Int J Theor Phys (2017) 56:3108–3116
DOI 10.1007/s10773-017-3478-4

Improvement of "Novel Multiparty Quantum Key Agreement Protocol with GHZ States"

Jun Gu[1] · **Tzonelih Hwang**[1]

Received: 19 January 2017 / Accepted: 10 July 2017 / Published online: 2 August 2017

Abstract Quantum key agreement (QKA) protocol is a method for negotiating a fair and secure key among mutually untrusted participants. Recently, Xu et al. (Quantum Inf. Process. 13:2587–2594, 2014) proposed a multi-party QKA protocol based on Greenberger-Horne-Zeilinger (GHZ) states. However, this study points out that Xu et al.'s protocol cannot provide the fairness property. That is, the last involved participant in the protocol can manipulate the final shared secret key without being detected by the other participants. Moreover, according to Yu et al.'s research (2015), Xu et al.'s protocol cannot avoid the public discussion attack too. To avoid these weaknesses, an improved QKA protocol is proposed.

Keywords Quantum key agreement · Participant attack · Quantum cryptography

1 Introduction

In 1984, Bennett and Brassard proposed a secure quantum key distribution (QKD) protocol [1], which is the first key distribution protocol that uses the principles of quantum mechanics to ensure security. Subsequently, several QKD protocols and related protocols have been proposed [5, 10–14, 22]. However, in these QKD protocols, the shared secret key is first determined by a participant or a third-party and then distributed to the other participants. Obviously in this approach, each involved participant does not contribute to the shared key equally.

Different from the QKD protocols to ensure that all participants have equal contribution to the shared key, quantum key agreement (QKA) protocols have been proposed. In other

✉ Tzonelih Hwang
hwangtl@ismail.csie.ncku.edu.tw

[1] Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, University Rd., Tainan City, 70101, Taiwan, Republic of China

words, QKA protocol has to not only guarantee the security of the shared key but also assure the fairness property. The fairness property in particular means that each participant has **equal contribution to the final shared key** [17]. That is, none proper subset of the involved participants can determine any part of the final key without being detected by the others. In 2004, Zhou et al. proposed the first QKA protocol based on the quantum teleportation technique [29]. However, in 2006, Liu et al. [9] pointed out that Zhou et al.'s QKA protocol cannot achieve the security property by the intercept and resend attack. That is, in the quantum particles transmission process, the outside attacker Eve can use the photons generated by herself instead of the participants' particles to obtain the final shared key without being detected. Subsequently, Chong and Hwang [3] proposed a QKA protocol based on BB84 [1] and He et al. proposed a QKA protocol with four-particle GHZ states. However, these QKA protocols are just for two participants to negotiate a key.

In 2013, Shi and Zhong [16] proposed the first multi-party quantum key agreement (MQKA) protocol based on Bell states and Bell measurements. The protocol uses quantum entanglement swapping technique to help several participants to establish a secure and fair key. However, Liu et al. [7] pointed out that Shi et al.'s protocol cannot achieve fairness property by the participant attack. In addition, they proposed an MQKA protocol based on single photons. Subsequently, Sun et al. [17] complained about the efficiency of Liu et al.'s protocol. Instead, they proposed an MQKA protocol to improve the efficiency of Liu et al.'s protocol. However, Huang et al. [6] pointed out that Sun et al.'s MQKA protocol cannot avoid the participant attack. In 2015, Sun et al. proposed an MQKA based on an entangled Six-qubit state [20]. But, according to Liu et al.'s research [8], Sun et al.'s protocol cannot avoid the collusive attack which also implies that Sun et al.'s protocol cannot achieve fairness property. In 2016, an MQKA based on quantum secret direct communication was proposed by Zeng et al. [28]. In addition to these, several MQKA protocols [18, 19] have been proposed.

Recently, Xu et al. [23] proposed an MQKA protocol based on GHZ states. They claimed that the proposed protocol allows the involved participants to share a fair and secure final key. However, this study will point out that Xu et al.'s protocol cannot achieve fairness property by the participant attack. That is, the last participant can manipulate the final key without being detected by others which is not allowed in the quantum key agreement. Moreover, the paper [27] has already shown that Xu et al.'s protocol cannot also avoid the public discussion attack. To avoid these two flaws, an improved protocol is proposed. According to the security analysis and the fairness analysis, the modification can ensure the involved participants to establish a secure and fair key.

The rest of this paper is organized as follows. Section 2 provides a brief review of Xu et al.'s protocol. Section 3 analyzes Xu et al.'s protocol and shows that their protocol cannot achieve the fairness property Section 4 introduces the improved protocol and discusses the security, the fairness and the cost of it. At last, a brief conclusion is given in Section 5.

2 Brief Review of Xu et al.'s Protocol [23]

In this section, we briefly review Xu et al.'s MQKA protocol, where several participants $A_1, A_2, \cdots, A_N$ use GHZ states $|\Psi_N\rangle = |\Psi\rangle_{q_1q_2\ldots q_N} = \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle_{q_1q_2\ldots q_N} + |11\ldots1\rangle_{q_1q_2\ldots q_N}\right)$ to establish a shared key The protocol is described as follows.

Step 1 A_1 generates m GHZ states $|\Psi_N\rangle$ and sends all the ith particles to the ith participant.

Step 2 A_2 checks whether there exists any eavesdropper or not by choosing a part positions of q_2 and sends the information of the selected positions to the other participants. The particles in these positions are used as decoy photons. For each decoy photon A_2 randomly uses either $X\{|+\rangle, |-\rangle\}$ basis or $Z\{|0\rangle, |1\rangle\}$ basis to measure it and informs the other participants to measure the decoy photons in the same basis. Subsequently, the other participants $\{A_1, A_3, A_4, \ldots, A_N\}$ send the measurement results to A_2. Upon receiving all the measurement results, A_2 checks whether all these measurement results are correct or not [23]. If the error rate exceeds a predetermined value, they abort this protocol. Otherwise, they continue the next step.

Step 3 Similar to the **Step 2**, each participant does the same eavesdropping checking one by one. If all participants finish the checking positively, they continue the next step. Otherwise, they abort this protocol.

Step 4 Each participant uses $Z\{|0\rangle, |1\rangle\}$ basis to measure the remaining particles and gets the measurement results. The measurement results are the final shared secret key K.

It appears that the final shared key is determined by the quantum uncertainty principle, i.e. none of the participants can manipulate the shared secret key. However, the next section will show that the last involved participant has the ability to manipulate the final shared key without being detected.

3 Problem with Xu et al.'s Protocol

In this section, we show that Xu et al.'s protocol cannot ensure the involved participants to share a fair and secure key by introducing two loopholes. The first loophole (the participant attack) is that the last participant can measure all the remaining particles at the beginning of his/her eavesdropping checking process and choose the preferred values to be the final key which is not allowed in QKA. The other loophole is that the paper [27] pointed out that Xu et al.'s protocol cannot avoid the public discussion attack where each of the involved participants can manipulate the final shared key by announcing a fake eavesdropping detecting result. The details of participant attack and public discussion attack in Xu et al.'s protocol are respectively described in Sections 3.1 and 3.2.

3.1 Participant Attack

Assume that the last participant, A_N, is a malicious participant who intends to manipulate the final shared key. In **Step 3**, to perform the attack, A_N uses $Z\{|0\rangle, |1\rangle\}$ basis to measure enough of the remained particles before he/she selects the positions for decoy photons. For simplicity, assume here that he/she measures all the remained particles with Z basis. Upon obtaining the measurement results, A_N intentionally divides the remaining particles into two sequences K' and C. More precisely, A_N chooses those positions of his/her preference to be the final shared key K', and sets the others to be C as the decoy photons which can be measured either in X basis or in Z basis. After the eavesdropping detection, all participants will use Z basis to measure the remaining particles to obtain the final shared key K' in **Step 4**.

It is obvious that A_N is able to choose preferred values as final shared key by using the above strategy. If we assume the final shared key is n bits and the number of remaining decoy photons which were measured by Z-basis is m, then according to the Combinatorics

[15], there are $C_{n+m}^{n} = C\,(n+m, n) = \frac{(n+m)!}{n!}$ alternatives to be chosen by A_N as the final shared key. Obviously, the probability of having different combinations is $1-2\times\frac{1}{2^{n+m}}$ which is closed to 1 if the number $n+m$ is large enough. Hence, A_N is able to choose a preferred one from the different combinations as the final shared key without being detected by the others. In this way, the final shared key of the MQKA could be completely decided by A_N.

As an example, we use a 4-bit key generation process to explain this attack. (see also Fig. 1). Here, eight particles are supposed to remain for A_N after the other participants $\{A_1, A_2, \ldots, A_{N-1}\}$ finish performing the eavesdropping detection processes in Step 2 and Step 3. Subsequently, A_N measures all the remaining particles $\{q_{N1}, q_{N2}, \ldots, q_{N8}\}$ in Z basis. If A_N's measurement results is 10110001 and according to the combinations of the measurement results {0000, 0001, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111} he/she prefers 0000 to be the final shared secret key K, then he/she classifies $\{q_{N2}, q_{N5}, q_{N6}, q_{N7}\}$ as K' and sets $\{q_{N1}, q_{N3}, q_{N4}, q_{N8}\}$ as C. After the eavesdropping detection, all participants will remove the decoy photons and subsequently use Z basis to measure the remaining particles $\{q_{i2}, q_{i5}, q_{i6}, q_{i7}\}$ to obtain the final shared key $K = K' = 0000$ which is a key determined by A_N.

3.2 Public Discussion Attack [27]

In Xu et al.'s protocol, during the public discussion process, if a malicious participant does not satisfy with the negotiated shared secret key to be the final shared key, he/she can deliberately abort the protocol and then impute the error to an eavesdropping incident without being detected by the other participants. For example, after the last participant A_N announces the positions of decoy photons during the public discussion process, each participant can remove the decoy photons and obtain the final shared key by measuring the

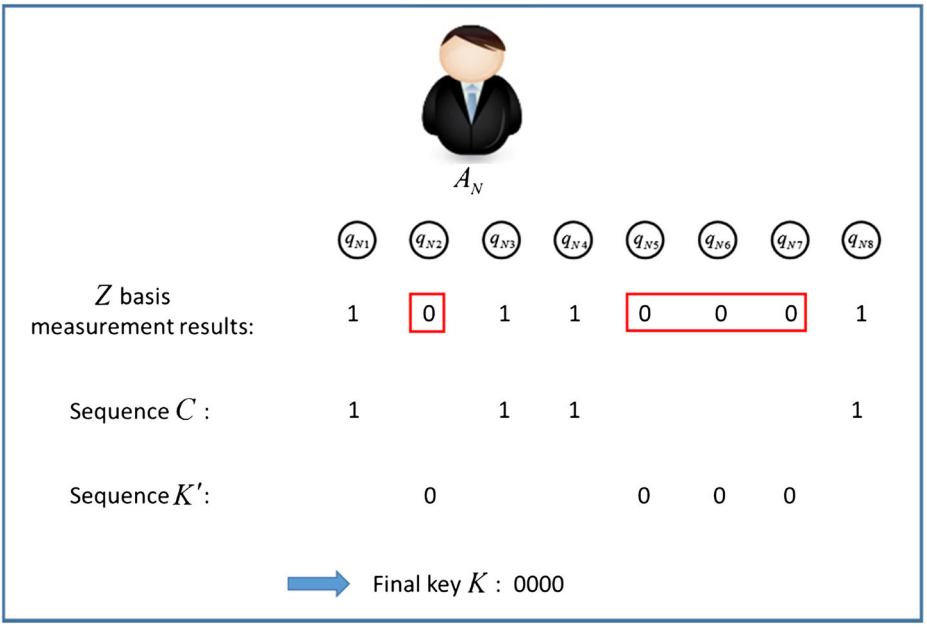

Fig. 1 Key manipulation by A_N

remaining particles with Z basis. At this moment, if any participant do not satisfy with the derived final shared key, he/she can deliberately announce a fake measurement result to fail the eavesdropping detection process. That is, this participant can let the other participants think that there is an eavesdropping. Hence, the protocol will be aborted and a new protocol will be started again. After several rounds, this participant could obtain a preferred final shared key. Obviously, this is against the fairness property. Though [27] pointed out this problem, they did not propose a corresponding modification to improve Xu et al.'s protocol.

4 Improvement on Xu et al.'s Protocol

This section first proposes an improvement to avoid the problems that we mentioned before, and then gives the security and fairness analyses.

4.1 Improved Protocol

To improve Xu et al.'s protocol, a modified version is described in detail as follows.

Step 1* A_1 prepares m GHZ states $|\Psi_N\rangle$ to form a quantum sequence S, i.e. $S = \left\{|\Psi_N\rangle_{q_1q_2\ldots q_N}, |\Psi_N\rangle_{q_1q_2\ldots q_N}, \cdots, |\Psi_N\rangle_{q_1q_2\ldots q_N}\right\}$. Subsequently, A_1 generates a random binary number sequence R_{H1} and performs $H_y = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + i|1\rangle\langle 0| - i|1\rangle\langle 1|)$ on S according to R_{H1} to obtain S_1. (For the ith particle, if the ith value of R_{H1} is 1, A_1 performs H_y on it. Otherwise, A_1 performs $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ on it.) Then A_1 sends S_1 to A_2. Upon receiving S_1, A_2 checks whether there is a Torjan horse attack [2, 4, 26] or not during the transmission. If there is a Torjan horse attack in the transmission, he/she aborts this protocol. Otherwise, similar to A_1, A_2 generates a random binary number sequence R_{H2} and performs H_y on S_1 according to R_{H2} to obtain S_2. Then sends it to A_3, so on and so forth. Again, after the Torjan horse checking, the ith participant A_i ($i \in \{3, 4, 5, \ldots, N-1\}$) generates R_{Hi} and performs H_y on S_{i-1} according to R_{Hi} to obtain S_i. Then A_i sends it to A_{i+1}. Subsequently, A_N performs H_y on the S_{N-1} according to R_{HN} to obtain $S_N = \left\{|\Psi_N\rangle_{q_1^N q_2^N \ldots q_N^N}, |\Psi_N\rangle_{q_1^N q_2^N \ldots q_N^N}, \cdots, |\Psi_N\rangle_{q_1^N q_2^N \ldots q_N^N}\right\}$ and sends all the q_i^N ($i \in \{1, 2, 3, \ldots, N-1\}$) to the ith participant (A_N sends all the ith particles of $|\Psi_N\rangle$ to the ith participant.).

Step 2* A_1 randomly chooses a subset out of S_N to be the decoy photon set for eavesdropping detection. Subsequently, he/she requests A_i ($i \in \{2, 3, 4, \ldots, N\}$) to announce the corresponding values of R_{Hi} which were performed on the decoy photons of A_1's choice. Notice that A_1 also has to announce the corresponding values of R_{H1} in the decoy photon set. After each participant gets the values of the other participants' R_H of the decoy photon set, they recover the original state of the decoy photons. Subsequently, for each decoy photon, A_1 randomly uses either X basis or Z basis to measure it and asks the others to measure the decoy photons in the same basis. Then, the other participants $\{A_2, A_3, A_4, \ldots, A_N\}$ send the measurement results to A_1 to check whether all participants' $\left\{A_1's, A_2's, \ldots, A_N's\right\}$ measurement results are satisfied or not [23]. If the error rate exceeds a predetermined value, they abort this protocol. Otherwise, they continue the next step.

Step 3* Similar to **Step 2***, the other participants do the same eavesdropping detection one by one. If the established particles are correct, they continue the next step. Otherwise, they abort this protocol.

Step 4* After all participants finish the eavesdropping detections, the ith ($i \in \{1, 2, 3, \ldots, N\}$) participant announces the remaining values of R_{Hi}. Subsequently, each participant recovers the remaining particles to the initial state $|\Psi_N\rangle$ and uses Z basis to measure them to get the final shared secret key K.

4.2 Security Analysis and Fairness Analysis

In this section, we analyze several well-known attacks (Measure-resend attack, Intercept-replace attack, Entangle-measure attack) to show that the proposed improvement can avoid the outside attacks. In addition, a fairness analysis is given to prove that the proposed improvement can achieve the fairness property.

4.2.1 Measure-Resend Attack Analysis

Suppose that Eve uses Z basis or X basis to measure the particles during the photon transmission and uses corresponding single photons instead of the original ones in Step 1* to try to obtain any useful information of the final shared key. It is obvious that this attack can be detected by the participants in Step 2* and Step 3*. That is, the involved participants will find that their particles have no correlations with the other participants' particles. For example, assume here that the initial state is $|\Psi_N\rangle = |\Psi\rangle_{q_1q_2\ldots q_N} = \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle_{q_1q_2\ldots q_N} + |11\ldots1\rangle_{q_1q_2\ldots q_N}\right)$ and none of the involved participants performs H_y on them. Subsequently, Eve uses Z basis to measure them and the measurement results are $|0\rangle_{q_1}|0\rangle_{q_2}\ldots|0\rangle_{q_N}$ or $|1\rangle_{q_1}|1\rangle_{q_2}\ldots|1\rangle_{q_N}$. According to these measurement results, Eve uses N single photons $|0\rangle^{\otimes N}$ or $|1\rangle^{\otimes N}$ instead of the original ones and sends them back to the participants. In Step 2* and Step 3*, for each pair of the decoy photons, the participants have a probability of $\frac{1}{2}$ to measure them with X basis. If the participants use X basis to detect the eavesdropping, for each qubit, there will be a probability of $\frac{1}{2}$ to get an incorrect measurement result. Overall, the probability of that Eve can avoid this detection is $\left(\frac{1}{2}\right)^l\left(\frac{1}{2}\right)^N$ (l is the number of decoy photon pairs). Hence, this attack can be detected with a probability of $1-\left(\frac{1}{2}\right)^l\left(\frac{1}{2}\right)^N \approx 1$ (if the number l is large enough). According to this, we can consider that this attack is unworkable.

4.2.2 Intercept-Replace Attack Analysis

Suppose that Eve intercepts the particles and uses several particles generated by herself instead of the original ones in Step 1* to try to obtain any useful information of the final shared key. Similar to the **Measure-resend attack analysis**, this attack can be detected by the involved participants in the eavesdropping detection. That is, because of that Eve cannot know whether the participants perform H_y on the particles or not, she cannot generate same states with the original ones. Hence, after all the participants recover the decoy

photons in Step 2* and Step 3*, the eavesdropping can be detected with a probability of $1-\left(\frac{1}{2}\right)^{l}\left(\frac{1}{2}\right)^{N}\approx 1$ (if the number l is large enough). According to this, we can think that the proposed improvement can avoid the Intercept-replace attack.

4.2.3 Entangle-Measure Attack Analysis

Suppose that Eve intercepts the particles and uses q_1 to be the control bit and uses a particle $|0\rangle$ to be the target bit T to perform the *C-NOT* operation ($C\text{-}NOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$). Subsequently, Eve can obtain a new $N+1$ bits GHZ state and send the particles $q_1, q_2, \ldots, q_N$ back to the participants. Obviously, the involved participants can detect this attack in the eavesdropping detection in Step 2* and Step 3*. For example, assume here that there are just two participants involved in the protocol, the original state will be $|\Psi_2\rangle = |\Psi\rangle_{q_1q_2} = \frac{1}{\sqrt{2}}\left(|00\rangle_{q_1q_2} + |11\rangle_{q_1q_2}\right)$. If none of the participants performs H_y on them, after Eve performs the *C-NOT* operations, T and $|\Psi_2\rangle$ will be transformed into $|\Psi_3\rangle = |\Psi\rangle_{Tq_1q_2} = \frac{1}{\sqrt{2}}\left(|000\rangle_{Tq_1q_2} + |111\rangle_{Tq_1q_2}\right)$. In the eavesdropping detections, the involved participants can use X basis to detect it. That is, with X basis, the state $|\Psi_3\rangle$ is $|\Psi_3\rangle = |\Psi\rangle_{Tq_1q_2} = \frac{1}{2}\left[|+\rangle_T\left(|{+}{+}\rangle + |{-}{-}\rangle\right)_{q_1q_2} + |-\rangle_T\left(|{+}{-}\rangle + |{-}{+}\rangle\right)_{q_1q_2}\right]$. For each pair of the decoy photons ($\{q_1, q_2\}$) there will be a probability of $\frac{1}{2}$ to get an incorrect measurement result. Obviously, this attack can be detected with a probability of $1-\left(\frac{1}{2}\right)^{l}\approx 1$ (if the number l is large enough). Hence, we can consider that the Entangle-measure attack is unworkable.

4.2.4 Fairness Analysis

In **Step 1***, after each participant performs H_y on each particle according to R_{Hi}, none of the participants can get the correct measurement results of the particles without knowing the others' R_{Hi}s. Because of that H_y operation can transform the p, article into another state ($H_y\left(|0\rangle\right) = |+\rangle_y$, $H_y\left(|1\rangle\right) = |-\rangle_y$, $H_y\left(|+\rangle\right) = |0\rangle_y$, $H_y\left(|-\rangle\right) = |1\rangle_y$). Hence, if the particle $|0\rangle$ has been transformed by H_y and the malicious participant uses Z basis to measure it, he/she will have a probability of $\frac{1}{2}$ to get $|0\rangle$ and a probability of $\frac{1}{2}$ to get $|1\rangle$. It is obvious that the malicious participant cannot make sure whether the measurement result is correct or not. In **Step 3***, though A_N can get all the other participants' R_{Hi} s($1 \le i \le N-1$) performed on the decoy-photon set, he/she cannot obtain the R_{Hi} s performed on the remaining particles which used for sharing the final key. Consequently, A_N cannot manipulate the final shared key with the method mentioned in Section 3.1. Hence, the participant attack can be avoided in the proposed improvement. Similarly, during the eavesdropping detection processes of the proposed improvement, none of the involved participants can obtain the final shared key. Hence the public discussion attack can be avoided too.

4.3 Comparison

Suppose that $\eta = \frac{c}{q}$ is the qubit efficiency of a quantum protocol [24–26], where c denotes the total number of shared classical bits and q denotes the total number of qubits generated in the protocols. Thus, the qubit efficiency of the proposed improvement is

Table 1 Comparison of QKA protocols with several multiparty participants

QKA protocol	Quantum resource	Fair	Qubit efficiency
Liu et al.'s protocol [7]	Single photons	No	$\frac{1}{2N(N-1)}$
Sun et al.'s protocol [17]	Single photons	No	$\frac{1}{N^2}$
Shi and Zhong's protocol [16]	Bell states	No	$\frac{1}{3N(N-1)}$
Xu et al.'s protocol [23]	GHZ states	No	$\frac{1}{2^{N-1}}$
Sun et al.'s protocol [21]	Six-qubit states	No	$\frac{1}{N^2}$
Proposed improvement	GHZ states	Yes	$\frac{1}{2^{N-1}N}$

$\eta = \frac{1}{2^{N-1}N}$, where $c = 1, q = 2^{N-1}N$, N denotes the total number of the involved participants. The comparison of several QKA protocols with multiparty participants is shown in Table 1. Though the proposed improvement does not have satisfactory qubit efficiency, the improvement can help each participant to share a fair and secure key.

5 Conclusion

This paper points out that Xu et al.'s multi-party quantum key agreement protocol suffers from the participant attack, which is against the fairness property of a QKA. To avoid this flaw and the public discussion attack [27], a modification is proposed in this paper. In addition, the security analysis and the fairness analysis shows that the modification can achieve both the security property and the fairness property. Though the modification can ensure the participants to share a secure and fair key, the efficiency of the modified protocol is not satisfactory. It would be interesting to design a secure and fair multi-party quantum key agreement protocol with better efficiency.

Acknowledgement We would like to thank the Ministry of Science and Technology of the Republic of China, Taiwan for partially supporting this research in finance under the Contract No. MOST 105-2221-E-006 -162 -MY2.

References

1. Bennett, H.Ch., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984), pp. 175–179 (1984)
2. Cai, Q.-Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
3. Chong, S.-K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
4. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)
5. Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P.: Quantum key distribution using gaussian-modulated coherent states. Nature **421**, 238–241 (2003)
6. 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)
7. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
8. Liu, B., Xiao, D., Jia, H.-Y., Liu, R.-Z.: Collusive attacks to "circle-type" multi-party quantum key agreement protocols. Quantum Inf. Process. **15**, 2113–2124 (2016)

9. Liu, S.-L., Zheng, D., Cheng, K.-F.: Analysis of information leakage in quantum key agreement. J. Shanghai Jiaotong Univ. (Science) **11**, 219–223 (2006)
10. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
11. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
12. Long, G.-L., Liu, X.-S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
13. Ouellette, J.: Quantum key distribution. Ind. Phys. **10**, 22–25 (2004)
14. Renner, R.: Security of quantum key distribution. Int. J Quantum Inf. **6**, 1–127 (2008)
15. Sachkov, V.N.: Combinatorial Methods in Discrete Mathematics. Cambridge University Press, Cambridge (1996)
16. Shi, R.-H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
17. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Improvements on "Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 3411–3420 (2013)
18. Sun, Z., Huang, J., Wang, P.: Efficient multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf. Process. **15**, 2101–2111 (2016)
19. Sun, Z., Sun, X., Wang, P.: Multiparty quantum key agreement protocol secure against collusion attacks. arXiv:1604.01112 (2016)
20. Sun, Z., Zhang, C., Wang, P., Yu, J., Zhang, Y., Long, D.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**, 1920–1929 (2016)
21. Sun, Z., Zhang, C., Wang, P., Yu, J., Zhang, Y., Long, D.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55.3**, 1920–1929 (2016)
22. Xu, G., Chen, X.-B., Dou, Z., Yang, Y.-X., Li, Z.: A novel protocol for multiparty quantum key management. Quantum Inf. Process. **14.8**, 2959–2980 (2015)
23. 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)
24. Yang, C.-W., Hwang, T.: Improved QSDC protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**, 3941–3950 (2012)
25. Yang, C.-W., Hwang, T.: Quantum dialogue protocols immune to collective noise. Quantum Inf. Process. **12**, 2131–2142 (2013)
26. Yang, C.-W., Hwang, T., Luo, Y.-P.: Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Inf. Process. **12**, 109–117 (2013)
27. Yu, K.-F., Yang, C.-W., Hwang, T., Li, C.-M., Gu, J.: Design of quantum key agreement protocols with fairness property. arXiv:1510.02353 (2015)
28. Zeng, G.-J., Chen, K.-H., Chang, Z.-H., Yang, Y.-S., Chou, Y.-H.: Multiparty Quantum Key Agreement based on Quantum Secret Direct Communication with GHZ states. arXiv:1602.00832 (2016)
29. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149–1150 (2004)