Quantum Group Signature Scheme Based on Chinese Remainder Theorem

Xin Sun¹, Ying Guo¹, Jinjing Shi¹, Wei Zhang¹, Qin Xiao¹, Moon Ho Lee²

¹School of Information Science & Engineering, Central South University, Changsha, China; ²Institute of Information and Communication, Chonbuk National University, Chonju, Korea. Email: sunxinshifeng@163.com, moonho@chonbuk.ac.kr

Received 2013

ABSTRACT

A novel quantum group signature scheme is proposed based on Chinese Remainder Theorem (CRT), in order to improve the security of quantum signature. The generation and verification of the signature can be successfully conducted only if all the participants cooperate with each other and with the message owner's and the arbitrator's help. The quantum parallel algorithm is applied to efficiently compare the restored quantum message to the original quantum message. All the operations in signing and verifying phase can be executed in quantum circuits. It has a wide application to E-payment system, Online contract, Online notarization and etc.

Keywords: Quantum Signature; Group Signature; Chinese Remainder Theorem

1. Introduction

Digital signature is one of the most important part of modern cryptography, which serves as a basic module to design cryptography protocols [1]. Digital signature is usually employed to guarantee the authenticity, integrity, and non-disavowal of transmitting messages. Group signature scheme was introduced in 1991 by Chaum and Heyst [2] firstly. In 1997, Camenisch and Stadler [3] improved Chaums scheme and developed the more efficient scheme CS97 for larger groups. CS97 was further enhanced by Bresson and Stern [4] to be revocable for group numbers. Moreover, Atienese and Camenisch [5] proposed a safe and efficient group signature scheme in 2000. Those are mostly based on the complexity of the system employed and they become increasingly vulnerable with more powerful computation. This difficulty can be overcome by quantum cryptography [6]. The biggest difference between quantum cryptography and classical cryptography is that quantum cryptography is the combination of quantum mechanics and cryptography, where the security is ensured by physical principles such as the Heisenberg uncertainty principle and the quantum no-cloning theorem. Now quantum cryptography has attracted a great deal of attention because it can stand against quantum attack, and has put forward many advances in quantum cryptography, including quantum secret sharing, quantum key distribution (QKD) [7-10] and quantum secure direct communication (QSDC) [10-14].

Taking advantage of the quantum properties of physical, many quantum signature schemes have been introduced. Zeng et al. introduced a quantum signature scheme based on the classical signature theory and quantum cryptography [15-18], whose algorithm is a symmetrical quantum key cryptosystem with Greenberger-Horne-Zeilinger (GHZ) triplet states. Li et al. proposed an arbitrated quantum signature scheme using Bell states [19]. Gottesman and Chuang proposed a quantum digital signature scheme based on quantum one-way function [20], and Lee also presented two quantum signature schemes with message recovery [21]. Unconditional security of the above quantum signature schemes have been proved, but they are not designed for 'group'. Therefore, a group signature can be devised based on quantum cryptography.

In this paper, we propose a group signature scheme based on Chinese Remainder Theorem (CRT). In our scheme, secret key is unforgeable, generated by the owner, and can be shared with the arbitrator based on QSCD protocol. The signing group contains two participants, and they collaborate to sign on the message by applying CRT with arbitrator and restore the message by performing the inverse CRT with arbitrator's assistance for the verification of signature. However, any t-1 or fewer participants can neither sign on the message nor restore the signed message. The message owner cooperate to verify the message by applying a quantum comparison circuit for comparing the restored quantum message to the original quantum message and arbitrator could inform message owner and group participants of
the verified result. Furthermore, all the quantum circuits and operation gates are packaged in black boxes [22] to enhance the security.

The rest of this paper is organized as follows. Sect. 2 introduces the basic knowledge about our scheme. Sect. 3 proposes a quantum group signature scheme which includes an initial phase, a signing phase, and a verification phase. Security analysis is made in Sect. 4, and a brief conclusions are drawn in Sect. 5.

2. Preliminaries

The original Chinese Remainder Theorem was proposed by SunZi and later republished in 1247 by Qin[23]. The CRT is often applied in computer science, such as RSA algorithm calculation, classical secret sharing and etc, and several versions of the Chinese Remainder Theorem have been proposed. The general CRT can be described as follows.

Lemma 1. Let \( n > 2, b_1, b_2, \ldots, b_n \) be relatively prime in pairs, and \( a_1, a_2, \ldots, a_n \in \mathbb{Z} \). The system of equations

\[
\begin{align*}
Y &= a_1 \mod b_1 \\
& \vdots \\
Y &= a_n \mod b_n
\end{align*}
\]

(1)

has solutions in \( \mathbb{Z} \) if \( \gcd(b_i, b_j) = 1 \), for all \( 1 \leq i \neq j \leq n \). The solution can be obtained as

\[
Y = \sum_{i=1}^{n} T_i B_i a_i \mod B
\]

(2)

where \( B = b_1 \times b_2 \times \cdots b_n \), \( B_i = B / b_i \), \( T_i \times B_i \mod b_i = 1 \), for all \( 1 \leq i \leq n \), and \( Y < B \).

According to this theorem, Alice can obtain the group signature. Suppose Alice sends the message number \( x \) to the Bob (group participants), Bob encrypts \( x \) by the secret key \( b_i \) based on Equation (1), and the result \( a_i \) is the element of the sequence of the signature. In this way, Alice can obtain his group signature.

3. Scheme Descriptions

The text above shows the basic signing algorithm of this scheme. Next the details of the scheme can be illustrated as follows, which contains three participants Alice (the message owner), G (the signing group), and Trent (the arbitrator). The three phases of our quantum signature scheme are introduced as follows.

3.1. Initial Phase

Step 1. Set up a signing group \( G \), whose participants are \( Bob_1(\xi = 1,2,\cdots,n) \). According to QSDC protocol, G can share the secret key \( K_\xi(\xi = 1,2,\cdots,n) \) with Trent, in which \( K_\xi \) denotes the own private key of \( Bob_\xi \) and \( K_\xi \) is relatively prime.

Step 2. In this paper, we discuss the binary 3-qubit system, which can be defined as

\[
|\psi\rangle_{sys} = \frac{1}{\sqrt{2}} \left[ |0xy\rangle + (-1)^z |1xy\rangle \right],
\]

(3)

where \( x, y, z \in \{0,1\} \).

3.2. Quantum Group Signing Phase

In this quantum group signature scheme, Alice prepares a quantum message. The group \( G \) generates a signature with assistance of Trent who doesn't understand the details about the signing algorithm. The participants of group \( G \) don't communicate with other.

Step 1. Alice's quantum message sequence \( |P\rangle \) contains \( m \) qubits, i.e.

\[
|P\rangle = \{ |p_0\rangle, |p_1\rangle, \ldots, |p_j\rangle, \ldots, |p_{m-1}\rangle \},
\]

(4)

where \( |p_j\rangle \) forms as Eq. (3).

Step 2. Alice sends the sequence \( |P\rangle \) to Trent with superdense coding. Alice encodes \( |p_j\rangle \) as \( |p_j^*\rangle \) with the unitary operations \( U_{sys} \). The transformations can be summarized as

\[
|p_{uvw}^*\rangle = U_{(xyz\overline{uvw})}|p_{xyz}^*\rangle,
\]

(5)

where \( x, y, z, u, v, w \in \{0,1\} \), binary strings \( xyz \) and \( uvw \) correspond to the decimal numbers, and

\[
\begin{align*}
U_{000} &= I \otimes I \otimes I, & U_{001} &= I \otimes I \otimes X, & U_{010} &= I \otimes X \otimes I, \\
U_{011} &= I \otimes X \otimes X, & U_{100} &= X \otimes I \otimes I, & U_{101} &= X \otimes I \otimes X, \\
U_{110} &= X \otimes X \otimes I, & U_{111} &= X \otimes X \otimes X.
\end{align*}
\]

Step 3. Trent receives the

\[
|P^*\rangle = \{ |p_0^*\rangle, |p_1^*\rangle, \ldots, |p_j^*\rangle, \ldots, |p_{m-1}^*\rangle \}.
\]

According to Eq. (3), the quantum message \( |P^*\rangle \) can be rewritten as

\[
|\psi\rangle_{sys} = \prod_{i=0}^{m-1} \frac{1}{\sqrt{2}} \left[ |0x_iy_i\rangle + ( -1 )^{z_i} |1x_iy_i\rangle \right],
\]

(6)

where \( x_i, y_i, z_i \in \{0,1\} \). The states of \( |P^*\rangle \) refer to a binary sequence \( R = \{x_0, y_0, x_1, y_1, \ldots, x_{m-1}, y_{m-1}\} \), so the corresponding classical message \( X \) can be acquired by Trent.

For example, if Trent receives a quantum sequence like \( |P^*\rangle = \{ |000\rangle, |001\rangle, |110\rangle \} \), it can be represented as

\[
\begin{align*}
|\psi\rangle_{sys} &= \frac{1}{2\sqrt{2}} \left[ |000\rangle + |111\rangle \right] \left[ |001\rangle - |110\rangle \right] \left[ |010\rangle - |101\rangle \right],
\end{align*}
\]

corresponding a binary sequence \( R = \{000111101\} \), and Trent can derive the decimal classical message \( X = 28 + 26 + 25 + 24 = 368 \). Then Trent sends \( X \) to the group \( G \).

Step 4. The participants of group \( G \) receives \( X \) collectively. As discussed in CRT's function in the paper, Bob
(Bob₁,Bob₂,...,Bobₙ) sign on the quantum message |P⟩ by transforming X as following algorithm

\[ S = X \mod K_ξ \]  \hspace{1cm} (7)

where \( K = \{ K_ξ \mid 1 ≤ K_ξ ≤ 64, ξ = 1,2,\cdots,t \} \) is the Bob_ξ’s private key, and \( S = \{ S_1,0 ≤ S_1 ≤ 63, ξ = 1,2,\cdots,t \} \) is the generated classical remainder. \( K_ξ \) and \( S_ξ \) can be represented by 6-bit binary sequence and according to Equation (3) the state can be shown as

\[ |ψ⟩_S = \prod_{ξ=0}^{2(ξ-1)} \frac{1}{2} \left[ |0x_ξy_ξ⟩ + (-1)^{ξ} |1x_ξy_ξ⟩ \right] \]  \hspace{1cm} (8)

Signature \( |S⟩ \) can be donated as follows

\[ |S⟩ = \left\{ S_1, S_2, \cdots, S_t, |ψ⟩_S \right\} \]  \hspace{1cm} (9)

where \( S_ξ \) is the classical remainder, \( |ψ⟩_S \) is the corresponding state of \( S_ξ \).

Step 5. Bob can send the signature \( |S⟩ \) to Trent.

### 3.3. Verification Phase

A verification algorithm is developed here based on the CRT such that Alice is able to verify Bob’s signature \( |S⟩ \). The verification process requires the assistance of Trent.

Step 1. When Trent receives Bob’s signatures \( |S⟩ \), he restores message as Equation (2) to \( X^* \). The algorithm can be shown as follows,

\[ X^* = \sum_{ξ=1}^{m} T_ξD_ξS_ξ \mod D \]  \hspace{1cm} (10)

where \( D = K_ξ \times K_ξ \times \cdots K_ξ, D_ξ = D/K_ξ \times T_ξ \times D_ξ \mod K_ξ = 1, \) for all \( ξ \in \{1,2,\cdots,t\} \). If \( X^* ≠ X \), the signature has obviously been forged and Trent may reject this signature immediately. If \( X^* = X \), Trent goes on for further verification.

Step 2. Trent transforms \( X^* \) to the binary sequence \( \tilde{X}^* \). The process can be described as follows,

\[ \tilde{X}^* = \begin{cases} \frac{X^* - \sum_{z=0}^{m-1} \tilde{X}^* z^{-dζ \cdot 1}}{dζ} \mod d_ξ, ζ > 0 \\ 0, ζ ≤ 0 \end{cases} \]  \hspace{1cm} (11)

where \( d = 2 \). The binary sequence can be represented as \( \tilde{X}^* = \{ \tilde{X}^*_0, \tilde{X}^*_1, \cdots, \tilde{X}^*_m \} \), which corresponds to the states of \( |\tilde{P}⟩ \). In this way, Trent gets the quantum message \( |\tilde{P}⟩ \).

Step 3. Trent performs the corresponding reverse transformations \( U_{-1}^{ξ} \) \( (x,y,z ∈ \{0,1\}) \) on each state of \( |\tilde{P}⟩ \). He can obtain the the states of \( |\tilde{P}⟩ \). According to Equation (3), \( |\tilde{P}⟩ \) can be described as

\[ |ψ⟩_P = \prod_{ξ=0}^{2(ξ-1)} \frac{1}{2} \left[ |0x_ξy_ξ⟩ + (-1)^{ξ} |1x_ξy_ξ⟩ \right] \]  \hspace{1cm} (12)

where \( x_ξ, y_ξ, z_ξ ∈ \{0,1\} \). At last the restored message is acquired. Then Trent input it into the quantum verification circuit which is shown in Figure 1 [24] directly, and sends the signature \( |S⟩ \) to Alice at the same time.

Step 4. The message owner Alice also input the original message \( |ψ⟩_P \) into the quantum verification circuit at the same time. Then Alice starts to wait for the verification from Trent.

Step 5. We generalize the qubit string comparator introduced by Ref. [25] with quantum parallel algorithm [22] which makes the quantum computation on quantum message more effectively to compare \( |ψ⟩_P \) with \( |ψ⟩_P \).

The quantum circuit which is presented in Figure 1. In a measurement of the outputs \( (O_1, O_2) \), if \( O_1 = 1 \) and \( O_2 = 0 \) then \( |ψ⟩_p > |ψ⟩_P \); if \( O_1 = 0 \) and \( O_2 = 1 \) then \( |ψ⟩_p < |ψ⟩_P \); at last, if \( O_1 = 0 \) and \( O_2 = 0 \) then \( |ψ⟩_p = |ψ⟩_P \). When \( O_1 = 0 \) and \( O_2 = 0 \), the arbitrator Trent informs Alice and Bob the signature is legal and credible, otherwise he informs them that signature is invalid.

### 4. Conclusions

So far we have proposed a group signature scheme based on CRT. Now let us discuss the security of the group signature scheme. A secure quantum signature scheme should satisfy two requirements: one is that the message should not be forged by the attacker and the other is the impossibility of disavowal by the message originator and the signatory.

![Figure 1. The quantum circuit for comparing |ψ⟩_p to |ψ⟩_P in the black box. Each particle of |ψ⟩_p and |ψ⟩_P is inputted into this quantum circuit from left, and (2) is a processing unit of (1).](image-url)
4.1. Impossibility of Forgery

In this scheme, the arbitrator Trent is trusted, \( K_o \) cannot be forged. Anyone attempts to forge Bob’s signature would definitely be detected.

Specifically, assuming that Eve wants to imitate Bob’s signature \( |S\rangle \) sign on X which corresponding the message \( |P\rangle \). As shown by Equation (7), Eve must know the secret keys \( K_e \), but \( K_e \) cannot be forged.

The signature is unforgeable even by the message owner Alice who knows the messages and the corresponding signatures because of the unforgeable secret keys.

4.2. Impossibility of Disavowal by the Signatory and the Message Originator

According to Equation (7), Bob(signatory) would send \( |S\rangle \) to Trent. Since \( |S\rangle \) includes the keys \( K_s \), which is only known by Bob and Trent, Bob cannot disavow his signature \( |S\rangle \).

Alice also cannot disavow his receiving. Because the verifier Bob who really has verified the signature cannot later deny his involvement in that his verification of the message needs the help of Trent. If he denies his involvement, Trent can confirm that he tells a lie.

5. Conclusions

In this paper, we present a group signature scheme based on Chinese Remainder Theorem in which participants share their own key with arbitrator while they don’t communicate with other. Only when all the t participants cooperate with each other and with the message owner’s and the arbitrator’s assistance, the signature can be generated and verified successfully. The analysis of this scheme and show that secure signature can be derived. Moreover, by allowing the arbitrator to keep a record of all intermediate transmissions and computations, it is able to arbitrate the dispute between two users.

6. Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61272495), the Program for New Century Excellent Talents in University of Ministry of Education of China (NCET-11-0510), the Hunan Provincial Innovation Foundation For Postgraduate (Grant Nos. CX2011B087), the Excellent Doctoral Dissertation Fund of Central South University (Grant Nos. 2011yb3z030) and WCU 32-2010-000-20014-0 NRF (Korea).

REFERENCES


