Improved quantum key agreement protocol with authentication

Ji-Hong Guo(郭继红), Ming-Qiang Bai(柏明强)†, Xiao-Yan Lei(雷小燕), Jia-Xin Xie(谢佳欣), and Zhi-Wen Mo(莫智文)

[1] *Institute of Intelligent Information and Quantum Information, Sichuan Normal University, Chengdu* 610068, *China*
[2] *Research Center of Sichuan Normal University, National-Local Joint Engineering Laboratory of System Credibility Automatic Verification, Chengdu* 610066, *China*
[3] *School of Mathematical Sciences, Sichuan Normal University, Chengdu* 610068, *China*

(Received 29 June 2022; revised manuscript received 22 September 2022; accepted manuscript online 19 October 2022)

In order to make the quantum key agreement process immune to participant attacks, it is necessary to introduce the authentication in the communication process. A quantum key agreement protocol with identity authentication that exploits the measurement correlation of six-particle entangled states is proposed. In contrast to some recently proposed quantum key agreement protocols with authentication, this protocol requires neither a semi-trusted third party nor additional private keys in the authentication process. The entire process of authentication and key agreement can be achieved using only n six-particle entangled states, which saves communication costs and reduces the complexity of the authentication process. Finally, security analysis shows that this scheme is resistant to some important attacks.

Keywords: quantum key agreement, authentication, six-particle entangled states

PACS: 03.67.Dd, 03.67.Hk, 03.67.Ac **DOI:** 10.1088/1674-1056/ac9b31

1. Introduction

Quantum cryptography is an important discipline in quantum information. It differs from classical cryptography in that its security is ensured based on some principles of quantum mechanics, such as Heisenberg's uncertainty principle, the quantum unclonable principle, etc. Therefore, quantum cryptography has absolute security in theory. Since the first quantum cryptographic protocol[1] appeared in 1984, many different kinds of quantum cryptographic protocols have been proposed one after another, such as quantum key distribution (QKD)[2–5], quantum secret sharing (QSS),[6–10] quantum secure direct communication (QSDC),[11–14] quantum privacy comparison (QPC),[15–18] quantum key agreement (QKA),[19–26] etc.

QKA means two or more participants working together to generate a final shared key, while each participant contributes equally to this final key. The first QKA protocol was proposed by Zhou *et al.*[27] in 2004, and many QKA protocols have been presented gradually.[28–30] However, none of the above QKA protocols introduce authentication of participants. We cannot guarantee that every participant is honest when a QKA protocol is designed, so it is necessary to consider identity authentication in the protocol. In recent years, some QKA protocols with identity authentication have been proposed.[31–35] In 2021, Zhu *et al.*[33] presented a QKA protocol for authentication with the help of a semi-trusted third party, Trent, using GHZ-like states. In the protocol, Trent is assumed to be an internal eavesdropper, and the probability that he can eavesdrop the session key K_{AB} is $(1/2)^L$ (L denotes the length of K_{AB}). Next, Zhu *et al.*[34] designed an authenticable QKA protocol using three-particle entangled states, in which the communicating parties can complete mutual authentication only with the help of the semi-honest server (SHS). The security analysis shows that the SHS has a probability of $1/2^n$ of obtaining K_{AB} (n refers to the ordered qubit sequences). Obviously, the dishonest behavior of these semi-trusted third parties will affect the security of the protocols. In the same year, Zhang *et al.*[35] proposed an authenticated QKA protocol based on a quantum search algorithm. The protocol only restricts P_0 from colluding with other participants, the agreement key is not eavesdropped, where P_0 refers to a semi-trusted third party. Unfortunately, this restriction is difficult to achieve in practical applications.

To address the security issues caused by semi-trusted third parties in current QKA protocols with identity authentication, this paper proposes a QKA protocol with authentication using six-particle entangled states, in which mutual authentication can be achieved without the participation of a semi-trusted third party. Moreover, there is no need to prepare additional private keys in the authentication process, thus saving resources. Finally, the security analysis also illustrates that our protocol is able to resist some attacks.

Section 2 presents some basics and the entanglement swapping of Bell states. Section 3 describes the protocol in detail and represents these processes in the form of a diagram. The security of the protocol is discussed in Section 4. Finally, Section 5 gives a concise summary and a comparison with other similar protocols.

†Corresponding author. E-mail: baimq@sicnu.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

2. Preliminary knowledge

2.1. Bell states' entanglement swapping, encoding, measurement

The four Bell states can be written as follows: $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. When any two of these Bell states are used as a tensor, the following equation is obtained: $|\phi^-\rangle_{12}|\phi^-\rangle_{34} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{2}(|\phi^-\rangle_{13}|\phi^-\rangle_{24} + |\phi^+\rangle_{13}|\phi^+\rangle_{24} + |\psi^-\rangle_{13}|\psi^-\rangle_{24} + |\psi^+\rangle_{13}|\psi^+\rangle_{24})$. According to the above equation, after the tensor operation on the initial Bell states, perform Bell measurements on particles 1,3, and assuming that the measurement result is $|\psi^-\rangle_{13}$, then particles 2,4 will collapse into the state $|\psi^-\rangle_{24}$. Based on the above Bell states' entanglement swapping measurement, four Bell states are encoded: $|\phi^+\rangle = 00$, $|\phi^-\rangle = 01$, $|\psi^+\rangle = 10$, $|\psi^-\rangle = 11$. The initial Bell states encoded in the equation do an iso-or operation as follows: $01 \oplus 01 = 00$, then the collapsed Bell states encoded in the equation do an iso-or operation as follows: $11 \oplus 11 = 00$. The above example shows that the results are the same after any two Bell states do the entanglement swapping. For a clearer understanding, the above process can be represented as shown in Table 1.

Table 1. Entanglement swapping and encoding between Bell states.

Initial Bell states (encoding)	Bell states after entanglement swapping (encoding)			
$\|\phi^-\rangle_{12}\|\phi^-\rangle_{34}$ $(01 \oplus 01)$	$\|\phi^-\rangle_{13}\|\phi^-\rangle_{24}$ $(01 \oplus 01)$	$\|\phi^+\rangle_{13}\|\phi^+\rangle_{24}$ $(00 \oplus 00)$	$\|\psi^+\rangle_{13}\|\psi^+\rangle_{24}$ $(10 \oplus 10)$	$\|\psi^-\rangle_{13}\|\psi^-\rangle_{24}$ $(11 \oplus 11)$

Bell state measurements always play a very important role in quantum communication. As early as 2001, Calsamiglia *et al.*[36] demonstrated that Bell state measurements could be achieved using a linear Bell state analyzer. Next, Grice *et al.*[37] improved the efficiency of Bell state measurement by introducing the method of entangled photon pairs with the same degree of freedom. Furthermore, homodyne detection[38,39] has become more popular due to its low noise and high sensitivity properties. Therefore, in the simulated design of this scheme, we will use homodyne detection to implement Bell state measurements.

2.2. The U operation

The four $U_{i_1 i_2}$ $(i_1, i_2 = 0, 1)$ operators can be expressed as $U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_{01} = X = |0\rangle\langle 1| + |1\rangle\langle 0|$, $U_{10} = Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $U_{11} = \mathrm{i}Y = |0\rangle\langle 1| - |1\rangle\langle 0|$. When $U_{i_1 i_2}$ $(i_1, i_2 = 0, 1)$ acts on the second particle of any Bell state, the initial Bell state is changed, and the changes are shown in Table 2.

Table 2. Changes between U operations and Bell states.

Bell state	$U_{00} \otimes U_{00}$	$U_{00} \otimes U_{01}$	$U_{00} \otimes U_{10}$	$U_{00} \otimes U_{11}$
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\varphi^+\rangle$	$\|\phi^-\rangle$	$\|\varphi^-\rangle$
$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\varphi^-\rangle$	$\|\phi^+\rangle$	$\|\varphi^+\rangle$
$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\phi^+\rangle$	$\|\varphi^-\rangle$	$\|\phi^-\rangle$
$\|\varphi^-\rangle$	$\|\varphi^-\rangle$	$\|\phi^-\rangle$	$\|\varphi^+\rangle$	$\|\phi^+\rangle$

2.3. Representation of a six-particle entangled state and its physical realization

The six-particle entangled state was proposed by Borras *et al.*[40] who found that this state is a highly entangled state. In addition, Choudhury *et al.*[41] also demonstrated that the entanglement of this state decays more slowly than that of the GHZ state, while the entanglement of this state is robust in depolarized channels. Therefore, this state is considered to be an important resource and is written as follows:

$$|\Psi\rangle_{123456} = \frac{1}{2}(|\phi^-\rangle_{16}|\phi^+\rangle_{25}|\phi^-\rangle_{34} + |\psi^-\rangle_{16}|\phi^-\rangle_{25}|\psi^+\rangle_{34} + |\phi^+\rangle_{16}|\psi^-\rangle_{25}|\psi^-\rangle_{34} + |\psi^+\rangle_{16}|\psi^+\rangle_{25}|\phi^+\rangle_{34}). \tag{1}$$

According to Eq. (1), we perform Bell measurements on particle pairs (1, 6), (2, 5), and (3, 4), respectively. The results will become $|\phi^-\rangle_{16}|\phi^+\rangle_{25}|\phi^-\rangle_{34}$, $|\psi^-\rangle_{16}|\phi^-\rangle_{25}|\psi^+\rangle_{34}$, $|\phi^+\rangle_{16}|\psi^-\rangle_{25}|\psi^-\rangle_{34}$, and $|\psi^+\rangle_{16}|\psi^+\rangle_{25}|\phi^+\rangle_{34}$ with a probability of $1/4$.

Since the six-particle entangled state was proposed, the way to achieve its physical realization has been an interesting topic to many scholars. Fortunately, You *et al.*[42] first proposed a method for the preparation of six-particle entangled states based on the concept of quantum erasure and confirmed the feasibility in experiments. Secondly, the preparation of this entangled state is achievable using the cavity QED technology in Ref. [43]. In addition, it is more interesting to use the ion trap principle[44] to prepare multi-particle entangled states. As shown in Fig. 1, we also try to give an alternative way of preparing six-particle entangled states utilizing a quantum circuit as follows.

(i) Assume that the 6-qubit initial state is in the ground state $|000000\rangle_{123456}$.

(ii) After performing the Hadamard operator on every particle, the result is $|++++++\rangle_{123456}$.

(iii) The operation $CZ = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$ is applied on particle pairs $(6, i)$, $i = 1, 2, \ldots, 6$, where particle 6 is the control bit. The result evolves to $|U_X\rangle$.

(iv) Applying the Hadamard operator on particle 6, the $|U_X\rangle$ transforms to $|U_Y\rangle$.

(v) The six-particle entangled state in Eq. (1) is obtained by performing a unitary transformation U_Z on the above re-

sultant state $|U_Y\rangle$, where U_Z is equivalent to a 64×64 unitary matrix.

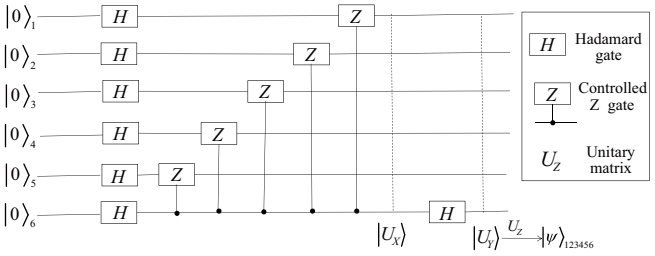


Fig. 1. Quantum circuit diagram of a six-particle entangled state.

3. Description of the authentication process and key agreement protocol

3.1. Authentication stage

Step 1 Alice prepares n $|\Psi\rangle_{123456}$ states and divides them into six sequences S_i $(i=1,\ldots,6)$. Then, Alice randomly selects some decoy particles from the set $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ and inserts them into the sequences S_3, S_4 to get the sequences S_3^*, S_4^*, which are sent to Bob. Alice retains the sequences S_1, S_6, S_2, S_5.

Step 2 After Bob receives the sequences S_3^*, S_4^*, they perform the first secure eavesdropping detection. Alice tells Bob the location of the corresponding decoy particles and the measurement basis, and Bob measures them. The measurement results are told to Alice, who compares the measurements with the initial decoy states. If the error rate is below the initially specified threshold, the authentication process is proven to be secure and there is no malicious external eavesdropper, and the protocol continues. Otherwise, the protocol is terminated and restarted.

Step 3 After the security detection, Bob discards the corresponding decoy particles in the sequences S_3^*, S_4^* and recovers the sequences S_3, S_4, then performs Bell measurements on the corresponding particles in the sequences. At the same time, Alice performs Bell measurements for the corresponding particles in the sequences S_1, S_6, S_2, and S_5, respectively. For the measurement results, Alice and Bob negotiate the corresponding encoding rules, which correspond to the following: $|\phi^+\rangle\rightarrow 00$, $|\phi^-\rangle\rightarrow 01$, $|\psi^+\rangle\rightarrow 10$, $|\psi^-\rangle\rightarrow 11$. Due to the measurement correlation of the six-particle entangled state $|\Psi\rangle_{123456}$, Alice and Bob can know each other's measurement results. Alice knows Bob's measurement results C_2, where $C_2=C_2^1\|C_2^2\|\cdots\|C_2^n$, and C_2^i denotes Bob's i-th measurement. Bob also knows Alice's measurement results C_1 for the corresponding particles in the sequences S_2, S_5, where $C_1=C_1^1\|C_1^2\|\cdots\|C_1^n$, and C_1^i denotes Alice's i-th measurement.

Step 4 Alice randomly selects some decoy particles from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them into the sequence S_2, then obtains the sequence S_2^* and sends it to Bob. At the same time, Bob sends the sequence S_4^* with the decoy particles inserted to Alice. After receiving the sequence from each other, Alice and Bob perform a second security eavesdropping detection. The second security detection is exactly equivalent to the first one, and if the error rate is within a suitable threshold, the protocol continues, otherwise, the protocol is terminated and started again.

Step 5 After the second safety detection, Alice has the sequences S_4, S_5 and performs Bell measurements on the corresponding particles. Bob also performs Bell measurements on the particles corresponding to the sequences S_2, S_3. At this point, the entanglement swapping of Bell states is completed. Alice's measurement results are C_1^*, where $C_1^*=C_{11}^*\|C_{12}^*\|\cdots\|C_{1n}^*$, and C_{1i}^* denotes Alice's i-th measurement. Bob's measurement results are C_2^*, where $C_2^*=C_{21}^*\|C_{22}^*\|\cdots\|C_{2n}^*$, and C_{2i}^* denotes Bob's i-th measurement.

Step 6 Alice announces C_1^* and Bob announces C_2^*. Alice computes whether $C_1\oplus C_2=C_1^*\oplus C_2^*$ holds, and if it does, Bob is proved to be a legitimate participant, indicating that authentication is complete. Since the mutual authentication of Alice and Bob is performed simultaneously, the authentication process of Bob to Alice is briefly described as follows.

Step I Repeating the above Step 1 to Step 3, Bob's measurement results on the corresponding particles in the sequences S_3, S_4 are $C_2=C_2^1\|C_2^2\|\cdots\|C_2^n$. Also, due to the measurement correlation of the multi-particle entangled state, Bob can know Alice's measurement results $C_1=C_1^1\|C_1^2\|\cdots\|C_1^n$.

Step II Repeating Step 4 and Step 5, after Alice and Bob swap the particles in the sequences S_2, S_4, Alice's measurement results of the particles in the sequences S_4, S_5 are $C_1^*=C_{11}^*\|C_{12}^*\|\cdots\|C_{1n}^*$ and Bob's measurements of the particles in the sequences S_2, S_3 are $C_2^*=C_{21}^*\|C_{22}^*\|\cdots\|C_{2n}^*$.

Step III Once Alice announces C_1^*, Bob computes whether $C_2\oplus C_1=C_2^*\oplus C_1^*$ holds, and if it does, it means that Alice is an honest participant.

3.2. Key agreement phase

Suppose Alice's and Bob's keys are denoted as follows: $K_{\rm A}=K_{\rm A}^1\|K_{\rm A}^2\|\cdots\|K_{\rm A}^n$, $K_{\rm B}=K_{\rm B}^1\|K_{\rm B}^2\|\cdots\|K_{\rm B}^n$, then the final key they negotiate is denoted as

$$K=(K_{\rm A}^1\|K_{\rm B}^1)\|(K_{\rm A}^2\|K_{\rm B}^2)\|\cdots\|(K_{\rm A}^n\|K_{\rm B}^n),$$

where $K_{\rm A}^i,K_{\rm B}^i\in\{00,01,10,11\}$ and $i=1,2,\ldots,n$. Alice and Bob can perform the following key agreement process only after they have passed the authentication.

Step 1 Alice performs $U_{i_1i_2}$ $(i_1,i_2=0,1)$ operation on the corresponding particles in the sequence S_6 according to her key $K_{\rm A}$ to obtain the sequence S_6^*, where i_1i_2 consistently corresponds to the values of $K_{\rm A}^i$ $(i=1,2,\ldots,n)$. And the permutation operation Π is applied to sequence S_1 to obtain sequence S_1^*. Alice selects enough decoy particles from the set

$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to insert into the sequences S_1^*, S_6^*, then the sequences S_1^{**}, S_6^{**} are obtained and sent to Bob.

Step 2 After Bob receives the sequences S_1^{**}, S_6^{**}, Alice announces the position of the decoy particles and the measurement basis used, and the permutation operation Π is implemented. Then Bob performs a third security eavesdropping detection. After the detection is completed, Bob discards the decoy states and reverts to the sequences S_1^*, S_6^*. Bob performs the inverse permutation operation on the sequence S_1^* to obtain the original sequence, and performs Bell measurements on the corresponding particles in the sequences S_1, S_6^*. Based on the measurement results and the initial Bell states of the corresponding particles in the sequences S_1, S_6, Bob is able to know Alice's key $K_{\rm A}$. Thus, the final agreement key K can be calculated.

Step 3 Bob publicly announces the value of $H_{\rm B} = K_{\rm B} \oplus C_1$. Alice is able to obtain $K_{\rm B}$ by computing $K_{\rm B} = H_{\rm B} \oplus C_1$, and thus is able to compute the final shared key K. By now both parties have completed the key agreement process.

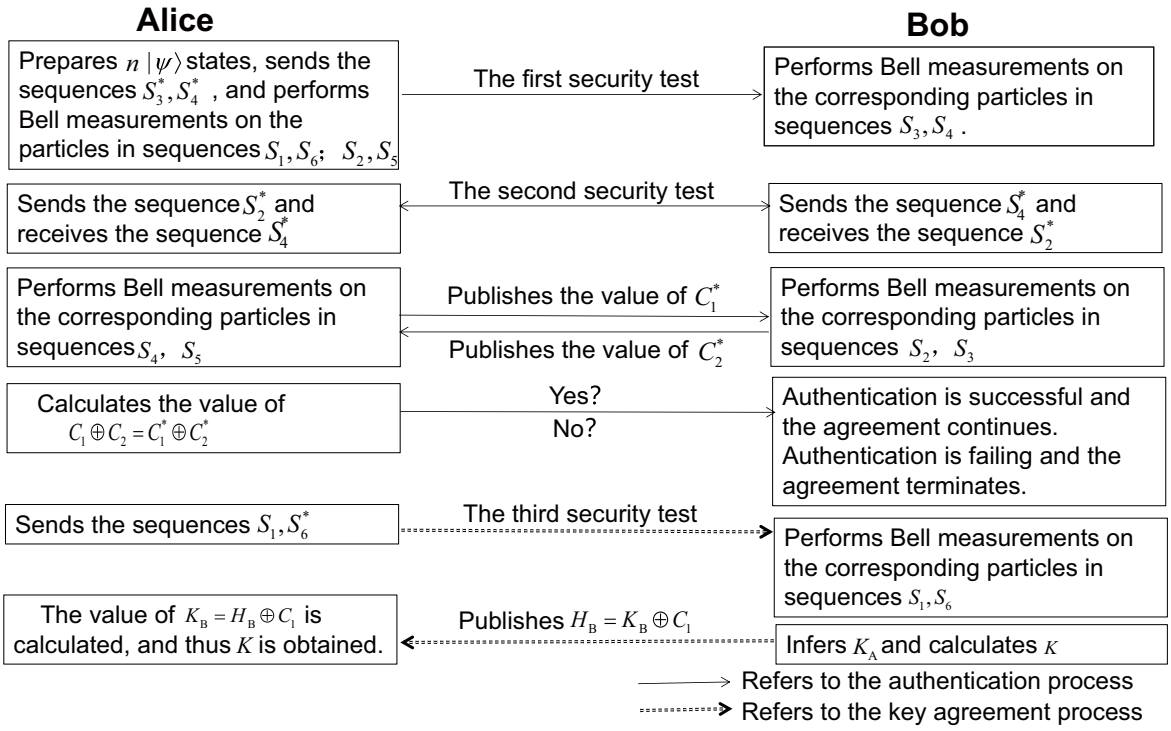


Fig. 2. The process of authentication and key agreement.

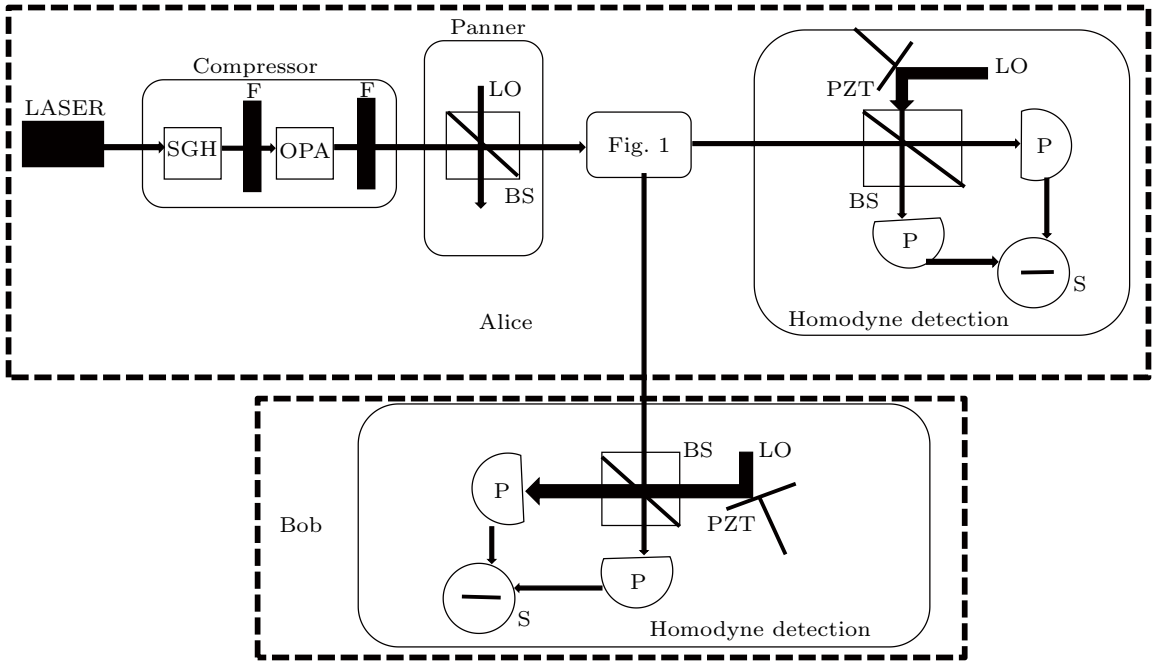


Fig. 3. Experimental scheme diagram of the QKA process.

To describe this scheme more clearly, figure 2 is a flowchart of the authentication and key agreement between Alice and Bob. Figure 3 is a diagram of the measurement implementation with the current technology. A description of the devices in Fig. 3 is given below. LASER is the laser light source, SGH is the nonlinear crystal, OPA is the optical parametric amplifier, F is the spectral filter, and LO is the intense beam generated by the native oscillator, which serves to translate and measure the signal beam. BS is the beam splitter, P is the photodiode, figure 1 is the preparation process of a six-particle entangled state quantum circuit, S is the subtractor, and PZT is the piezoelectric transducer.

4. Security analysis

For a QKA protocol, it is extremely important to discuss its security. Since we include authentication of participants in this protocol, we are able to guarantee that both Alice and Bob are legitimate participants when their key agreement is completed. Therefore, the security discussion in this section focuses on some external attacks, such as impersonation attacks, intercept-resend attacks, man-in-the-middle attacks, etc.

4.1. Impersonation attacks

Suppose Eve impersonates Alice during key agreement with Bob. Due to the measurement correlation of $|\Psi\rangle_{123456}$ states, Eve does not know Alice's measurement results C_1. Eve will prepare a random sequence of Bell states and send the first particle in the sequence to Bob, while Bob still complies with the previous operation and sends the particles in the sequence S_4 to Eve. After receiving the sent particles from each other, Alice and Eve complete the entanglement swapping of Bell states. At this point, they perform Bell measurements on each other's particles in the sequences, and after the measurements are completed Eve announces her measurements $C_{\rm E}$ and Bob announces his measurements C_2^*. Since $C_1 \oplus C_2 \neq C_{\rm E} \oplus C_2^*$, it is known that Eve is an illegitimate impostor. Similarly, Eve cannot successfully pass the authentication process when she impersonates Alice for key agreement.

4.2. Intercept-resend attacks

The intercept-resend attack is when a malicious attacker Eve first intercepts the sequences S_3^*, S_4^*, then resends new sequences to Bob with the measurement results. Since the sequences S_3^*, S_4^* contain decoy particles, Eve does not know which are the decoy particles and which are the initial particles. Eve's measurement will act on some decoy particles. Suppose she chooses the Z-basis to measure the particles $\{|+\rangle, |-\rangle\}$, then she will have $3/4$ probability of success. Thus, the probability of Eve's attack failure is $1-(3/4)^m$, where m refers to the number of decoy particles inserted into the particle sequences. The probability of Eve's attack failure is 1 when m is a relatively large number. When Eve measures the sequence S_2^*, the attack will also fail with the same probability.

4.3. Man-in-the-middle attacks

A man-in-the-middle attack means that Eve pretends to be a legitimate user of the communication process and obtains the content of both sides of the communication by intercepting the sequence in the channel. Suppose Eve first intercepts the sequences S_3^*, S_4^* sent by Alice to Bob, and subsequently performs the first security detection. Since Eve does not know the position of the decoy particles in the sequence, the result after the measurement will be different from the result announced by Alice, and thus Eve will not successfully pass the first eavesdropping detection. After Eve intercepts the sequence S_2^*, similarly, this malicious operation will be detected in the second security detection.

4.4. Information leaking

The issue of information leakage in quantum cryptographic protocols was first raised by Gao *et al.*[45] In Subsection 3.2 of this paper, there are two possibilities of information leakage. The first one is that Eve is able to infer the decoded U operation by comparing the results of the corresponding particles in the measurement sequences S_1, S_6^* with the results of the initial Bell states. The second one is that when Bob discloses the value of $H_{\rm B}$ through the classical channel, the information may also leak to Eve. Obviously, the amount of information leaked to Eve during the quantum communication process can be expressed as

$$I = -\sum_{i=1}^{16} p_i \log_2 p_i = -16 \times \frac{1}{16} \log_2 \frac{1}{16} = 4 \text{ bit}. \tag{2}$$

Therefore, there is no information leakage in this protocol.

5. Conclusion

In this paper, a QKA protocol with authentication is proposed based on six-particle entangled states. This QKA protocol does not require the help of a semi-trusted third party and some keys for authentication, unlike other QKA protocols.[32,34,35] Therefore, this protocol can reduce the complexity of authentication and save communication costs. Moreover, the security analysis also proves that our scheme is secure, reliable and feasible. Although Zhu's[31] protocol also does not require the participation of semi-trusted third parties, Bob's private keys $\rm ID_B$ are transmitted directly in the traditional channel, which makes the $\rm ID_B$ at risk of being eavesdropped. The following Table 3 compares our protocol with some other QKA protocols with identity authentication and shows that our protocol has obvious advantages.

Table 3. Comparison of our protocols and some existing QKA protocols.

QKA protocol	Whether to introduce semi-trusted party	Whether to prepare the authentication key	Measurement basis
Zhu's[31]	no	yes	single-particle
Wu's[32]	yes	yes	GHZ-basis
Zhu's[34]	yes	yes	single-particle
Zhang's[35]	yes	yes	single-particle
Ours	no	no	Bell state

Acknowledgments

Project supported by the National Science Foundation of Sichuan Province, China (Grant No. 2022NSFSC0534), Major Science, and Techonolgy Application Demonstration Project in Chengdu (Grant No. 2021-YF09-0116-GX).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, December 10–12, 1984, Bangalore, India, p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Li H W, Shi J H, Cai Q Y and Sun C P 2022 *Quantum Inf. Process.* **21** 142
[4] Yan B Z, Li Q, Mao H K and Chen N 2022 *Quantum Inf. Process.* **21** 130
[5] Gao F, Guo F Z, Wen Q Y and Zhu F C 2006 *Phys. Lett. A* **349** 53
[6] Xiao L, Lu L G, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[7] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett. A* **324** 420
[8] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev. A* **72** 044302
[9] Deng F G, Li X H and Zhou H Y 2008 *Phys. Lett. A* **372** 1957
[10] Gu B, Mu L L, Ding L G, Zhang C Y and Li C Q 2010 *Opt. Commun.* **283** 3099
[11] Rong Z B, Qiu D W, Meteus P and Zou X F 2021 *Quantum Inf. Process.* **20** 58
[12] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[13] Sheng Y B, Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[14] Wu X D, Zhou L, Zhong W and Sheng Y B 2020 *Quantum Inf. Process.* **19** 354
[15] Siddhu V and Arvind 2015 *Quantum Inf. Process.* **14** 3005
[16] Liu W and Wang Y B 2012 *Int. J. Theor. Phys.* **51** 3596
[17] Jia H Y, Wen Q Y, Li Y B and Gao F 2012 *Int. J. Theor. Phys.* **51** 1187
[18] Liu W, Wang Y B, Jiang Z T and Cao Y Z 2012 *Int. J. Theor. Phys.* **51** 69
[19] Chong S K and Hwang T 2010 *Opt. Commun.* **283** 1192
[20] Tsai C W, Wang S H and Hwang T 2010 *Opt. Commun.* **283** 5285
[21] Chong S K, Tsai C W and Hwang T 2011 *Int. J. Theor. Phys.* **50** 1793
[22] Shi R H and Zhong H 2013 *Quantum Inf. Process.* **12** 921
[23] Li Z H, Xue K P, Jia Q D, Liu J Q and Yu N H 2022 *Quantum Inf. Process.* **21** 192
[24] Xu Y G, Wang C N, Wang X Y and Zhu H F 2022 *Quantum Inf. Process.* **21** 91
[25] Yang Y G, Wang Y C, Li J, Zhou Y H and Shi W M 2021 *Quantum Inf. Process.* **20** 376
[26] Zhou Y H, Wang M F, Shi W M, Yang Y G and Zhang J 2020 *Quantum Inf. Process.* **19** 100
[27] Zhou N, Zeng G and Xiong J 2004 *Electron. Lett.* **40** 1149
[28] Xu G B, Wen Q Y, Gao F and Qin S J 2014 *Quantum Inf. Process.* **13** 2587
[29] Wang S S, Jiang D H, Xu G B, Zhang Y H and Liang X Q 2019 *Quantum Inf. Process.* **18** 190
[30] Huang X, Zhang S B, Chang Y, Qiu C, Liu D M and Hou M 2021 *Int. J. Theor. Phys.* **60** 838
[31] Zhu H F, Wang L W and Zhang Y L 2020 *Quantum Inf. Process.* **19** 1
[32] Wu Y T, Chang H, Guo G D and Lin S 2021 *Int. J. Theor. Phys.* **60** 4066
[33] Zhu H F, Wang C N and Li Z X 2021 *Int. J. Theor. Phys.* **18** 1
[34] Zhu H F, Liu T H and Wang C N 2021 *Int. J. Theor. Phys.* **60** 929
[35] Zhang X, Wang N and Lin S 2021 arXiv: 2112.07929v1
[36] Calsamiglia J and Lütkenhaus N 2001 *Appl. Phys. B* **72** 67
[37] Grice W P 2011 *Phys. Rev. A* **84** 042331
[38] Luís R S, Puttnam B J and Shinada S 2015 *IEEE Photonic. Tech. L.* **27** 608
[39] Miyazaki T 2006 *IEEE Photonic. Tech. L.* **18** 388
[40] Borras A, Plastino A R, Batle J, Zander C and Plastino A 2007 *J. Phys. A: Math. Theor.* **40** 13407
[41] Choudhury S, Muralidharan S and Panigrahi P K 2009 *J. Phys. A: Math. Theor.* **42** 115303
[42] You J, Li J H and Xie X T 2005 *Chin. Phys. B* **14** 1329
[43] Xu Y, Li Y, Nie L and Li X 2013 *Int. J. Theor. Phys.* **52** 3086
[44] Haeffner H, Haensel W, Roos C F and Benhelm J 2005 *Nature* **438** 643
[45] Gao F, Qin S J, Wen Q Y and Zhu F C 2008 *Phys. Lett. A* **327** 3333