Quantum threshold signature based on divisible quantum entanglement and p-unitary operator

Zhen-Hu Ning

College of Computer Science, Beijing University of Technology, Beijing 100124, China

e-mail address: nzh41034@163.com

Abstract: Different from the existing quantum threshold signature schemes, which are mainly based on the classical Shamir's threshold signature scheme, we construct the map from the multiple binary information to a quantum and support a new threshold signature scheme based on divisible quantum entanglement and p-unitary operator, which are well defined in the paper. Compared with the existing the schemes, the scheme involved fewer quanta. The scheme also meets the requirement of "Threshold Signature", that is to say, only the number of participants is not less than the threshold, they can execute the signature or the verification.

Keywords Quantum signature , Threshold signature, divisible quantum entanglement, p-unitary operator,

As an important Quantum cryptography, quantum secure direct communication(QSDC) has attracted many attentions and a lot of achievements are obtained [10~23], such that the QSDC protocol based on the idea each bit of key can contains one bit of secret message and a additional classical information[11,12,16,22], the QSDC protocol based on the idea quantum dense coding with an EPR pair[5] and the QSDC protocol based on the idea order rearrangement[19,20].

Many quantum threshold signatures have been obtained[2-9]. A classic quantum threshold signature was given by [6,7] , which are based on the classical Shamir's threshold signature scheme[24] and the map from one binary information to one quantum.

In this paper, Different from the existing quantum threshold signature schemes, we support a new threshold signature scheme which are not based on the classical Shamir's threshold signature scheme. Firstly, we define divisible quantum entanglement and p-unitary operator. Secondly, we construct the map from the multiple binary information to a quantum. Finally, we support the threshold signature scheme based on divisible quantum entanglement and p-unitary operator. Compared with the existing the schemes, the scheme involved fewer quanta. The scheme also meets the requirement of "Threshold Signature", that is to say, only the number of participants is not less than the threshold, they can execute the signature or the verification.

1. Key Definitions

We introduce the key definitions of the scheme.

(1) Divisible quantum entanglement

Let $s, N_1 \geq 2, k, t_1, t_2 \geq 1$ are integers satisfying $N_1 = (t_1 + t_2)k$, and

$$|\varphi\rangle = \frac{1}{\sqrt{s}} \sum_{i=1}^{s} \lambda_i \,|\, a_{i,1} a_{i,2} .....a_{i,N_1} \rangle , \tag{1}$$

be a quantum entanglement, where

$$\lambda_i \in \{-1,1\}, a_{i,j} \in \{0,1\} \quad i=1,\cdots,s, j=1,\cdots,N_1. \qquad (2)$$

We say $|\varphi\rangle$ is a divisible quantum entanglement if

$$\sum_{j=1}^{t_1} P_{i,j} \bmod p = \sum_{j=t_1+1}^{t_1+t_2} P_{i,j} \bmod p \quad \text{for any } i=1,\cdots,s, \qquad (3)$$

where $p = 2^k$ and

$$P_{i,j} = 2^{k-1}a_{i,(j-1)k+1} + 2^{k-2}a_{i,(j-1)k+2} + ... + a_{i,jk} \qquad i=1,\cdots,s, j=1,\cdots,t_1+t_2.$$

The following is some examples $|\varphi\rangle$ of divisible quantum entanglement.

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Which implies $t_1 = t_2 = k = 1, s = N_1 = 2$.

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle).$$

Which implies $t_1 = t_2 = 2, k = 1, s = N_1 = 4,$.

(2) p -unitary operator

Let $p \geq 1$ be a integer and U be a unitary operator defined on the complex field C, that is to say, U satisfies

$$U^{*T}U = UU^{*T} = I,$$

where U^{*T} denotes that U transposes and all components of U takes the conjugation.

We say U is a p -unitary operator if

$$U^p = I, U^i \neq I \; i=1,\cdots,p-1 \;. \qquad (4)$$

The following is a typical 2×2 p -unitary operator:

$$U = \begin{pmatrix} \cos(\frac{m}{p}\cdot 2\pi) & -\sin(\frac{m}{p}\cdot 2\pi) \\ \sin(\frac{m}{p}\cdot 2\pi) & \cos(\frac{m}{p}\cdot 2\pi) \end{pmatrix},$$

where $(m,p)=1$, which means m and p are coprime.

It can be easily proved that

$$U^i=\begin{pmatrix}\cos(\frac{i\times m}{p}\cdot 2\pi) & -\sin(\frac{i\times m}{p}\cdot 2\pi)\\ \sin(\frac{i\times m}{p}\cdot 2\pi) & \cos(\frac{i\times m}{p}\cdot 2\pi)\end{pmatrix}$$

Then

$$U^p=I,\, U^i\neq I\;\; i=1,\cdots,p-1.$$

2. The quantum threshold signature

Let $R^U=\{R_1,\cdots,R_{m+n}\}$ be the group of the participators of the threshold signature scheme, $R^B=\{R_1,\cdots,R_n\}$ be the group of signers and $R^F=\{R_{n+1},\cdots,R_{n+m}\}$ be the group of verifiers.

Let TTP be the trusted third party . TTP chooses a divisible quantum entanglement.

$$|\varphi\rangle=\frac{1}{\sqrt{s}}\sum_{i=1}^{s}\lambda_i\,|a_{i,1}a_{i,2}.....a_{i,N_1}\rangle$$

with integers $s,N_1\geq 2,k\geq 1,1\leq t_1\leq n,1\leq t_1\leq m,\; N_1=(t_1+t_2)k$ and $p=2^k$.

Let the message to be signed be $M=(c_1,c_2,\cdots,c_N)$, where $N\geq 1$, $0\leq c_i<p$, $i=1,\cdots,N$.

In the process of threshold signature, for simplifying the signature , we assume $R_1,\cdots,R_{t_1}$ signs, $R_{n+1},\cdots,R_{n+t_2}$ verifies the signature.

This scheme contains four steps: the generation of an individual private key, the generation of threshold signature, the verification of the signature and the security analysis.

2.1 the generation of an individual private key $K_j,\, j=1,\cdots t_1,n+1.....,n+t_2$.

TTP generates N_1 quanta $|a_1\rangle,|a_2\rangle,.....|a_N\rangle$ following the quantum entanglement for N times,

$$|\varphi\rangle=\frac{1}{\sqrt{s}}\sum_{i=1}^{s}\lambda_i\,|a_{i,1}a_{i,2}.....a_{i,N}\rangle$$

and sends them to $R_1,\cdots,R_{t_1},R_{n+1},\cdots,R_{n+t_2}$ by the quantum secure direct communication schemes [15,16]. Note that TTP generates $N_1 * N$ quanta in all.

For each time, R_i receives

$$(b_{i,1}, b_{i,2}, ..., b_{i,k}) = (a_{(i-1)k+1}, a_{(i-1)k+2}, ..., a_{ik}), \quad i = 1, \cdots t_1$$

$$(b_{i,1}, b_{i,2}, ..., b_{i,k}) = (a_{(i+t_1-n-1)k+1}, a_{(i+t_1-n-1)k+2}, ..., a_{(i+t_1-n)k}), \quad i = n+1 ....., n+t_2$$

R_i calculates

$$k_i = 2^{k-1} b_{i,1} + 2^{k-2} b_{i,2}, + ... + b_{i,k} \qquad i = 1, \cdots t_1, n+1 ....., n+t_2$$

as its part individual private key. By the property of the quantum entanglement and the formula (3), we have

$$\sum_{i=1}^{t_1} k_i \bmod p = \sum_{i=n+1}^{n+t_2} k_i \bmod p \tag{5}$$

For N times, R_j obtains a series of part individual private keys

$$K_j = (k^j{}_1, k^j{}_2, \cdots, k^j{}_N), \qquad j = 1, \cdots t_1, n+1 ....., n+t_2$$

as its individual private key.

2.2 the generation of threshold signature

In the process, $R_1, \cdots, R_{t_1}$ signs the message $M = (c_1, c_2, \cdots, c_N)$.

(i) R_1 generates a quantum state for the message $M = (c_1, c_2, \cdots, c_N)$.

$$|\phi_0\rangle = (|\phi_{1,0}\rangle, |\phi_{2,0}\rangle, ..., |\phi_{i,N}\rangle)$$

Where

$$|\phi_{i,0}\rangle = \cos(\frac{c_i}{p} \cdot 2\pi)|0\rangle + \sin(\frac{c_i}{p} \cdot 2\pi)|1\rangle . \tag{6}$$

The single quanta encode quantum state $|\phi_0\rangle$ form M sequence.

(ii) R_{j-1} $(1 < j \le t_1)$ exerts a unitary operator on $|\phi_{i,j-1}\rangle$:

$$|\phi_{i,j}\rangle = U^{K_j} |\phi_{i,j-1}\rangle \qquad i = 1, \cdots, N$$

where U is a 2×2 p -unitary operator:

$$U=\begin{pmatrix}\cos(\frac{1}{p}\cdot 2\pi) & -\sin(\frac{1}{p}\cdot 2\pi)\\ \sin(\frac{1}{p}\cdot 2\pi) & \cos(\frac{1}{p}\cdot 2\pi)\end{pmatrix}.$$

$R_{j-1}(1<j\le t_1)$ sends $|\phi_{i,j}\rangle\ i=1,\cdots,N$ to R_j.

（iii） R_{t_1} sends M, $|\phi_{i,t_1}\rangle\ i=1,\cdots,N$ to R_{n+1}.

Remark: To check eavesdropping, we use a similar method as in [6,7] as follows.

$R_{j-1}(1<j\le t_1)$ prepares some sample quanta as (6) ,and inserts these single quanta randomly into the M sequence. R_{j-1} makes a record of the insertion positions of the sample quanta for eavesdropping check. The sample quanta for eavesdropping check form C sequence. Then R_{j-1} sends all the quanta to R_j. After ensuring R_j has received all the quanta from R_{j-1}, R_{j-1} publicly announces the positions and the states of sample quanta. Then R_j measures these quanta by using the same bases as R_{j-1} announced. Comparing the results, R_j can determine the error rate. If the error rate exceeds the threshold, the process is aborted.

Similarly, We also check eavesdropping by the method as in the generation phase of threshold signature from R_{t_2} to R_{n+1}.

2.3 the verification of the signature

In the process, $R_{n+1},\cdots,R_{n+t_2}$ verifies the signature of the message $M=(c_1,c_2,\cdots,c_N)$.

(i) R_{n+1} receives all the quanta from R_t. R_{n+1} and lets $|\varphi_{i,0}\rangle=|\phi_{i,t_1}\rangle\ i=1,\cdots,N$.

(ii) $R_{n+j-1}(1<j\le t_2)$ exerts a unitary operator on $|\varphi_{i,j-1}\rangle$ as follows.

$$|\varphi_{i,j}\rangle=U^{-K_j}|\varphi_{i,j-1}\rangle \qquad i=1,\cdots,N$$

where

$$U=\begin{pmatrix}\cos(\frac{1}{p}\cdot 2\pi) & -\sin(\frac{1}{p}\cdot 2\pi)\\ \sin(\frac{1}{p}\cdot 2\pi) & \cos(\frac{1}{p}\cdot 2\pi)\end{pmatrix}.$$

$R_{n+j-1}(1<j\le t_2)$ sends $|\varphi_{i,j}\rangle\ i=1,\cdots,N$ to R_{n+j}.

（iii） R_{n+t_2} generates single quanta with quantum state $|\phi_0\rangle = (|\phi_{1,0}\rangle, |\phi_{2,0}\rangle, ..., |\phi_{i,N}\rangle)$ from the message $M = (c_1, c_2, \cdots, c_N)$.

By Quantum Swap Test Circuit (QSTC)[25], we execute the comparison between $|\phi_{i,0}\rangle$ and $|\varphi_{i,n+t_2}\rangle$, $i = 1, \cdots, N$. If n $|\phi_{i,0}\rangle$ and $|\varphi_{i,n+t_2}\rangle$ are equal, for all $i = 1, \cdots, N$. the signature is valid.

The validity of the scheme is guaranteed by the fact.

With (4) and (5), for all $i = 1, \cdots, N$, we have

$$|\varphi_{i,n+t_2}\rangle = U^{\sum_{j=1}^{t_1} k^j{}_i} U^{\sum_{j=n+1}^{n+t_2} -k^j{}_i} |\phi_{i,0}\rangle = U^{\sum_{j=1}^{t_1} k^j{}_i \bmod p} U^{-\sum_{j=n+1}^{n+t_2} k^j{}_i \bmod p} U^{cp} |\phi_{i,0}\rangle = |\phi_{i,0}\rangle .$$

We also check eavesdropping by the method as in the generation phase of threshold signature, from $R_{n+j-1} (1 < j \le t_2)$ to R_{n+j}.

2.4 security analysis

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

(i) intercept-resend attack. In the scheme, $R_j \quad (j = 1, \cdots, t_1 - 1)$ or $R_{n+j} \quad (j = 1, \cdots, t_2 - 1)$ sends the quanta as (6). By the uncertainty principle, the attacker cannot exert the prober unitary operator on each quantum. Then if the attacker take the intercept-resend attack, the rate that the attacker is not cheched is $\frac{1}{p^m}$.

(ii) $(t-1)$-party cheating attack. Assume t-1 signers or verifiers want to achieve the signing or the verifying. Since

$$\sum_{j=1}^{t_1} k^j{}_i \bmod p = \sum_{j=n+1}^{n+t_2} k^j{}_i \bmod p \ i = 1, \cdots, N ,$$

and

$$U^p = I, U^i \ne I \ i = 1, \cdots, p-1.$$

Then the rate that t-1 signers or verifiers achieve the signing or the verifying successfully is $\frac{1}{p^m}$.

3. Conclusion

In this paper, we give the definition of divisible quantum entanglement and p -unitary operator, construct the map from the multiple binary information to a quantum and support a new threshold signature scheme. Compared with the existing the schemes, the scheme is not based on the classical Shamir's threshold signature scheme and involved fewer quanta. The scheme also meet the requirement of "Threshold Signature", that is to say, only the number of participants is not less than the threshold, they can execute the signature or the verification.

Remark:

This scheme also suit for the threshold signature shemewithout a trusted party as in[6,7], where signers and verifiers belong to the same group.

Reference

[1]. Zeng G H, Christoph K. An arbitrated quantum signature scheme. Phys Rev A, 2002, 65: 042312

[2]. Grasbon F, Paulus GG, Chin SL, Walther H, Muth-Bohm J, Becker A, Faisal FHM , Signatures of symmetry-induced quantum-interference effects observed in above-threshold-ionization spectra of molecules, PHYSICAL REVIEW A, 2001, 63(4): 041402.

[3] Borgonovi F, Celardo GL, Berman GP, Quantum signatures of the classical topological nonconnectivity threshold ,PHYSICAL REVIEW B,2005,72(22): 224416.

[4]Yang YG, Multi-proxy quantum group signature scheme with threshold shared verification, CHINESE PHYSICS B,2008, 17(2), pp 415-418.

[5] Bivona S, Bonanno G, Burlon R, Gurrera D, Leone C, Signature of quantum interferences in above-threshold detachment of negative ions by a short infrared pulse, PHYSICAL REVIEW A, 2008, 77(5)A: 051404.

[6] Yang YG, Wen QY, Threshold proxy quantum signature scheme with threshold shared verification, SCIENCE IN CHINA SERIES G-PHYSICS MECHANICS & ASTRONOMY, 2008, 51(8),pp 1079-1088.

[7] Yang YG, Wen QY, Quantum threshold group signature, SCIENCE IN CHINA SERIES G-PHYSICS MECHANICS & ASTRONOMY, Vol. 21, 2008.pp 1505-1514.

[8] Shi JJ , Shi RH, Guo Y, Peng XQ , Lee MH, Park D, A (t, n)-Threshold Scheme of Multi-party Quantum Group Signature with Irregular QuantumFourier Transform, INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS, 2012,51(4), pp 1038-1049.

[9]Shi JH, Zhang SL,Chang ZG, The security analysis of a threshold proxy quantum signature scheme, 2013, 56(3),pp 519-523.

[10]. Beige A, Englert B G, Kurtsiefer C H, et al. Secure communication with a publicly known key. Acta Phys Pol A, 2002, 101: 357-368.

[11]. Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89:187902-1-4.

[12] .Wójcik A. Eavesdropping on the "Ping-Pong" quantum communication protocol. Phys Rev Lett, 2003, 90:157901-1-4.

[13]. Zhang Z J, Man Z X, Li Y. Improving Wójcik's eavesdropping attack on the ping-pong protocol. Phys Lett A,2004, 333: 46-50.

[14].Cai Q Y. The "Ping-Pong" protocol can be attacked without eavesdropping. Phys Rev Lett, 2003, 91: 109801.

[15]. Cai Q Y, Li B W. Deterministic secure communication without using entanglement. Chin Phys Lett, 2004, 21: 601-603.

[16]. Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69:052319-1-4.

[17]. Cai Q Y, Li B W. Improving the capacity of the Boström-Felbinger protocol. Phys Rev A, 2004, 69: 054301-1-3.

[12]. Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum super dense coding. Phys Rev A, 2005, 71: 044305-1-4.

[18]. Zhu A D, Xia Y, Fan Q B, et al. Secure direct communication based on secret transmitting order of particles.Phys Rev A, 2006, 73: 022338-1-4.

[19] .Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons. Phys Lett A, 2006, 358: 256-258.

[20]. Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Phys Rev Lett, 2005, 94:140501-1-4.

[21]. Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317-1-4.

[22] .Cao H J, Song H S. Quantum secure direct communication with W state. Chin Phys Lett, 2006, 23: 290-292.

[23] Li X H, Zhou P, Liang Y J, et al. Quantum secure direct communication network with two-step protocol. Chin Phys Lett, 2006, 23: 1080-1083.

[24]. Shamir A. How to share a secret. Commun ACM, 1979, 22(11): 612-613.

[25]Buhrman H, Cleve R, Watrous J, et.al. Quantum Fingerprinting. Phys. Rev.Lett. 2001,87.167902-167904.