A Novel Quantum Blind Signature Scheme with Four-particle GHZ States

Ling Fan[1,2] · Ke-Jia Zhang[1] · Su-Juan Qin[1] · Fen-Zhuo Guo[1]

Received: 10 February 2015 / Accepted: 7 July 2015 / Published online: 19 July 2015

Abstract In an arbitrated quantum signature scheme, the signer signs the message and the receiver verifies the signature's validity with the assistance of the arbitrator. We present an arbitrated quantum blind signature scheme by using four-particle entangled Greenberger-Horne-Zeilinger (GHZ) states. By using the special relationship of four-particle GHZ states, we cannot only support the security of quantum signature, but also guarantee the anonymity of the message owner. It has a wide application to E-payment system, E-government, E-business, and etc.

Keywords Blind signature · Quantum cryptography · GHZ states

1 Introduction

The digital signature is a vital technique in the informational world realizing the identification of the original information and confirmation of the disavowal. In the quantum information processing and computation, quantum cryptography can provide unconditionally secure communication based on the laws of physics, especially with the no-cloning theorem that Eve cannot duplicate unknown quantum state. These properties make the quantum channel more secure than that of classical channel.

Compared with the classical signature protocol, many quantum signature schemes have been proposed. In 2001, Gottesman and Chuang proposed the first quantum signature protocol in Ref. [1]. Then Buhrman et al. [2] and Barnum et al. [3] made some significant

✉ Ling Fan
fanling@bupt.edu.cn

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

[2] School of Ethnic education, Beijing University of Posts and Telecommunications, Beijing, 100876, China

attempts to quantum signature, respectively. In 2002, a pioneering signature protocol named arbitrated quantum signature (AQS) was given by Zeng and Keitel (ZK protocol) [4]. Here a trusted arbitrator is introduced to help the receiver to verify the signature and judges who tells a lie if a disputation happens. Since then, many quantum signature protocols have been studied. In 2009, Li et al. presented a Bell-states-based AQS protocol, which simplified ZK protocol by replacing Greenberger-Horne-Zeilinger (GHZ) states with Bell ones as the carrier [5]. Then, Zou et al. further simplified this protocol by achieving AQS without entangled states [6]. However, Gao et al. pointed out there exist some security loopholes in the previous AQS protocols [7]. They showed that the receiver can make Pauli forgery of the signature, and the signer can successfully disavow the signature. Later, Choi et al. provided an improved idea to prevent the receiver's Pauli forgery attack with the example of ZK protocol [8]. Recently, Hwang et al. [9] also discussed the security of Zou et al.'s AQS protocol under the denial-of-service attack [10, 11] and Trojan horse attack [12, 13]. Recently, Zhang et al. further analyze the security of AQS [14, 15] and propose some improved ideas [16].

Meanwhile, some special quantum signature protocols have been presented based on the merits of AQS. From 2008, Yang et al. successively proposed some multiparty quantum signature protocols [17–19]. In 2011, they also gave an arbitrated quantum signature protocol against collective amplitude damping noise [20]. At the same time, Wang et al. presented some contributions to the practical quantum signature protocols. In 2010, Wang et al. proposed a fair quantum blind signature protocol based on the fundamental properties of quantum mechanics [21]. A one-time proxy signature with decoherence-free states was also presented to prevent the collective noise in 2012 [22].

A secure quantum signature requires the following conditions: 1) Any two of Trent, message owner and signer will not conspiracy. 2) The scheme will be done strictly by three parties, in the signature process.

In this paper, we will pay attentions to quantum blind signature. In a common digital signature, the original information is visible to signers, which does not match the request of the anonymity of the information holder. To protect the privacy of the information holders, such as electric cash, electric voting and electric auction etc, blind signature makes the related information invisible to signers. The original information is made ”blinded” by the holder before it is delivered to signers. Quantum blind signature is a new research topic combining with classic blind signature and quantum techniques. Similarly with classical blind signature, a secure quantum blind signature also requires the following conditions:

1) Unforgeability. Nobody can generate a valid blind signature except for the legal signer.
2) Undeniability. Once the signer issues a blind signature, he (she) cannot deny it.
3) Blindness. The signer cannot know the content of the message that he has signed.
4) Verifiability. Anyone can verify the validity of blind signatures.
5) Traceability. Once some disagreement emerges, the signer and the receiver can trace the message owner with the help of a trusted entity.

In this paper, we focus on a practical economical situation. When an electric transaction is made in a bank, the consumer needs anonymity and convenience, the shop requests reliability, and the bank requires that no digital cash is reused and that the electric transmitter is not illegally forged. The concrete process is as follows (See Fig. 1)

(1) The consumer sets up an account for electric transactions in a bank. Both the bank and the consumer agree on saving a sum of digital cash in a local computer or digital card.
(2) The consumer purchases goods or service from the shop using the digital cash.

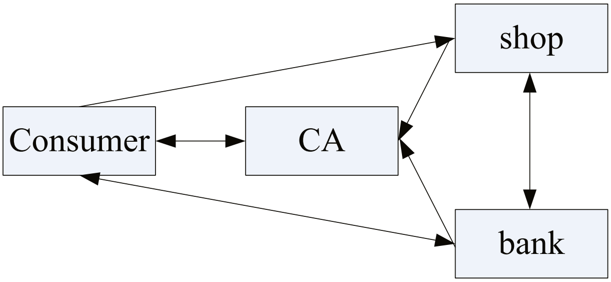

Fig. 1 An electric transaction. In the economical situation, blind signature can be applied

(3) The shop verifies the digital money received from the consumer through the verification centre in the bank. After the money is proved to be true, it sends to the bank to get paid.

(4) The bank receives and verifies the request of the payment, then makes the payment to the shop. In this process there is some consumer information that is to be given to the bank secretly, such as consumer personal information. So the consumer must blind the messages before sending to bank to sign.

In order to describe the quantum version of blind signature protocol which can be applied in the above situation, the rest of this paper is organized as follows. In Section 2, we will review the quantum relations of four-particle GHZ states. The corresponding results will be further used in the protocol design. In Section 3, our quantum blind signature protocol is proposed. Furthermore, its security analysis is presented in Section 4. It can be seen the security requirements can be achieved in this protocol. At last, a conclusion is given in Section 5.

2 Basic Theory

In this section, we will describe the correlation of four-particle GHZ states. Without loss of generality, the X-basis and Y-basis are described as

$$|+X\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle);\ |-X\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \tag{1}$$

$$|+Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle);\ |-Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle). \tag{2}$$

In order to show the correlation, we consider the following situations:

(1) All the participants measure the four-particle GHZ state with X-basis.

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \\ &= \frac{1}{2\sqrt{2}}(|+X+X+X+X\rangle + |-X-X-X-X\rangle + |+X+X-X-X\rangle \\ &+ |-X-X+X+X\rangle + |+X-X+X-X\rangle + |-X+X-X+X\rangle \\ &+ |+X-X-X+X\rangle + |-X+X+X-X\rangle) \end{aligned} \tag{3}$$

(2) All the participants measure the four-particle GHZ state with Y-basis.

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \\
&= \frac{1}{2\sqrt{2}}(|+Y+Y+Y+Y\rangle + |-Y-Y-Y-Y\rangle + |+Y+Y-Y-Y\rangle \\
&+ |-Y-Y+Y+Y\rangle + |+Y-Y+Y-Y\rangle + |-Y+Y-Y+Y\rangle \\
&+ |+Y-Y-Y+Y\rangle + |-Y+Y+Y-Y\rangle)
\end{aligned} \tag{4}$$

(3) Any two of them use X-basis and the other two use Y-basis to measure their particles.

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \\
&= \frac{1}{2\sqrt{2}}(|-X-X+Y-Y\rangle + |-X-X-Y+Y\rangle + |+X-X-Y-Y\rangle \\
&+ |-X+X-Y-Y\rangle + |+X+X+Y-Y\rangle + |+X+X-Y+Y\rangle \\
&+ |-X+X+Y+Y\rangle + |+X-X+Y-Y\rangle)
\end{aligned} \tag{5}$$

(4) Any three of them use X-basis (Y-basis) and the other one measures with Y-basis (X-basis) to measure their particles. Without loss of generality, we just discuss the following case.

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \\
&= \frac{1}{4}[(1-i)|+X+X+X+Y\rangle + (1+i)|+X+X+X-Y\rangle \\
&+ (1+i)|+X+X-X+Y\rangle + (1-i)|+X+X-X-Y\rangle + (1+i)|+X-X+X+Y\rangle \\
&+ (1-i)|+X-X+X-Y\rangle + (1-i)|+X-X-X+Y\rangle + (1+i)|+X-X-X-Y\rangle \\
&+ (1+i)|-X+X+X+Y\rangle + (1-i)|-X+X+X-Y\rangle + (1-i)|-X+X-X+Y\rangle \\
&+ (1+i)|-X+X-X-Y\rangle + (1-i)|-X-X+X+Y\rangle + (1+i)|-X-X+X-Y\rangle \\
&+ (1+i)|-X-X-X+Y\rangle + (1-i)|-X-X-X-Y\rangle]
\end{aligned} \tag{6}$$

Here we discuss the relative phases of the measurement states. From the case (1) and (2), it can be seen the number of ”+” and ”-” is even. From the case (3), the number of ”+” and ”-” is odd. From the case (4), there exists no correlation about the relative phases. Furthermore, except for the case (4), three participants’ measurement results will determine the other one’s measurement sate.

3 The Proposed Scheme

In this scheme, four participants are involved: Alice, Bob, Charlie and Trent. Alice is the owner of the message, Bob is the signer, Charlie is the verifier and Trent is the third trusted entity. Specially, Charlie and Alice can be one person in the practice application. The detailed procedure can be seen as follows.

3.1 Initializing Phase

In this phase, Alice, Bob, Charlie and TR share a secret quantum key, and share the GHZ particles for each other.

(I1) Quantum key distribution.

Trent shares secret key K_{TB} with Bob, K_{TC} with Charlie. In addition, Alice shares secret key K_{AB} with Bob, K_{AC} with Charlie. These distribution tasks can be achieved by using some practical quantum key distribution (QKD) techniques [23–27].

(I2) Shared GHZ states.

Trent prepares m GHZ states $|G\rangle_{ABCT} = \{|g\rangle^1_{ABCT}, |g\rangle^2_{ABCT}, \cdots, |g\rangle^m_{ABCT}\}$. We denote the ordered M four-qubit GHZ states with

$$[(g^1_A, g^1_B, g^1_C, g^1_T), (g^2_A, g^2_B, g^2_C, g^2_T), \cdots, (g^m_A, g^m_B, g^m_C, g^m_T)]$$

where $|g\rangle^i_{ABCT} = (|0000\rangle + |1111\rangle)/\sqrt{2}$. The superscript represents the order of each four-qubit GHZ state in the sequence, and the subscripts A, B, C, and T indicate the four photons of each GHZ state.Trent sends the particle $|G\rangle_A$ to Alice, $|G\rangle_B$ to Bob, $|G\rangle_C$ to Charlie and keeps the last one $|G\rangle_T$.

In the paper, All subscripts A, B, C and T denote Alice, Bob, Charlie and Trent, respectively. All superscript $1, 2, \cdots, i$ denote marshalling sequence.

3.2 Blinding Messages

(B1) Alice generates the message P and transform it into $H = |h(P)\rangle$ by quantum fingerprinting [2].

(B2) Alice randomly selects X-basis or Y-basis to measure her qubits $|G\rangle_A = \{|g\rangle^1_A, |g\rangle^2_A, \cdots, |g\rangle^m_A\}$ and notes the measurement basis she randomly chosen as $|B\rangle = \{|b\rangle^1, |b\rangle^2, \cdots, |b\rangle^m\}$. If Alice uses X-basis to measure her qubit $|g\rangle^i_A$, she notes $|b\rangle^i = 0$. Otherwise if Alice uses Y-basis to measure the qubit, $|b\rangle^i = 1$.

(B3) Alice encodes the measured states according to the following rules: if Alice gets $|-X\rangle$ or $|-Y\rangle$, let $t^i_A = 1$, otherwise she gets $|+X\rangle$ or $|+Y\rangle$, let $t^i_A = 0$. Then the measured state sequence is denoted as $T_A = \{t^1_A, \cdots, t^m_A\}$.

(B4) Alice generates $|M\rangle = \{|m^1\rangle, \cdots, |m^m\rangle\}$, here $|m^i\rangle = |h^i \oplus t^i_A\rangle$ and $\oplus$ means adding mod2.

3.2.1 *Signing Phase*

(S1) Alice sends $E_{K_{AB}}\{|M\rangle, |B\rangle\}$ to Bob by use of the quantum encryption algorithm [28] with the key K_{AB}.

(S2) After receiving Alice's notification, he obtains $(|M\rangle, |B\rangle)$. According to the measurement basis $|B\rangle$, he measures his participle $|G\rangle_B$. Similarly, if Bob gets $|-X\rangle$ or $|-Y\rangle$, let $t^i_B = 1$, otherwise she gets $|+X\rangle$ or $|+Y\rangle$, let $t^i_B = 0$. Then the measured state sequence is denoted as $T_B = \{t^1_B, \cdots, t^m_B\}$.

(S3) Bob encrypts $|V\rangle = E_r(T_B)$ with his chosen random number r. Then Bob gets $|M_B\rangle = \{|m^1_B\rangle, \cdots, |m^m_B\rangle\}$, here $|m^i_B\rangle = |m^i \oplus t^i_B\rangle$. Finally, he generates the signature $|S\rangle = E_{K_{BT}}\{|M_B\rangle, |V\rangle\}$ and sends it to Alice.

3.2.2 *Verifying Phase*

(V1) Alice receives $|S\rangle$, then encrypts $|Y\rangle = E_{K_{AC}}\{|S\rangle, |H\rangle, |B\rangle, E_{K_{AT}}(T_a)\}$ and sends $|Y\rangle$ to Charlie.

(V2) Charlie decrypts $|Y\rangle$ and measures his participle $|G\rangle_C$ with the basis $|B\rangle$. The same as Alice and Bob's performance, Charlie obtains the sequence $T^C = \{t^1_C, \cdots, t^m_C\}$.

(V3) Charlie encrypts $|Y_{CT}\rangle = E_{K_{CT}}\{|S\rangle, |H\rangle, |B\rangle, E_{K_{AT}}(T_A), T_C\}$ and sends it to Trent.

(V4) Trent decrypts $|Y_{CT}\rangle$. Similarly, Trent gets the measurement result $T^T = \{t_T^1, \cdots, t_T^m\}$.

(V5) Trent recovers $|M_B\rangle$ and generates $|H'\rangle = \{h'^1, \cdots, h'^m\}$, here $|h'^i\rangle = |m_B^i\rangle \oplus |t_C^i\rangle \oplus |t_T^i\rangle \oplus |t_A^i\rangle$. Trent compares $|H\rangle$ and $|H'\rangle$. If $|H'\rangle = |H\rangle$, he will accept the signature, and continue the next step, otherwise, he drops the signature.

(V6) If Bob raised an objection to the signature, he also can verify the signature. Trent generates $|T\rangle$ such that $|t^i\rangle = |t_A^i\rangle \oplus |t_C^i\rangle \oplus |t_T^i\rangle$. Then he encrypts $(|T\rangle, |V\rangle)$ to $|Y_{BT}\rangle = E_{K_{BT}}\{|T\rangle, |V\rangle\}$ and sends it to Bob.

(V7) Bob decrypts $|Y_{BT}\rangle$ to get $|V\rangle$. Furthermore, he can get $|T_B\rangle$ and $|T\rangle$. When the testing condition $t^i \oplus t_B^i = |0\rangle$ is satisfied, Bob accepts the signature.

Here, all the participants measure the four-particle GHZ state with the same basis lead to $t^i \oplus t_B^i = t_A^i \oplus t_B^i \oplus t_C^i \oplus t_T^i = 0$

In step V3 and V4, if the owner of the message and verifier are one person, who is named Alice. Alice computes $T_C \oplus T_A$ and directly sends $|Y_{CT}\rangle = E_{K_{CT}}\{|S\rangle, |H\rangle, |B\rangle, T_A \oplus T_C\}$ to Trent.

4 Security Analysis and Discussion

With the development of quantum cryptography, some feasible attack strategies have been proposed such as intercept-resend attacks [29], entanglement-swapping attacks [30, 31], teleportation attacks [32], dense-coding attacks [33, 34], channel-loss attacks [35, 36], denial-of-service attacks [10, 11], correlation-extractability attacks [37–39], Trojan horse attacks [12, 13], participant attacks [31, 34] and so on. Furthermore, some cryptanalysis of quantum signature have been presented [7–9, 14–16]. Here we analyze the quantum blind signature from the exist ideas. The detailed security analysis can be seen as follows.

4.1 Unforgeability

If the malicious message owner Alice attempts to counterfeit the signatory Bob's signature $|S\rangle$ to her own benefit, she has to know K_{AB}, r and the state $|T_B\rangle$ of Bob. However, this is impossible due to the unconditionally secure quantum key distribution. In the worst situation, for instance, in which the secret keys are exposed to Alice, Alice still cannot forge the signature, since he cannot create appropriate $|T_B\rangle$ related to the new message. So Alice's forgery can be avoided.

Similarly, suppose Alice repudiates the receipt of the signature. Then Trent also can confirm that Alice has received the signature $|S\rangle$, since she needs the assistance of the Trent to verify the signature.

If the attacker Eve tries to forge Bob's signature $|S\rangle$ for his own sake, he also should know Bob's secret key K_{AB}, r and the state $|T_B\rangle$. In the step (V7), Bob can find his forgery. The public information that he can obtain betrays nothing. So the forgery for Eve is also impossible.

4.2 Undeniability

If Bob wants to disavow his signature, Alice, Charlie and Trent can expose him. Alice, Charlie and Trent can lead to recovery $|h'^i\rangle = |m_B^i \oplus t_A^i \oplus t_C^i \oplus t_T^i\rangle = |h^i\rangle$ without the help of Bob, If $|H'\rangle = |H\rangle$, they will accept the signature.

4.3 Blindness

In our scheme, Bob is kept blind from the message content. In all above steps, Bob the first and foremost only contacts his own qubit and $|m^i\rangle = |h^i \oplus t_A^i\rangle$, which not help him to know $|H\rangle$. There is one more point, $H = |h(P)\rangle$ is transformed by quantum fingerprinting.

In fact, Bob is not necessary to know the Alice's transaction content, but he could sign the message $|M\rangle$ for Alice. And Charlie could verify and accept the payment message $|M\rangle$ signed by the Bob.

4.4 Traceability

In case of any dispute about Bob, Trent submits $|V\rangle$ to Bob, Bob can make sure his private key r and believe it is its own signature. Once some disagreement emerges with Alice, according to $\{K_{BC}, |M\rangle, |B\rangle\}$ and the measuring results of particles, the referee can trace the message owner and judge whether the process is valid or not.

5 Conclusion

In this paper, we present a blind signature scheme based on the correlation of four-particle GHZ states. In our scheme, the signatory is kept blind from the signed message content. However, he could still be able to trace the message owner if some disagreement emerges. Specially, the singer also cannot trail his signature, but he can make sure whether it is his own signature or not. The security of our scheme is guaranteed by the one-time pad and quantum key distribution.

Acknowledgments This work is supported by NSFC (Grant Nos. 61272057, 61170270), Beijing Higher Education Young Elite Teacher Project (Grant Nos. YETP0475, YETP0477).

References

1. Gottesman, D., Chuang, I.: Quantum Digital Signatures. arXiv:quant-ph/0105032v2 (2001)
2. Buhrman, H., Cleve, R., Watrous, J., et al.: Quantum fingerprinting. Phys. Rev. Lett. **87**, 167902 (2001)
3. Buhrman, H., Crepeau, C., Gottesman, D., et al.: Authentication of quantum messages, pp. 449–458. IEEE Computer Society Press, Washington DC (2002)
4. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2002)
5. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**, 054307 (2009)
6. Zou, X.F., Qiu, D.W.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **82**, 042325 (2010)
7. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**, 022344 (2011)
8. Choi, J.W., Chang, K.Y., Hong, D.: Security problem on arbitrated quantum signature schemes. Phys. Rev. A **84**, 062330 (2011)
9. Hwang, T., Luo, Y.P., Chong, S.K., Chong S.K.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **85**, 056301 (2012)
10. Cai, Q.Y., The, Q.Y.: The "Ping-Pong" Protocol Can Be Attacked without Eavesdropping. Phys. Rev. Lett. **91**, 109801 (2003)
11. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Consistency of shared reference frames should be reexamined. Phys. Rev. A **77**, 014302 (2008)
12. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)

13. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
14. Zhang, K.J., Qin, S.J., Sun, Y., Song, T.T., Su Q.: Reexamination of arbitrated quantum signature: The impossible and the possible. Quantum Inf. Proc. **12**(7), 3127–3141 (2013)
15. Zhang, K.J., Li, D., Su, Q.: Security of the arbitrated quantum signature protocols revisited. Phys. Scr. **89**, 015102 (2014)
16. Zhang, K.J., Zhang, W.W., Li, D.: Improving the security of arbitrated quantum signature against the forgery attack. Quantum Inf. Proc. **12**(8), 2655–2669 (2013)
17. Yang, Y.G.: Multi-proxy quantum group signature scheme with threshold shared verification. Chin. Phys. B **17**, 415 (2008)
18. Yang, Y.G., Wen, Q.Y.: Threshold proxy quantum signature scheme with threshold shared verification. Sci. Chin. Ser. G: Phys. Mech. Astron. **51**, 1079–8C1088 (2008)
19. Yang, Y.G., Wang, Y., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Scalable arbitrated quantum signature of classical messages with multi-signers. Commun. Theor. Phys. **54**, 84 (2010)
20. Yang, Y.G., Wen, Q.Y.: Arbitrated quantum signature of classical messages against collective amplitude damping noise. Opt. Commun. **283**, 3198–3201 (2010)
21. Wang, T.Y., Wen, Q.Y.: Fair quantum blind signatures. Chin. Phys. B **19**, 060307 (2010)
22. Wang, T.Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography, Quantum Information Proceedings. doi:10.1007/s11128-011-0258-6 (2012)
23. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179. IEEE Press, New York (1984)
24. Ekertm, A.K.: Quantum cryptography based on bell theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
25. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
26. Bennett, C.H., Brassard, G., et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
27. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Quantum key distribution without alternative measurements and rotations. Phys. Lett. A **349**, 53–58 (2006)
28. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**, 042317 (2003)
29. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection. Phys. Rev. Lett. **101**, 208901 (2008)
30. Zhang, Y.S., Li, C.F., Guo, G.C.: Quantum key distribution without alternative measurements and rotations. Phys. Rev. A **63**, 036301 (2001)
31. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the bradler-dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
32. Gao, F., Wen, Q.Y., Zhu, F.C.: Teleportation attack on the QSDC protocol with a random basis and order. Chin. Phys. B **17**, 3189 (2008)
33. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Dense-coding attack on three-party quantum key distribution protocols. IEEE J. Quantum Electron. **47**, 630 (2011)
34. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys. Lett. A **357**, 101 (2006)
35. W'ojcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. **90**, 157901 (2003)
36. W'ojcik, A.: Comment on Quantum dense key distribution. Phys. Rev. A **71**, 016301 (2005)
37. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: "Quantum exam". Phys. Lett. A **360**, 748 (2007)
38. Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: A Special Eavesdropping on One-Sender Versus N-Receiver QSDC Protocol. Chin. Phys. Lett. **25**, 1561 (2008)
39. Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **283**, 192 (2010)