A Hybrid Encryption Protocol for Quantum Digital Signature

Xin Lü[+] Deng-guo Feng

State Key Laboratory of information security

Graduate School, Chinese Academic of Sciences, Bejing, 100039,China

+ Email: lx@is.ac.cn Homepage: http://www.is.ac.cn/personalweb/lvxin/index.htm

Abstract: Digital signature is one of the important tasks of modern cryptography, which is concerned with the "authenticity" of data on channel. In this paper, a hybrid encryption protocol for quantum digital signature is proposed and the realization of the algorithm needs the assistance of an arbitrator. The scheme uses private key algorithm to ensure the security of the message on channel and employs quantum public-keys to perform signature. By introducing redundancy information, we can sign a general unknown quantum state indirectly. The protocol using maximally entangled Greenberger-Horner-Zeilinger (GHZ) triplet states to realize the transmission of quantum state. The security of the scheme is based on so called quantum one-time-pad and the existence of quantum one-way functions. Based on quantum correct code, we also give an improved scheme. Security analysis show that the proposed quantum signature scheme is provable security.

Key words: quantum cryptography; digital signatures; quantum error correction code

1 Introduction

A major future research theme for cryptography is to weaken the assumptions on which security proofs are based, in particular computational intractability assumptions [1]. Quantum cryptography is one candidate for exploring the unconditional security cryptosystems. The idea of introducing quantum mechanics to cryptography was traced to Wiesner in1970s and published till 1983 [2], which proposed that if single-quantum states could be stored for long periods of time they could be used as counterfeit-proof money. Bennett and Brassard [3] gave the first quantum key distribution protocol, called BB84, which is provable security [4,5].

Digital signature and message authentication play the important role in modern cryptography and are widely used in network communication systems [6]. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. Many signature schemes could be constructed under some computational assumption and mathematics methods, such as Number Theory and Algebra. Quantum digital signature (QDS) systems, however, are more difficult to deal with than classical ones due to the fundamental feature of quantum information, such as no

cloning [7] theorems and entanglement, which has no analogous classical counterpart.

Gottesman and Chuang proposed a quantum digital system [8] based on quantum one-way functions and the scheme is absolutely secure, even against powerful cheating strategies. The input of the scheme is a classical bit-string and the public key of the sender is quantum state. Unfortunately, the digital system couldn't sign a general quantum superposition state, but only can deal with quantum basis state.

Zeng GH provided an arbitrated quantum signature scheme, the security of which is due to the correlation of the GHZ triplet states and the use of quantum one-time pads [9]. The scheme requires that the signed quantum state is known to the signatory (always call Alice, and the receiver Bob). It seems impossible to sign a general unknown quantum state [8,10].

In this paper, we present a quantum digital signature scheme which is unconditional secure. The scheme could indirectly sign a general unknown quantum state by introducing classical redundancy information. The security of the algorithm is due to the quantum one-time-pad and the existence of quantum one-way functions.

Section 1 introduces some preliminary knowledge about quantum computation and quantum cryptography we will use in this article. In Section 2, the quantum signature scheme is proposed and the security is considered in Section 3. Based on quantum error correction code, we give an improved scheme in Section 4. Conclusions and open questions are given in Section 5.

Further information about quantum computation and quantum cryptography can refer to Ref. [11-13].

2 Preliminaries

2.1 Quantum message encryption

Quantum key distribution cares about how to use some special quantum state (such as EPR pair) secretly transferring classical keys along quantum channel. Quantum message encryption, however, considers how two parties could send quantum state with perfect security. Boykin gave a quantum one-time-pad encryption protocol, which using 2n bits classical secret keys to encrypt n qubit, and shown this scheme is optimal [14]. The encryption protocol described as below

(1) Alice and Bob share some classical keys $k \in F_2^{2n}$, where $k = (\alpha \mid \beta) = (\alpha_1, \cdots, \alpha_n \mid \beta_1, \cdots, \beta_n)$.

(2) Suppose Alice has *n*-qubit state ρ. Alice applies unitary operation U_k to ρ according to k and obtains the cipher text $\rho_c = U_k \rho U_k^+$. Alice sends ρ_c to Bob.

Here $U_k = X^\alpha Z^\beta$, $X^\alpha = \otimes_{i=1}^n \sigma_x^{\alpha_i}$, $Z^\beta = \otimes_{i=1}^n \sigma_z^{\beta_i}$, and

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

(3) Bob applies unitary operation U_k^+ specified by his secret key k and obtains the plaintext ρ.

For an eavesdropper Eve, what she always "sees" in the quantum channel is a totally mixed state and she can't learn anything from the plaintext because two processes that output the same density matrices are indistinguishable.

2.2 Quantum Swap Test Circuit

Unlike classical information, comparing of two unknown quantum state is difficult. Buhrman et al [15] proposed a quantum circuit (see fig.1), called quantum swap test circuit (QSTC), which could test whether two unknown quantum states are identical or not with one-sided error. The circuit is presented as Fig.1.

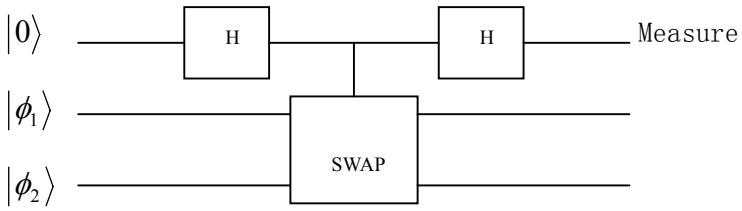

Fig.1: Quantum swap test circuit (QSTC)

The function of the circuit is to test if $|\phi_1\rangle = |\phi_2\rangle$ or $|\langle\phi_1 | \phi_2\rangle| \le \delta$ by the procedure that measures and outputs the fist qubit of the state $(H \otimes I)(c-SWAP)(H \otimes I)|0\rangle|\phi_1\rangle|\phi_2\rangle$. Here H is the Hadmard transform, SWAP is to map $|\phi_1\rangle|\phi_2\rangle$ to $|\phi_2\rangle|\phi_1\rangle$, and C-SWAP is the controlled-SWAP. If the measurement result of the first qubit is $|0\rangle$, the swap test is passed, which always happens if $|\phi_1\rangle = |\phi_2\rangle$. If $|\langle\phi_1 | \phi_2\rangle| \le \delta$ holds, the measurement result $|0\rangle$ happens with probability at most $(1+\delta^2)/2$. The result $|1\rangle$ occurs only when $|\phi_1\rangle \ne |\phi_2\rangle$ with probability $(1-\delta^2)/2$. The idea is that an equality test exists, but fails with nonzero probability. If there are k copies of quantum state $|\phi_1\rangle^{\otimes k}$ and $|\phi_2\rangle^{\otimes k}$, $k = O(\log_2(1/\varepsilon))$, QSTC is performed *k* times and the error probability of the test could be reduced to any $\varepsilon > 0$.

2.3 Quantum stabilizer code

Quantum error correction code (QECC) is a way of encoding quantum data (having *m* qubits) into *n* qubits (m<n), which protects quantum states against the effects of noise. A general theory of QECC was first established by Calderbank and Shor [16] and Stean [17], in which definitions and constructions were given. Quantum stabilizer code was introduced by Gottesman [18] and independently Calderbank et al [19]. Quantum stabilizer code is an important class of QECC and has been used to the other subject of quantum information, such as quantum cryptography [5].

The Pauli operators $\{\pm I,\pm\sigma_x,\pm\sigma_y,\pm\sigma_z\}$ constitute a group of order 8. The *n*-fold tensor products of single qubit Pauli operators also form a group $G_n=\pm\{I,\sigma_x,\sigma_y,\sigma_z\}^{\oplus n}$, of order 2^{2n+1}. We refer to G_n as the n-qubit Pauli group. Let *S* denote an abelian subgroup of the n-qubit Pauli group G_n. Then the *stabilizer code* $H_S\subseteq H_{2^{2n}}$ satifies,

$$|\psi\rangle\in H_S \text{, iff } M|\psi\rangle=|\psi\rangle \text{ for all } M\in S. \tag{2}$$

The group *S* is called the stabilizer of the code, since it preserves all of the codewords.

For stabilizer code [[*n*, *k*, *d*]], the generators M_i and the errors E_a, write

$$M_iE_a=(-1)^{s_{ia}}E_aM_i,\ i=1,\cdots,n-k \tag{3}$$

The s_{ia}'s constitute a *syndrome* for the error E_a, as $(-1)^{s_{ia}}$ will be the result of measuring M_i if the error E_a happens. For a nondegenerate code, s_{ia}'s will be distinct for all $E_a\in\varepsilon$, so that measuring the $n-k$ stabilizer generators will diagnose the error completely.

3 A Quantum Signature Scheme

3.1 Security requirements

In the paper, our scheme is a cryptographic primitive involving three entities: an signer Alice，a receiver Bob of the signature, and an arbitrator Trent ,who authenticates and validates the signed message. The security of the signature scheme depends much on the trustworthiness of the arbitrator who has access to the contents of the messages. The existence of the arbitrator ensures that we can indirectly sign an unknown quantum state without Alice's deceiving.

The general requirements for QDS discussed in this article should satisfy the following:

(1) Each user (Alice) can efficiently generates his own signature on messages of his choice;

(2) A receiver Bob can efficiently verify whether a given string is a signature of another user on specific message;

(3) The signatory can't disavow that he has signed a message;

(4) It is infeasible to produce signatures of other users to message they didn't sign.

3.2 Signature scheme

3.2.1 Initialization phase

(1) Key Generation. Alice and Bob agree on some random binary strings K_A, K_B, K_C and K_D. K_A and K_B are shared between Alice and Trent and between Bob and Trent for encrypting quantum message. K_C and K_D are shared between Alice and Bob and between Bob and Trent for encrypting classical message. Here we can also leave out K_C and K_D by enlarging the length of K_A and K_B, but the increased parts of K_A and K_B will be the double length of K_C and K_D. So we prefer the four-keys strings to two-key ones for economizing the key recourse. To ensure that the scheme is unconditional security, we can generate the keys using quantum key distribution protocols, such as BB84 or EPR protocol [11].

(2) Triplet GHZ states distribution. Alice, Bob and Trent each have $s+k+k\lceil \log_2 m \rceil$ particles form $s+k+k\lceil \log_2 m \rceil$ triplet GHZ pairs. The triplet GHZ state we selects in the article is

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{4}$$

To gain the unspoiled GHZ state, we can employ the entanglement purification protocol [20] to produce a high-quality fewer GHZ pairs by sacrificing some of the particles of the larger ones.

3.2.2 Signing phase

(1) Alice's Public key generation.

(a) Generate 2k random secret strings $|u_{i,j}\rangle$, $u_{i,j} \in F_2^n$, $1 \le i \le k, j \in \{0,1\}$.

(b) Compute $|y_{ij}\rangle = |f(u_{ij})\rangle$, $1 \le i \le k, j \in \{0,1\}$. The function $f(u)$ is

$$|f(u)\rangle = \frac{1}{\sqrt{m}} \sum_{l=1}^{m} (-1)^{E_l(u)} \cdot |l\rangle, \tag{5}$$

where E: $\{0,1\}^n \to \{0,1\}^m$ is an error correcting code with fixed c>1, 0< δ <1 and m=cn. $E_l(u)$ denotes the lth bit of $E(u)$. The distance between distinct code words $E_l(u_1)$ and $E_l(u_2)$ is at least $(1-\delta)m$. Since two distinct code words can be equal in at most δm positions, for any $u_1 \neq u_2$ w have $\langle f(u_1)|f(u_2)\rangle \le \delta m / m = \delta$. Here $f(u)$

can be regard as a class of quantum one-way function [8,10], which is easy to compute, but difficult to reverse.

(c) Alice has $2k$ key pair $\{|u_{i,j}\rangle, |y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le k}$ and then publicly announces $\{|y_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le k}$ as her public key and keeps $\{|u_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le k}$ as her private key.

(2) Introduce redundancy information. Suppose Alice has a quantum state $|\varphi\rangle \in H_s$ (H_s represent s dimensional Hilbert space). Alice selects a random bit $|x\rangle = |x_1, \cdots, x_k\rangle$ $(x_i \in F_2, 1 \le i \le k)$ and generates the signature according to her key $K \in \{y_{i,j}, z_{i,j} \mid 1 \le i \le k, j = 0,1\}$

$$QSig_K(|x\rangle = |x_1, x_2, \cdots, x_k\rangle) = |y_{1,x_1}, \cdots, y_{k,x_k}\rangle = |a_1, a_2, \cdots, a_k\rangle = |a\rangle \tag{6}$$

Alice appends $|x\rangle$ and the signature $|a\rangle$ to the end of $|\varphi\rangle$ and now has a whole state $|\psi\rangle$ in H_N. Alice quantum encrypts (q-encrypts) $|\psi\rangle$ as ρ by K_A and sends it to Trent.

(3) Permutation. Trent receives ρ and q-decrypts it as $|\psi\rangle$. Then he measures the quantum basis state $|x\rangle$ by Z basis ($|0\rangle, |1\rangle$) and keeps the measurement result. Trent can do these operations because we suppose he knows the construction of the state Alice gives him. Trent applies a random N bit permutation P to $|\psi\rangle$ as $|\psi'\rangle$, then uses K_A to q-encrypt the state as τ and sends it back to Alice.

(4) Measurement I. Alice q-decrypts τ as $|\chi\rangle$ by K_A, but she doesn't know the structure of the state and any change of the quantum state will later be detected by Trent and Bob with large probability. Alice then combines $|\chi\rangle$ with her GHZ particles, and measures the pair in the Bell basis

$$|\Psi_{\pm}\rangle_{Aa} = \frac{1}{2}(|00\rangle_A + |11\rangle_A); \qquad |\Phi_{\pm}\rangle_{Aa} = \frac{1}{2}(|01\rangle_A + |10\rangle_A) \tag{7}$$

For one qubit $|\chi_i\rangle = \alpha|0\rangle + \beta|1\rangle$ of $|\chi\rangle$ as example, we give the measurements procedure, which was used to construct quantum security sharing protocol in Ref.[21]. We can express the four-particle state $|\Omega\rangle_4$ as

$$|\Omega\rangle_4 = \frac{1}{2}[|\Psi_+\rangle_{Aa}(\alpha|00\rangle_{bt} + \beta|11\rangle_{bt}) + |\Psi_-\rangle_{Aa}(\alpha|00\rangle_{bt} - \beta|11\rangle_{bt}) +$$

$$\left|\Phi_{+}\right\rangle_{Aa}(\beta\left|00\right\rangle_{bt}+\alpha\left|11\right\rangle_{bt})+\left|\Phi_{-}\right\rangle_{Aa}(-\beta\left|00\right\rangle_{bt}+\alpha\left|11\right\rangle_{bt})] \tag{8}$$

Here a,β are complex numbers and satisfy $\left|\alpha^{2}\right|+\left|\beta\right|^{2}=1$. After measurement, Alice will gain $2N$ classical bit ω and encrypt them using K_C as W by classical one-time-pad and sends them to Bob through classical channel. Here we use classical one-time-pad to ensure the unconditional security.

3.2.3 **Verification phase**

(1) Measurement II. Bob receives W and decrypts it as ω. Bob then measures each of his particles in the x direction and obtains either $\left|+x\right\rangle_b$ or $\left|-x\right\rangle_b$, where $\left|\pm x\right\rangle=\frac{1}{\sqrt{2}}(\left|0\right\rangle\pm\left|1\right\rangle)$. Bob encodes the measurement results $\left|r\right\rangle$ as ω',

$$\omega'=\begin{cases}0, & if\ \left|r\right\rangle=\left|+x\right\rangle\\ 1, & if\ \left|r\right\rangle=\left|-x\right\rangle\end{cases}. \tag{9}$$

Bob has N classical bit ω' and encrypts ω together with ω' as W' by K_D. Bob sends W' to Trent by classical channel.

(2) Measurement III and Reverse permutation. Trent decrypts W' and has Alice and Bob's measurement information. Now he can reconstruct Alice's qubit by performing some unitary transformation to each of his particles according to Alice and Bob's measurement results. (See Table 1)

Table 1 Trent's operation rules

	$\left\|\Psi_{+}\right\rangle_{Aa}$	$\left\|\Psi_{-}\right\rangle_{Aa}$	$\left\|\Phi_{+}\right\rangle_{Aa}$	$\left\|\Phi_{-}\right\rangle_{Aa}$
$\left\|+x\right\rangle_b$	I	σ_z	σ_x	$\sigma_x\sigma_z$
$\left\|-x\right\rangle_b$	σ_z	I	$\sigma_x\sigma_z$	σ_x

Here, $I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, σ_x and σ_z satisfies Eq. (1). Trent now has Alice's quantum state $\left|\psi'\right\rangle$ and then applies the reverse bit permutation P^{-1} and obtains $\left|\psi\right\rangle$. Trent q-encrypts $\left|\psi\right\rangle$ using K_B as π and sends the result to Bob.

(3) Verification. Bob receives the N qubits and q-decrypts π as $\left|\psi\right\rangle=\left|\varphi\right\rangle\left|x\right\rangle\left|a\right\rangle$. Bob keeps Alice's message $\left|\varphi\right\rangle$ and uses $\left|a\right\rangle$ and the quantum basis state $\left|x\right\rangle$ to verify the validity of the signature according to Alice's public key $\{\left|y_{i,j}\right\rangle\}_{j\in\{0,1\}}^{1\le i\le k}$.

$$QVer_K(|x\rangle,|a\rangle) = True \Leftrightarrow |a_i\rangle = |y_{i,x_i}\rangle \tag{10}$$

We can use the QSTC described in 1.2 to compare whether $|f(a_i)\rangle$ and $|y_{i,x}\rangle$ are the same or not. Because there are k qubits to be compared, so the error probability of the test can be reduced to $\left(\frac{1+\delta^2}{2}\right)^k$, where $\langle f_i | f_j \rangle \le \delta$ with $i \neq j$, and k is the security parameter. Let the number of the incorrect keys be e_j, and then rejects it as invalid signature if $e_j > cM$. Here c is a threshold for reject and acceptance in the protocol.

Theorem 1. (Correctness) Suppose all the entities involved in the scheme follow the protocol, then Eq. (10) holds.

Proof. The correctness of the scheme can be seen by inspection. In the absence of intervention, Alice, Bob and Trent will share the GHZ triple state at the end of the initialization phase. Similar to teleportation, after Trent sends the Alice's state recovered to Bob, Bob's output will be exactly the state of Alice's. Because Alice signs her message according to Eq. (6), it's easy to verify that Eq. (10) holds. □

4 Analysis of the signature Scheme

4.1 Forgery

Theorem 2. Other entities forge Alice's signature with a success probability at most $2^{-[n-\lceil \log_2 m \rceil]}$, even when they knows Alice and Trent's keys K_A, P and K_D.

Proof. First we consider that Bob is dishonest and want to forger Alice's signature. Because Bob doesn't know Alice's private key $\{|u_{i,j}\rangle\}_{j\in\{0,1\}}^{1\le i\le k}$, so Bob has difficulties to sign a legal signature of Alice. By Holevo's theorem[11], Bob can gain at most $\lceil \log_2 m \rceil$ bit of classical information from Alice's public key. Since he lack $n - \lceil \log_2 m \rceil$ bits of information about any public key which Alice hasn't revealed, he will only guess correctly at most on about $2^{-[n-\lceil \log_2 m \rceil]}$. Even In the worst case that Bob knows Alice and Trent's keys K_A, P and K_C, his successful probability to forge Alice's signature is at most $2^{-[n-\lceil \log_2 m \rceil]}$. But, in fact, Bob doesn't know anything about Alice and Trent's keys K_A, P and K_C.

For attacker Eve, because she doesn't share the GHZ triple state with Alice and Trent, so she has much more trouble to forger Alice's signature than Bob does. □

4.2 Repudiation

Alice can't denial for her signature. When dispute between Alice and Bob happens, they will

resort to Trent. Because Trent has one copy of Alice's public key and the information $|x\rangle$, he could tests the validity of Alice's signature and reveals Alice's cheating.

Theorem 3. Alice's success probability of replacing $|\varphi\rangle$ with another quantum state $|\tilde{\varphi}\rangle$ without Bob and Trent's detection is at most $s!/(s+k+k\lceil \log_2 m \rceil)!$.

Proof. Consider Alice replaces $|\varphi\rangle$ with another quantum state $|\tilde{\varphi}\rangle$ before her measurement. In the scheme, however, Trent applies bit permutation *P* in (3) of the signing phase could prevent Alice from doing replacement because Alice doesn't know anything about the structure of the state after Trent's permutation. Alice's random change of $|\psi'\rangle$ will unavoidably disturb the information $|x\rangle$ and her signature $|a\rangle$, which could be detected in the verification phase by Bob and Trent with probability $(k+k\lceil \log_2 m \rceil)!/(s+k+k\lceil \log_2 m \rceil)!$. So Alice's success probability of replacement is at most $s!/(s+k+k\lceil \log_2 m \rceil)!$. Alice's successful cheating probability decreases exponentially in the security parameter *k*. □

Bob can't denial receiving Alice's message because Bob can't obtain Alice's whole qubits without Trent's help.

4.3 Notes of the Scheme

(1) Encryption is necessary in quantum digital scheme. What should point out is, for quantum digital signature, plaintext $|\varphi\rangle$ can't be present on channel, but for the classical digital signature, this restriction is not required. For classical digital signature, the signatory always sends the message together with the signature $\{m, Sig(m)\}$ to Bob. Consider in the quantum case Alice sends $\{|\varphi\rangle \otimes |Sig(\varphi)\rangle\}$ to Bob without encryption. Suppose Eve controls the quantum channel and holds the information on channel, she can prepare a state entangled with $|\varphi\rangle$ by the operation $U|\varphi\rangle|0\rangle = |\varphi\rangle|\psi\rangle$ and keeps $|\psi\rangle$. After Bob's verifying of the signature, Eve measures every qubit of $|\psi\rangle$ with *z* bases, which leads that Bob's state destroys beyond his notice. So encryption is necessary in the quantum digital systems due to the entanglement-based attack. As declared in initialization phase, the "four-key" scheme K_A, K_B, K_C and K_D can be reduced to "two-key" one which includes only K_A, K_B, but the cost is to "transferring" the double

length of K_C and K_D to K_A, K_B.

(2) In the signing phase, the quantum public keys of Alice may be generated several copies. In our protocol, two copies of the public keys are enough, one for Bob and one for the arbitrator. What should point out is that the increase of the copies of the public keys will compromise the security of the system, so the copies must be limited to a lower number. Another disadvantages of public keys are that it is impossible to be distributed by a broadcast channel, so we must resort to special key distribution policy.

(3) The permutation P by Trent is necessary. To ensure that if the state Bob received is the original quantum state $|\varphi\rangle$, several means could be considered. One way is sending a copy of $|\varphi\rangle$ to Bob， which requires that Alice must know $|\varphi\rangle$. Even this requires met, comparing of two unknown quantum states by Bob is still difficult and fails with noticeable probability. Sending k copies of $|\varphi\rangle$, comparing by the quantum swap test circuit, to Bob will inevitably cause information leakage and the uncontrolled increases of keys. In our scheme, the quantum state $|\varphi\rangle$ can be an unknown state for Alice. The permutation P employed by Trent can prevent Alice from changing the state because Alice can't distinguish $|\varphi\rangle$ from $|x\rangle$ and the signature $|a\rangle$. Alice's replacements of the quantum state will be detected by Bob and Trent in the verification phase.

5 An improved protocol

From Theorem 3, we find that the probability of Alice's successful cheating isn't still satisfactory, even Bob and Trent can reveal her falsification with noticeable probability. Here we give an improved protocol using QECC to reduce the soundness error of the protocol.

Quantum error correcting code is not only a useful tool to combat noise in quantum computation, but also it plays an important role in some of unconditionally quantum key distribution schemes. Here, we use quantum stabilizer code to ensure that the completeness of the message and prevent Alice's cheating. The improved protocol is described as bellow.

(1) In the initialization phase, the bit permutation P is replaced by a stabilizer code $\{Q_k\}$ and a random bit string z shared by Trent and Bob. K_A, K_B, K_C and K_D are conserved except adjusting their length according to the corresponding length of the encrypted message. The step (2) is the same as the protocol of section 2 but distributing many more GHZ triplet state to the three entities.

(2) In signing phase, the bit permutation P by Trent in step (3) is superseded by the stabilizer code $\{Q_k\}$ and secret key z. After Trent decrypts (q-decrypts) ρ as $|\psi\rangle$ and measures the quantum basis state $|x\rangle$ by Z basis, he encodes $|\psi\rangle$ as $|\psi'\rangle$ according to Q_k for the code Q_k with syndrome z. He uses K_A to q-encrypt the state as τ and sends it back to Alice. Here, we note that the length K_A has been added. In step (2) of signing phase, Alice sent the encrypted $|\psi\rangle$ using parts of K_A are adequate.

(3) What needs to be reconsidered in verification phase is step (2) and (3). In step (2), after Trent reconstructs Alice's encoded qubit and q-encrypts $|\psi'\rangle$ using K_B as π, then he sends π to Bob.

(4) Bob receives and decrypts π as $|\psi'\rangle$. Bob measures the syndrome y' of the code Q_k on $|\psi'\rangle$. Bob compares if y' and y are equal. Then Bob verifies Alice's signature as described in section 2. If Bob's verification of the signature is passed, but Bob finds that y' and y are not equal, then he can decide Alice's cheating occurs during step (4) of the signing phase.

From the improved protocol, we can see that the change of Alice's quantum message will be unavoidably detected by Bob due to the quantum stabilizer code introduced.

6 Conclusion

Because of quantum no-cloning theorem and entanglement property, it is difficult to construct quantum digital signature. Several difficulties should be conquered when constructing a secure QDS scheme.

First, copies of general unknown quantum message are forbidden due to the no-cloning theorem;

Second, it's important to construct private quantum channels among entities to avoid the entanglement-based attack.

Third, it must be cautious to compare two unknown quantum state, because the comparing results are not always definite.

Considering the difficulties, a quantum digital signature scheme is proposed in this article. One

feature of the protocol is that the signatory can sign a general unknown quantum state by introducing redundancy information. The privacy key algorithm ensures that the security of the information on channel and the quantum public keys are used to sign message. The authenticity of the quantum information is obtained by a random bit permutation or stabilizer code. The security of the protocol is studied and the results show that it is provable security.

An open problem is that it's still not known whether there exists a general quantum message signature scheme that doesn't need the presence of an arbitrator.

Acknowledgement We thank Ma Zhi for helpful discussions on quantum cryptography.

References:

[1] Ueli M. Cryptography 2000±10. Lecture Notes in Computer Science, Springer-Verlag, 2001, 2000: 63-85.

[2] Wiesner S. Conjugate coding. SIGACT News, 1983,15: 78-88.

[3] Bennett C, Brassard G. Quantum cryptography reinvented. SIGACT News, 1987,18: 51-53.

[4] Lo H, Chau H F. Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances. Science, 1999, 283: 2050–2056.

[5] Shor P, Priskill J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Physical Review Letters, 2000, 85: 441 – 444.

[6] Menezes A, van Oorschot P, and Vanstone S. Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997

[7] Wootters W and Zurek W. A single quantum cannot be cloned, Nature, 1982,299: 802.

[8] Gottesman D, Chuang I. Quantum digital signatures, http://arxiv.org/abs/quant-ph/0105032,2001.

[9] Zeng GH, Christoph K. An arbitrated quantum signature scheme, http://arxiv.org/abs/quant-ph/0109007, 2001.

[10] Barnum C, Gottesman D, Smith A *et al*. Authentication of Quantum Messages, Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02), 2002.

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

[12] Xia PS. Quantum computation, Chinese Journal of Computer Research and Development, 2001,10:1153-1171 (in Chinese with English abstract).

[13] Priskill J. Quantum Information and Quantum Computation. California Institute of Technology, 1998.

[14] Boykin P, Roychowdury V. Optimal encryption of quantum bits. http://arxiv.org/abs/quant-ph/0003059, 2000.

[15] H. Buhrman, R. Cleve, J. Watrous, R. Wolf, Quantum fingerprinting, Physical Review Letters, 87:167902-167904, 2001.

[16] Calderbank A R, Shor P W. Good quantum error–correcting codes exist. Phys. Rev. A, 54:1098–1105, 1996.

[17] Steane A M. Multiple particle interference and quantum error correction. Proc. Roy. Soc. Lond. A, 1996,452:2551–2577.

[18] Gottesman D. Class of quantum error-correcting codes saturating the quantum hamming bound. Physical Review A, 1996,54:1862–1868.

[19] Calderbank A R, Rains E M, Sloane N J A and Shor P W. Quantum error correction and orthogonal geometry. Physical Review Letters, 1997,78:405–409.

[20] Bennett C, Brassard G, Popescu S *et al*. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Physical Review Letters, 1996, 76:722-726.

[21] M. Hillery, V. Buzek A. Berthiaume. Quantum secret sharing, Physical review A, 1999, 59:1829-1835.