International Journal of Theoretical Physics (2018) 57: 3505–3513
https://doi.org/10.1007/s10773-018-3865-5

Three-Party Quantum Key Agreement Protocol with Seven-Qubit Entangled States

Nan-Run Zhou[1] · Shi-Qi Min[2] · Hua-Ying Chen[3] · Li-Hua Gong[1]

Received: 1 May 2018 / Accepted: 11 August 2018 / Published online: 17 August 2018

Abstract
A new three-party quantum key agreement protocol based on seven-qubit states is proposed. In this protocol, each participant adopts different encryption methods to transmit a secret key of the same length. Subsequently, the participants utilize joint measurement to gain the ultimate shared secret key. No participant can determine the ultimate shared key by himself/herself. In addition, the proposed three-party quantum key agreement protocol could resist several well-known attacks. Compared with typical quantum key agreement protocols, our proposed three-party quantum key agreement protocol is more efficient.

Keywords Quantum key agreement protocol · Seven-qubit entangled state · Quantum cryptography

1 Introduction

As a significant branch of quantum cryptography, quantum key agreement (QKA) can build secure key between or among participants and even can maintain the fairness of the participants' contribution to the shared secret key.

Zhou et al. proposed the first weak quantum key agreement protocol based on quantum teleportation without considering the fairness [1]. In the same year, a two-party quantum key agreement protocol with the maximally entangled states [2] was proposed, however, Hwang and Tsai et al. hold that this protocol has security issues, because an eavesdropper can obtain the entire final shared secret key by executing CNOT attack and intercept-resend attack without being detected. Meanwhile, they proposed a new quantum key agreement protocol [3, 4] to withstand the resistance attack. Chong et al. [5] presented a quantum key agreement protocol based on BB84 which makes the best use of unitary operations and delayed measurement [6]. Shi et al. successfully extended the two-party QKA protocol into

✉ Li-Hua Gong
lhgong@ncu.edu.cn

[1] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[2] Department of Computer Science and Technology, Nanchang University, Nanchang 330031, China

[3] Department of Physics, Nanchang University, Nanchang 330031, China

a multi-party QKA protocol [7]. However, Liu et al. pointed out that it was insecure and unfair since dishonest participants could determine the final shared secret key by themselves and proposed a QKA protocol [8] that only utilized single photons for encryption to resist the participant attack. Sun improved Liu et al.'s protocol by adding unitary operations. Huang et al. [9] conducted a detailed analysis on Sun's protocol and came up with a method to resist the attacks at the cost of qubit efficiency. Shukla et al. [10] put forward a multi-party quantum key agreement (MQKA) protocol with Bell states, which was a protocol in travelling mode [11]. Unfortunately, an eavesdropper can flip qubit of the final shared secret key of Shukla's protocol without introducing any error [12]. Huang et al. improved the travelling mode of MQKA protocol [13]. In recent years, researchers have shifted their focus on the multi-qubit states. Sun et al. put forward an MQKA protocol based on genuinely maximally entangled six-qubit states [14]. Four-qubit cluster states were also utilized in quantum key agreement protocol [15–17]. In addition, multi-qubit states can be generated by combining multiple states [18–23]. Thus, how to make full use of the characteristics of multi-qubit states is of great significance for quantum communication.

Based on seven-qubit entangled states, a three-party quantum key agreement protocol is devised. Each participant adopts different encryption methods and utilizes the characteristics of the seven-qubit entangled states to generate six-bit shared secret keys. In Section 2, the related quantum gates and the seven-qubit entangled states will be introduced. Section 3 will offer a detailed description of the proposed three-party QKA protocol. In Section 4, the security analysis will be given. Comparisons among previous QKA protocols and our proposed QKA protocol will be provided in Section 5. Finally, a brief conclusion will be drawn in Section 6.

2 Quantum Gate and Qubit

In this section, several unitary operations, Controlled NOT gate, Bell states and seven-qubit entangled states are introduced.

2.1 Quantum Gate

Quantum information processing is a series of unitary evolutions of the quantum states encoded. Quantum logic gate refers to the most fundamental unitary operations of qubits. The basic one-qubit gates are as follows:

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad Y=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}. \tag{1}$$

As for the controlled NOT (CNOT) gate, the first qubit is called the control bit, while the second quantum bit is called the target bit. The unitary operation of the CNOT gate is:

$$\mathrm{CNOT}=\begin{pmatrix}I&\mathbf{0}\\\mathbf{0}&X\end{pmatrix} \tag{2}$$

Bell states are four specific maximally entangled quantum states of two qubits. Four Bell states can be expressed as:

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle) \tag{3}$$

$$|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \tag{4}$$

Suppose four local unitary operations are respectively denoted by U_{00}, U_{01}, U_{10} and U_{11} such as $U_{00} \equiv I$, $U_{01} \equiv X$, $U_{10} \equiv YZ$, $U_{11} \equiv H$, where the subscripts are the encoded bits associated with their operations. Furthermore, two sets of orthogonal bases are Z-basis and X-basis. $|0\rangle$ and $|1\rangle$ form the Z-basis, while $|+\rangle$ and $|-\rangle$ form the X-basis, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

2.2 Seven-Qubit Entangled State

Zha et al. presented a seven-qubit entangled state $|\psi\rangle_{1234567}$ [24], which is a maximally multipartite entangled state [25]. This state is more highly entangled than the previously discovered states [26]. The seven-qubit entangled state whose marginal density matrices for subsystems of one and two qubits are wholly mixed and most but not all of the marginal density matrices of three qubits are completely mixed.

$$\begin{aligned}|\psi\rangle_{1234567} = \frac{1}{4\sqrt{2}}[&(|\mathbf{0}\rangle + |\mathbf{3}\rangle + |\mathbf{13}\rangle + |\mathbf{14}\rangle)\\ &+(|\mathbf{17}\rangle - |\mathbf{18}\rangle + |\mathbf{28}\rangle - |\mathbf{31}\rangle)\\ &-(|\mathbf{37}\rangle + |\mathbf{38}\rangle - |\mathbf{40}\rangle - |\mathbf{43}\rangle)\\ &+(|\mathbf{52}\rangle - |\mathbf{55}\rangle - |\mathbf{57}\rangle + |\mathbf{58}\rangle)\\ &-(|\mathbf{68}\rangle + |\mathbf{71}\rangle - |\mathbf{73}\rangle - |\mathbf{74}\rangle)\\ &+(|\mathbf{85}\rangle - |\mathbf{86}\rangle - |\mathbf{88}\rangle + |\mathbf{91}\rangle)\\ &+(|\mathbf{97}\rangle + |\mathbf{98}\rangle + |\mathbf{108}\rangle + |\mathbf{111}\rangle)\\ &+(|\mathbf{112}\rangle - |\mathbf{115}\rangle + |\mathbf{125}\rangle - |\mathbf{126}\rangle)]_{1234567}\end{aligned} \tag{5}$$

where the bold numbers represent the decimal system, for example, $|\mathbf{0}\rangle$ denotes $|0000000\rangle$. By factoring (5), the new expression of maximally entangled seven-qubit state is as follows.

$$\begin{aligned}|\psi\rangle_{1234567} = \frac{1}{4}[&(|00\rangle|\phi^+\rangle + |11\rangle|\psi^+\rangle)_{1267}|\mathbf{0}\rangle_{345} - (|10\rangle|\phi^+\rangle + |01\rangle|\psi^+\rangle)_{1267}|\mathbf{1}\rangle_{345}\\ &+(|01\rangle|\phi^+\rangle + |10\rangle|\psi^+\rangle)_{1267}|\mathbf{2}\rangle_{345} + (|11\rangle|\phi^+\rangle + |00\rangle|\psi^+\rangle)_{1267}|\mathbf{3}\rangle_{345}\\ &+(|11\rangle|\phi^-\rangle + |00\rangle|\psi^-\rangle)_{1267}|\mathbf{4}\rangle_{345} + (|01\rangle|\phi^-\rangle + |10\rangle|\psi^-\rangle)_{1267}|\mathbf{5}\rangle_{345}\\ &-(|10\rangle|\phi^-\rangle + |01\rangle|\psi^-\rangle)_{1267}|\mathbf{6}\rangle_{345} + (|00\rangle|\phi^-\rangle + |11\rangle|\psi^-\rangle)_{1267}|\mathbf{7}\rangle_{345}]\end{aligned} \tag{6}$$

3 Three-Party QKA Protocol

The three-party quantum key agreement protocol with seven-qubit entangled states is shown in Fig. 1, where there are three participants in the considered protocol, i.e., Alice, Bob and Charlie. They plan to share secret key K via quantum channel, and adopt different encryption methods to transmit a secret key. For example, Alice uses the method of introducing a new sequence related to secret key, Bob utilizes the CNOT operation method, while Charlie employs the four unitary operations. The detailed process of the three-party QKA protocol is described as follows.

Step. 1 The participants randomly generate $2n$-bit strings as secret keys, $K_A = \{K_A^i | i = 1, 2, \ldots, n\}$, $K_B = \{K_B^i | i = 1, 2, \ldots, n\}$ and $K_C = \{K_C^i | i = 1, 2, \ldots, n\}$, respectively. Every participant negotiates that the encoding rule is I : 00, X :

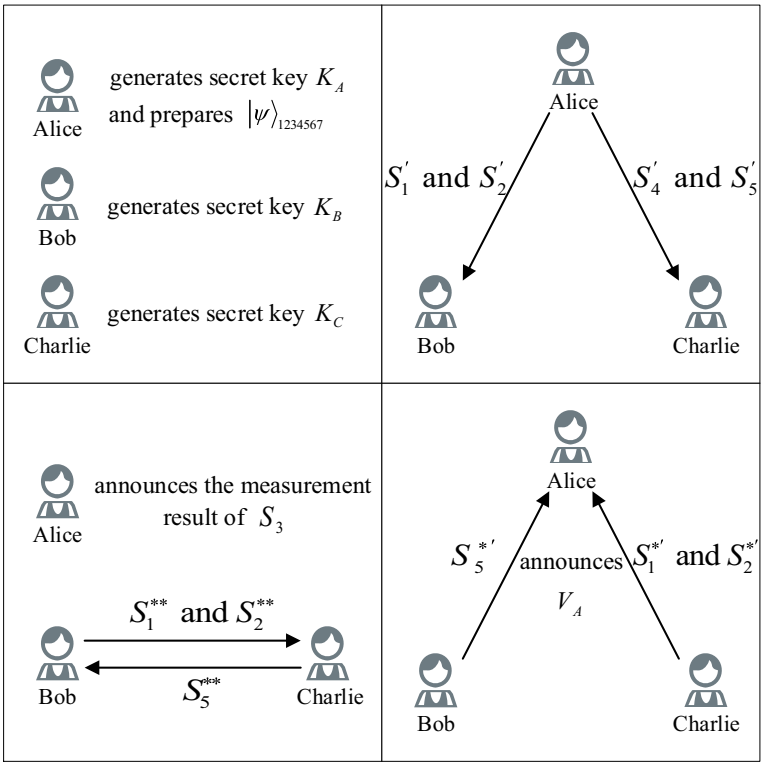

Fig. 1 Three-party quantum key agreement protocol

01, $YZ : 10$, $H : 11$, and represents the Bell states correspondingly, i.e., $|\phi^+\rangle : 00$, $|\phi^-\rangle : 01$, $|\psi^+\rangle : 10$, $|\psi^-\rangle : 11$.

Step. 2 Alice prepares n seven-qubit entangled states and divides all the particles into seven ordered sequences $S_j (j = 1, 2, \ldots, 7)$. Then, Alice randomly selects decoy states in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ and randomly inserts them into S_1, S_2, S_4 and S_5, respectively. Alice sends the mixed sequences S_1' and S_2' (S_4' and S_5') to Bob (Charlie).

Step. 3 After confirming that Bob and Charlie have received the sequences, eavesdropping check should be executed. Alice announces the positions of the decoy states and their corresponding measurement bases $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Afterward, Bob and Charlie measure the decoy states with correct bases and tell Alice the measurement results. Alice compares the measurement results of Bob and Charlie with the initial decoy states and computes the error rate among the measurement results. If the error rate exceeds the predetermined value associated with the channel state information, all participants will abandon this round of communication and restart after a random time. Otherwise, they will proceed to the next step.

Step. 4 Bob and Charlie remove the inserted decoy states. Moreover, Bob performs the Z-basis measurement on every state in S_1 and S_2. Similarly, Charlie performs Z-basis measurement on every state in S_4 and S_5. In addition, Bob and Charlie compare the measurement results of S_1 with that of S_4 to see whether the measurement results are same. In the end, Alice announces the measurement results

of S_3 and that of Bell states denoted by $M_A = \{M_A^i | i = 1, 2, \ldots, n\}$, where M_A^i is the corresponding code of Alice's i-th states in S_6 and S_7. The characteristics of the highly entangled seven-qubit states can be used to obtain the initial states. For example, assume that Bob's measurement result of S_1 and S_2 is $|00\rangle$, if the comparison result between Bob's and Charlie's is same, then the measurement result of S_4 and S_5 is $|00\rangle$. Otherwise, the result is $|11\rangle$. After Alice announces the measurement result of S_3, Bob and Charlie can obtain the initial states of the seven-qubit entangled states in terms of $|00\rangle_{12}|000\rangle_{345}$ or $|00\rangle_{12}|100\rangle_{345}$.

Step. 5 According to $K_B = \{K_B^i | i = 1, 2, \ldots, n\}$, Bob performs the CNOT operations on every state in S_1 and S_2. K_B is called the control bit, while S_1 and S_2 are the target bits. The rule is described as follows. If K_B^i is equal to 00, 01, 10 or 11, Bob performs the unitary operations in S_1 and S_2, i.e., $I^{S_1} \otimes I^{S_2}$, $I^{S_1} \otimes X^{S_2}$, $X^{S_1} \otimes I^{S_2}$ or $X^{S_1} \otimes X^{S_2}$, where the new sequences S_1^* and S_2^* are obtained. According to $K_C = \{K_C^i | i = 1, 2, \ldots, n\}$, Charlie performs four unitary operations U_{00}, U_{01}, U_{10} and U_{11} in S_5. Then Charlie obtains a new sequence S_5^*. Charlie (Bob) prepares enough decoy states and randomly inserts them into S_5^* (S_1^* and S_2^*). Charlie (Bob) sends the mixed sequence(s) S_5^{**} (S_1^{**} and S_2^{**}) to Bob (Charlie).

Step. 6 After receiving the sequence, Bob and Charlie begin to check eavesdropping. The whole process is similar to that in Step 3.

Step. 7 Bob and Charlie remove the decoy states. Charlie announces the positions corresponding to the states performed operation U_{11} in S_5^*. Subsequently, Bob performs Z-basis or X-basis on every state in S_5^*. Charlie performs Z-basis on each state in S_1^* and S_2^*. At this moment, Bob and Charlie could gain secret keys from each other. Bob (Charlie) randomly inserts enough decoy states into S_5^* (S_1^* and S_2^*). Hence Bob and Charlie send the mixed sequences $S_1^{*\prime}$, $S_2^{*\prime}$ and $S_5^{*\prime}$ to Alice.

Step. 8 Alice, Bob and Charlie perform eavesdropping check as demonstrated in Step 3.

Step. 9 After receiving sequences $S_1^{*\prime}$, $S_2^{*\prime}$, $S_5^{*\prime}$, Alice announces $V_A^i = K_A^i \oplus M_A^i$ via the classical authentication channel. Since Bob and Charlie know the initial states of the seven-qubit entangled states, they can compute the final shared secret key $K = \{K_B^i K_C^i K_A^i | i = 1, 2, \ldots, n\}$. Besides, Alice removes the decoy states and measures $S_1^{*\prime}$, $S_2^{*\prime}$, $S_5^{*\prime}$ with correct bases. Finally, Alice obtains the final shared secret key, too.

4 Security Analysis

In this section, it will be shown that the proposed three-party QKA protocol is secure under some common attacks.

4.1 Trojan Horse Attack

Since the same states are transmitted more than once in the channel, the protocol may be subject to Trojan horse attack. Gisin et al. [27] pointed out how an eavesdropper gains information of the shared secret key with Trojan horse attack. To avoid this attack, each participant should install two quantum optical devices, i.e., the wavelength quantum filter and the photon number splitter (PNS). Specifically, the wavelength quantum filter can filter out Eve's invisible photons [28], and PNS can discover the delay photons by dividing photons [29, 30]. The proposed three-party quantum key agreement protocol could resist Trojan horse attack if the two quantum optical devices are installed.

4.2 Intercept-Resend Attack

Suppose that Eve successfully intercepts the transmitted sequences of particles and resends the prepared fake sequences. First of all, since only sequences S_1, S_2, S_4 and S_5 are transmitted in quantum channel while S_3, S_6 and S_7 are kept home by Alice, Eve cannot intercept all states to acquire the final shared secret key. Secondly, since participants will randomly insert decoy states into the encoded states before their transmission, Eve does not know the positions and the measurement bases of the random decoy states before the sender's announcement. Participants calculate the error rate by the eavesdropping check method, then Eve's attack behavior will be detected with a probability $1-\left(\frac{3}{4}\right)^m$ (m denotes the number of decoy states used to detect in this attack). Therefore, it is impossible for Eve to obtain the final shared secret key with intercept-resend attack without being detected.

4.3 Entangling Attack

The entangling attack means that Eve intercepts the particles transmitted and entangles an ancillary system $|\varepsilon\rangle$ prepared beforehand with it. Finally, Eve resends intercepted particles to the receiver and measures the ancillary system to obtain useful information about the final shared secret key. To perform the entangling attack, Eve intercepts the particles in the sequences S_1', S_2', S_4', S_5', S_1^*, S_2^*, S_5^*, $S_1^{*\prime}$, $S_2^{*\prime}$ and $S_5^{*\prime}$, and entangles them with the ancillary system $|\varepsilon\rangle$. Subsequently, Eve resends intercepted sequences to the receiver and measures the ancillary system. Since the decoy states involved in our protocol are random in four states, i.e., $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, without loss of generality, Eve's unitary operator U_e should satisfy

$$U_e|0\rangle|\varepsilon\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \tag{7}$$

$$U_e|1\rangle|\varepsilon\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle \tag{8}$$

$$\begin{aligned} U_e|+\rangle|\varepsilon\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle + c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle) \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle)] \\ &\quad + \frac{1}{2}[|-\rangle(a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle)] \end{aligned} \tag{9}$$

$$\begin{aligned} U_e|-\rangle|\varepsilon\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle - c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle) \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle)] \\ &\quad + \frac{1}{2}[|-\rangle(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle)] \end{aligned} \tag{10}$$

where $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$. If Eve passes the eavesdropping detection without being detected in Steps. (3), (6) and (8), she must ensure the conditions such as $a = d = 1$, $b = c = 0$ and $|e_{00}\rangle = |e_{11}\rangle$. Thus, only if Eve's ancillary states and the decoy states are in state $|0\rangle$ or $|1\rangle$, eavesdropper will not be detected. However, since Eve can't distinguish $|e_{00}\rangle$ from $|e_{11}\rangle$ and must disturb the random decoy states in the two states $|+\rangle$

and $|-\rangle$, she cannot obtain any useful information about the participants' secret key with the entangling attack.

4.4 Participant Attack

Since dishonest participants grasp a part of shared secret key information, they may collaborate to predetermine the final shared secret key without being detected. Then they decide the final shared secret key by changing subkey. To resist participant attack, the protocol should employ delayed measurement technique [6] and quantum authentication technique [31, 32]. In other words, all participants obtain the final shared secret key simultaneously and fairly. For example, suppose that Bob and Charlie are dishonest participants, and they want to determine the final shared secret key. Until Alice announces V_A^i, Bob and Charlie cannot derive K_A^i from the known M_A^i. In addition, Alice is an honest participant necessary to work out K with the measurement results of $S_1^{*\prime}$, $S_2^{*\prime}$ and $S_5^{*\prime}$ after announcing V_A^i. It is impossible for the participants to obtain the final shared secret key in advance.

4.5 Information Leakage

Since Alice announces measurement results of S_3 and V_A^i, Eve may attempt to gain the final shared secret key. However, Eve does not know the initial states of the seven-qubit entangled states, and sequence S_3 does not carry any useful information about the secret key. Even if Eve luckily obtains the secret key of Alice, there is still no information leakage problem in the proposed three-party QKA protocol, since the final shared secret key has 2^{6n} possible outcomes.

5 Comparison

Cabello [33] put forward the qubit efficiency η in quantum key distribution protocol.

$$\eta = \frac{c}{q+b} \tag{11}$$

where c indicates the length of the final shared secret key generated, q indicates the total number of used qubits, i.e. the quantum states and decoy particles prepared by each participant, b is the total number of classical bits exchanged for decoding the message. A simple comparison with similar QKA protocols from the aspects of quantum resource, the length of the shared secret key, qubit efficiency is shown in Table 1. To generate $6n$ bits of shared secret key in our three-party QKA protocol, the qubit efficiency is:

$$\eta = \frac{6n}{(7n+10m)+(n+2n)} \tag{12}$$

where $q = 7n + 10m$, $b = n + 2n$, m denotes the total number of decoy particles. In addition, $7n$ denotes that Alice prepares n seven-qubit entangled states, $n + 2n$ is that Alice announces the measurement results of S_3 and V_A^i. If m is same as n, then η will be up to 30%. It is obvious that our three-party QKA protocol has higher efficiency.

Table 1 Comparison of QKA protocols

Protocol	Quantum resource	Length of the shared secret key	Qubit efficiency (%)
Ref. [14]	Single photon	n	8.33
Ref. [15]	Single photon	n	16.67
Ref. [22]	Six-qubit entangled state	$2n$	16.67
Ref. [24]	Cluster state	$2n$	13.33
Ref. [25]	Cluster state	$4n$	26.67
Ref. [26]	GHZ state	$2n$	16.67
Ours	Seven-qubit entangled state	$6n$	30

6 Conclusion

In conclusion, a new three-party quantum key agreement protocol based on the seven-qubit entangled states is investigated. In this three-party QKA protocol, each participant adopts different encryption methods to establish a secret key. The negotiation process of the protocol is more diverse and flexible. It is demonstrated that this proposed three-party QKA protocol can effectively resist outside and participants attacks and has higher qubit efficiency due to the multi-qubit entanglement states.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 61561033), and the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002).

References

1. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149–1150 (2004)
2. Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states. Proc. Inf. Sec Conf. In: Proceedings of the 14th Information Security Conference, pp. 236–242. National Taiwan University of Science and Technology, Taipei (2004)
3. Tsai, C.W., Chong, S.K., Hwang, T.: Comment on quantum key agreement protocol with maximally entangled states. In: Proceedings of the 20th Cryptology and Information Security Conference, pp. 210–213. National Chiao Tung University, Hsinchu (2010)
4. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on quantum key agreement protocol with maximally entangled state. Int. J. Theor. Phys. **50**, 1793–1802 (2011)
5. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Comm. **283**, 1192–1195 (2010)
6. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**, 2097 (2004)
7. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
8. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
9. Huang, W., Wen, Q.-Y., Liu, B., Su, Q., Gao, F.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. Quantum Inf. Process. **13**, 1651–1657 (2014)
10. Shukla, C., Alam. N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. **13**, 2391–2405 (2014)
11. Liu, B., Gao, F., Huang, W.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
12. Zhu, Z.C., Hu, A.Q., Fu, A.M.: Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. **14**, 4245–4254 (2015)

13. Huang, W., Su, Q., Xu, B.: Improved multiparty quantum key agreement in travelling mode. Sci. China. Phys: Mech. Astron. **59**, 120311 (2016)
14. Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**, 1920–1929 (2016)
15. Shen, D.S., Ma, W.P., Wang, L.L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**, 2313–2324 (2014)
16. Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process. **15**, 373–384 (2016)
17. He, Y.F., Ma, W.P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**, 3483–3498 (2015)
18. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. **13**, 2587–2594 (2014)
19. He, Y.F., Ma, W.P.: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Quantum Inf. **14**, 1650007 (2016)
20. He, Y.F., Ma, W.P.: Two-party quantum key agreement with five-particle entangled states. Int. J. Quantum Inf. **15**, 1750018 (2017)
21. Xu, L., Zhao, Z.: Quantum private comparison protocol based on the entanglement swapping between χ^+ state and W-Class state. Quantum Inf. Process. **16**, 1–15 (2017)
22. Min, S.Q., Chen, H.Y., Gong, L.H.: Novel multi-party quantum key agreement protocol with G-Like states and Bell states. Int. J. Theor. Phys. **57**, 1811–1822 (2018)
23. Chou, Y.H., Zeng, G.J., Chang, Z.H.: Dynamic group multi-party quantum key agreement. Sci. Rep. **8**, 4633 (2018)
24. Zha, X., Song, H., Qi, J.: A maximally entangled seven-qubit state. J. Phys. A: Math. Theor. **45**, 255302 (2012)
25. Zha, X., Yuan, C., Zhang, Y.: Generalized criterion for a maximally multi-qubit entangled state. Laser Phys. Lett. **10**, 045201 (2013)
26. Borras, A., Plastino, A.R., Batle, J.: Multiqubit systems: highly entangled states and entanglement distribution. J. Phys. A: Math. Theor. **40**, 13407 (2007)
27. Gisin, N., Fasel, S., Kraus, B., et al.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)
28. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
29. Deng, F.G., Li, X.H., Zhou, H.Y., et al.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
30. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**, 054302 (2006)
31. Ma, H., Huang, P., Bao, W., et al.: Continuous-variable quantum identity authentication based on quantum teleportation. Quantum Inf. Process. **15**, 2605–2620 (2016)
32. Hong, C., Heo, J., Jang, J.G., et al.: Quantum identity authentication with single photon. Quantum Inf. Process. **16**, 236 (2017)
33. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5633–5638 (2000)