A Blind Signature Scheme Applying on Electronic Payment Scene Based on Quantum Secret Sharing

Jia-lei Zhang[1], Ming-sheng Hu[1(✉)], Bei Gong[2], Zhi-Juan Jia[1], and Li-Peng Wang[1]

[1] College of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, Henan, China
295533745@qq.com, 874667607@qq.com
[2] College of Computer Science, Beijing University of Technology, Beijing 100124, China

Abstract. The basic idea of quantum secret sharing is to share classical information through quantum schemes. In reality, the number of secret bits shared will vary according to the actual situation. For this reason, a secret sharing scheme of double qubits is constructed based on single particle. At the same time, combined with the needs of real life in e-commerce, this paper proposes a quantum blind signature protocol suitable for electronic cash payment scenarios. In this protocol, the blinding of the message is an XOR operation, which makes the solution simpler and easier to implement, and the owner of the message cannot be tracked. Moreover, we use quantum key distribution protocol and quantum one-time pad to guarantee its unconditional security. The quantum blind signature applied to the electronic payment system proposed in this paper could protect user's anonymity as the traditional E-payment systems do, and also have unconditional security which the classical E-payment systems cannot provide. Security analysis shows that our scheme is unforgeability, undeniability, blindness and unconditionally secure.

Keywords: Quantum secret sharing · Bell measurement · Quantum blind signature · Controlled non-gate · Unconditionally secure

Supported by the National Natural Science Foundation of China (Grant No. U1304614, U1204703), Henan Province Education Science Plan General Topic "Research on Trusted Degree Certification Based on Block-chain" (Grant No. (2018)-JKGHYB-0279), Zhengzhou Innovative Science and Technology Talent Team Construction Project Fund Project (Grant No. 131PCXTD597), Henan Science and Technology Project (Grant No. 162102310238).

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 3–14, 2019.
https://doi.org/10.1007/978-3-030-21373-2_1

1 Introduction

In 1979, Shamir and Blakley proposed a secret sharing scheme based on Lagrange interpolation polynomial [1] and photographic geometry theory [2]. With the development of quantum cryptography, the classic secret sharing scheme starts with vector sub-secret sharing. Quantum cryptography is a new type of cryptosystem based on classical cryptography and quantum mechanics. It uses quantum mechanics to realize unconditional information exchange. In 1984, Bennett et al. proposed the concept of quantum cryptography [3]. Since then, quantum cryptography has become a hot research topic in the field of information security. Compared with the secret sharing based on the classical cryptosystem, the research on secret sharing based on quantum theory has begun to appear. In 1999, Hillery et al. proposed the first quantum multi-party secret sharing scheme using quantum entangled states combined with quantum teleportation [4].

The research of quantum multi-party secret sharing mainly focuses on the use of quantum technology to realize the secret sharing of classical information [5] and the use of quantum teleportation to reconstruct unknown quantum states [6] to realize the secret sharing of quantum information. The idea of quantum secret sharing is that: if needs to pass secret information to multiple agents, all agents can cooperate to recover secret information, but one or a part of agents cannot recover secret information. With the development of quantum cryptography, many quantum secret sharing schemes have been proposed. In 1999, Karlsson et al. proposed a new quantum secret sharing protocol based on two-particle entanglement [7]. For the first time, they systematically analyzed the security of protocols in several situations. In 2002, Tyc et al. first proposed a continuous variable quantum secret sharing scheme [8]. In 2003, Guo et al. first proposed the use of multi-particle product states to achieve quantum secret sharing [9]. In 2005, Yan et al. proposed a single-photon-based threshold quantum secret sharing scheme [10] for the first time. In 2008, Markham et al. used the Graph state to design a quantum secret sharing protocol [11]. In 2016, Li et al. proposed a quantum secret sharing scheme based on GHZ state [12], which requires partial particles to detect channels and reduce particle utilization. In 2018, Gao et al. proposed a multi-party secret sharing scheme based on quantum theory [13]. In the above secret sharing scheme, the shared quantum states are single-particle states. In this paper, based on the quantum secret sharing of a four-particle entangled state, the shared quantum state is extended to the two-particle state, which makes the formation of relatively perfect quantum secret sharing mechanism.

In 1983, Chaum first presented a blind signature [14]. When signed, the message is disguised to ensure privacy. In other words, it allows a signatory to sign a message for a user in such a way that she cannot learn the content of the message. In 1996, Fan and Lei also proposed a blind signature based on quadratic residues problem [15]. However, these schemes are more and more vulnerably with the advent of quantum computer, hence researchers have shown great interest in quantum blind signature [16–19]. Based on the characteristics of blind signature, this technology plays an important role in protecting user anonymity in applications such as electronic payment and electronic voting. In the electronic

payment system, the bank is required to complete the signature of the electronic bill while ensuring the anonymity of the users consumption content. Although there are many signature schemes based on quantum cryptography, combined with the complexity of the current electronic cash system, there are few solutions for applying blind signatures based on quantum secret sharing to electronic cash system scenarios.

Based on the above problems, combined with the needs of real life, this paper proposes a quantum blind signature scheme that can be adapted to the electronic cash payment system. The scheme realizes secret sharing and reconstruction based on quantum secret sharing. At the same time, the shared secret is a double quantum state, which improves the information amount of the transmitted message, and provides a new method for the transmission of multi-qubit in quantum secure communication. In addition, the scheme of this paper combines quantum secret sharing and blind signature technology to provide a basis for the security of electronic payment. Moreover, the blinding of the message is an XOR operation, which makes the solution simpler and easier to implement, the owner of the message cannot be tracked. Furthermore, quantum key distribution and one-time pad are adopted in our scheme in order to guarantee unconditional security.

2 Basic Knowledge

2.1 Quantum Secret Sharing

In the quantum secret sharing scheme, the owner of any single part cannot effectively obtain the original complete information. Only through the unanimous cooperation of the various parts of the owner the owner of a certain part can get the complete information. In the process, if someone eavesdrops or one of the message owner is disloyal and wants to steal information, they will be detected back.

2.2 Bell State

The four Bell states of 2-qubit are

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{1}$$

2.3 Controlled Non-gate

Assume that the two qubits of the controlled non-gate are M and N, respectively. Where M is the control bit and N is the target bit. Its function is as follows: when the control bit is $|0\rangle$, the target bit does not change; when the control bit is $|1\rangle$, the target bit is inverted ($|0\rangle \leftrightarrow |1\rangle$). The controlled non-gate circuit diagram Fig. 1 and the truth Table 1 are as follows.

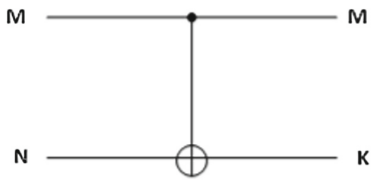

Fig. 1. Controlled non-gate circuit diagram

3 Quantum Secret Sharing Scheme

Based on the quantum secret sharing protocol of three-particle entangled state, the quantum secret sharing scheme proposed in this paper increases the shared secret quantum state from single particle to multi-particle state. Furthermore, the quantum blind signature scheme based on the secret sharing is discussed.

Table 1. Controlled non-gate truth table

M	N	$K = M \oplus N$	M^*	N^*
0	0	0	0	0
0	1	1	0	1
1	0	1	1	1
1	1	0	1	0

Suppose there are three legal participants Peter, Bob and David. Peter is the sender of the message, Bob and David are the agents of the message. Peter wants to send an unknown two-particle state to Bob or David as follows

$$|\varphi\rangle_M = (\alpha|00\rangle + \beta|11\rangle)_{12}, \tag{2}$$

in which $|\alpha|^2 + |\beta|^2 = 1$.

Suppose Peter, Bob and David share an entangled W-state particle as follows

$$|\xi\rangle_W = \frac{1}{\sqrt{3}}(|010\rangle + |100\rangle + |001\rangle)_{345}, \tag{3}$$

Particles 1 and 3 are given to Peter, and particle 2 is given to Bobparticles 4 and 5 are given to David. The distribution of particles is shown in Fig. 2.

The resulting five-particle state is

$$|T\rangle_{12345} = |\varphi\rangle_M \otimes |\xi\rangle_W$$

$$= (\alpha|00\rangle + \beta|11\rangle)_{12} \otimes \frac{1}{\sqrt{3}}(|010\rangle + |100\rangle + |001\rangle)_{345}$$

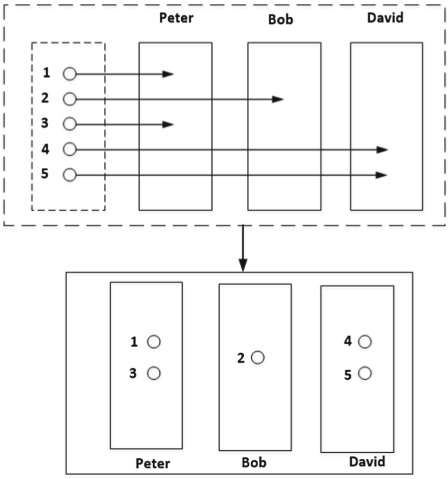

Fig. 2. Schematic diagram of particle distribution

$$= \frac{1}{\sqrt{3}}|\phi^+\rangle_{13}(\alpha|010\rangle + \beta|100\rangle + \alpha|001\rangle)_{245} +$$
$$= \frac{1}{\sqrt{3}}|\phi^-\rangle_{13}(\alpha|010\rangle - \beta|100\rangle + \alpha|001\rangle)_{245} +$$
$$= \frac{1}{\sqrt{3}}|\psi^+\rangle_{13}(\alpha|000\rangle + \beta|101\rangle + \beta|110\rangle)_{245} +$$
$$= \frac{1}{\sqrt{3}}|\psi^-\rangle_{13}(\alpha|000\rangle + \beta|101\rangle - \beta|110\rangle)_{245}$$

(1) Peter performs a Bell measurement on particles 1 and 3, Bob and David's particles will collapse. Bob and David judge the state of their particles based on Peters measurement results.
(2) Two control operations between Peter and Bob were performed. First, particle 2 is used as the control qubit, particle 4 is the target qubit to control the non-gate operation; then particle 4 is the control qubit, and particle 2 is the target qubit to control the non-gate operation.

(a) The result of the first control of the non-gate operation is $|T\rangle_{245}^{1}$:

$$\frac{1}{\sqrt{6}}(\alpha|010\rangle + \beta|110\rangle + \alpha|001\rangle)_{245};$$
$$\frac{1}{\sqrt{6}}(\alpha|010\rangle - \beta|110\rangle + \alpha|001\rangle)_{245};$$
$$\frac{1}{\sqrt{6}}(\alpha|000\rangle + \beta|111\rangle + \beta|100\rangle)_{245};$$

$$\frac{1}{\sqrt{6}}(\alpha|000\rangle - \beta|111\rangle - \beta|100\rangle)_{245}.$$

(b) The result of the second control of the non-gate operation is $|T\rangle_{245}^{2}$:

$$\frac{1}{\sqrt{6}}(\alpha|110\rangle + \beta|010\rangle + \alpha|001\rangle)_{245};$$
$$\frac{1}{\sqrt{6}}(\alpha|110\rangle - \beta|010\rangle + \alpha|001\rangle)_{245};$$
$$\frac{1}{\sqrt{6}}(\alpha|000\rangle + \beta|011\rangle + \beta|100\rangle)_{245};$$
$$\frac{1}{\sqrt{6}}(\alpha|000\rangle - \beta|011\rangle - \beta|100\rangle)_{245}.$$

(3) If Peter's measurement result is $|\phi^{-}\rangle_{13}$, then Bobs and Davids state is

$$|T\rangle_{245} = \frac{1}{\sqrt{6}}(\alpha|110\rangle - \beta|010\rangle + \alpha|001\rangle)_{245}$$
$$= \frac{1}{\sqrt{6}}[\alpha|10\rangle_{45} \otimes |1\rangle_{2} + (\alpha|01\rangle - \beta|10\rangle)_{45} \otimes |0\rangle_{2}]$$

(4) If Bob's measurement result of particle 2 is $|0\rangle_2$, then David's particle 5 collapses to $|T\rangle_{45} = (\alpha|01\rangle - \beta|10\rangle)_{45}$, so David has to do a $I \otimes i\sigma_y$ operation to get $|T\rangle_{45} = (\alpha|00\rangle + \beta|11\rangle)_{45}$. Otherwise, David cannot get the quantum state transmitted by Peter. For other cases, the relationship between Peter's, Bob's measurement results and David's operation is listed in Table 2.

Table 2. The relationship between Peter's, Bob's measurement results and David's operation

Peter's result	$\|T\rangle_{245}^{2}$	David's state after Bob operation	David's operation
$\|\phi^{+}\rangle_{13}$	$(\alpha\|110\rangle + \beta\|010\rangle + \alpha\|001\rangle)_{245}$	$(\alpha\|01\rangle + \beta\|10\rangle)_{45}$	$I \otimes \sigma_x$
$\|\phi^{-}\rangle_{13}$	$(\alpha\|110\rangle - \beta\|010\rangle + \alpha\|001\rangle)_{245}$	$(\alpha\|01\rangle - \beta\|10\rangle)_{45}$	$I \otimes i\sigma_y$
$\|\psi^{+}\rangle_{13}$	$(\alpha\|000\rangle + \beta\|011\rangle + \beta\|100\rangle)_{245}$	$(\alpha\|00\rangle + \beta\|11\rangle)_{45}$	$I \otimes I$
$\|\psi^{-}\rangle_{13}$	$(\alpha\|000\rangle - \beta\|011\rangle - \beta\|100\rangle)_{245}$	$(\alpha\|00\rangle - \beta\|11\rangle)_{45}$	$I \otimes \sigma_z$

4 Quantum Blind Signature for Electronic Payment Scenarios

Blind signature is a special kind of digital signature which allows a signatory to generate a message signature under the condition that he knows nothing about the content of the message.

Our blind signature scheme involves three participants: (1) Peter: the massage owner (the consumer); (2) Bob: the signer (the bank); (3) David: the verifier (the merchant).

The functions implemented by the protocol are as follows: the consumer Peter blinds the message m containing the privacy purchase content to obtain the message m_1, the bank Bob signs the blinded message m_1 to obtain $sig(m_1)$, and David verifies the legitimacy of the message m and the signature $sig(m_1)$. The intrinsic relationship between the message m and the signature $sig(m_1)$ cannot be found, so identity tracking cannot be implemented for consumers. The specific process diagram of the scheme is shown in Fig. 3.

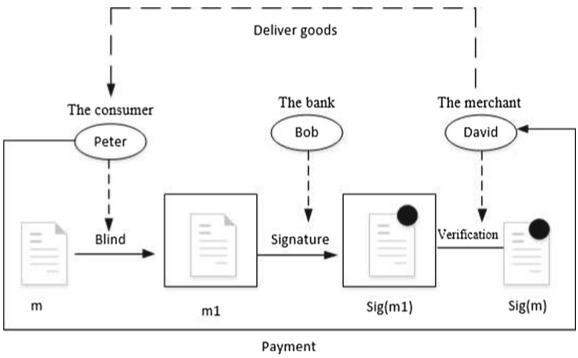

Fig. 3. Schematic diagram of electronic payment protocol

4.1 Initial Phase

Step1. Peter divides her purchase information M into two parts: m^*, involving the amount that Peter ought to pay; m, including Peters purchase information which cannot be seen by others. So Peter needs to blind the part m. The segmentation of the message is shown in Fig. 4.

Step2. Peter and Bob share a secret key K_{PD}, K_{BD} with David, respectively. Peter and Bob share a secret key K_{PB}. All these keys are distributed via QKD protocols, which have been proved unconditionally secure.

Step3. According to the secret sharing scheme described above, suppose Peter, Bob and David get sub-secrets are t_P, t_B and t_D, respectively.

Step4. Peter, Bob and David share a hash function H.

Step5. The message to be signed is m. Peter encrypts with the secret key K_{PD} to get

$$O_{PD} = K_{PD}(m) \tag{4}$$

Then she sends O_{PD} to David. We adopt one-time pad [18] as the encryption algorithm to guarantee the unconditional security.

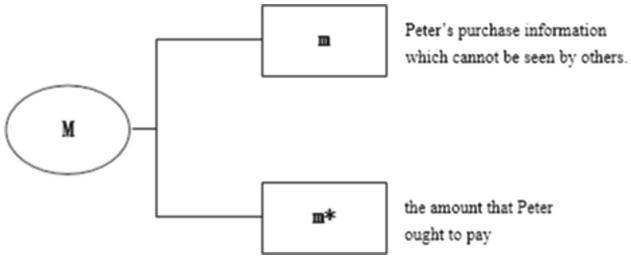

Fig. 4. Segmentation of the message

4.2 Blind the Message Phase

Step1. Peter gets the blind message m_1 by the following method

$$m_1 = m \oplus t_P. \tag{5}$$

Step2. Peter encrypts m_1 with the secret key K_{PB} to get the message

$$O_{PB} = K_{PB}(m_1). \tag{6}$$

then she sends O_{PB} to Bob.

4.3 Trading Purchase Phase

Step1. David performs a hash operation on t_D to get $H(t_D)$ and encrypts it with the secret key K_{BD} to get the message

$$O_{BD} = K_{BD}(H(t_D)) \tag{7}$$

Then he sends O_{BD} to Bob.
Step2. After Bob receives the message O_{PB}, he decrypts it with the secret key K_{PB} to get the message m_2 and get the message m_3

$$m_3 = m_2 \oplus t_B. \tag{8}$$

Step3. Bob encrypts m_3 with the secret key K_{BD} to get the message

$$S_{BD} = K_{BD}(m_3) = sig(m_1) \tag{9}$$

Then he sends $sig(m_1)$ to David.

4.4 Verifying Phase

Step1. David decrypts O_{PD} with the secret key K_{PD} to get the message m_4.
Step2. David decrypts S_{BD} with the secret key K_{BD} to get the message m_5 and get the message m_6:

$$m_6 = m_5 \oplus t_D. \tag{10}$$

Step3. If $m_6 = m_4$, the signature is valid. Otherwise, David will reject it.

4.5 Trading Payment Phase

Step1. David encrypts t_D with the secret key K_{BD} to get the message

$$O^*_{BD} = K_{BD}(t_D) \tag{11}$$

Then he sends it to Bob.
Step2. Bob decrypts O^*_{BD} with the secret key K_{BD} to get the message t^*_D. Then Bob performs a hash operation on t^*_D to get $H(t^*_D)$.
Step3. Bob decrypts O_{BD} with the secret key K_{BD} to get the message $H(t^{'}_D)$. If

$$H(t^{'}_D) = H(t^*_D) \tag{12}$$

the signature is valid.
Step4. If there is no dispute, the merchant David should send the corresponding goods to Peter. After Peter receives goods from the merchant, she will pay for the bank.

5 Security Analysis

5.1 Security Analysis of Quantum Secret Sharing

The secret sharing adopts the method of quantum teleportation. The secret quantum state is not known by any participant in the transmission process, which greatly improves the security of secret reconstruction.

(1) Internal attack
In the secret sharing scheme, suppose that one or several participants want to acquire secrets by means of deception and cooperation, it is impossible, because they must know the quantum state of the particles in the hands of the legal secret restorer to succeed. Even if the particles belonging to the secret restorer are intercepted by a dishonest agent and sent by another particle instead, the interception attack will also be discovered.
(2) Intercept-resend attack
Since secret reconstruction is realized by quantum teleportation, the attacker Eve stealing the detection quantum will inevitably lead to the change of the quantum state and thus be perceived. If Eve resends the intercepted particle with another quantum substitution, it will break the original particle value $|0\rangle$ and $|1\rangle$, which will cause the actual Bell measurement result to be wrong, and the secret cannot be reconstructed.

5.2 Security Analysis of Quantum Blind Signature

(1) Impossible of Forgery
No one other than the signer can forge a signature. Suppose that an attacker or eavesdropper Eve want to forge Bobs signature. However, he not be able to know the secret key K_{BD} shared between Bob and David, so he cannot send message encrypted by K_{BD}, in other words, it is impossible for Eve to forge Bobs signature. Assume that Eve guesses K_{BD} randomly, then he can produce the valid signature with the probability at most $\frac{1}{2^n}$, which vanishes zero if n is large enough. Therefore, Eve cannot forge Bobs signature.

(2) Impossible of Denial
On the one hand, if the legal signature is signed by Bob, he will not be able to deny it, because Bob encrypts m_3 with the secret key K_{BD} to get the message S_{BD}. So Bob could not deny that he had signed it. On the other hand, David cannot deny that he indeed have received the signature. It is obvious that the process of the verifying indicates he has received it. Therefore, David could not deny that he had received it.

(3) Blindness
The signature is blind. In this scheme, according to $m_1 = m \oplus t_P$, Peter gets the message m_1. Therefore, the message m is blinded to m_1, so the signer Bob cannot know the specific content of the original message m. At the same time, the message owner Peter could not know Bobs message based on the message passed by David, because David passed the hash value to Peter during the audit, and the Hash function has unidirectionality.

(4) Quantum security
Our scheme ensures security from the following two aspects. First, the protocol BB84 is adopted for quantum key distribution; Second, our protocol is based on the secure quantum channel, which has instantaneous transmission not restricted by distance, time or obstacles, all of these are proved to be unconditional security.

5.3 Performance Analysis

The efficiency analysis of the scheme is considered from the following aspects:

1. Consider the number of bits of the message transmitted in the channel. In this paper, the message transmitted is a double quantum state. Compared with scheme [13], the message transmitted by this paper contains a relatively large amount of information, which improves the information amount of the transmitted message, and provides a new method for the transmission of multi-qubit in quantum secure communication.
2. Consider the complexity of signatures and verification. In this paper, the XOR operation of the blinding of the message is low in complexity and easy to implement. And this paper uses fewer classical bits in the signature process.
3. Considering the method used in the secret sharing scheme, the secret sharing of this paper is based on the entangled W state, and the efficiency is higher than other entanglements.

4. Combining quantum secret sharing and quantum blind signature, this paper proposes a signature protocol suitable for electronic cash payment system, which is the application of quantum technology in e-commerce.
5. In this protocol, the message owner cannot be tracked, which guarantees the anonymity of the consumer.

6 Conclusion

Combined with the actual needs of real life, this paper proposes a quantum blind signature scheme for electronic payment systems based on quantum secret sharing protocol. The scheme can realize that the signer signs the blind message to obtain a blind signature, and the blinding process adopts an XOR operation, and the operation is simple. At the same time, the owner of the message cannot be tracked, which guarantees the anonymity of the consumer. In addition, the scheme sets the audit phase to ensure the legitimacy of the e-payment process. Moreover, the scheme proposed in this paper is not limited by the computing power of the new party. Even if the attacker has very powerful computing resources, the scheme cannot be broken. Furthermore, the scheme realizes secret sharing and reconstruction based on quantum secret sharing. At the same time, the shared secret is a double quantum state, which improves the information amount of the transmitted message, and provides a new method for the transmission of multi-qubit in quantum secure communication.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys. IEEE Comput. Soc. **48**, 313–317 (1979)
3. Shen, C.: Research on trusted computing and its development. Sci. China Inf. Sci. **53**(3), 405–433 (2010)
4. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
5. Kogias, L., Xiang, Y., He, Q.Y., et al.: Unconditional security of entanglement based quantum secret sharing schemes. Phys. Rev. A **95**(1), 012315 (2017)
6. Long, Y.X., Long, D.Y., Qiu, D.W.: Sharing classic secret information with maximum true entangled hexagonal state. J. Comput. Sci. Technol. **6**(5), 465–472 (2012)
7. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**(1), 162–168 (1999)
8. Tyc, T., Sanders, B.C.: How to share a continuous-variable quantum secret by optical interferometry. Phys. Rev. A **65**, 042310 (2002)
9. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247–251 (2003)
10. Yan, F.L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A **72**, 012304 (2005)
11. Markham, D., Sanders, B.C.: Graph States for Quantum Secret Sharing. arXiv:0808.1532v1 (2008)

12. Li, W.Z., Liu, Z.W.: Multi-party quantum secret sharing scheme based on GHZ state for flawless operation. Comput. Appl. Res. **33**(2), 491–494 (2016)
13. G, M., W, X.M.: A multi-party secret sharing scheme based on quantum theory. Appl. Res. Comput. **35**(7), 2135–2145 (2018)
14. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology, pp. 199–203. Springer, Boston (1983). https://doi.org/10.1007/978-1-4757-0602-4_18
15. Fan, C., Lei, C.: Efficient blind signature scheme based on quadratic residues. Electron. Lett. **32**(9), 811–813 (1996)
16. Zhang, J.L., Zhang, J.Z., Xie, S.C.: Improvement of a quantum proxy blind signature scheme. Int. J. Theor. Phys. **57**(6), 1612–1621 (2018)
17. Zhang, J.L., Xie, S.C., Zhang, J.Z.: An elaborate secure quantum voting scheme. Int. J. Theoret. Phys. **56**(10), 3019–3028 (2017)
18. Guo, W., Zhang, J.Z., Li, Y.P., et al.: Multi-proxy strong blind quantum signature scheme. Int. J. Theor. Phys. **55**(8), 3524–3536 (2016)
19. Zhang, J.L., Zhang, J.Z., Xie, S.C.: A choreographed distributed electronic voting scheme. Int. J. Theoret. Phys. **57**(9), 2676–2686 (2018)