based on use of the quantum one-way function (Gottesman & Chuang, 2001). 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 & Chuang, 2001):

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). 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 & Chuang, 2001). 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 & Chuang, 2001).

Fig. 4 represents a general scheme of the methods of quantum secure telecommunication systems construction for their purposes and for using some quantum technologies.

### 2.5 Review of commercial quantum secure telecommunication systems

The world's first commercial quantum cryptography solution was *QPN Security Gateway (QPN-8505)* (QPN Security Gateway, 2011) proposed by *MagiQ Technologies (USA).* This system (fig. 5 a) is a cost-effective information security solution for governmental and financial organisations. It proposes VPN protection using QKD (up to 100 256-bit keys per second, up to 140 km) and integrated encryption. The QPN-8505 system uses BB84, 3DES (NIST, 1999) and AES (NIST, 2001) protocols.

The Swiss company *Id Quantique* (Cerberis, 2011) offers a systems called *Clavis*$^2$ (fig. 5 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 quantum key distribution. 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.

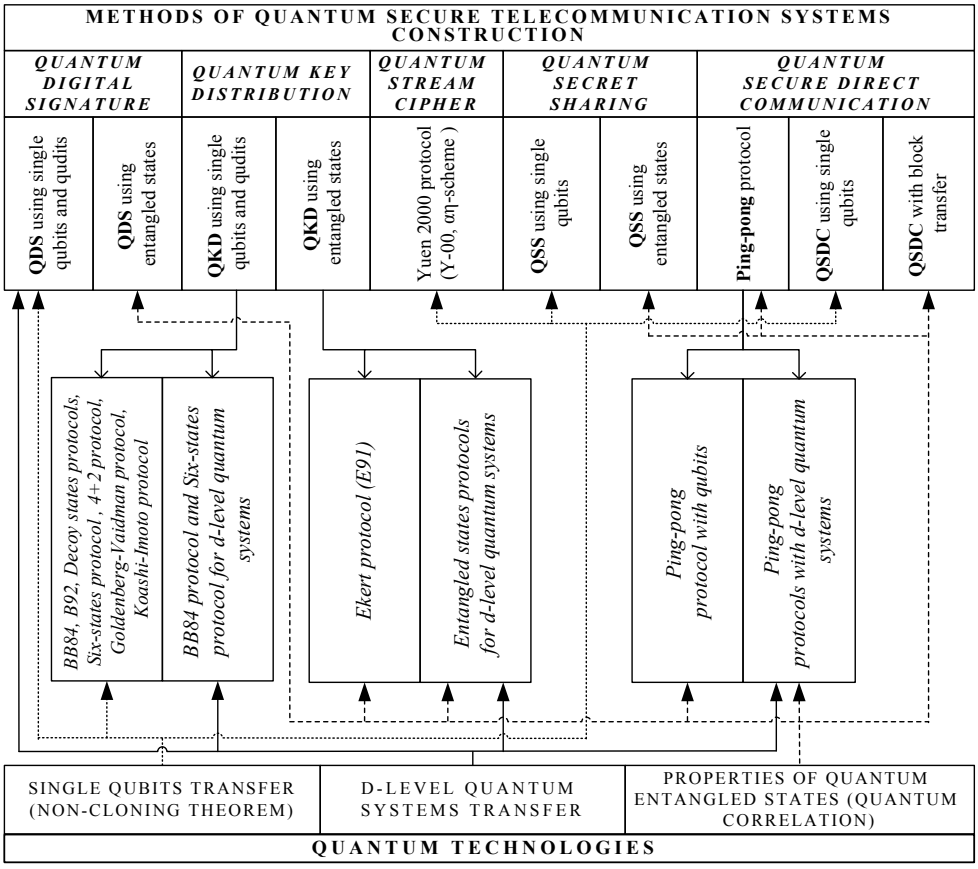


Fig. 4. Methods of quantum secure telecommunication systems construction.

*Toshiba Research Europe Ltd (Great Britain)* recently presented another QKD system named *Quantum Key Server* (QKS, 2011). This system (fig. 5 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 Megabit per second of key material over a distance of 50 km — sufficiently long for metropolitan coverage. Toshiba's system uses a

simple "one-way" architecture, in which the photons travel from sender to receiver. This design has been rigorously proven as secure from most types of eavesdropping attack. Toshiba has pioneered active stabilisation technology that allows the system to distribute key material continuously, even in the most challenging operating conditions, without any user intervention. This avoids the need for recalibration of the system due to temperature-induced changes in the fibre lengths. Initiation of the system is also managed automatically, allowing simple turn-key operation. It has been shown to work successfully in several network field trials. The system can be used for a wide range of cryptographic applications, e.g., encryption or authentication of sensitive documents, messages or transactions. A programming interface gives the user access to the key material.


a) b) c)

Fig. 5. Some commercial quantum secure telecommunication systems.

Another British company, *QinetiQ*, realised the world's first network using quantum cryptography – *Quantum Net (Qnet)* (Elliot et al., 2003; Hughes et al., 2002). 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 addition the world's leading scientists are actively taking part in the implementation of projects such as *SECOQC (Secure Communication based on Quantum Cryptography)* (SECOQC White Paper on Quantum Key Distribution and Cryptography, 2007), *EQCSPOT (European Quantum Cryptography and Single Photon Technologies)* (Alekseev & Korneyko, 2007) and *SwissQuantum* (Swissquantum, 2011).

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.

Following no-cloning theorem, QKD only can provide point-to-point (sometimes called "1:1") connection. So the number of links will increase $N(N-1)/2$ as $N$ represents the number of nodes. If a node wants to participate into the QKD network, it will cause some issues like constructing quantum communication line. To overcome these issues, SECOQC was started. SECOQC network architecture (fig. 6) can by divided by two parts. Trusted private network and quantum network consisted with QBBs (Quantum Back Bone). Private network is conventional network with end-nodes and a QBB. QBB provides quantum

channel communication between QBBs. QBB is consisted with a number of QKD devices that are connected with other QKD devices in 1:1 connection. From this, SECOQC can provide easier registration of new end-node in QKD network, and quick recovery from threatening on quantum channel links.

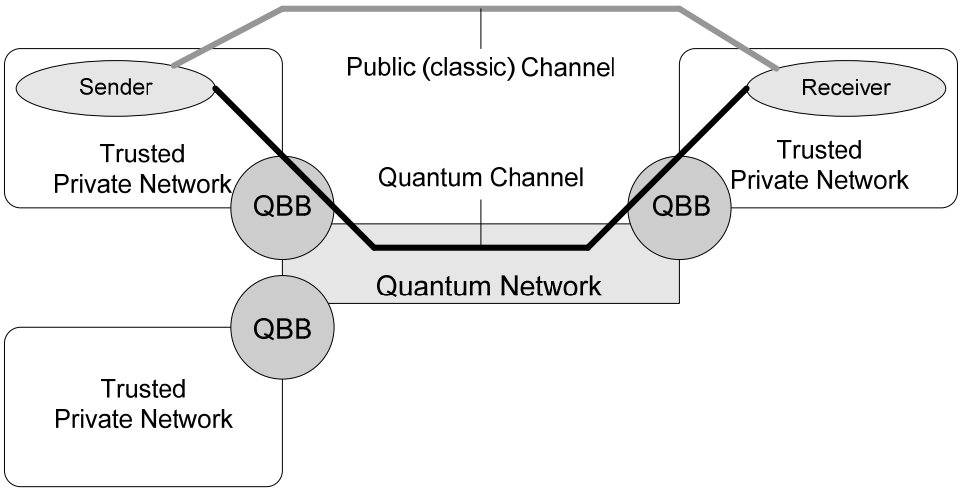


Fig. 6. Brief network architecture of SECOQC.

We also note that during the project SECOQC the seven most important QKD systems have been developed or refined (Kollmitzer & Pivk, 2010). 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 used 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 proposed to protect these transactions using the shared secret stored in a personal hand-held transmitter. Thereby Alice's module is integrated within a small device such as a mobile telephone, or personal digital

assistant, and Bob's module consists of a fixed device such as a bank asynchrone transfer mode.

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.

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:

- Quantum Layer. This layer performs Quantum Key Exchange.
- *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).
- *Application Layer*. In this layer, various cryptographic services use the keys distributed to provide secure communications.

There are many practical and theoretical research projects concerning the development of quantum technology 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.

## 3. Conclusion

This chapter 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 secure telecommunication systems 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 information security level than appropriate classical schemes.

Other secure quantum technologies in practice have not been extended beyond laboratory experiments yet. But there are many theoretical cryptographic schemes that provide high information security level up to the information-theoretic security. QSDC 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 information security level of confidential data transmission using the existing level of technology with security amplification methods. Another category of QSDC is protocols with transfer qubits by blocks that have unconditional security, but these need a large quantum memory which is out of the capabilities of modern technologies today. It must be noticed 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 information security 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 quantum technologies is also faced to some technological difficulties.

Thus, in recent years quantum technologies are rapidly developing and gradually taking their place among other means of information security. Their advantage is a high level of security and some properties, which classical means of information security do not have. One of these properties is the ability always to detect eavesdropping. Quantum technologies therefore represent an important step towards improving the security of telecommunication systems against cyber-terrorist attacks. But many theoretical and practical problems must be solved for wide practical use of quantum secure telecommunication systems.

## 4. Acknowledgment

Special thanks should be given to **Rector of National Aviation University (Kyiv, Ukraine) – Mykola Kulyk.** We would not have finished this chapter without his support.

## 5. References

Alekseev, D.A. & Korneyko, A.V. (2007). Practice reality of quantum cryptography key distribution systems, *Information Security*, No. 1, pp. 72–76.

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

Bennett, C. (1992). Quantum cryptography using any two non-orthogonal states, *Physical Review Letters*, Vol.68, No.21, pp. 3121–3124.

Bennett, C.; Bessette, F. & Brassard, G. (1992). Experimental Quantum Cryptography, *Journal of Cryptography*, Vol.5, No.1, pp. 3–28.

Bennett, C.; Brassard, G.; Crépeau, C. & Maurer, U. (1995). Generalized privacy amplification, *IEEE Transactions on Information Theory*, Vol.41, No.6, pp. 1915–1923.

Boström, K. & Felbinger, T. (2002). Deterministic secure direct communication using entanglement, *Physical Review Letters*, Vol.89, No.18, 187902.

Boström, K. & Felbinger, T. (2008). On the security of the ping-pong protocol, *Physics Letters A*, Vol.372, No.22, pp. 3953–3956.

Bourennane, M.; Karlsson, A. & Bjork, G. (2002). Quantum key distribution using multilevel encoding, *Quantum Communication, Computing, and Measurement 3*. N.Y.: Springer US, pp. 295–298.

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

Bradler K. (2005). Continuous variable private quantum channel, *Physical Review A*, Vol.72, No.4, 042313.

Branciard, C.; Gisin, N.; Kraus, B. & Scarani, V. (2005). Security of two quantum cryptography protocols using the same four qubit states, *Physical Review A*, Vol.72, No.3, 032301.

Brassard, G.; Lutkenhaus, N.; Mor, T. & Sanders, B. (2000). Limitations on practical quantum cryptography, *Physical Review Letters*, Vol.85, No.6, pp. 1330–1333.

Bruss, D. (1998). Optimal Eavesdropping in Quantum Cryptography with Six States, *Physical Review Letters*, Vol.81, No.14, pp. 3018–3021.

Bruss, D. & Macchiavello C. (2002). Optimal eavesdropping in cryptography with three-dimensional quantum states, *Physical Review Letters*, Vol.88, No.12, 127901.

Cai, Q.-Y. & Li, B.-W. (2004a). Deterministic Secure Communication Without Using Entanglement, *Chinese Physics Letters*, Vol.21 (4), pp. 601–603.

Cai, Q.-Y. & Li B.-W. (2004b). Improving the capacity of the Bostrom–Felbinger protocol, *Physical Review A*, Vol.69, No.5, 054301.

Cerberis. 01.10.2011, Available from: http://idquantique.com/products/cerberis.htm.

Cerf, N.J.; Bourennane, M.; Karlsson, A. & Gisin, N. (2002). Security of quantum key distribution using d-level systems, *Physical Review Letters*, Vol.88, No.12, 127902.

Chamoli, A. & Bhandari, C.M. (2009). Secure direct communication based on ping-pong protocol, *Quantum Information Processing*, Vol.8, No.4, pp. 347–356.

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

Conti A.; Ralph, S.; Kenneth A. et al. *Patent* No 7539308 USA, H04K 1/00 (20060101). Quantum steganography, publ. 21.05.2004.

Corndorf, E., Liang, C. & Kanter, G.S. (2005). Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks, *Physical Review A*, Vol.71, No.6, 062326.

Deng, F.G.; Long, G.L. & Liu, X.S. (2003). Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. *Physical Review A*, 2003. Vol.68, No.4, 042317.

Deng, F. G.; Li, X. H.; Zhou, H. Y. & Zhang, Z. J. (2005). Improving the security of multiparty quantum secret sharing against Trojan horse attack, *Physical Review A*, Vol.72, No.4, 044302.

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

Durt, T.; Kaszlikowski, D.; Chen, J.-L. & Kwek, L.C. (2004). Security of quantum key distributions with entangled qudits, *Physical Review A*, Vol.69, No.3, 032313.

Ekert, A. (1991). Quantum cryptography based on Bell's theorem, *Physical Review Letters*, Vol.67, No.6, pp. 661–663.

Elliot, C.; Pearson, D. & Troxel, G. (2003). Quantum Cryptography in Practice, *arXiv:quant-ph/0307049*.

Fuchs, C.; Gisin, N.; Griffits, R. et al. (1997). Optimal Eavesdropping in Quantum Cryptography. Information Bound and Optimal Strategy, *Physical Review A*, Vol.56, No.2, pp. 1163–1172.

Gao, T.; Yan, F.L. & Wang, Z.X. (2005). Deterministic secure direct communication using GHZ-states and swapping quantum entanglement. *Journal of Physics A: Mathematical and Theoretical*, Vol. 38, No.25, pp. 5761–5770.

Gao, F.; Guo, F.Zh.; Wen, Q.Y. & Zhu, F.Ch. (2008). Comparing the efficiencies of different detect strategies in the ping-pong protocol, *Science in China, Series G: Physics, Mechanics & Astronomy*, Vol.51, No.12. pp. 1853–1860.

Gisin, N.; Ribordy, G.; Tittel, W. & Zbinden, H. (2002). Quantum cryptography, *Review of Modern Physics*, Vol.74, pp. 145–195.

Gnatyuk, S.O.; Kinzeryavyy, V.M.; Korchenko, O.G. & Patsira, Ye.V. (2009). *Patent* No 43779 UA, MPK H04L 9/08. System for cryptographic key transfer, 25.08.2009.

Goldenberg, L. & Vaidman, L. (1995). Quantum Cryptography Based On Orthogonal States, *Physical Review Letters*, Vol.75, No.7, pp. 1239–1243.

Gottesman, D. & Chuang, I. (2001). Quantum digital signatures, *arXiv:quant-ph/0105032v2*.

Hayashi, M. (2006). *Quantum information. An introduction*. Berlin, Heidelberg, New York: Springer, 430 p.

Hillery, M.; Buzek, V. & Berthiaume, A. (1999). Quantum secret sharing, *Physical Review A*, Vol.59, No.3, pp. 1829–1834.

Hirota, O. & Kurosawa, K. (2006). An immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol, *arXiv:quant-ph/0604036v1.*

Hirota, O.; Sohma, M.; Fuse, M. & Kato, K. (2005). Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme, *Physical Review A*, Vol.72, No.2, 022335.

Holevo, A.S. (1977). Problems in the mathematical theory of quantum communication channels, *Report of Mathematical Physics*, Vol.12, No.2, pp. 273–278.

Hughes, R.; Nordholt, J.; Derkacs, D. & Peterson, C. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night, *New Journal of Physics*, Vol.4, 43 p.

Huttner, B.; Imoto, N.; Gisin, N. & Mor, T. (1995). Quantum Cryptography with Coherent States, *Physical Review A*, Vol.51, No.3, pp. 1863–1869.

Imai, H. & Hayashi, M. (2006). *Quantum Computation and Information. From Theory to Experiment*. Berlin: Springer-Verlag, Heidelberg, 235 p.

Imre, S. & Balazs, F. (2005). *Quantum Computing and Communications: An Engineering Approach,* John Wiley & Sons Ltd, 304 p.

Inamori, H.; Rallan, L. & Vedral, V. (2001). Security of EPR-based quantum cryptography against incoherent symmetric attacks, *Journal of Physics A*, Vol.34, No.35, pp. 6913–6918.

Kaszlikowski, D.; Christandl, M. et al. (2003). Quantum cryptography based on qutrit Bell inequalities, *Physical Review A*, Vol.67, No.1, 012310.

Koashi, M. & Imoto, N. (1997). Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps, *Physical Review Letters*, Vol.79, No.12, pp. 2383–2386.

Kollmitzer, C. & Pivk, M. (2010). Applied Quantum Cryptography, *Lecture Notes in Physics 797*. Berlin, Heidelberg: Springer, 214 p.

Korchenko, O.G.; Vasiliu, Ye.V. & Gnatyuk, S.O. (2010a). Modern quantum technologies of information security against cyber-terrorist attacks, *Aviation.* Vilnius: Technika, Vol.14, No.2, pp. 58–69.

Korchenko, O.G.; Vasiliu, Ye.V. & Gnatyuk, S.O. (2010b). Modern directions of quantum cryptography, "*AVIATION IN THE XXI-st CENTURY*" – "*Safety in Aviation and Space Technologies*": *IV World Congress: Proceedings* (September 21–23, 2010), Kyiv, NAU, pp. 17.1–17.4.

Korchenko, O.G.; Vasiliu, Ye.V.; Nikolaenko, S.V. & Gnatyuk, S.O. (2010c). Security amplification of the ping-pong protocol with many-qubit Greenberger-Horne-Zeilinger states, *XIII International Conference on Quantum Optics and Quantum Information (ICQOQI'2010):* Book of abstracts (May 28 – June 1, 2010), pp. 58–59.

Li, Q.; Chan, W. H. & Long, D-Y. (2009). Semi-quantum secret sharing using entangled states, *arXiv:quant-ph/0906.1866v3*.

Li, X.H.; Deng, F.G. & Zhou, H.Y. (2006). Improving the security of secure direct communication based on the secret transmitting order of particles. *Physical Review A*, Vol.74, No.5, 054302.

Lin, S.; Wen, Q.Y.; Gao, F. & Zhu F.C. (2008). Quantum secure direct communication with chi-type entangled states, *Physical Review A*, Vol.78, No.6, 064304.

Liu, Y.; Chen, T.-Y.; Wang, J. et al. (2010). Decoy-state quantum key distribution with polarized photons over 200 km, *Optics Express*, Vol. 18, Issue 8, pp. 8587-8594.

Lomonaco, S.J. (1998). A Quick Glance at Quantum Cryptography, *arXiv:quant-ph/*9811056.

Lütkenhaus, N. & Jahma, M. (2002). Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, *New Journal of Physics*, Vol.4, pp. 44.1–44.9.

Lütkenhaus, N. & Shields, A. (2009). Focus on Quantum Cryptography: Theory and Practice, *New Journal of Physics*, Vol.11, No.4, 045005.

Nair, R. & Yuen, H. (2007). On the Security of the Y-00 (AlphaEta) Direct Encryption Protocol, *arXiv:quant-ph/0702093v2*.

Navascués, M. & Acín, A. (2005). Security Bounds for Continuous Variables Quantum Key Distribution, *Physical Review Letters*, Vol.94, No.2, 020505.

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). 01.10.2011, Available from: <http://csrc.nist.gov/publications/fips>.

NIST. "FIPS-46-3: Data Encryption Standard." (1999). 01.10.2011, Available from: <http://csrc.nist.gov/publications/fips>.

Ostermeyer, M. & Walenta N. (2008). On the implementation of a deterministic secure coding protocol using polarization entangled photons, *Optics Communications*, Vol. 281, No.17, pp. 4540–4544.

Overbey, J; Traves, W. & Wojdylo J. (2005). On the keyspace of the Hill cipher, *Cryptologia*, Vol.29, No.1, pp. 59–72.

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*, Vol.98, No.1, 010505.

Pirandola, S.; Mancini, S.; Lloyd, S. & Braunstein S. (2008). Continuous-variable quantum cryptography using two-way quantum communication, *Nature Physics*, Vol.4, No.9, pp. 726–730.

Qin, S.-J.; Gao, F. & Zhu, F.-Ch. (2007). Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol, *Physical Review A*, Vol.76, No.6, 062324.

QKS. Toshiba Research Europe Ltd. 01.10.2011, Available from: <http://www.toshiba-europe.com/research/crl/QIG/quantumkeyserver.html>.

QPN Security Gateway (QPN–8505). 01.10.2011, Available from: <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*, Vol.98, No.1, 010503.

Sangouard, N.; Simon, C.; de Riedmatten, H. & Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics, *Review of Modern Physics,* Vol.83, pp. 33–34.

Scarani, V.; Acin, A.; Ribordy, G. & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, *Physical Review Letters*, Vol.92, No.5, 057901.

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

SECOQC White Paper on Quantum Key Distribution and Cryptography. (2007). *arXiv:quant-ph/0701168v1*.

Shaw, B. & Brun, T. (2010). Quantum steganography, *arXiv:quant-ph/1006.1934v1.*

Schumacher, B. & Westmoreland, M. (2010). *Quantum Processes, Systems, and Information*. Cambridge: Cambridge University Press, 469 p.

Terhal, B.M.; DiVincenzo, D.P. & Leung, D.W. (2001). Hiding bits in Bell states, *Physical review letters,* Vol.86, issue 25, pp. 5807-5810.

Vasiliu, E.V. (2011). Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits, *Quantum Information Processing,* Vol.10, No.2, pp. 189–202.

Vasiliu, E.V. & Nikolaenko, S.V. (2009). Synthesis if the secure system of direct message transfer based on the ping–pong protocol of quantum communication, *Scientific works of the Odessa national academy of telecommunications named after O.S. Popov*, No.1, pp. 83–91.

Vasiliu, E.V. & Mamedov, R.S. (2008). Comparative analysis of efficiency and resistance against not coherent attacks of quantum key distribution protocols with transfer of multidimensional quantum systems, *Scientific works of the Odessa national academy of telecommunications named after O.S. Popov*, No.2, pp. 20–27.

Vasiliu, E.V. & Vorobiyenko, P.P. (2006). The development problems and using prospects of quantum cryptographic systems, *Scientific works of the Odessa national academy of telecommunications named after O.S. Popov*, No.1, pp. 3–17.

Vedral, V. (2006). *Introduction to Quantum Information Science*. Oxford University Press Inc., New York, 183 p.

Wang, Ch.; Deng, F.G. & Long G.L. (2005a). Multi – step quantum secure direct communication using multi – particle Greenberger – Horne – Zeilinger state, *Optics Communications*, Vol. 253, No.1, pp. 15–20.

Wang, Ch. et al. (2005b). Quantum secure direct communication with high dimension quantum superdense coding, *Physical Review A*, Vol.71, No.4, 044305.

Wang, J.; Zhang, Q. & Tang, C. (2006). Quantum signature scheme with single photons, *Optoelectronics Letters*, Vol.2, No.3, pp. 209–212.

Wen, X.-J. & Liu, Y. (2005). Quantum Signature Protocol without the Trusted Third Party, *arXiv:quant-ph/0509129v2*.

Williams, C.P. (2011). *Explorations in quantum computing, 2nd edition*. Springer-Verlag London Limited, 717 p.

Wooters, W.K. & Zurek, W.H. (1982). A single quantum cannot be cloned, *Nature*, Vol. 299, p. 802.

Xiu, X.-M.; Dong, L.; Gao, Y.-J. & Chi F. (2009). Quantum Secure Direct Communication with Four-Particle Genuine Entangled State and Dense Coding, *Communication in Theoretical Physics*, Vol.52, No.1, pp. 60–62.

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*, Vol.25, No.4, pp. 1187–1190.

Yin, Z.-Q.; Zhao, Y.-B.; Zhou Z.-W. et al. (2008). Decoy states for quantum key distribution based on decoherence-free subspaces, *Physical Review A*, Vol.77, No.6, 062326.

Yuen, H.P. (2001). *In Proceedings of QCMC'00*, Capri, edited by P. Tombesi and O. Hirota New York: Plenum Press, p. 163.

Zhang, Zh.-J.; Li, Y. & Man, Zh.-X. (2005a). Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss, *Physics Letters A*, Vol.341, No.5–6, pp. 385–389.

Zhang, Zh.-J.; Li, Y. & Man, Zh.-X. (2005b). Multiparty quantum secret sharing, *Physical Review A*, Vol.71, No.4, 044301.

Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K. & Qian, L. (2006a). Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber, *Proceedings of IEEE International Symposium on Information Theory*, pp. 2094–2098.

Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K. & Qian, L. (2006b). Experimental Quantum Key Distribution with Decoy States, *Physical Review Letters*, Vol.96, No.7, 070502.