Int J Theor Phys (2012) 51:455–461
DOI 10.1007/s10773-011-0922-8

A Blind Quantum Signature Scheme with χ-type Entangled States

Xun-Ru Yin · Wen-Ping Ma · Wei-Yan Liu

Received: 6 April 2011 / Accepted: 8 August 2011 / Published online: 6 September 2011

Abstract A blind quantum signature scheme with χ-type entangled states is proposed, which can be applied to E-voting system. In this scheme, the particles in χ-type state sequence are used for quantum key distribution first, and then for quantum signature. Our scheme is characterized by its blindness, impossibility of forgery, impossibility of disavowal. In addition, our scheme can perform an audit program with respect to the validity of the verification process in the light of actual requirements. The security of the scheme is also analyzed.

Keywords Blind quantum signature · χ-type entangled states · Quantum key distribution

1 Introduction

Since the first quantum key distribution protocol (QKD) [1–7] was proposed by Bennett and Brassard in 1984 [1], which has been proved to be unconditionally secure, many branches of quantum cryptography have progressed quickly, including quantum secure direct communication (QSDC), quantum secret sharing, quantum signature, quantum steganography, and so on. Quantum digital signature combines quantum theory with classical digital signature. The main goal of this field is to take advantage of quantum effects to provide unconditionally secure information exchange. Blind signature is a special digital signature in which the message owner's anonymity could be protected to ensure privacy. In blind signature, the message owner could always get the authentic signature of his own message even though

X.-R. Yin (✉) · W.-P. Ma
Key Lab. of Computer Network and Information Security Ministry of Education, Xidian University, Xi'an 710071, China
e-mail: yxr03@yahoo.com.cn

X.-R. Yin
School of Mathematics, Taishan University, Taian 271021, China

W.-Y. Liu
School of Science, Northwestern Polytechnical University, Xi'an 710072, China

the signatory knows nothing about the content that he signed. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

Applying the complexity of factoring large integers, Chaum [8] proposed the first blind signature scheme in 1983. With discrete logarithm, Harn [9] introduced a blind signature scheme in 1995. Different from these classic digital signatures, recently, many quantum signature schemes have been presented, the security of which is assured by the quantum mechanics principles rather than the difficulty of computation. In 2001, Zeng et al. [10] have presented a quantum signature scheme based on the correlation of quantum entanglement states. Gottesman and Chuang [11] have proposed a quantum digital signature scheme based on quantum one-way function. Lee et al. [12] have presented two quantum signature schemes with message recovery. Moreover, Wen et al. [13] have proposed a weak blind signature scheme based on quantum cryptography.

In this paper, a blind quantum signature scheme is proposed, based on four-qubit χ-type entangled state [14, 15]

$$\begin{aligned}\left|\chi^{00}\right\rangle_{3214} = \frac{1}{2\sqrt{2}}(&|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle \\ &+ |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)_{3214},\end{aligned} \tag{1}$$

where the subscripts denote different particles. In our scheme, Alice is defined as the message owner(voter). Charlie is defined as the signatory, who is a representative of the electoral management center. And Bob is defined as the verifier. There are three phases in this scheme. First of all, we set up the system and generate the secret keys by preparing χ-type state sequence. Secondly, Charlie sends a particle sequence to Alice and Bob, respectively. Alice blinds the message m into the blinded message m' by measuring her particles and Charlie signs the blinded message m' to make a blind signature by measuring his particles. Finally, Bob measures his particles and verifies the signature based on the correlation of χ-type entangled state. After that, Bob makes public the message m. Furthermore, we give an audit program to prevent Bob's dishonesty in Sect. 3.

2 The Blind Quantum Signature Scheme

The four-qubit entangled state $|\chi^{00}\rangle_{3214}$ is not reducible to a pair of Bell states and does not belong to the well-known three types of multipartite entangled states, i.e., GHz state, W state, and linear cluster state. The state $|\chi^{00}\rangle_{3214}$ has many properties. If the Pauli operations are performed on qubits 3 and 1, respectively, arbitrary one of sixteen different χ-type entangled states will be formed. All of them can construct an orthonormal basis set

$$FMB = \left\{\left|\chi^{ij}\right\rangle_{3214} = \left(\sigma_3^i \otimes \sigma_1^j\right)\left|\chi^{00}\right\rangle_{3214} | i, j = 0, 1, 2, 3\right\} \tag{2}$$

for the four-qubit Hilbert space. Here σ^i is one of the four Pauli operators, i.e., $\sigma^0 = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma^1 = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma^2 = |0\rangle\langle 1| - |1\rangle\langle 0|$, $\sigma^3 = |0\rangle\langle 0| - |1\rangle\langle 1|$. Meanwhile, these states are maximally entangled states and both the corresponding reduced density matrices of the qubits (3, 1) and (2, 4), are equal to the complete mixture, $\rho = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$. Hence, no experiment performed on the qubits (3, 1) or (2, 4) can discriminate these states. But a measurement on four qubits can perfectly distinguish these states from each other.

By regrouping terms, the state $\left|\chi^{00}\right\rangle_{3214}$ can be rewritten in the following way,

$$\left|\chi^{00}\right\rangle_{3214} = \frac{1}{2}(|\Phi_1^-\rangle|0+\rangle + |\Phi_1^+\rangle|0-\rangle + |\Psi_1^-\rangle|1+\rangle + |\Psi_1^+\rangle|1-\rangle)_{3214} \tag{3}$$

$$= \frac{1}{2}(|\Phi_2^+\rangle|+0\rangle + |\Phi_2^-\rangle|-0\rangle - |\Psi_2^+\rangle|+1\rangle - |\Psi_2^-\rangle|-1\rangle)_{3214}. \tag{4}$$

Here, $|\Phi_1^{\pm}\rangle = (|\phi^+\rangle \pm |\psi^-\rangle)/\sqrt{2}$, $|\Psi_1^{\pm}\rangle = (|\psi^+\rangle \pm |\phi^-\rangle)/\sqrt{2}$, $|\Phi_2^{\pm}\rangle = (|\phi^+\rangle \pm |\psi^+\rangle)/\sqrt{2}$, $|\Psi_2^{\pm}\rangle = (|\psi^-\rangle \pm |\phi^-\rangle)/\sqrt{2}$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, where $|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ are the four Bell states. In addition, we define orthonormal basis sets for the two-qubit Hilbert space:

$$AMB_1 = \{|\Phi_1^+\rangle, |\Phi_1^-\rangle, |\Psi_1^+\rangle, |\Psi_1^-\rangle\} \qquad BMB_1 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$$

$$AMB_2 = \{|\Phi_2^+\rangle, |\Phi_2^-\rangle, |\Psi_2^+\rangle, |\Psi_2^-\rangle\} \qquad BMB_2 = \{|+0\rangle, |-0\rangle, |+1\rangle, |-1\rangle\}$$

In the following we describe the three phases of the scheme.

(I) *Initial phase*. This phase generates the keys and sets up the system. In order to generate the keys, we may use the scheme in [7]. Nevertheless, we propose another solution according to [16].

(1) Charlie and Bob agree that the four Pauli operations represent two-bit classical information, i.e., $\sigma^0 \mapsto' 00'$, $\sigma^1 \mapsto' 01'$, $\sigma^2 \mapsto' 10'$, $\sigma^3 \mapsto' 11'$.

(2) Charlie prepares an ordered four-qubit state sequence $[P_1^1, P_2^1, P_3^1, P_4^1, P_1^2, P_2^2, \ldots, P_3^n, P_4^n, P_1^{n+1}, P_2^{n+1}, \ldots, P_3^{n+N}, P_4^{n+N}]$. Here, the subscripts represent four different particles in one χ-type state and the superscripts indicate the entangled pair orders in the sequence. In addition to those particles used for the eavesdropping check, n and N are dependent on the key length and the message length, respectively. Charlie takes one particle from each entangled pair to form the ordered particle sequences: $S_i : [P_i^1, P_i^2, \ldots, P_i^n]$, $S_i' : [P_i^{n+1}, P_i^{n+2}, \ldots, P_i^{n+N}]$, $i = 1, 2, 3, 4$. He keeps particle sequences S_1 and S_3, and sends sequences S_2 and S_4 to Bob.

(3) The eavesdropping check between Charlie and Bob is performed based on measuring basis sets AMB_i and BMB_i $(i = 1, 2)$. For details, see [16].

(4) In order to generate secret keys, Charlie applies the local unitary operation on the remainder of particles (encoding particles) in his site. For example, Charlie generates randomly $'k_1k_2k_3k_4'$, where $k_i \in \{0, 1\}$. He performs the operations $\sigma^{2k_1+k_2}$ and $\sigma^{2k_3+k_4}$ on the qubits 3 and 1, respectively. After that, Charlie sends these encoding particles to Bob.

(5) Bob measures the particles in his site by the basis FMB and gains the secret keys transmitted by Charlie.

Thus, Charlie can share secret key K_{BC} with Bob by using the steps above. Similarly, Bob prepares χ-type state sequence, and shares secret key K_{AB} with Alice.

(II) *Signing phase*. In this phase, Alice blinds the message and Charlie signs the blinded message. Following steps are required:

(1) Charlie sends particle sequences S_1' and S_4' to Alice and Bob ,respectively, and he keeps sequences S_2' and S_3'.

(2) Charlie chooses randomly a sufficiently large subset from S_2' and S_3' sequences and measures these particles in the basis AMB_1 or AMB_2. And then Charlie broadcasts publicly the positions of these particles and his measurement basis. Alice and Bob measure the corresponding particles in the sequences S_1' and S_4' in the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, respectively. Finally, three parties present their measurement outcomes to check quantum channels.

If the error rate exceeds the threshold, the process is aborted. Otherwise, the scheme goes on.

(3) Alice measures the remainder of particles in the sequence S_1' according to the message $m = (m(1), m(2), \ldots, m(l))$, $m(i) \in \{0, 1\}$. The measurements are made in the order of the positions of particles. If $m(i) = 0$, she measures the corresponding particle in the basis $\{|0\rangle, |1\rangle\}$. If $m(i) = 1$, Alice chooses the basis $\{|+\rangle, |-\rangle\}$. Alice can record the measurement results as $\{|m_1\rangle, |m_2\rangle, \ldots, |m_l\rangle\}$, where $|m_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. We encode the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ into classical bits 00, 01, 10, 11, respectively. Then, all the measurement results can be written as $m' = (m'(1), m'(2), \ldots, m'(l))$, where $m'(i) \in \{00, 01, 10, 11\}$. After that, the message m has been blinded into m'. Then, Alice encrypts m' based on one-time pad with the key K_{AB} and gets the secret message $M = E^1_{K_{AB}}(m')$.

(4) Bob measures the corresponding particles in the sequence S_4' based on the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. The measurements are made in the order of the positions of particles. In the same way, we encode $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ into 00, 01, 10, 11, respectively. Bob records all the measurement results as $B = (b(1), b(2), \ldots, b(l))$, where $b(i) \in \{00, 01, 10, 11\}$. In order to provide the basis of post-audit for electoral management center, Bob must transform B into quantum state by quantum fingerprinting [17]

$$|h(x)\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |E_i(x)\rangle, \tag{5}$$

for each $x \in \{0, 1\}^{2l}$. Here, $E : \{0, 1\}^{2l} \to \{0, 1\}^m$ is an error correcting code (such as Justesen codes) and $m = 2cl$ for fixed $c > 1$. Then Bob encrypts $|h(B)\rangle$ by use of the quantum encryption algorithm [18] with the key K_{BC} and gets

$$|H\rangle = E^2_{K_{BC}}(|h(B)\rangle). \tag{6}$$

After that, Bob sends $|H\rangle$ to Charlie.

(5) After receiving $|H\rangle$, Charlie measures the corresponding particles in sequences S_2' and S_3' in the basis AMB_1 or AMB_2. The measurements are made in the order of the positions of particles. We encode the states $|\Phi_1^+\rangle$, $|\Phi_1^-\rangle$, $|\Psi_1^+\rangle$, $|\Psi_1^-\rangle$, $|\Phi_2^+\rangle$, $|\Phi_2^-\rangle$, $|\Psi_2^+\rangle$, $|\Psi_2^-\rangle$ into 0, 1, 2, 3, 4, 5, 6, 7, respectively. Then, the measurement results are able to be written as $C = (c(1), c(2), \ldots, c(l))$, where $c(i) \in \{0, 1, \ldots, 7\}$. In this step, Charlie do not know Alice's measurement result because he can not deduce B from $|h(B)\rangle$. Charlie encrypts C based on one-time pad with the key K_{BC} to get the blind signature $S = E^3_{K_{BC}}(C)$.

(6) Charlie sends the blind signature S to the verifier Bob.

In this scheme, the management center is considered to be authentic according to the practical situation. Therefore, Bob is asked to leave quantum fingerprinting of the measurement results in the signing phase to prevent his dishonesty.

(III) *Verification phase*. The verification phase is executed by the following procedure:

(1) Alice sends M to the verifier Bob.

(2) Bob decrypts M with his key K_{AB} to get the blind message m' and transforms m' into the original message m. For example, if $m' = (00110110)$, then $m = (0101)$.

(3) Bob decrypts S with his key K_{BC} to get the measurement result C.

(4) Bob accepts S as the valid blind signature for message m if the parameters $m'(i)$, $b(i)$, and $c(i)$ satisfy the validation rule which is shown in Tables 1 and 2, for each $i \in \{1, 2, \ldots, l\}$. Otherwise, he rejects it.

For example, if $m'(i) = 00$ and $b(i) = 10$, then Alice's measurement result is $|0\rangle$, while Bob's is $|+\rangle$. Thus, Charlie's measurement outcome is $|\Phi_1^-\rangle$ according to (3), i.e., $c(i) = 1$.

Table 1 Validation rule of the blind signature. Here, for each $i \in \{1, 2, \ldots, l\}$, the first column and the first row represent all possible values of $m'(i)$ and $b(i)$, respectively. In addition, c_j $(j = 0, \ldots, 7)$ and the figures denote the values that $c(i)$ may take, where c_j can be seen in Table 2

	00	01	10	11
00	c_0	c_1	1	0
01	c_2	c_3	3	2
10	4	6	c_4	c_5
11	5	7	c_6	c_7

Table 2 The corresponding values of c_j based on the different measurement basis chosen by Charlie

Measurement basis	c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7
AMB_1	{0, 1}	{0, 1}	{2, 3}	{2, 3}	{1, 3}	{0, 2}	{1, 3}	{0, 2}
AMB_2	{4, 5}	{6, 7}	{4, 5}	{6, 7}	{4, 6}	{4, 6}	{5, 7}	{5, 7}

However, if $m'(i) = 01$ and $b(i) = 00$ (Alice and Bob choose the same basis), i.e., the states of particles 1 and 4 are $|1\rangle$ and $|0\rangle$, respectively, then particles 3 and 2 collapse into $|\psi^+\rangle$ according to equation (1). So, Charlie's measurement result must be $|\Psi_1^+\rangle$ or $|\Psi_1^-\rangle$ if he chooses the basis AMB_1. Then, c_2 take either 2 or 3. If Alice and Bob choose the same basis $\{|+\rangle, |-\rangle\}$, we may transform equation (1) into

$$\begin{aligned}\left|\chi^{00}\right\rangle_{3214} = \frac{1}{2\sqrt{2}}(&|++++\rangle - |-+++\rangle - |+---\rangle + |+--+\rangle \\ &+ |---+\rangle + |+++-\rangle + |-++-\rangle + |----\rangle)_{3214}. \end{aligned} \tag{7}$$

In the same way, we can get the value of c_j for each $j \in \{0, \ldots, 7\}$.

(5) Bob publishes the message m. And he declares his measurement outcomes to provide the basis of post-audit.

3 Security Analysis and Discussion

In this section, we will demonstrate the security of our scheme. In initial phase of our scheme, we propose the quantum key distribution with χ-type entangled states based on quantum secure direct communication. It is known that QSDC has a higher demand for security than QKD. So, our scheme in this phase is secure based on the security analysis in [16]. In signing phase, Alice gets the blinded message by measuring her particles in her site, and encrypts it with one-time pad, by which the security is guaranteed. Next, Bob transforms his measurement result by quantum fingerprinting and encrypts it by quantum encryption algorithm which has been shown to be unconditionally secure. After that, he sends to Charlie. But Charlie do not know Bob' measurement result because quantum fingerprinting is a one-way function. Thus, Charlie is kept blind from the message content. In addition, since the blinded message that Alice sent to Bob includes the secret key which is only known by Alice and Bob, Alice cannot disavow her message. Similarly, Charlie cannot disavow his signature.

Suppose Eve is an evil attacker who wants to tamper the message and forge the signature, the common attack methods that he will employ are as follows:

The intercept-resend attack. Eve captures the particles 1 that Charlie sent to Alice, but if Eve tampers the message m or m' by replacing the original particles with her own parti-

cles, she will inevitably introduce some errors and be detected in step (2) in signing phase. In addition, Eve may intercept particles 1, 4 and prepares another χ-type entangled state $|\chi^{00}\rangle_{3'2'1'4'}$. She sends particles $1'$, $4'$ instead of 1, 4 to Alice and Bob, respectively. After receiving these particles, Alice and Bob measure them, and when three parties present their measurement results (Charlie's is public), Eve may eavesdrop the corresponding information. For example, Alice' measurement result is $|0\rangle$ and Bob's is $|-\rangle$. So, Eve chooses the basis BMB_1 to measure the particles 1 and 4 in her site. It can be seen that there are four possible results: $|0+\rangle$, $|0-\rangle$, $|1+\rangle$, $|1-\rangle$ and these results appear with equal probability. Obviously, the probability that Eve get the same measurement results on particles 1 and 4 as Alice's and Bob's is 25%. Thus, Eve can not pass the eavesdropping check in the condition that the errors occur.

The man-in-the-middle attack. Eve counterfeits Alice and sends the message to the verifier Bob, but she has not the secret key K_{AB}, which is shared with Bob and generated in the initial phase. Moreover, Alice adopts one-time pad as the encryption to encrypt her message. So, it is impossible for Eve to tamper the message. If Eve counterfeits Charlie and sends the blind signature to the verifier Bob, similarly, due to Eve has not secret key K_{BC} with Bob, she cannot forge the signature.

In our scheme, Charlie (management center) is considered to be authentic according to the practical situation and Alice casts a vote as her wish. In the verification phase, since Bob shares the secret keys K_{AB} and K_{BC} with Alice and Charlie, respectively, it is possible for Bob to forge Alice's message or Charlie's signature. Therefore, the electoral management center can perform audit program with respect to the validity of the verification phase according to actual requirements. There are the following steps:

Step 1. Let B' denote the measurement result which Bob has published. Charlie can know m' according to the public message m. After replacing B with B' in Table 1, Charlie may reject the message m if the correlation measurement results of m', B', and C dissatisfy the rule which is shown in Table 1 and Table 2. Otherwise, Charlie goes on for further program to the next step.

Step 2. Charlie transforms B' into $|h(B')\rangle$ by (5).

Step 3. Charlie decrypts $|H\rangle$ which has been received in the step (5) in signing phase by quantum encryption algorithm with the key K_{BC} and obtains $|h(B)\rangle$.

Step 4. Charlie compares $|h(B)\rangle$ with $|h(B')\rangle$. If the two states are equal, then the audit program can be passed. Otherwise, Charlie considers that the verification process is not legitimate.

4 Conclusion

We present a blind quantum signature scheme based on χ-type entangled states in this paper. The particles in four-qubit state sequence are used to generate secret key and set up the whole system first, and then for signature process. So, the scheme is highly efficient. Moreover, The signatory knows nothing about the content that he signed in our scheme. The voter cannot disavow her message, nor can signatory disavow his signature, and the signature cannot be forged. Furthermore, the electoral management can perform an audit program with respect to the validity of the verification process according to actual needs. Our scheme is secure by the security analysis.

Acknowledgements This work was supported by National Science Foundation of China under grant No. 61072140, the 111 Project under grant No. B08038, Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 20100203110003, the Fundamental Research Funds for the Central Universities under grant No. JY10000901034.

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, p. 175. IEEE Press, New York (1984)
2. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
4. Goldenberg, L., Vaidman, L.: Phys. Rev. Lett. **75**, 1239 (1995)
5. Lee, J., Lee, S., Kim, J., et al.: Phys. Rev. A **70**, 032305 (2004)
6. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
7. Gao, G.: Int. J. Theor. Phys. **49**, 1870 (2010)
8. Chaum, D.: In: Proc. CRYPTO'82, p. 199 (1983)
9. Harn, L.: Electron. Lett. **31**(14), 1136 (1995)
10. Zeng, G.H., Ma, W.P., et al.: Acta Electron. Sin. **29**(8), 1098 (2001) (in Chinese)
11. Gottesman, D., Chuang, I.: arXiv:quant-ph/0105032v2 (2001)
12. Lee, H., Hong, C., et al.: Phys. Lett. A **321**(C5-C6), 295 (2004)
13. Wen, X.J., Niu, X.M., Ji, L.P., Tian, Y.: Opt. Commun. **282**, 666 (2009)
14. Yeo, Y., Chua, W.K.: Phys. Rev. Lett. **96**, 060502 (2006)
15. Wang, X.W., Yang, G.J.: Phys. Rev. A **78**, 024301 (2008)
16. Lin, S., et al.: Phys. Rev. A **78**, 064304 (2008)
17. Buhrman, H., et al.: Phys. Rev. Lett. **87**, 167902 (2001)
18. Zhou, N.R., Zeng, G.H.: Chin. Phys. **14**(11), 2164 (2005)