Vol 17 No 2, February 2008
1674-1056/2008/17(02)/0415-04

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Multi-proxy quantum group signature scheme with threshold shared verification*

Yang Yu-Guang(杨宇光)[a)b)]

[a)] *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100022, *China*

[b)] *State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing* 100049, *China*

(Received 17 January 2007; revised manuscript received 13 March 2007)

A multi-proxy quantum group signature scheme with threshold shared verification is proposed. An original signer may authorize a proxy group as his proxy agent. Then only the cooperation of all the signers in the proxy group can generate the proxy signature on behalf of the original signer. In the scheme, any t or more of n receivers can verify the message and any $t-1$ or fewer receivers cannot verify the validity of the proxy signature.

Keywords: quantum signature, multi-proxy quantum group signature, threshold shared verification
PACC: 0365, 4230

1. Introduction

Quantum cryptography is one of the most remarkable applications of quantum mechanics to quantum information. Quantum cryptography exploits the principles of quantum mechanics to enable a provably secure distribution of private information, including quantum key distribution(QKD),[1−5] quantum secure direct communication(QSDC)[6−10] and so on.

With the development of quantum cryptography, quantum signature has been pursued by some groups.[11−15] Gottesman and Chuang[11] applied quantum one-way function to quantum signature. Zeng and Christoph[12] proposed an arbitrated quantum signature scheme in which signature and verification processes were performed with the help of a trusted third party.

In some special situations, for example, an original signer cannot make a signature because of some reasons such as the line of duty, illness and so on, and he may authorize a proxy group as his signature proxy agent. Only the cooperation of all members in the proxy group can generate the proxy signature on behalf of the original signer. However, the proposed schemes in Refs.[11–15] cannot meet such a requirement.

In this paper, we present a multi-proxy quantum group signature scheme with threshold shared verification. An original signer may authorize a proxy group as his proxy agent. Then only the cooperation of all the signers in the proxy group can generate the proxy signature on behalf of the original signer. In the scheme, any t or more of n receivers can verify the message while any $t-1$ or fewer receivers cannot verify the validity of the proxy signature. The present scheme follows some ideas of the classical Shamir's threshold signature one.[16]

2. Description of the present scheme

The present scheme includes the following three steps: the distribution phase of individual proxy key; the generation phase of the signature receivers' verification keys; the generation phase of proxy signature; and the threshold shared verification phase.

*Project supported by the National Basic Research Program of China (973 Program) (Grant No 2007CB311100), the National High Technology Research and Development Program of China (Grant Nos 2006AA01Z419 and 20060101Z4015), the Major Research plan of the National Natural Science Foundation of China (Grant No 90604023), 2008 Scientific Research Common Program of Beijing Municipal Commission of Education，The Scientific Research Foundation for the Youth of Beijing University of Technology (Grant No 97007016200701), the National Research Foundation for the Doctoral Program of Higher Education of China (Grant No 20040013007), the National Laboratory for Modern Communications Science Foundation of China (Grant No 9140C1101010601), and the Doctor Scientific Research Activation Foundation of Beijing University of Technology (Grant No 52007016200702).

2.1. Distribution phase of individual proxy key

An original signer shares a random key K with the agents using quantum secret sharing such as the ones in Refs.[17,18].

$$K = (a_1, b_1, a_2, b_2, \ldots, a_m, b_m), \tag{1}$$

$$K_j = (a_1^{[j]}, b_1^{[j]}, a_2^{[j]}, b_2^{[j]}, \ldots, a_m^{[j]}, b_m^{[j]}), \tag{2}$$

$$K = \oplus_{j=1}^{n} K_j, \tag{3}$$

where a_i, b_i, $a_i^{[j]}$, $b_i^{[j]}$ are in {0,1}; K_j is the jth agent's secret share in quantum secret sharing process and used as the jth agent's proxy key; $\oplus$ denotes addition modulo 2.

2.2. Generation phase of the signature receivers' verification keys

1) The signer makes n shares, $S_1, \ldots, S_n$ of K, similar to the classical Shamir's secret sharing scheme[16] over F_{2^N} as follows, where $N = 2m$. The signer shares n different $2m$-bits, and nonzero-valued x_j for $j = 1, \ldots, n$, with the receivers using quantum secret sharing schemes such as the ones in Refs.[17,18]. Also he chooses (randomly and independently) secret a_i for $i = 1, \ldots, t-1$ in F_{2^N}. He computes $S_j = f(\tilde{x}_j)$ for $j = 1, \ldots, n$ over F_{2^N}, where $\tilde{x}_j$ is a polynomial representation of x_j for $j = 1, \ldots, n$, where

$$\begin{aligned} f(x) =& a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots \\ &+ a_1 x + a_0 \text{ bmod } 2^N. \end{aligned} \tag{4}$$

$f(0) = a_0 = \tilde{K}$, where $\tilde{K}$ is the polynomial representation of K.

2) The signer sends $\tilde{S}_j$ to the receiver R_j for $j = 1, \ldots, n$, using the quantum secure direct communication schemes such as the ones in Refs.[9,10], where $\tilde{S}_j$ is the binary representation of S_j.

3) The receivers compute the preliminary information for the following verification procedure. The preliminary information depends on which subset of receivers is chosen for collaboration. Here, for simplicity in description, we assume the t receivers, $R_1, \ldots, R_t$, collaborate to do that.

For $j = 1, \ldots, t$, R_j calculates and secretly stores the following values given by the Lagrange interpolation formula:

$$A_j = S_j \prod_{1 \le l \le t, l \ne j} \frac{\tilde{x}_l}{\tilde{x}_l - \tilde{x}_j} \tag{5}$$

over F_{2^N}. Let

$$A^{[j]} = (e_1^{[j]}, f_1^{[j]}, e_2^{[j]}, f_2^{[j]}, \ldots, e_m^{[j]}, f_m^{[j]}) \tag{6}$$

be the binary representation of A_j in F_{2^N}, where $e_i^{[j]}$ and $f_i^{[j]}$ are in {0,1}. Although each secret value $S_j(A_j)$ is kept in each receiver R_j locally, these values satisfy the following equations globally:

$$\tilde{K} = \sum_{j=1}^{t} A_j \tag{7}$$

over F_{2^N}. In the binary representation, Eq.(7) can be written as

$$K = \oplus_{j=1}^{t} A^{[j]}, \tag{8}$$

where $\oplus$ represents bitwise exclusive-OR. Note that even in the following collaborative procedure, $K_j(A^{[j]})$ is kept secret to R_j and the original key $\tilde{K}(K)$ is not recovered.

2.3. Generation phase of proxy signature

Suppose that the signer wants to authorize the proxy group to sign a secret message M.

$$M = (c_1, c_2, \ldots, c_m), \tag{9}$$

where c_i is in {0,1}, $i = 1, \ldots, m$.

1) the first agent U_1 generates a quantum state for the secret message M

$$\begin{aligned} |\phi_1\rangle =& |\psi_{c_1 \oplus a_1^{[1]}, b_1^{[1]}}\rangle \otimes |\psi_{c_2 \oplus a_2^{[1]}, b_2^{[1]}}\rangle \otimes \cdots \\ & \otimes |\psi_{c_m \oplus a_m^{[1]}, b_m^{[1]}}\rangle, \end{aligned} \tag{10}$$

where for $i = 1, \ldots, m$, a qubit $|\psi_{c_i \oplus a_i^{[1]}, b_i^{[1]}}\rangle$ is one of the following states:

$$\begin{aligned} |\psi_{0,0}\rangle &= |0\rangle, \\ |\psi_{1,0}\rangle &= |1\rangle, \\ |\psi_{0,1}\rangle &= (|0\rangle + |1\rangle)/\sqrt{2}, \\ |\psi_{1,1}\rangle &= (|0\rangle - |1\rangle)/\sqrt{2}. \end{aligned} \tag{11}$$

The value of $b_i^{[1]}$ determines the measurement basis. If $b_i^{[1]}$ is 0, then $c_i \oplus a_i^{[1]}$ is encoded in the Z basis $\{|0\rangle, |1\rangle\}$; if $b_i^{[1]}$is 1, then $c_i \oplus a_i^{[1]}$ is encoded in the X basis $\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$.

Then he sends the quantum state $|\phi_1\rangle$ to U_2.

2) For $j = 2, \ldots, t$, U_j receives the $|\phi^{[j-1]}\rangle$ from U_{j-1}. To check a Trojan horse attack,[19–21] he measures the state $|\phi^{[j-1]}\rangle$ with some photon number splitters (PNSs: 50/50) and some detectors. The measurements will have at least two outcomes if the quantum signal is a multiphoton one. If the quantum signal

is a single one, then he applies $W^{[j]}$ to $|\phi^{[j-1]}\rangle$. $W^{[j]}$ is defined as

$$W^{[j]} = U_1^{[j]}V_1^{[j]} \otimes U_2^{[j]}V_2^{[j]} \otimes \cdots \otimes U_m^{[j]}V_m^{[j]}, \quad (12)$$

where

$$\begin{aligned} U_i^{[j]} =& U(a_i^{[j]}), \\ V_i^{[j]} =& V(b_i^{[j]}), \\ U(1) =& \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \\ U(0) =& |0\rangle\langle 0| + |1\rangle\langle 1|, \\ V(1) =& H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| \\ & + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|, \\ V(0) =& |0\rangle\langle 0| + |1\rangle\langle 1|. \end{aligned} \quad (13)\ (14)$$

U_j then obtains $|\phi^{[j]}\rangle$ by the unitary transformation

$$W^{[j]} : |\phi^{[j-1]}\rangle \longrightarrow |\phi^{[j]}\rangle. \quad (15)$$

If $j < t$, U_j sends $|\phi^{[j]}\rangle$ to U_{j+1}. Otherwise, the proxy signature process has been completed.

2.4. Threshold shared verification phase

From Eqs.(3) and (8), we can have

$$\begin{aligned} & (a_1^{[1]} \oplus \cdots \oplus a_1^{[n]}, \ldots, a_m^{[1]} \oplus \cdots \oplus a_m^{[n]}) \\ =& (e_1^{[1]} \oplus \cdots \oplus e_1^{[t]}, \ldots, e_m^{[1]} \oplus \cdots \oplus e_m^{[t]}), \quad (16) \\ & (b_1^{[1]} \oplus \cdots \oplus b_1^{[n]}, \ldots, b_m^{[1]} \oplus \cdots \oplus b_m^{[n]}) \\ =& (f_1^{[1]} \oplus \cdots \oplus f_1^{[t]}, \ldots, f_m^{[1]} \oplus \cdots \oplus f_m^{[t]}). \quad (17) \end{aligned}$$

Let $|\phi^{[t]}\rangle = |\psi^{[0]}\rangle$.

1) R_1 receives the state $|\psi^{[0]}\rangle$ from U_t. He checks the Trojan horse attack.[19−21] If the quantum signal is a single one, then he applies $Q^{[1]}$ to $|\psi^{[0]}\rangle$. $Q^{[j]}$ is defined as

$$Q^{[j]} = U_1^{[j]}V_1^{[j]} \otimes U_2^{[j]}V_2^{[j]} \otimes \cdots \otimes U_m^{[j]}V_m^{[j]}, \quad (18)$$

where

$$U_i^{[j]} = U(e_i^{[j]}), V_i^{[j]} = V(f_i^{[j]}). \quad (19)$$

R_1 then obtains $|\psi^{[1]}\rangle$ by the unitary transformation

$$Q^{[1]} : |\psi^{[0]}\rangle \longrightarrow |\psi^{[1]}\rangle. \quad (20)$$

Then he sends the quantum state $|\psi^{[1]}\rangle$ to R_2.

2) For $j = 2, \ldots, t$, R_j receives the state $|\psi^{[j-1]}\rangle$ from R_{j-1}. He checks the Trojan horse attack.[19−21] If the quantum signal is a single one, then he applies $Q^{[j]}$ to $|\psi^{[j-1]}\rangle$. R_j then obtains $|\psi^{[j]}\rangle$ by the unitary transformation

$$Q^{[j]} : |\psi^{[j-1]}\rangle \longrightarrow |\psi^{[j]}\rangle. \quad (21)$$

If $j < t$, R_j sends $|\psi^{[j]}\rangle$ to R_{j+1}. Otherwise, he proceeds to step 3).

3) R_t measures $|\psi^{[t]}\rangle$ on the basis $(0, 0, \ldots, 0)$ and obtains $(c'_1, c'_2, \ldots, c'_m)$. If $(c'_1, c'_2, \ldots, c'_m) = (c_1, c_2, \ldots, c_m)$, then the signature is valid.

3. Security analysis

Now we will analyse some possible cases: 1) intercept–resend attack; 2) individual cheating attack; 3) $(t-1)$-party cheating attack.

1) intercept–resend attack

The quantum state sent by R_j is multi-qubit tensor product. Each qubit is randomly in one of two conjugated bases. Without the information of $b_i^{[j]}$, the eavesdropper cannot perform the correct unitary operation on each qubit. If he takes an intercept–resend attack, the probability that this attack is not detected is $(1/4)^m$.

2) individual cheating attack

Before R_j receives the quantum state sent by R_{j-1}, the eavesdropper Eve can take the Trojan horse attack,[19−21] i.e. he intercepts it and sends another multi-photon quantum state to R_j. Eve expects to obtain R_j's secret operation information by measuring the quantum state operated by R_j with some photon number splitters (PNSs: 50/50) and some detectors. However his Trojan horse attack will be detected by R_1 in step 3) of the generation phase of group signature. It is similar to the case with the cheater being $R_i \quad i \neq j$.

3) $(t-1)$-party cheating attack

Suppose a dishonest member R_i aims to find out another member R_j's share and then forge the signature together with other $t-2$ members. R_i prepares a false signal and sends it to R_j. Then from the fake signal operated by R_j, R_i tries to gain R_j's share.

Without loss of generality, we assume that R_j performs one of four kinds of operations on every qubit with equal probability and that every single-qubit operation is independent. So it is sufficient to consider R_i's eavesdropping on one qubit.

R_i's false signal can be presented as $|\theta\rangle = |0\rangle(a|0\rangle+b|1\rangle)+|1\rangle(c|0\rangle+d|1\rangle)$, where $|a|^2+|b|^2+|c|^2+|d|^2 = 1$. For simplicity, we regard every probability

amplitude as a real number, but the security proof is fitted for a complex number. R_i sends the first qubit to R_j and keeps the second one.

R_j encodes his share by performing one of four kinds of operations with equal probability. The state can be expressed by

$$\begin{aligned} w =& \frac{1}{4}|\theta\rangle\langle\theta| + \frac{1}{4}(I\otimes I)|\theta\rangle\langle\theta|(U^+\otimes I) \\ &+ \frac{1}{4}(U\otimes I)|\theta\rangle\langle\theta|(U^+\otimes I) \\ &+ \frac{1}{4}(V\otimes I)|\theta\rangle\langle\theta|(I\otimes V^+) \\ &+ \frac{1}{4}(UV\otimes I)|\theta\rangle\langle\theta|(V^+U^+\otimes I). \end{aligned} \tag{22}$$

The mutual information between R_i and R_j that can be extracted from this state is given by the von-Neumann entropy, $I(R_i, R_j) \leq S(\mathrm{Tr}_e(w))$. In order to calculate the von-Neumann entropy, we need to calculate the eigenvalues of $\mathrm{Tr}_e(w)$, which are the roots of the characteristic polynomial $\det(\mathrm{Tr}_e(w) - \lambda I)$ as follows:

$$\lambda_{1,2} = \frac{1}{2}(1 + 2ab + 2cd). \tag{23}$$

So we have

$$I(R_i, R_j) \leq -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2. \tag{24}$$

For $\lambda_1 = \lambda_2 = \frac{1}{2}$, $I(R_i, R_j)$ reaches a maximal value 1 bit. So R_i can eavesdrop 1 bit of 2 bit operation information on one qubit.

However, $I(R_i, R_j)$ can also reach a maximal value when R_i prepares a legal qubit, namely the values of a, b, c and d are chosen to meet the condition $ab + cd = 0$. Due to the large number of the chosen a, b, c, d meeting the above condition, the values of a, b, c and d are not given here. So R_i cannot gain more information by sending a false signal than by sending a legal signal. R_i's eavesdropping will introduce errors and cause the signature to be invalid.

4. Conclusion

In this paper, we present a multi-proxy quantum group signature scheme with threshold shared verification. An original signer may authorize a proxy group as its proxy agent. Then only the cooperation of all the signers in the proxy group can generate the proxy signature on behalf of the original signer. In the scheme, any t or more of n receivers can verify the message and any $t-1$ or fewer receivers may not verify the validity of the proxy signature. The present scheme follows some ideas of the classical Shamir threshold signature one.[16]

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York) 173

[2] Ekert A 1991 *Phys. Rev. Lett.* **67** 661

[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 3995 (in Chinese)

[5] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[6] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[7] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[8] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[9] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[10] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601

[11] Gottesman D and Chuang I Technical Report, http://arxiv.org/abs/quant-ph/0105032,2001.

[12] Zeng G H and Christoph K 2002 *Phys. Rev.* A **65** 042312

[13] Lee H, Hong C, Kim H, Lim J and Yang H J 2004 *Phys. Lett.* A **321** 295

[14] Lu X and Deng F G 2004 *CIS*2004 *Lecture Notes in Computer Science* vol. 3314

[15] Lu X and Deng F G 2004 http://arxiv.org/abs/quant-ph/0403046,2004

[16] Shamir A 1979 *Commun. ACM* **22** 612

[17] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329

[18] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[19] Cai Q Y 2006 *Phys. Lett.* A **351** 23

[20] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[21] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101