SECURE DIRECT COMMUNICATION USING QUANTUM CALDERBANK-SHOR-STEANE CODES

Xin Lü, Zhi Ma
State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences,
Beijing, 100039,China
email: lx@is.ac.cn

Deng-Guo Feng
State Key Laboratory of Information Security,
Software Institute of Chinese Academy of Sciences,
Beijing, 100080,China

ABSTRACT

The notion of quantum secure direct communication (QSDC) has been introduced recently in quantum cryptography as a replacement for quantum key distribution, in which two communication entities exchange secure classical messages without establishing any shared keys previously. In this paper, a quantum secure direct communication scheme using quantum Calderbank-Shor-Steane (CCS) error correction codes is proposed. In the scheme, a secure message is first transformed into a binary error vector and then encrypted(decrypted) via quantum coding(decoding) procedures. An adversary Eve, who has controlled the communication channel, can't recover the secrete messages because she doesn't know the deciphering keys. Security of this scheme is based on the assumption that decoding general linear codes is intractable even on quantum computers.

KEY WORDS

Quantum cryptography; Secure direct communication

1 Introduction

Quantum key distribution provides a novel way to obtain ultimate security based on quantum mechanics, which cares about agreeing classical keys between two communication entities over quantum channel [1]. Different from quantum key distribution, quantum secure direct communication permits important messages to be communicated directly without establishing a random shared key to encrypt them. QSDC can be used in some special environments, with an example where it is difficult to establish a session key between two communication parties. As a secure QSDC scheme, it requires that the secure messages encoded in the quantum states should not leak to an eavesdropper Eve even if she has controlled the communication channel. A "good" QSDC scheme also expects that no additional classical messages are needed to exchange between communication entities except the encoded quantum messages.

Several QSDC protocols have been addressed recently. In 2002, Beige $et\ al.$ proposed a QSDC scheme based on sigle-photon two qubit states [2]. In their scheme, the secure message can be read only after a transmission of an additional classical message for each qubit. Boström and Felbingeer addressed a Ping-Pang QSDC protocol [3] using Einstein-Podolsky-Rosen (EPR) pairs as quantum information carriers, in which the secure messages can be decoded during the transmission and no final transmission of additional information is needed. However, wöjcik proved that, in this scheme, Eve can get a part of the secure message with some probability, especially in a noisy quantum channel. Recently, Deng $et\ al.$ [4] put forward a quantum one-time-pad based QSDC scheme, in which batches of single photons were used to serve as a one-time-pad to encode the secret messages. However, all the existed QSDC schemes need to publicize some additional classical messages to check out whether there exist eavesdroppers over the quantum communication channel.

In this paper, we propose a QSDC scheme using quantum Calderbank-Shor-Steane codes, more usually known as CSS codes, after the initials of the inventors of this class of codes. In the proposed scheme, we suppose that the channel between communication entities is noiseless. In this scheme, the receiver Bob sends some quantum states encoded using quantum CSS codes. Alice transforms the secure messages into some error vectors and applies these errors on the qubits and sends them to Bob. Bob receives the messages and recovers the secure messages. Security of this scheme is based on the fact that decoding an arbitrary linear code is NP-hard and Goppa cods have efficient decoding algorithm. The remainder of this paper are arranged as follows:

Section 2 introduces the preliminaries and definitions that we will use in this paper. Section 3 describes the proposed QSDC scheme. Security analysis is performed in section 4. Conclusions are made in section 5.

2 Preliminaries

2.1 Quantum CSS Codes

The constructions of quantum CSS codes rely heavily on the properties of classical error-correcting codes [6, 7]. Here, we first review the basic definitions of binary classical linear codes. Let's consider vectors and codes over the field $\mathbb{F}_2$, including two elements, one and zero. The number of one's in a binary vector $v \in \mathbb{F}_2$ is called *Hamming* *weight*, noted as $w(v)$. *Hamming distance* $d(v, u)$ between two binary vectors v and u is $w(v+w)$, which denotes the number of bits differing from each other between v and u. A binary linear code C is an $[n, k]$ linear code over the finite field $\mathbb{F}_2$, or an $[n, k]$ code, for short. If C has minimum distance d, which denotes the minimum distance between two distinct codewords, then C is called an $[n, k, d]$ linear code over $\mathbb{F}_2$. A linear code c is always specified by an n by k generator matrix G whose entries are all zeroes and ones. The generator matrix G maps k bits of information to a set of binary vectors of length n, called codewords. Binary linear codes can be alternatively (but equivalently) formulated by so called parity matrix, which is used to perform error-correction. The parity matrix H of a linear code $[n, k]$ is an $(n-k) \times n$ matrix such that

$$Hx = 0 \tag{1}$$

for all those and only those vectors x in the code C. The rows of H are $n-k$ linearly independent vectors, and the code space is the space of vectors that are orthogonal to all of these vectors.

A quantum bit, or a qubit, is a two-level system which can be in state

$$|\psi\rangle = a|0\rangle + b|1\rangle. \tag{2}$$

The numbers α and β are complex numbers, always noted as $\alpha, \beta \in \mathbb{C}$, such that $(\alpha, \beta) \neq (0,0)$ and $|a|^2 + |b|^2 = 1$. The way a qubit differs from a classical bit is that a qubit can be the superposition state $\alpha|0\rangle + \beta|1\rangle$, not definitely in basis state $|0\rangle$ or $|1\rangle$. An n-qubit state is a non-zero vector in the tensor product space $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$. We usually choose the following orthonormal basis of $\mathbb{C}^{2^n}$:

$$\begin{aligned}\{|a_0 a_1 \cdots a_{n-1}\rangle = |a_0\rangle \otimes |a_1\rangle \otimes \cdots \otimes |a_{n-1}\rangle \\ \mid (a_0, \cdots, a_{n-1}) \in \mathbb{F}_2^n\}\end{aligned} \tag{3}$$

Thus an n-qubit state can be expressed by

$$\begin{aligned}|\psi\rangle &= \sum_{(a_0,\cdots,a_{n-1})\in\mathbb{F}_2^n} c_{a_0,\cdots,a_{n-1}} |a_0, \cdots, a_{n-1}\rangle \\ &= \sum_{a\in\mathbb{F}_2^n} c_a |a\rangle\end{aligned} \tag{4}$$

where $c_a \in \mathbb{C}$.

A quantum error correcting code ($QECC$) Q:[[n, k, d]] is a 2^k-dimensional subspace of the Hilbert space $\mathbb{C}^{2^n}$. It is a way of encoding k-qubit quantum states into n qubits ($k < n$) such that any error in $\leq [\frac{d-1}{2}]$ qubits can be measured and subsequently corrected without disturbing the encoded states. d is called the *minimal distance* of Q. Quantum CSS codes can be constructed by using classical linear codes:

Theorem 1 *[6] Suppose that there exist two classical binary linear codes* $C_1 = [n,\ k_1,\ d_1]$, $C_2 = [n,\ k_2,\ d_2]$, *and* ${C_1}^{\perp} \subseteq C_2$ *(so that* $n \leq k_1 + k_2$*). Then there exists a QECC* $Q : [[n,\ k = k_1 + k_2 - n,\ \min\{d_1, d_2\}]]$. *A set of its basis states can be expressed as*

$$\{|c_w\rangle = \frac{1}{2^{\frac{n-k_1}{2}}} \sum_{v\in{C_1}^{\perp}} |w+v\rangle \ |w \in C_2/C_1^{\perp}\}. \tag{5}$$

Let $G_i,\ H_i$ be the generator matrix and parity check matrix of C_i respectively, $(i = 1, 2)$. Without loss of generality, we may assume that $G_2 = \begin{pmatrix} H_1 \\ D \end{pmatrix}$ by ${C_1}^{\perp} \subseteq C_2$, here the rank of D is $k = k_1 + k_2 - n$. Then each k-qubit basis state

$$|m\rangle = |m_1 \cdots m_k\rangle \ \ (m \in \mathbb{F}_2^k)$$

can be encoded into a quantum codeword

$$\begin{aligned}|c_m\rangle &= \frac{1}{2^{\frac{n-k_1}{2}}} \sum_{v\in{C_1}^{\perp}} |v + m\cdot D\rangle \\ &= \frac{1}{2^{\frac{n-k_1}{2}}} \sum_{v\in{C_1}^{\perp}} \left|v + m_1 D^{(1)} + \cdots + m_k D^{(k)}\right\rangle\end{aligned} \tag{6}$$

where $D^{(j)}$ is the $j'th$ row of D, $1 \leq j \leq k$.

Quantum errors will occur when quantum states are transmitted over quantum channels. There are three basic errors on a qubit: bit error, phase error and their composition, which can be described by Pauli matrices respectively:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{7}$$

For any $a \in \{x, y, z\},\ r = (r_1, \cdots, r_n) \in \mathbb{F}_2^n$, let

$$\sigma_a^{[r]} = \sigma_a^{[r_1]} \otimes \cdots \otimes \sigma_a^{[r_n]},$$

where

$$\sigma_a^{[r_i]} = \begin{cases} I & if \quad r_i = 0 \\ \sigma_a & if \quad r_i = 1\ . \end{cases}$$

Then every error on n qubits can be represented as $e = \sigma_x^{[X]} \sigma_z^{[Z]}$, here $X = (x_1, \cdots, x_n),\ Z = (z_1, \cdots, z_n) \in \mathbb{F}_2^n$. For convenience, we also use binary vector $\vec{e} = (X|Z)$ to describe the error $\sigma_x^{[X]} \sigma_z^{[Z]}$. Then the error e acts on an n-qubit basis state $|V\rangle = |v_1,\ \cdots,\ v_n\rangle$ $(V \in \mathbb{F}_2^n)$ as follows

$$\begin{aligned}e\,|V\rangle &= (-1)^{Z\cdot V}\,|X + V\rangle \\ &= (-1)^{z_1\cdot v_1 + \cdots + z_n\cdot v_n}\,|x_1 + v_1, \cdots, x_n + v_n\rangle\end{aligned} \tag{8}$$

The number of error positions on the quantum state $|V\rangle$ can be expressed as

$$w_q(\vec{e}) = \sharp\{i|(X_i, Z_i) \neq (0,0), 1 \leq i \leq n\} \tag{9}$$

.

2.2 Goppa Codes

Goppa codes are an important class of linear codes, some of which can meet the Gilbert-Varshamov bound. Goppa codes have been widely used to construct public-key encryption systems and message authentication codes since they have a fast decoding algorithm and a large number of nonequivalent classes[8]. here we only consider binary Goppa Codes.

Definition 1 *Suppose $g(z)$ is a polynomial of degree t over finite fields $\mathbb{F}_{2^m}$. Let $L = \{\gamma_0,\ \gamma_1,\ \cdots,\ \gamma_{n-1}\} \subset \mathbb{F}_{2^m}$ such that $|L| = n$ and $g(\gamma_i) \neq 0$ for $0 \leq i \leq n-1$. Then the Goppa code $\Gamma(L,\ g)$ with Goppa polynomial $g(z)$ is defined to be the set of codewords*

$$\{c = (c_0,\ c_1,\ \cdots,\ c_{n-1}) \in \mathbb{F}_2^n \mid \sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} \equiv 0 \pmod{g}(z). \qquad (10)$$

From the above definitions, it's easy to know that Goppa code $\Gamma(L,\ g)$ is uniquely determined by $g(z)$ and L and has parameters $[n,\ k \geq n - mt,\ d \geq t+1]$. By some computing results over finite fields we know that Goppa codes have a large number of nonequivalent classes, which makes it possible to construct cryptosystems by using Goppa codes. The specific description of Goppa codes can refer to Ref.[11].

3 The Proposed Scheme

Let $C_i = \Gamma(L_i\ ,\ g_i(z)) = [n, k_i, d_i](i = 1, 2)$ be both binary Goppa codes such that $C_1^{\perp} \subseteq C_2$, $d = \min\{d_1\ ,\ d_2\}$, the *Hamming* weight of the error vectors $t = \lfloor \frac{d-1}{2} \rfloor$, $k = k_1 + k_2 - n$. We assume that the quantum channel used in this scheme is noiseless channel.

3.1 Encoding

Bob randomly chooses a generator matrix G_i and parity check matrix H_i of $C_i (i = 1,\ 2)$ such that $G_2 = \left(\begin{array}{c} H_1 \\ D \end{array}\right)$, here the rank of D is $k = k_1 + k_2 - n$. He then randomly prepares a basis state $|m\rangle$ such that $m \in \mathbb{F}_2^k$ and encodes it into $|c\rangle$ using quantum CSS codes Q according to equation (6). Bob acts some error $\vec{e'} = (X'|Z')$ on $|c\rangle$ as

$$\begin{aligned} &|\psi\rangle = e'\,|c\rangle \\ &= \tfrac{1}{2^{\frac{n-k_1}{2}}} \sum_{v \in C_1{}^{\perp}} (-1)^{(v+m\cdot D)\cdot Z'}\,|v + m\cdot D + X'\rangle \end{aligned} \qquad (11)$$

such that $w_q(\vec{e'}) \leq [\frac{t}{2}]$ and $t = [\frac{min\{d_1,d_2\}-1}{2}]$, d_1 and d_2 are defined the same as in Theorem 1. Bob keeps the matrix G_i, C_i, D $(i = 1, 2)$ and the bits string $\vec{e'}$, m as his private keys and sends $|\psi\rangle$ to Alice over a public quantum channel.

3.2 Encryption

Suppose that Alice has a privacy message p in hand and wants to transmit it to Bob securely. She firstly applies an algorithm (algorithm 1) to transform p into a binary error vector $\vec{e''} = (X''|Z'')$ such that $t'' = w_q(\vec{e''}) \leq [\frac{t}{2}]$. Alice receives Bob's qubits $|\psi\rangle$ and applies error e'' on them as

$$\begin{aligned} &|\psi'\rangle = e''|\psi\rangle \\ &= \tfrac{1}{2^{\frac{n-k_1}{2}}} \sum_{v \in C_1{}^{\perp}} (-1)^{(v+m\cdot D)\cdot Z'\cdot Z''}\,|v + m\cdot D + X' + X''\rangle \end{aligned} \qquad (12)$$

Alice sends $|\psi\rangle$ back to Bob.

For quantum CCS codes, there are $3^{t''} \cdot \left(\begin{array}{c} N \\ t'' \end{array}\right)$ error vectors whose Hamming weight is t''. Borrowing the idea from the literature [15], we can construct one-to-one correspondence between this set of quantum error vectors $e'' = (X''|Z'')$ and integer p if they satisfy $0 \leq p < 3^{t''} \left(\begin{array}{c} N \\ t'' \end{array}\right)$.

Then, an algorithm can be devised to transform any integer p described above into a quantum error vector e'' using the order-preserving mapping induced by the lexicographic order of the vectors and the natural order of the integers.

Algorithm 1
$s \leftarrow \lfloor p/3^{t''} \rfloor; u \leftarrow t''; v \leftarrow p;$
$\omega \leftarrow v - 3^u \cdot \lfloor p/3^u \rfloor$
For $i = 1, 2, \cdots, t''$ $\{$
if $\omega \geq 2 \cdot 3^{m-i}$ *then* $\{$
$b_i = 2;\ u_i \leftarrow 1;\ v_i \leftarrow 1$ $\}$
else if $3^{m-i} \leq \omega < 2 \cdot 3^{m-i}$*=0*
then $\{$
$b_i = 1;\ u_i \leftarrow 1;\ v_i \leftarrow 0\}$
else $b_i = 0;\ u_i \leftarrow 0;\ v_i \leftarrow 1;$
$\}$
i=1;
For $j = 1, 2, \cdots, N$ $\{$
if $s \geq \left(\begin{array}{c} N-j \\ t'' \end{array}\right)$ *then* $\{x''_j \leftarrow u_i;\ z''_j \leftarrow v_i;\ i \leftarrow i+1;$
$s \leftarrow \left(s - \left(\begin{array}{c} N-j \\ t'' \end{array}\right)\right); t'' \leftarrow (t''-1);\}$
else $x''_j \leftarrow 0;\ z''_j \leftarrow 0;$
$\}$

3.3 Decoding

Let $H_1^{(i)}$, $H_2^{(j)}$ represent the i'th row of H_1 and the j'th row of H_2 respectively, $1 \leq i \leq n-k_1$, $1 \leq j \leq n-k_2$. Bob receives the quantum state C and measures the eigenvalues of $\sigma_x^{[H_1^{(i)}]}$ and $\sigma_z^{[H_2^{(j)}]}$ (say $(-1)^{z(i)}$ and $(-1)^{x(j)}$, $z(i)\ ,\ x(j) \in F_2$) respectively. After that, Bob obtains the syndromes Y_1 and Y_2. i.e.

$$\begin{aligned} \sigma_x^{[H_1^{(i)}]}\,|\Psi\rangle &= (-1)^{z(i)}\,|\Psi\rangle\ ,\ 1 \leq i \leq n-k_1 \\ \sigma_z^{[H_2^{(j)}]}\,|\Psi\rangle &= (-1)^{x(j)}\,|\Psi\rangle\ ,\ 1 \leq j \leq n-k_2 \\ Y_1 &= (z(1)\ ,\ \cdots\ ,\ z(n-k_1)), \\ Y_2 &= (x(1)\ ,\ \cdots\ ,\ x(n-k_2)). \end{aligned}$$

Bob computes $Z = (z_1, \cdots, z_n)$, $X = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ such that

$$H_1 \cdot Z^T = Y_1^T, \qquad (13)$$

$$H_2 \cdot X^T = Y_2^T. \qquad (14)$$

Bob obtains the error vector $e = (X|Z)$ and recovers $|m'\rangle$ by decoding the quantum codes $|\psi'\rangle$. He measures $|m'\rangle$ using computationally basis $\{|0\rangle, |1\rangle\}$ and compares the measurement result m' with his original bits m. If $m \neq m'$, he believes that eavesdropping happens in the quantum channel. Otherwise, he computes $e'' = (X''|Z'')$

$$e'' = e + e' \tag{15}$$

and performs algorithm 2 to recover Alice's secrete bits p.

Algorithm 2
$u \leftarrow t''; i = 0;$
For $j = 1, 2, \cdots, N$ {
$b_i \leftarrow 0;$
if $(x''_j = 1) \vee (z''_j = 1)$ *then* {
$s \leftarrow \left(s + \left(\begin{array}{c} N-j \\ t'' \end{array}\right)\right); t'' \leftarrow (t'' - 1);$
if $(x''_j = 1) \wedge (z''_j = 1)$ *then* {
$b_i = 2;$}
else if $(x''_j = 1) \wedge (z''_j = 0)$ *then* {
$b_i = 1;$}
else $b_i = 0;$}
i=i+1;
}
$k = \sum_{i=0}^{t''} b_i \cdot 3^i;$
$p = s \cdot 3^u + k.$

4 Analysis

4.1 Correctness

Theorem 2 *(Correctness) Supposing all the entities involved in the scheme follow the protocol, then Bob obtains Alice's secret messages correctly.*

Proof. The correctness of this scheme can be easily seen by inspection. In the absence of intervention and noise over quantum channel, Bob and Alice add some errors e' and e'' on the encoded messages respectively in the encoding and encryption phases. Because the summation of the numbers of error positions of e' and e'' is not larger than t, which can be corrected without disturbing the quantum states. Bob can obtain Alice's secret message p by computing $e'' = e' + e$ and performing algorithm 2 in the end of the decoding phase. By comparing the decoded bits m' with m, Bob can detect the existence of eavesdropper in the communication channel.

4.2 Security against eavesdropping

In this subsection, we consider an adversary Eve who has controlled the quantum channel linking Alice and Bob and tries to recover the plaintext p that Alice has sent to Bob. Supposing Eve knows the parity check matrix H_1 and H_2, she can obtain the error vectors if she can compute X and Z from the equations (13) and (14). We know that resolving equations (13) and (14) equals to the problem of decoding general linear codes, which is an NP-C problem [8]. Though quantum algorithms are shown exponentially faster than classical ones when coping with some problems, such as integer factor and discrete logarithm problem, it is widely believed that NP-C problems are still intractable by quantum (probabilistic) polynomial-time Turing machines [10]. We know that the Goppa codes used in the proposed scheme are uniquely decided by polynomials $g(Z)$ and ordered sets L. Therefore, if Eve wants to get the fast decoding algorithm of Goppa codes C_1 , C_2, she must find $g(z)$ and L. But the computational complexity of quantum Grover search algorithm to obtain $g(z)$ and L by the key G_2 , H_1 is $O((2^{mt}n!)^{\frac{1}{2}})$, it's still infeasible to break this cryptosystem by quantum searching algorithm in polynomial time. In fact, Eve doesn't know the matrix H_1, H_2 and G_2 because the generation matrices G_1, G_2 and the parity check matrices H_1, H_2 are Bob's private keys. Therefore, the difficulties of Eve's recovering of the secret messages are at least as decoding general linear codes.

The essential difference between this scheme with the EPR protocol[3], Ping-Pong protocol [5] and one-time-pad based [4] protocol is that it doesn't need to establish a quantum entangled channel and doesn't need to exchange (or broadcast) any additional classical messages to detect the existence of eavesdropper. In the proposed scheme, eavesdropping can be detected just by comparing some recovered bits m' and Bob's original bits m.

4.3 Man-in-the-middle attack

Just like all the existed QSDC schemes and Quantum key distribution, the proposed scheme does not also support the authenticity of the transferred message itself and works well only on an authenticated quantum channel. Similar to Diffie-Hellman protocol [13], this scheme permits Alice to communicate securely with Bob over an authenticated quantum channel without knowing Bob's secret keys. An active adversary in the middle of the communication between Alice and Bob can recover the secure messages and deceive both sides. This type of attack is so called man-in-the-middle attack (see protocol 1).

Protocol 1 (man-in-the-middle attack)

1. *Bob encodes $|m\rangle$ using quantum CSS codes Q and adds some error e$'$, and sends the states $|\psi\rangle$ to Alice.*

2. *Eve intercepts $|\psi\rangle$ and chooses a vicious message p' and transforms it to error vector e_a. She applies error e_a on $|\psi\rangle$ and obtains $|\psi_a\rangle$, and she impersonates Alice to send them back to Bob. At the same time, she prepares another quantum states $|\psi_e\rangle$ using her own CSS codes Q' ($Q \neq Q'$) and impersonates Bob to send them to Alice.*

3. *Alice performs algorithm* 1 *and transforms her secrete messages p to e''. She appplies error e'' on her re-*

ceived quantum states $|\psi_e\rangle$ and sends them back to Bob.

4. *Eve intercepts Alice's encoded states and decodes them as e''. She can do this because she knows the fast decoding algorithm of Q'. Eve recovers p using algorithm 2 and obtains Alice's secrete states.*

5. *The states Bob received in the decoding phase are the states that Eve has sent and the messages Bob recovers are Eve's spurious messages p'.*

There are two possible methods to avoid this kind of attack. One is to establish an quantum authenticated channel between the communication entities. Another way is that the communication entities Alice and Bob should preshare some secret keys. Studies of quantum message authentication are beyond the scope of this paper and the reader can refer to the literature [16]. Though the security of this scheme should be based on the existence of quantum authenticated channel, it can be used to securely transmit messages in some special cases in which the transmission time is urgent and it is difficult to establish session keys between two communication parties.

5 Conclusions

Error correcting codes have been widely used to construct cryptosytems in modern cryptography, including private-key and public-key encryption schemes. In this paper, a QSDC scheme is proposed using quantum CSS codes. In the proposed scheme, Alice can securely transmit some classical messages to Bob over an authenticated quantum channel without establishing any pre-shared keys and transforming any additional classical information. In this scheme, Alice firstly maps her secure messages to some error vector and applies this error on the encoded states that Bob sent to her. Eve can't recover the plaintext because she knows nothing about Bob's secrete keys. The security of the proposed scheme is based on the fact that decoding general linear codes is NP-C problem and Goppa cods have efficient decoding algorithm.

References

[1] Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India (1984) 175–179.

[2] Beige A., Englert B.G., Kurtsierfer C. *et al.*: Secure communication with a publicly known key, Acta Phys. Pol. A. **101** (2002) 357–368.

[3] Boström K., Felbinger T.: Deterministic Secure Direct Communication Using Entanglement, Physics Review Letter. **89** (2002) 187902.

[4] Deng F.G., and Long G.L.: Secure direct communication with a quantum one-time pad , Physical Review A. **69** (2004) 052319.

[5] Wòjcik. A.: Eavesdropping on the "Ping-Pong" Quantum Communication Protocol , Physics Review Letter. **90** (2003) 157901.

[6] Calderbank A. R., Shor P. W.: Good quantum error-correcting codes exist, Physics Review A. **54** (1996) 1098-1105.

[7] Steane A.M.: Multiple particle interference and quantum error correction, Proc. Roy. Soc. Lond. A. **452** (1996) 2551-2577.

[8] McEliece R.J.: A public-key cryptosystem based on algebraic coding theory, DSN Prog. Rep., Jet Prop. Lab., Caltech, Jan (1978) 114-116.

[9] Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review. **41** (1999) 303–332.

[10] Okamoto.T., Tanaka K., Uchiyama S.: Quantum public-key cryptosystems, In: Advances of Cryptology-CRYPTO 2000, Lecture Notes in Computer Science, Vol. 1880, Springer-Verlag, Berlin Heidelberg New York (2000) 147–165.

[11] MacWilliams F. J., Sloane N. J. A.: The theory of error-correcting codes, North-Holland, Amsterdam, 1977.

[12] Grover, L. K.: A fast quantum mechanical algorithm for database search. In: Proceedings of 28th STOC. (1996) 212–219.

[13] Diffie, W., Hellman, M.E.: New directions in cryptography, IEEE Trans. Info. Theory, IT-22(6) (1976) 644–654.

[14] Nielson, M, Chuang, I.: Quantum computation and quantum Information, Cambridge university press, 2000.

[15] Park, C.S. Computer Networks. **44** (2004) 265–273.

[16] Barnum, C., Gottesman, D., Smith, A. *et al.*: Authentication of Quantum Messages. In: Proceedings of 43rd Annual IEEE Symposium on the Foundations of Computer Science, Vancouver, Canada (2002) 449–458.