ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.3, March 2006, pp.509−515
DOI: 10.1360/jos170509

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于量子 Calderbank-Shor-Steane 纠错码的量子安全直接通信*

吕 欣[1,2+], 马 智[3], 冯登国[1]

[1](信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

[2](国家信息中心,北京 100045)

[3](中国人民解放军信息工程大学 信息研究系,河南 郑州 450002)

Quantum Secure Direct Communication Using Quantum Calderbank-Shor-Steane Error Correcting Codes

LÜ Xin[1,2+], MA Zhi[3], FENG Deng-Guo[1]

[1](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

[2](State Information Center, Beijing 100045, China)

[3](Department of Information Research, PLA Information Engineering University, Zhengzhou 450002, China)

+ Corresponding author: Phn: +86-10-88256433, Fax: +86-10-88258713, E-mail: lxdcs@hotmail.com, http://www.is.ac.cn

Lü X, Ma Z, Feng DG. Quantum secure direct communication using quantum Calderbank-Shor-Steane error correcting codes. *Journal of Software*, 2006,17(3):509−515. http://www.jos.org.cn/1000-9825/17/509.htm

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 (CSS) 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: information security; quantum cryptography; secure direct communication; quantum error correction codes

摘 要: 量子安全直接通信是继量子密钥分配之后提出的又一重要量子密码协议,它要求通信双方在预先不需要建立共享密钥的情况下就可以实现消息的保密传输.给出了一个新的量子安全直接通信方案,该方案利用量子 Calderbank-Shor-Steane(CSS)纠错码和未知量子态不可克隆等性质,方案的安全性建立在求解一般的线性码的译码问题是一个 NP 完全问题、Goppa 码有快速的译码算法和量子图灵机不能有效求解 NP 完全问题的基础上.在协议中,发送方 Alice 把要发送的秘密消息转化为一一对应的错误向量,把错误向量加到其接收到的、

* Supported by the National Science Foundation of China for Distinguished Young Scholars under Grant No.60025205 (国家杰出青年科学基金); the National Natural Science Foundation of China under Grant Nos.60403004, 60273027 (国家自然科学基金); the Graduate Innovation Foundation of Chinese Academic of Sciences (中国科学院研究生创新基金)

Received 2004-10-12; Accepted 2005-05-25

Bob 编码过的量子态上,并发给接收方 Bob.Bob 利用其私钥,通过测量、解码可以得到错误向量,并可以用相应的算法恢复出秘密消息.控制量子信道的攻击者 Eve 不能恢复出秘密消息,因其不知道 Bob 的密钥.与已有的量子安全直接通信方案相比,该方案不需要交换任何额外的经典信息和建立量子纠缠信道.

关键词: 信息安全;量子密码;安全直接通信;量子纠错码
中图法分类号: TP309 文献标识码: A

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, Wòjcik proved that, in this scheme, Eve can get a part of the secure message with some probability, especially in a noisy quantum channel[4]. Recently, Deng et al. put forward a quantum one-time-pad based QSDC scheme[5], 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 new QSDC scheme using quantum 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 codes have efficient decoding algorithm.

2 Preliminaries

2.1 Quantum CSS codes[6−9]

The constructions of quantum CSS codes rely heavily on the properties of classical error-correcting codes. Here, we first review the basic definitions of binary classical linear codes. Let's consider vectors and codes over the field F_2 including two elements, one and zero. The number of one's in a binary vector $\boldsymbol{v}$ over F_2 is called Hamming weight, noted as $w(\boldsymbol{v})$. Hamming distance $d(\boldsymbol{v},\boldsymbol{u})$ between two binary vectors $\boldsymbol{v}$ and $\boldsymbol{u}$ is $w(\boldsymbol{v}+\boldsymbol{u})$, which denotes the number of bits differing from each other between $\boldsymbol{v}$ and $\boldsymbol{u}$. A binary linear code C is an $[n,k]$ linear code over the finite field 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 F_2. A linear code C is always specified by an n by k generator matrix $\boldsymbol{G}$ whose entries are all zeroes and ones. The generator matrix $\boldsymbol{G}$ 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 $\boldsymbol{H}$ of a linear code $[n,k]$ is an $(n-k)\times n$ matrix such that $H_x=0$ for all those and only those vectors x in the code C. The rows of $\boldsymbol{H}$ 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 error correcting code (QECC) Q:$[[n,k,d]]$ is a 2^k-dimensional subspace of the Hilbert space C^{2^n}. It is a way of encoding k-qubit quantum states into n qubits ($k<n$) such that any error in $\le\left\lfloor\frac{d-1}{2}\right\rfloor$ 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 $n\le k_1+k_2$). 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

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

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 $G_2=\begin{pmatrix}H_1\\D\end{pmatrix}$, here the rank of $\boldsymbol{D}$ is $k=k_1+k_2-n$. Then each k-qubit basis state

$$|m\rangle=|m_1\ldots m_k\rangle(m\in F_2^k) \tag{2}$$

can be encoded into a quantum codeword

$$|c_w\rangle=\frac{1}{2^{\frac{n-k_1}{2}}}\sum_{v\in C_1^{\perp}}|v+m\cdot D\rangle=\frac{1}{2^{\frac{n-k_1}{2}}}\sum_{v\in C_1^{\perp}}|v+m\cdot D^{(1)}+\ldots+m_kD^{(k)}\rangle \tag{3}$$

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

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:

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix} \tag{4}$$

For any $a\in\{x,y,z\}$, $r=(r_1,\ldots,r_n)\in F_2^n$, let $\sigma_a^{[r]}=\sigma_a^{[r_1]}\otimes\cdots\otimes\sigma_a^{[r_n]}$, where

$$\sigma_a^{[r_i]}=\begin{cases}I, & \text{if } r_i=0\\ \sigma_a, & \text{if } r_i=1\end{cases} \tag{5}$$

Then every error on n qubits can be represented as $e=\sigma_x^{[X]}\sigma_z^{[Z]}$, here $X=(x_1,\ldots,x_n)$, $Z=(z_1,\ldots,z_n)\in F_2^n$.For convenience, we also use binary vector $e=(X|Z)$ to describe the error $e=\sigma_x^{[X]}\sigma_z^{[Z]}$.

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[10]. Here we only consider binary Goppa Codes.

Definition 1. Suppose $g(z)$ is a polynomial of degree t over finite fields F_{2^m}. Let

$$L=\{\gamma_0,\gamma_1,...,\gamma_{n-1}\}\subset F_{2^m} \tag{6}$$

such that $|L|=n$ and $g(\gamma_i)\neq 0$ for $0\leq i\leq n-1$.Then the Goppa code $\Gamma(L,g(z))$ with Goppa polynomial $g(z)$ is defined to be the set of codewords

$$\left\{c=(c_0,c_1,...,c_{n-1})\in F_2^n \left| \sum_{i=0}^{n-1}\frac{c_i}{z-\gamma_i}\equiv 0 \bmod g(z)\right.\right\} \tag{7}$$

From the above definitions, it's easy to know that Goppa code $\Gamma(L,g(z))$ is uniquely determined by $g(z)$ and L. It can also be proved that $\Gamma(L,g(z))$ has parameters $[n,k>n-mt,d\geq t+1]$[11]. 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.

3 The Proposed Quantum Secure Direct Communication Scheme

This section describes a QSDC scheme using quantum CSS codes introduced in Section 2. In the scheme, Alice transforms a secure message p into a binary error vector and then encrypts it via quantum coding procedures. Bob can recover the message because he has the fast decoding algorithm of the error correction codes. The scheme is specified as follows.

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 $t=\left\lfloor\frac{d-1}{2}\right\rfloor$, $k=k_1+k_2-n$. We assume that the quantum channel used in this scheme is noiseless channel.

Step 1. Encoding

Bob randomly chooses a generator matrix G_i and parity check matrix H_i of C_i (i=1,2) such that $G_2=\begin{pmatrix}H_1\\ D\end{pmatrix}$, here the rank of $\boldsymbol{D}$ is $k=k_1+k_2-n$.He then randomly prepares a basis state $|m\rangle$ such that $m\in F_2^k$ and encodes it into $|c\rangle$ using quantum CSS codes Q according to equation (3). Bob acts some error $e'=(X'|Z')$ on $|c\rangle$ as

$$|\psi\rangle=e'|c\rangle=\frac{1}{2^{\frac{n-k_1}{2}}}\sum_{v\in C_1^{\perp}}(-1)^{(v+m\cdot D)\cdot Z'}|v+m\cdot D+X'\rangle \tag{8}$$

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

Step 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 $e''=(X''|Z'')$ such that $t''=w_q(e'')\leq\left\lfloor\frac{t}{2}\right\rfloor$. Alice receives Bob's qubits $|\psi\rangle$ and applies error e'' on them as

$$|\psi'\rangle=e''|\psi\rangle=\frac{1}{2^{\frac{n-k_1}{2}}}\sum_{v\in C_1^{\perp}}(-1)^{(v+m\cdot D)\cdot Z'\cdot Z''}|v+m\cdot D+X'+X''\rangle \tag{9}$$

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

For quantum CCS codes, there are $3^{t''}\cdot\begin{pmatrix}N\\ t''\end{pmatrix}$ error vectors whose Hamming weight is t''. Borrowing the idea from Ref.[12], we can construct one-to-one correspondence between this set of quantum error vectors $e''=(X''|Z'')$

and integer p if they satisfy $0\le p< 3^{t''}\cdot\binom{N}{t''}$.

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.

$s\leftarrow\lfloor p/3^{t''}\rfloor; u\leftarrow t''; v\leftarrow p$

$\omega\leftarrow v-3^{u}\cdot\lfloor p/3^{t''}\rfloor$

for i=1,…, t'' {

if $\omega\ge 2\cdot 3^{m-i}$ then {

b_i=2; $u_i\leftarrow$1; $v_i\leftarrow$1}

else if $3^{m-i}\le\omega<2\cdot 3^{m-i}$

then {

$b_i\leftarrow$0; $u_i\leftarrow$0; $v_i\leftarrow$1;}

i=1

for j=1,…,N{

if $s\ge\binom{N-j}{t''}$ then $x_j''\leftarrow u_i; z_j''\leftarrow v_i; i\leftarrow i+1;$

$s\leftarrow\left(s-\binom{N-j}{t''}\right); t''\leftarrow(t''-1);$

else $x_j''\leftarrow 0; z_j''\leftarrow 0;$

}

Step 3. Decoding

Let $H_1^{(i)}, H_2^{(j)}$ represent the i'th row of H_2 respectively, $1\le i\le n-k_1, 1\le j\le n-k_2$. Bob receives the quantum state $|\psi'\rangle$ and measures the eigenvalues of $\sigma_x^{\left[H_1^{(i)}\right]}$ and $\sigma_z^{\left[H_2^{(i)}\right]}$ (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.

$$\sigma_x^{\left[H_1^{(i)}\right]}|\psi'\rangle=(-1)^{z(i)}|\psi'\rangle, 1\le i\le n-k_1 \tag{10}$$

$$\sigma_z^{\left[H_2^{(j)}\right]}|\psi'\rangle=(-1)^{x(j)}|\psi'\rangle, 1\le j\le n-k_2 \tag{11}$$

$$Y_1=(z(1),\ldots,z(n-k_1)),\ Y_2=(x(1),\ldots,x(n-k_2)) \tag{12}$$

Bob computes $Z=(z_1,\ldots,z_n)$, $X=(x_1,\ldots,x_n)\in F_2^n$ such that

$$H_1\cdot Z^T=Y_1^T \tag{13}$$

$$H_2\cdot X^T=Y_2^T \tag{14}$$

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 $m\ne m'$, he believes that eavesdropping happens in the quantum channel. Otherwise, he computes $e''=(X''|Z'')$, $e''=e+e'$ and performs Algorithm 2 to recover Alice's secrete bits p.

Algorithm 2.

$u\leftarrow t''$, $i\leftarrow$0;

for j=1,…,N{

b_i=0;

if $(x''_j=1)\vee(z''_j=1)$ then {

$s\leftarrow\left(s+\binom{N-j}{t''}\right);t''\leftarrow(t''-1);$

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 p 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 Eqs.(13),(14). We know that resolving Eqs.(13),(14) equals to the problem of decoding general linear codes, which is an NP-C problem[10]. Though quantum algorithms are shown exponentially faster than classical ones when coping with some problems, such as integer factor and discrete logarithm problem[13], it is widely believed that NP-C problems are still intractable by quantum (probabilistic) polynomial-time Turing machines[14]. 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. However the computational complexity of quantum Grover search algorithm to obtain $g(z)$ and L by the key C_2,H_1 is $O((2^{mt}n!)^{1/2})$, and it is 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 the general linear codes.

The essential difference between this scheme with the EPR protocol, Ping-Pong protocol and one-time-pad based 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.

5 Conclusions

Error correcting codes have been widely used to construct cryptosystems in modern cryptography. 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 cannot 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 codes have efficient decoding algorithm.

References:

[1] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proc. of the IEEE Int'l Conf. on Computers Systems and Signal Processing. Bangalore: IEEE, 1984. 175−179.

[2] Beige A, Englert BG, Kurtsierfer C. Secure communication with a publicly known key. Acta Physica Polonica A, 2002,101(3):357−368.

[3] Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Physics Review Letters, 2002,89(18): 187902.

[4] Wòjcik A. Eavesdropping on the "ping-pong" quantum communication protocol. Physics Review Letters, 2003,90(15):157901.

[5] Deng FG, Long GL. Secure direct communication with a quantum one-time pad. Physical Review A, 2004,69(5):052319.

[6] Calderbank AR, Shor PW. Good quantum error-correcting codes exist. Physics Review A, 1996,54(2):1098−1105.

[7] Steane AM. Multiple particle interference and quantum error correction. Proc. of the Royal Society A: Mathematical, Physical and Engineering Sciences, 1996,452(1954):2551−2577.

[8] Calderbank AR, Rains EM, Shor PW, Sloane NJA. Quantum error correction via codes over GF(4). IEEE Trans. on Information Theory, 1998,44(4):1369−1387.

[9] Ma Z, Lü X, Feng DG. Computationally secure uncloneable encryption scheme. In: Surakampontorn W, ed. Int'l Symp. on Communications and Information Technologies. Sapporo: IEEE, 2004. 927−930.

[10] McEliece RJ. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42−49, Jet Propulsion Lab. Caltech, 1978. 114−116.

[11] Patterson NJ. The algebraic decoding of Goppa codes. IEEE Trans. on Information Theory, 1975,21(2):203−207.

[12] Park CS. Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems. Computer Networks, 2004,44(2):265−273.

[13] Nielson M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000.

[14] Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems, In: Bellare M, ed. Advances of Cryptology-CRYPTO 2000. LNCS 1880, Heidelberg: Springer-Verlag, 2000. 147−165.

LÜ Xin was born in 1977. He is an assistant professor at the National Information Center. His current research areas are information and network security, cryptography protocols, etc.

MA Zhi was born in 1973. She is an associate professor at the PLA Information Engineering University. Her current research areas are information security and cryptography.

FENG Deng-Guo was born in 1965. He is a professor at the Institute of Software, Chinese Academic of Sciences. His current research interests are information and network security.