International Journal of Theoretical Physics (2021) 60:293–303
https://doi.org/10.1007/s10773-020-04692-x

Semi-Honest Three-Party Mutual Authentication Quantum Key Agreement Protocol Based on GHZ-Like State

Hongfeng Zhu[1] · Chaonan Wang[1] · Zexi Li[1]

Received: 7 October 2020 / Accepted: 14 December 2020 / Published online: 14 January 2021

Abstract

Quantum key agreement (QKA) is an important branch of quantum cryptography. In this paper, we propose a mutual authenticated semi-honest key agreement scheme with Greenberger-Home-Zeilinger-like (GHZ-like) state. A semi-honest third-party Trent can help Alice and Bob to achieve mutual authentication and key agreement without getting any information about the session key between them. Firstly, Alice and Bob have shared necessary information with Trent respectively in a secure way, and keep each other confidential. Trent prepares the three-particle GHZ-like states and shares them with Alice and Bob. Secondly, Trent uses hash security function to get a set with equal subscripts, and then divides into authentication set and negotiation set. The authentication set is used to realize the security authentication of three-party identities, while the negotiation set is used for negotiating the session key. Finally, on the premise of passing the three-party authentication, Alice and Bob carry out the GHZ-like states encryption communication according to the negotiation subset provided by the third party. Through security analysis and efficiency analysis, our proposed protocol can effectively resist external eavesdropping and internal eavesdropping, and have high communication efficiency.

Keywords Quantum key agreement · Mutual authentication · GHZ-like state · Semi-honest party

✉ Hongfeng Zhu
zhuhongfeng1978@163.com

Chaonan Wang
915521870@qq.com

Zexi Li
895197771@qq.com

[1] Software College, Shenyang Normal University, No.253, HuangHe Bei Street, HuangGu District, Shenyang P.C 110034, China

1 Introduction

Different from traditional encryption, quantum cryptography is based on Heisenberg's uncertainty principle and quantum no-cloning theorem to ensure the security of quantum communication, for example, Quantum states are used as Truly Random Numbers carrier to realize the secure transmission of information. In recent years, with the continuous expansion of the application field of quantum cryptography, quantum key agreement (QKA) has become a research focus and an important part of quantum cryptography [1–11].

In 2004, Zhou et al. [1] propoesd the first QKA protocol, in which the communication parties jointly determine the shared key. However, Tsai and Hwang [2] pointed out that Zhou et al.'s protocol can fully determine the share key by one-party. In 2006, Liu and Zheng [3] proposed that there may be man-in-the-middle attack in QKA protocol, which may lead to information leakage. In 2010, Chong et al. [4] put forward a new QKA protocol based on BB84 to establish and share the key between the communication parties, and used the technique of delayed measurement to provide security. In 2013, Liu et al. [5] proposed the first secure multi-party QKA protocol for internal attack and external attack. Then Shi and Zhong [6] pointed out that Liu et al.'s protocol exsited dishonest participants. On this basis, a two-party or multi-party QKA protocol which can achieve security communication without the help of a third party was proposed. However, the efficiency of the above-mentioned protocols were not satisfactory. Then in 2016, Sun et al. [7] proposed a secure multi-party QKA protocol without entanglement states and can reduce the complexity of the computation and improve the efficiency of the protocol. One year later, Mohajer and Eslami [8] pointed out that Sun et al.'s protocol cannot provide security when participants are not authenticated, and made further improvements for this attack. Only a few multi-party QKA can achieve real security and effiency. So Huang et al. [9] proposed an multi-party QKA with single photons, which had high quantum bit efficiency and measurement efficiency. In 2019, Huang and Yang [10] designed a secure QKA and introduced a trusted third party to detect dishonest participants to resist participant attacks. In 2020, Tang et al. [11] proposed a circle-type multiparty QKA, which is based on two non-orthogonal bases single particles.

Most of the above researches on QKA protocols mainly focus on two-party or multi-party, without mentioning entanglement resources. In practical applications, the QKA protocol combined with entangled resources has more practical value, such as Bell state, GHZ state and cluster state [12–23].

As early as 2004, Hsued and Chen [12] have proposed a QKA protocol with maximum entanglement states. In 2011, Chong et al. [13] pointed out that there were two security flaws in the QKA protocol proposed by Hsued and Chen, and proposed a possible solution. In 2014, Shukla et al. [14] proposed two QKA protocols based on Bell state and Bell measurement, which had high security. Then Zhu and Hu [15] pointed out that Shukla et al.'s protocols were not safe for any participant in the protocol can directly obtain other two participants' secret keys. Compared with other exsited two-party QKA protocols, Shen et al. [16] proposed two-party QKA scheme based on cluster state, which can effectively resist participant attack and external attack. In the same year, Xu and Wen [17] put forward a new three-party QKA protocol based on GHZ states, and everyone need to perform single-particle measurements only. However, Gu et al. [18] pointed out that Xu et al.'s protocol cannot provide relative fairness between participants and proposed an improved QKA protocol. In 2015, He and Ma [19] propoesd a two-party and a three-party QKA protocols based on unitary operations and Cluster state, which can effectively resist participant attack and external attack, and had high qubit efficiency. In 2016, He and Ma [20] propoesd a two-party QKA protocols based on GHZ states and the double CNOT operation, which realized the fair establishment of shared key, and can resist common attacks without information leakage. One year later, He and Ma [21] proposed two robust QKA protocols based on logical GHZ states and Bell states, with the help of decoy state technology can resist external attacks. In 2020, Zhou et al. [22] propoesd a semi-quantum key agreement protocol based on four-qubit cluster state, which enables more parties to participate in and reduces the quantum channel. Later, Tang and Shi [23] put forward a two-party and a three-party controlled QKA based on GHZ states and Bell measurements.

Combined with entanglement resources, QKA protocols have been applied well. In this paper, based on the QKA protocol, we introduce a third party and implement secure communication with GHZ-like state. The third party Trent provides entangled resources for authentication and key agreement. On the one hand, Trent can achieve pairwise authentication with both sides of the communication, thus providing higher security. On the other hand, according to the encryption rules, the subset provided by Trent can be used for the key agreement of communicators.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. In Section 3, we describe the concrete steps of quantum dialogue. Next, a security analysis is described in Section 4. Then, an efficiency analysis is given in section 5. This paper is finally concluded in Section 6.

2 Preliminaries

2.1 GHZ-Like States

The GHZ-like state is prepared with GHZ state and Hadamard operation. To begin with, the three-particle GHZ state is widely used in quantum communication, it can be expressed as:

$$|GHZ\rangle_{123} = \frac{\sqrt{2}}{2}(|000\rangle + |111\rangle)_{123} \tag{1}$$

Secondly, the Hadamard operation can be expressed as:

$$H = \frac{\sqrt{2}}{2}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|] \tag{2}$$

$$|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) \tag{3}$$

And the main calculation formulas can be expressed as:

$$|{+}{+}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle), \quad |{-}{-}\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \tag{4}$$

Thirdly, the GHZ-like state can be expressed as:

$$\begin{aligned} |GHZ{-}like\rangle_{123} = H_1H_2H_3|GHZ\rangle_{123} &= \frac{\sqrt{2}}{2}(|{+}{+}{+}\rangle + |{-}{-}{-}\rangle)_{123} \\ &= \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)_{123} \end{aligned} \tag{5}$$

The QKA protocol we designed is based on GHZ-like state, and the GHZ-like state is described in Eq. (5). In the ideal situations, all the measurement results of the three parties should meet Table 1. "0" represents the measurement result $\{|0\rangle, |+\rangle\}$ and "1" represents the measurement result $\{|1\rangle, |-\rangle\}$..

In this study, there are three participants in the communication, Alice, Bob and Trent. Alice and Bob play the roles of legitimate participants in the communication, while Trent is a semi-honest third party. K_{AT} and K_{BT}represent the shared keys of Alice, Bob with Trent, respectively. Trent performs secure hash function H to obtain a set C. C can also provide authentication set and negotiation set to determine the measurement base. All three parties keep their secrets to each other. The whole communication consists of three stages, including initialization and measurement stage, authentication stage and key agreement stage. The following text details the different stages of communication Figs. 1 and 2.

2.2 Notations

The concrete notations used here after are shown in Table 2.

2.3 Semi-Honest Party

Semi-honest parties [24] follow the protocol steps, but they try to extract information about other entities' input or output. For different system and goals, semi-honest has the different meanings. For example, in Fig. 3, Alice and Bob want to authenticate each other and get session key by the helping Trent, because Trent has their authenticated information. In this case, Trent is a semi-honest party, because he follows the protocol steps faithfully, and they also want get the session key between Alice and Bob.

3 The Proposed Protocol

3.1 Initialization and Measurement Stage

StepI1 Alice and Bob have shared K_{AT} and K_{BT} with Trent. Trent selects a large random number r and computes $\overline{K_{AT}} = H(K_{AT} \| r)$ and $\overline{K_{BT}} = H(K_{BT} \| r)$, which are used to determine authentication set and negotiation set. Trent prepares D groups of GHZ-like state, it can be denoted as: $P_1(1), P_1(2), P_1(3); P_2(1), P_2(2), P_2(3); \ldots; P_D(1), P_D(2), P_D(3)$. Trent is responsible for collecting each group of GHZ-like state to form three groups of

Table 1 Measuring results of three parties

Measuring base	Trent	Alice	Bob
Z-base	1	0	1
		1	0
	0	1	1
		0	0
X-base	1	1	1
	0	0	0

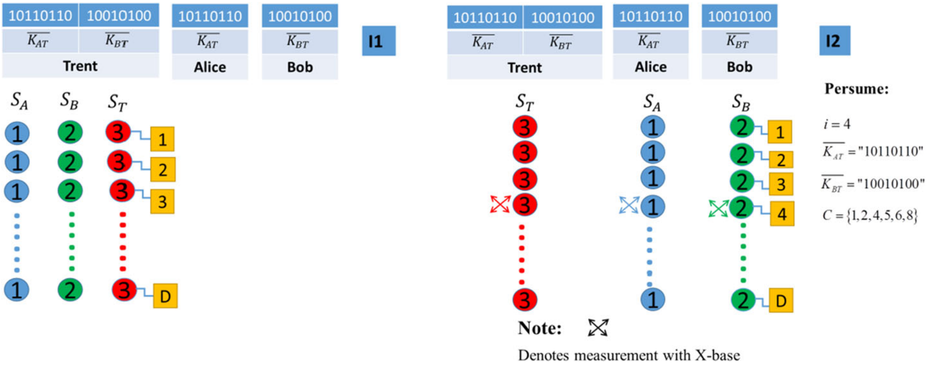

Fig. 1 Process of initialization stage

particle sequences $S_A,\ S_B,\ S_T$. Trent sends S_A and r to Alice, and sends S_B and r to Bob and keeps S_T by itself. $S_A,\ S_B,\ S_T$ can be expressed as:

$$\begin{aligned}
S_A &: [P_1(1), P_2(1), P_3(1), P_4(1), \ldots, P_D(1)] \\
S_B &: [P_1(2), P_2(2), P_3(2), P_4(2), \ldots, P_D(2)] \\
S_T &: [P_1(3), P_2(3), P_3(3), P_4(3), \ldots, P_D(3)]
\end{aligned}$$

StepI2 Alice and Bob execute $\overline{K_{AT}}$ and $\overline{K_{BT}}$ respectively. Both Alice and Bob keep confidential from each other. At this stage, Alice and Bob wait for the notification of Trent. Trent performs $\overline{K_{AT_i}} = \overline{K_{BT_i}}$ and gets a set C whose corresponding bits are equal. Trent randomly

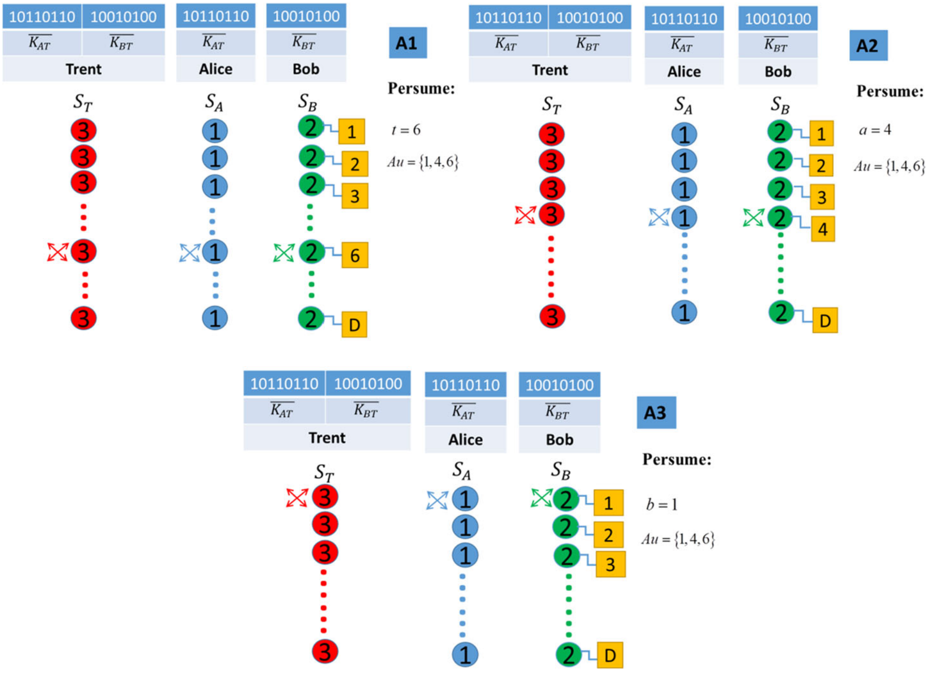

Fig. 2 Process of authentication stage

Table 2 Notations

Symbol	Definition
K_{AT}	Alice's communication identity ID
K_{AT}	Bob's communication identity ID
$\overline{K_{AT}}$	$\overline{K_{AT}} = H(K_{AT} \| r)$
$\overline{K_{BT}}$	$\overline{K_{BT}} = H(K_{BT} \| r)$
K_{AB}	The final session key between Alice and Bob
H	secure hash function
r	a random number
$\|$	concatenation operation
C	a set of equal subscripts operated on by the H
Au	an authentication set corresponding to bit 1
Ne	a negotiation set corresponding to bit 0
$Sub(i)$	a subset of set C

chooses a subset $Sub(i)$ from C and measures the corresponding particle $P_i(3)$ in S_T. Later, Trent sends $Sub(i)$ to Alice and Bob. According to Table 3 (The Rule), Trent, Alice and Bob select Z-base for measurement when $\overline{K_{AT_i}} = \overline{K_{BT_i}} = 0$. Trent, Alice and Bob select X-base for measurement when $\overline{K_{AT_i}} = \overline{K_{BT_i}} = 1$. Alice combines $Sub(i)$ and $\overline{K_{AT}}$ to know which corresponding bit is equal to Bob. Then Alice measures the corresponding particle $P_i(1)$ in S_A, Bob measures the corresponding particle $P_i(2)$ in S_B. Under ideal conditions, measurement results of the three parties shall meet Table 1. For instance, Trent randomly chooses $Sub(4)$ from C and measures the corresponding particle $P_4(3)$ in S_T. Trent sends $Sub(4)$ to Alice and Bob, they measure $P_4(1)$ and $P_4(2)$ respectively. All the processes of initialization and measurement stage can be see in the Fig. 1.

3.2 Authentication Stage

In the Fig. 2, Trent finds out a subset which conform to $\overline{K_{AT_i}} = \overline{K_{BT_i}} = 1$ and named them set Au, we use X-base to measure the corresponding particles. Trent informs Alice and Bob about the orders of Au through classical channel.

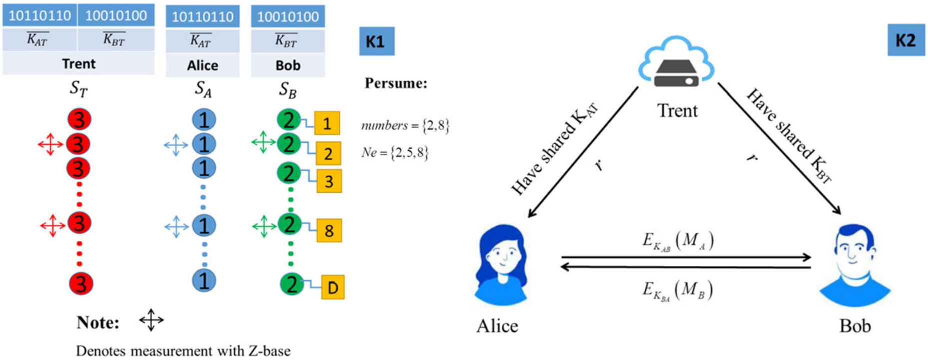

Fig. 3 Process of key agreement stage

Table 3 Measuring bases

	Trent, Alice, Bob
$\overline{K_{AT_i}} = \overline{K_{BT_i}} = 0$	Z-base
$\overline{K_{AT_i}} = \overline{K_{BT_i}} = 1$	X-base

Remark1: Inform the orders (subscripts) will not reveal the final measured values of the Au: For example, $\overline{K_{AT}} = 10110110; \overline{K_{BT}} = 10010100$, the $Au = \{1, 4, 6\}$, Trent informs Alice and Bob the sets $\{1, 4, 6\}$, and anyone (including Eve, based on the Kerckhoffs principle: anyone knows all the protocol's process except the secret keys) know the real values are $\{111\}$ and to measure these particles by X-base, but this is meaningless, because these entangled particles have been distributed to Alice and Bob, and only Alice and Bob can confirm the final values of the particles by measurement (see Table 1).

StepA1 We need Au to authenticate that Trent is honest. Trent randomly selects a number t from Au and measures the corresponding particle $P_t(3)$ in S_T. Trent informs Alice and Bob about t and measurement results. Alice and Bob measure the corresponding particle $P_t(1)$ and $P_t(2)$ in S_A and S_B. Then, they release measurement results through the classical channel. According to Table 3, the measurement results of the three parties should be consistent. Alice calculates the error rate from Trent and Bob's measurement results. Bob does the same thing. If the error rate is higher than a threshold, Trent might be an eavesdropper. Alice and Bob should announce stopping this communication.

StepA2 Alice can be authenticated through Au. Alice randomly selects a remaining number a from Au and measures the corresponding particle $P_a(1)$ in S_A. The following steps are the same as StepA1.

StepA3 After authenticating Alice and Trent, we need authenticate Bob. Bob randomly selects a remaining number b from Au and measures the corresponding particle $P_b(2)$ in S_B. Bob performs the same authentication operation just like Alice and Trent.

3.3 Key Agreement Stage

After the three parties have been authenticated each other, the communication enters the key agreement stage. Trent finds out a subset which conform to $\overline{K_{AT_i}} = \overline{K_{BT_i}} = 0$ and named them set Ne. According to $\overline{K_{AT_i}} = \overline{K_{BT_i}} = 1$ stipulated in the authentication stage, we use Z-base to measure corresponding particles.Trent informs Alice and Bob about Ne through classical channel.

Remark2: Inform the orders (subscripts) will not reveal the final measured values of the Ne which has the same explanation with Remark1.

StepK1 Trent randomly selects some numbers from Ne and measures the corresponding particles in S_T. Trent informs Alice and Bob about sequence numbers and measurement results. Alice and Bob measure the corresponding particles in S_A and S_B respectively.

StepK2 Based on the encryption rule E_Q, Alice and Bob encode their own particle sequences. The encryption rule E_Q is:

(1) When Trent's corresponding measurement reslut is 1, Alice negotiates with Bob. If Bob's corresponding measurement reslut is 1, Alice performs the unitary operation $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. If Bob's corresponding measurement result is 0, Alice performs the unitary operation $X = |0\rangle\langle 1| + |1\rangle\langle 0|$.

(2) When Trent's corresponding measurement result is 0, Alice negotiates with Bob. If Bob's corresponding measurement reslut is 1, Alice performs the constant operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. If Bob's corresponding measurement reslut is 0, Alice performs the constant operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$.

After encryption rule E_Q, Alice and Bob get corresponding particle sequences $S'_A$and S'_B respectively. And it is denoted as:

$$\begin{array}{l} K_{AB} = S'_A = [P_1(1), P_2(1), P_3(1), \ldots, P_K(1)] \\ K_{BA} = S'_B = [P_1(2), P_2(2), P_3(2), \ldots, P_K(2)] \end{array}$$

At this point, Trent gets nothing inofrmation about the session key K_{AB} between Alice and Bob, and the communication information between Alice and Bob can be encrypted by are K_{AB}/(K_{BA}), which can be expressed as Alice sends $E_{K_{AB}}(M_A)$ to Bob and Bob sends $E_{K_{BA}}(M_B)$ to Alice, see in the Fig. 3.

4 Security Analysis

4.1 Semi-Honest Trent Attack

In the proposed semi-honest three-party authentication quantum key agreement protocol, the third-party Trent participates in the communication as the authenticator and resource provider, and Trent is responsible for preparing and allocating entangled particles to Alice and Bob. Compared with other QKA protocols, this protocol provides effective mutual authentication among the three-party by using entanglement resources.

Supposed that Trent is an internal eavesdropper (or called semi-honest party) who has access to some entangled resources from the beginning, and he can follow the protocol steps faithfully, but he tries to extract session key K_{AB} between Alice and Bob in our instance.

Then in the initialization stage, Trent prepared three-particle GHZ-like state, S_A, S_B, S_T, if Trent wants to cheat before allocating entangled particles and measure S_A and S_B, then Alice and Bob will analyze this behavior in later error rate calculation to determine Trent's dishonesty. If Trent allocates entangled resources according to the normal process, it can successfully distribute the authentication subset Au to Alice and Bob, although the three parties choose the same base to measure in the authentication stage. In the authentication, Trent must follow the protocol steps faithfully or Alice/Bob will detect it immediately. In the authentication, based on $\overline{K_{AT_i}} = \overline{K_{BT_i}} = 1$, all the three-party will use X-base to measure their own local particles and authenticate each other. Although Trent knows all the values of Alice and Bob based on Table 1, this is just authenticated phase which is not affecting the values of negotiation phase between Alice and Bob.

Next, if Trent, Alice and Bob achieve mutual authentication, they can provide negotiation subset Ne successfully in the key agreement stage. Trent chooses Z-base to measure, according to Table 1 and encryption rule E_Q, when Trent's corresponding particle is 1 or 0, it cannot judge the measurement result of Alice and Bob. In other words, there is no cheating before Trent distributes entangled resources S_A and S_B, the probability of not being found is $\frac{1}{2}$ for each qubit for Trent. In addition, the probability of Trent's attack being found is $1-\left(\frac{1}{2}\right)^L$. L denotes the length of K_{AB}. We can find that with the increase of K_{AB}, and the probability of Trent's attack being found tends to be 1. Therefore, we can effectively resist internal attack (semi-honest Trent attack).

4.2 External Attack

In external eavesdropping, eavesdropper Eve often uses eavesdropping-resending, measuring-resending and entanglement–measurement to obtain information [25].

Eve is supposed to obtain the initial state of entangled particles to launch eavesdropping-resending, measuring-resending attacks. If Eve measures the obtained particles, randomly selects Z-base or X-base for three-party authentication. According to the quantum collapse principle, this will bring high error rate. If they can enter the negotiation stage successfully, Alice and Bob encrypt the information to be sent by using the encryption rule E_Q after negotiation. Since the entangled particle state of Alice and Bob cannot be calculated, the communication information between Alice and Bob cannot be stolen.

While in entanglement–measurement attacks, Eve entangles the intercepted particles with the prepared particles, and uses the entangled particles to obtain useful information. However, according to Heisenberg's uncertainty principle and quantum no-cloning theorem, Eve cannot directly obtain useful information, because Alice and Bob use E_Q encryption when sending information, which affects the entanglement between intercepted particles and prepared particles.

5 Efficiency Analysis

According to references [26], the efficiency of quantum communication is measured by η:

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

In QKA protocols, c, q, b are numbers of bit of shared key generated by protocol, the used qubits, classical information used to decode, respectively. In our protocol, the initial length of each group of particles is D, we also need D bits of classical information to decode. Thus, $b = D$.. Compared with key agreement stage, the particles used in the authentication stage can be ignored. Besides, the length of q and c depends on the set C. Suppose the length of C is D, we take $\frac{1}{3}D$ bits for key sharing. Thus, $c=\frac{1}{3}D$. In order to maximize the encryption strength, the key consumed in the key agreement state can be approximately equal to the length of the shared key. In other words, $q\approx\frac{1}{3}D$. Then:

$$\eta=\frac{c}{q+b}=\frac{\frac{1}{3}D}{\frac{1}{3}D+D}=25\%$$

In the following part (Table 4), we will make a simple comparison between other QKA protocols and ours from the following aspects: η, third party, authentication and quantum state

Table 4 Comparison between other QKA protocols and ours

Protocols	η(%)	Semi-honest attribute	Quantum state used	Mutual Authentication
Ref. [14]	14.29	No third party	Bell state	No
Ref. [19]	26.67	No third party	Cluster state	No
Ref. [20]	36.36	No third party	GHZ state	No
Ref. [22]	2.08	No Semi-honest attribute	Cluster state	No
Ours	25	Yes	GHZ-like state	Yes

used. Compared with other QKA protocols, our efficiency is in the middle. We add a semi-honest third party and implement mutual authentication. Besides, negotiation phase and authentication phase must be close connection. If negotiation phase is independent of authentication phase, then Eve will may steal information only by attacking negotiation part, which will make the protocol unsecure.

6 Conclusion

In this paper, we proposed a semi-honest three-party AQKA protocol based on three-particle GHZ-like states to achieve mutual authentication, true random session key and a semi-honest Trent. In the whole protocol, Trent prepares entangled particles and performs hash security function to get the authentication set Au and negotiation set Ne. According to the Au, all the three-party realize mutual authenticate. After successful authentication, they enter the negotiation stage. Alice and Bob use the Ne to negotiate but Trent gets nothing about the session key between Alice and Bob. According to the encryption rule E_Q, Alice and Bob combined with their own particle sequences K_{AB} to encrypt information, they can achieve multiple communications. Compared with the existing QKA protocols, the efficiency of this protocol is feasible. In the future, we will explore N-qubit entangled states and combine classical cipher technologies to achieve diversified quantum schemes, such as quantum homomorphic encryption, blind quantum computation with quantum entangled states.

Acknowledgements This work was supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 2019-MS-286), and Basic Scientific Research Project of Liaoning Provincial Department of Education (Grant No. LJC202007).

References

1. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**(18), 1149–1150 (2004)
2. Tsai, C.W., Hwang, T.: On Quantum Key Agreement Protocol. Technical Report C-S-I-E, NCKU, Taiwan (2009)
3. Liu, S.L., Zheng, D., Chen, K.F.: Analysis of information leakage in quantum key agreement. J. Shanghai Jiaotong Univ. (Sci.). **E-11**(2), 219–223 (2006)
4. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
5. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
6. Shi, R.-H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)

7. Sun, Z., Huang, J., Wang, P.: Efficient multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf. Process. **15**(5), 2101–2111 (2016)
8. Mohajer, R., Eslami, Z.: Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf. Process. **16**(8), Article number: 197 (2017)
9. Huang, W., Su, Q., Liu, B., He, Y.-H., Fan, F., Xu, B.-J.: Efficient multiparty quantum key agreement with collective detection. Sci. Rep. **7**(1), (2017)
10. Huang, W.-C., Yang, Y.-K., Jiang, D., Gao, C.-H., Chen, L.-J.: Designing secure quantum key agreement protocols against dishonest participants Int. J. Theor. Phys. **58**(12), 4093–4104, (2019)
11. Tang, R.-H., Zhang, C., & Long, D.-Y.: An efficient circle-type multiparty quantum key agreement protocol with single particles. Int. J. Mod. Phys. B. (12), **2050199**, 1–19, (2020)
12. Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states. In: Proceed ings of the 14th Information Security Conference (ISC 2004), pp. 236–242. National Taiwan University of Science and Technology, Taipei, Taiwan, 10–11 Jun. (2004)
13. Chong, S.-K., Tsai, C.-W., Hwang, T.: Improvement on "quantum key agreement protocol with maximally entangled states". Int. J. Theor. Phys. **50**, 1793–1802 (2011)
14. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using bell states and bell measurement. Quantum Inf. Process. **13**(11), 2391–2405 (2014)
15. 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**(11), 4245–4254 (2015)
16. Shen, D.-S., Ma, W.-P., Wang, L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**(10), 2313–2324 (2014)
17. Xu, G.-B., Wen, Q.-Y., Gao, F., Qin, S.-J.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. (2014). https://doi.org/10.1007/s11128-014-0816-9
18. Gu, J., Hwang, T.: Improvement of "novel multiparty quantum key agreement protocol with GHZ states". Int. J. Theor. Phys. **56**, 3108–3116 (2017). https://doi.org/10.1007/s10773-017-3478-4
19. He, Y.-F., Ma, W.-P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**(9), 3483–3498 (2015)
20. He, Y.-F., Ma, W.-P.: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Quantum. Inf. **14**(1), 1650007 (2016) (8 pages)
21. He, Y., Ma, W.: Two robust quantum key agreement protocols based on logical GHZ states. Mod. Phys. Lett. B. **31**(03), 1750015 (2017)
22. Zhou, N.-R., Zhu, K.-N., Wang, Y.-Q.: Three-party semi-quantum key agreement protocol. Int. J. Theor. Phys. **59**, 663–676 (2020)
23. Jie Tang, Lei Shi, Jiahua Wei.: Controlled quantum key agreement based on maximally three-qubit entangled states. Modern Physics Letters B. **34**, (18) 2050201 (2020)
24. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. **12**(5), 1981–1990 (2013)
25. Zheng, X., Kuang, C., Liang, W.: Controlled quantum dialogue with authentication protocol on a basis of GHZ-like state. Quantum Inf. Process. **19**(8), (2020)
26. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5633–5638 (2000)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.