# Quantum Multi-Signature Protocol Based on Teleportation

Xiao-Jun Wen, Yun Liu, and Yu Sun

School of Electronic Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Reprint requests to X.-J. W.; E-mail: wxjun36@gmail.com, szwxjun@sina.com

Z. Naturforsch. **62a,** 147 – 151 (2007); received January 11, 2007

In this paper, a protocol which can be used in multi-user quantum signature is proposed. The scheme of signature and verification is based on the correlation of Greenberger-Horne-Zeilinger (GHZ) states and the controlled quantum teleportation. Different from the digital signatures, which are based on computational complexity, the proposed protocol has perfect security in the noiseless quantum channels. Compared to previous quantum signature schemes, this protocol can verify the signature independent of an arbitrator as well as realize multi-user signature together. – PACS numbers: 03.67.Dd; 03.67.-a

*Key words:* Quantum Signature; Quantum Teleportation; Multi-User.

## 1. Introduction

Suppose a very important document, which is signed by Alice and Charlie, is sent to Bob. Once Bob receives it, he will verify its content and the signatures. If he confirms that the signatures were made by Alice and Bob together, he will accept this document, otherwise he rejects it. This is a typical digital multi-signature question in classical cryptography, and many schemes have been proposed to resolve it, but how to resolve it in quantum cryptography?

As we know, cryptography includes two important parts: encryption and authentication. The main goal of encryption is to prevent eavesdroppers from obtaining confidential information, such as encrypting the plain text into a cipher text and secret sharing. The main goal of authentication is to avoid that the messages are attacked such as forgery by others, authentication often includes three aspects: message authentication, user authentication and digital signature [1].

Digital signature is developed so far for this purpose as an addition to a message such that the message can neither be disavowed by the signatory nor can it be forged by the receive or a possible attacker, its idea comes from the conventional (handwritten) signature in our real life. The security of many digital signature schemes is based on computational complexity, such as *EIGamal* and *DSA*, however, it is vulnerable to threats of powered computing, and the emergence of the quantum computer would break these schemes easy. In quantum computation, we can compute complex problems, such as the factoring problem and the discrete logarithm problem, more rapidly with smaller source than classical computation by using quantum parallelism.

Different from classical cryptography, quantum cryptography is based on the physical characters [2 – 5], for example, eavesdropping can be detected by collapse of a quantum state during measurements. Quantum information signature (QMS) [6 – 8] is one of the technologies which combine quantum theory with classical cryptography and utilize quantum effects to achieve unconditional security.

Zeng [9, 10] had researched the quantum information signature scheme which was based on the Greenberger-Horne-Zeilinger (GHZ) [11] triplet states, but his scheme belongs to an arbitrated signature scheme, it requires a trusty arbitrator and only has one signatory. Lee [12] had proposed two quantum signature schemes with message recovery, one scheme used a public board and the other did not, however, his schemes relied on the availability of an arbitrator, and can be signed only by one user too. In these arbitrated signature schemes, the arbitrator such as system manager can access to the contents of the messages, therefore, the security of most arbitrated signature schemes depends heavily on the trustworthiness of the arbitrator. Furthermore, the existence of an arbitrator will reduce the communication efficiency of the whole system.

Quantum teleportation plays important roles in quantum information technology; it was invented by

Bennett et al. [13], and developed by many other scientists. The controlled quantum teleportation scheme was first presented by Karlsson and Bourennane [14], its idea was similar with the quantum secret sharing which was presented by Hillery et al. [15]. According to their scheme, a third party is included, so that the quantum channel is supervised by this additional party, the initial state can not be teleported unless all three parties agree to cooperate [16].

In this paper we propose a protocol for quantum information signature based on GHZ states and the controlled quantum teleportation. The feature of our protocol is that the message can be signed by the multi-user and it does not rely on an arbitrator.

The paper is outlined as follows. In Section 2, we introduce the basic theory how the controlled quantum teleportation can be applied in quantum signature. In Section 3, we propose the signature and verification protocol based on the controlled quantum teleportation. A preliminary security analysis is given in Section 4. In Section 5 we discuss the results and present some conclusions.

## 2. Basic Theory

The GHZ state is an entangled state of a three-qubit system, which is expressed as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}. \tag{1}$$

Suppose that the sender Alice, who possessed the particles, chooses one style transform on above state as follows:

*Transform 1*: If Alice performs a $C_{\mathrm{NOT}}$ operation on the first two qubits (the first qubit as the target qubit and the second qubit as the control qubit), the state of the tripartite system is transformed into

$$\begin{aligned} |\pi\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |011\rangle)_{123} \\ &= |0\rangle_1 \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{23}. \end{aligned} \tag{2}$$

The tripartite system has been divided into two independent subsystems and the last two qubits just in a Bell state $|\Phi^+\rangle$.

*Transform 2*: If Alice performs a unitary operation

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3}$$

on the third qubit of the GHZ state, she gets

$$|\psi'\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)_{123}. \tag{4}$$

Then she performs the $C_{\mathrm{NOT}}$ operation on the above state as the method of *transform 1* and she will get

$$\begin{aligned} |\pi'\rangle &= \frac{1}{\sqrt{2}}(|001\rangle + |010\rangle)_{123} \\ &= |0\rangle_1 \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{23}, \end{aligned} \tag{5}$$

where subsystem of the last two qubits is also in another Bell state $|\psi^+\rangle$.

Now, we suppose that Alice wants to teleport the single photons $M$'s state to Bob; the state is written as

$$|\psi\rangle_M = a|0\rangle + b|1\rangle, \tag{6}$$

where $a$ and $b$ satisfy $|a|^2 + |b|^2 = 1$. So she announces which transform she had chosen, then keeps particle 1 in her hand and sends the particle $M$ to Charlie with particle 2 as well as the particle 3 to Bob.

The particles $M$, 2 and 3 would become one of the states

$$|\phi_1\rangle_{M23} = (a|0\rangle + b|1\rangle)_M \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{23}, \tag{7}$$

$$|\phi_2\rangle_{M23} = (a|0\rangle + b|1\rangle)_M \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{23}. \tag{8}$$

This can be rewritten as

$$\begin{aligned} &|\phi_1\rangle_{M23} = \\ &\frac{1}{2}\big[|\Phi^+\rangle_{M2}(a|0\rangle + b|1\rangle)_3 + |\Psi^+\rangle_{M2}(a|1\rangle + b|0\rangle)_3 \\ &\quad + |\Phi^-\rangle_{M2}(a|0\rangle + b|1\rangle)_3 + |\Psi^-\rangle_{M2}(a|1\rangle + b|0\rangle)_3\big], \end{aligned} \tag{9}$$

$$\begin{aligned} &|\phi_2\rangle_{M23} = \\ &\frac{1}{2}\big[|\Phi^+\rangle_{M2}(a|1\rangle + b|0\rangle)_3 + |\Psi^+\rangle_{M2}(a|0\rangle + b|1\rangle)_3 \\ &+ |\Phi^-\rangle_{M2}(a|1\rangle + b|0\rangle)_3 + |\Psi^-\rangle_{M2}(a|0\rangle + b|1\rangle)_3\big], \end{aligned} \tag{10}$$

which

$$\begin{aligned} |\Phi^{\pm}\rangle_{M2} &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{M2}, \\ |\Phi^{\pm}\rangle_{M2} &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{M2}. \end{aligned} \tag{11}$$

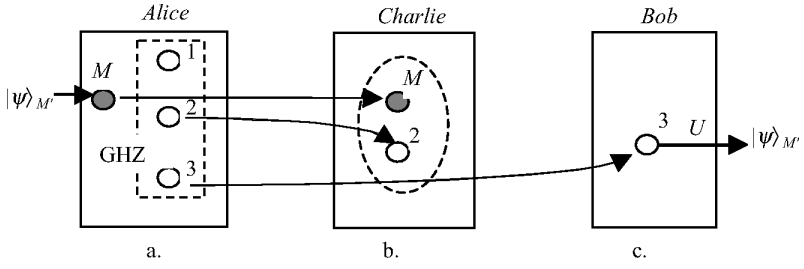


Fig. 1. Scheme of our signature protocol. (a) Alice performs transform on GHZ states to obtain $S_A$. (b) Charlie does Bell-base measurement on $M2$ to obtain $S_C$. (c) Bob performs transform on particle 3 to verify signatures.

After having received the particles $M$, 2 from Alice, Charlie performs a Bell-base measurement on qubits $M2$, and then announces his measurement outcome. Depending on Alice's transform choice and Charlie's four possible measurement outcomes $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\}$, Bob can recover the particle $M$'s original state to particle 3:

$$|\psi\rangle_3 = (a|0\rangle + b|1\rangle)_3 \tag{12}$$

by the corresponding transforms as listed in Table 1, where the matrices in the third column are

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{13}$$

Let us now see how the original state of particle $M$ can be reconstructed. Suppose Alice announced that she had performed *transform 1* on one triplet GHZ particle, then sends particle $M$ combined with particle 2 to Charlie while sends particle 3 to Bob. If Charlie performs a Bell-base measurement on qubits $M2$, and announces his measurement outcome is $|\Phi^-\rangle$, then Bob may perform the $\hat{\sigma}_z$ operation on the particle 3 to recover the state of particle $M$. We conclude that the original state $|\Psi\rangle_M$, using the GHZ particles as the channels, can be teleported to Bob by the help of Charlie.

## 3. Signature Protocol Description

Let us now see how to accomplish quantum message signature by Alice and Charlie, and then verify the message and its signature by Bob (see Fig. 1). We denote the message which Alice sends to Bob as $M$, signature of Alice as $S_A$ and signature of Charlie as $S_C$.

### *3.1. Initial Phase*

1) Alice prepares $n$ triplets of particles system in state $|\psi\rangle_{123}$, which are expressed as $\{|\psi(1)\rangle_{123}, |\psi(2)\rangle_{123}, \ldots, |\psi(n)\rangle_{123}\}$.

Table 1. Alice's transform choice, Charlie's measurement outcomes and the corresponding transforms by Bob.

| Alice's choice of transform on GHZ particles | Charlie's measurement outcome of particles $M$ and 2 | Bob's transform on particle 3 |
|---|---|---|
| *Transform 1* | $\|\Phi^+\rangle$ | $I$ |
| | $\|\Phi^-\rangle$ | $\hat{\sigma}_z$ |
| | $\|\Psi^+\rangle$ | $\hat{\sigma}_x$ |
| | $\|\Psi\rangle$ | $\hat{\sigma}_z\hat{\sigma}_x$ |
| *Transform 2* | $\|\Phi^+\rangle$ | $\hat{\sigma}_z$ |
| | $\|\Phi^-\rangle$ | $\hat{\sigma}_z\hat{\sigma}_x$ |
| | $\|\Psi^+\rangle$ | $I$ |
| | $\|\Psi\rangle$ | $\hat{\sigma}_z$ |

2) Alice prepares qubits in the eigenstates $(|0\rangle, |1\rangle)$, which correspond to the classical message $M$. These $n$ particles' states are expressed as

$$|\psi\rangle_M = \{|\psi(1)\rangle_M, |\psi(2)\rangle_M, \ldots, |\psi(n)\rangle_M\} = \{a_1|0\rangle + b_1|1\rangle, a_2|0\rangle + b_2|1\rangle, \ldots, a_n|0\rangle + b_n|1\rangle\}, \tag{14}$$

where ($|a_i| = 0$ and $|b_i| = 1$) or ($|a_i| = 1$ and $|b_i| = 0$).

3) To keep the signature secret, Alice shares a quantum key $K_a$ with Bob as well as Charlie shares a quantum key $K_c$ with Bob. They may establish the secret keys by the famous BB84 protocol.

### *3.2. Signature Phase*

Step 1: Alice performs *transform 1* or *transform 2* on each triplet according to $K_a$. If $K_a^i = 0$, she performs *transform 1* on $|\psi(i)\rangle_{123}$. If $K_a^i = 1$, she performs *transform 2* on $|\psi(i)\rangle_{123}$. Alice records this as $T_A = \{T(1), T(2), \ldots, T(n)\}$ ($T(i) \in \{$ "*transform 1*", "*transform 2*"$\}$) and encrypts $T_A$ and $(a_i, b_i)$ with the key $K_a$. She gets her signature

$$S_A = E_{K_a}\{T_A, (a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)\}. \tag{15}$$

Step 2: To each triplet, Alice leaves particle 1 to herself, and sends particles $\{M(i)\}$ combined with the corresponding particle 2 to Charlie. At the same time,

she sends $S_A$ with particle 3 to Bob. By now, Alice has already finished her steps for signing the message $M$.

Step 3: After having received $\{M(i)\}$ and particle 2 from Alice, Charlie performs a Bell-base measurement on qubits $M2$ in each triplet, and records the outcomes as $\beta_C = \{\beta(1), \beta(2), \ldots, \beta(n)\}$ ($\beta(i) \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$). He encrypts $\beta_c$ with $K_c$ to get $S_C = E_{K_C}(\beta_C)$; $S_C$ is Charlie's signature to the message $M$.

Step 4: Charlie sends $S_C$ to Bob.

### *3.3. Verification Phase*

Bob can verify Alice's and Bob's signature directly by the following steps:

Step 1: After having received $S_A$ with particle 3 from Alice and $S_C$ from Charlie, Bob decrypts $S_A$ to obtain $T_A$ and $\{(a_i, b)_i\}$ by $K_a$ as well as decrypts $S_C$ to obtain $\beta_C$ by $K_c$.

Step 2: Bob performs the corresponding transformation $U$ on particle 3 in each triplet according to the values of $T(i)$ and $\beta(i)$. The transformation methods refer to Table 1.

For example, if $T(1) =$ "*transform* 1" and $\beta(1) = |\Phi^+\rangle$ then Bob performs $I$ operator on particle 3 of the first triplet.

Step 3: By Bob's transformations, particle 3 is recovered to the state

$$|\psi(i)\rangle_3 = (a'_i|0\rangle + b'_i|1\rangle)_3. \tag{16}$$

Bob measures the state of particle 3 in each triplet using measurement basis $\{|0\rangle, |1\rangle\}$, and reads out the values of $a'_i$ and $b'_i$.

Step 4: Bob compares $(a'_i, b'_i)$ with $(a_i, b_i)$. If $a'_i = a_i$ and $b'_i = b_i$, then he accepts $S_A$ and $S_C$ as the truthful signature of message $M$ signed by Alice and Charlie, respectively.

## 4. Security Analysis and Discussion

The message to be signed can not be tampered. In our protocol, Alice sends $\{M(i)\}$ to Charlie thus Charlie must know the content of the message which he had signed. In addition, anyone else who captures these particles could read out the information by measuring them, but this can not make trouble to our protocol, because Alice sends $\{(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)\}$ encrypted by $K_a$ to Bob; thus any forgery of the message would be found by Bob.

The security of a signature protocols requires that the signature can not be forged as well as the signatory can not disavow his signature. We will demonstrate that the present signature protocol has perfect security as follows.

### *4.1. Impossibility of Forgery*

In our protocol, Alice's signature $S_A$ is encrypted by $K_a$ and Charlie's signature $S_C = K_c(\beta_C)$ is encrypted by $K_c$. Because $K_a$ and $K_c$ are distributed via QKD protocol proved as unconditionally secure [2, 3], so the attacker Eve can not forge $S_A$ and $S_c$ which are secret for her. If Eve randomly selects the two string $K'_a$ and $K'_c$ to execute the protocol, her attack strategy will be detected by Bob with the probability lager than $1 - 1/2^{|K_a|+|K_c|}$, where $|K_a|$ and $|K_c|$ denote the length of $K_a$ and $K_c$, respectively. If $|K_a| + |K_c| \gg 0$, the probability of being detected approximates to 1.

We assume that Alice is dishonest and try to counterfeit her signature, however, because her signature comes from transformation performed on each triplet according to $K_a$, so her signature must be identical with $K_a$ known to Bob. Alice may have a cheating strategy that though sends $T_A = \{T(1), T(2), \ldots, T(n)\}$ included in $S_A$ according to $K_a$. In fact she performed opposite transformation on each triplet to cheat Bob. But she does not know Charlie's measurement results, that is to say, she is able to counterfeit the contents of column 1 in Table 1, but can not counterfeit the contents of column 2, so this cheating strategy would destroy the correlation of teleportation and be detected by Bob.

Suppose that Charlie is dishonest and try to counterfeit his signature $S_C$, he would deliberately choose some false Bell states (one of $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$) to replace his exact measurement results. That is to say, he is able to counterfeit the contents of column 2 in Table 1, but can not counterfeit the contents of column 1 which educe to $S_A$, so his forgery would cause that their results dissatisfy the correlation of teleportation.

This protocol needs Alice and Charlie to cooperate to accomplish the message signature, so never mind that Alice in collusion with Charlie cheats Bob.

### *4.2. Impossibility of Disavowal*

For the signatures $S_A$ contains Alice's secret key $K_a$ as well as $S_C$ contains Charlie's secret key $K_c$, Alice and Charlie can not disavow their respective signature. But in the direct check signature technique of classical

cryptography, the message signatory possibly says that his private key has lost so as to disavow his signature. However, our protocol is based on quantum characters; any disturbance to the entangled particles by attackers, such as Eve's interception and measurement, will destroy the correlations of these entangled states, and this is very easy to be detected. So, Alice, Charlie and Bob can not disavow that they have performed respective operations on these particles. In other words, the signatories can not disavow their signatures, and the verifier can not disavow having received these signatures.

### *4.3. Asymetry Problem between the Parties Alice and Charlie*

Because Alice's status is different from that of Charlie, Alice should prepare the message and act as the first signatory. But Charlie needs only to sign the message as the second signatory; thus it is natural that there is an asymetry between the parties Alice and Charlie in the protocol.

In practice, we can add another user who replaces Alice to prepare the GHZ states, but this would reduce the communication efficiency of the protocol. In fact, it always exists the possibility that one of th users signs the message firstly, so it is having an asymetry between the parties Alice and Charlie.

## 5. Conclusions

In summary, we propose a protocol which can be used in quantum multi-user signature. The realization of signature and verification is based on the characters of GHZ states and the controlled quantum teleportation. Our protocol is designed to use quantum key distribution and the correlation of GHZ states to guarantee perfect security. Different from the classical digital signatures which are based on computational complexity, our protocol is based on physical characters. Compared to the former presented quantum signature scheme [9, 10, 12], it does not rely on an arbitrator. So our protocol is more secure and provides higher communication efficiency.

It is worthwhile to note that for the existence of all kinds of unavoided noises in the communication channels [17], the qualities of quantum entangled states would be debased with the increment of communication time and distance, and this would reduce the security and efficiency of our scheme. To guarantee the unconditional security of quantum communication, how to eliminate further influences caused by the noises is a permanent topic.

*Acknowledgements*

This work was supported by the National Natural Science Foundation of China, Grants No. 60572035 and by the Foundation of Beijing Municipality Key Laboratory of Communication and Information System (No. JD100040513). We are indebted to the anonymous referee for valuable comments.

[1] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York 1996.
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] D. Mayers, J. ACM **48**, 351 (2001).
[4] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000).
[5] G. Guo and G. Guo, Phys. Lett. A **310**, 247 (2003).
[6] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, FOCS′02, Vancouver 2002, p. 449.
[7] D. Gottesman and I. Chuang, Technical report http://arxiv.org/abs/quant-ph/0105032 (2001).
[8] X. Wen, Y. Liu, and Z. Zhang, J. Electron. Info. Tech. **27**, 811 (2005) (in Chinese).
[9] G. Zeng, W. Ma, X. Wang, and H. Zhu, Acta Electron. Sin. **29**, 1098 (2001).
[10] G. Zeng and K. Christoph, Phys. Rev. A **65**, 042312 (2002).
[11] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[12] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, Phys. Lett. A **321**, 295 (2004).
[13] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[14] A. Karlsson and M. Bourennane, Phys. Rev. A **58**, 4394 (1998).
[15] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[16] T. Gao, Z. Naturforsch. **59a**, 597 (2004).
[17] S. Xiang and K. Song, Acta Phys. Sin. **55**, 529 (2006).