Quantum Information Processing (2022) 21:290
https://doi.org/10.1007/s11128-022-03640-4

Mutual authentication quantum key agreement protocol based on Bell states

Ye-Feng He[1] · Yibo Pang[1] · Man Di[1]

Received: 17 March 2022 / Accepted: 27 July 2022 / Published online: 13 August 2022

Abstract
A mutual authentication quantum key agreement protocol can authenticate participants' identities before establishing shared keys fairly. Therefore, it is more in line with the actual demand than the general quantum key agreement protocols. With Bell states and their entanglement exchange relations, a new mutual authentication quantum key agreement protocol is proposed. The participants can mutually authenticate each other's identity by using their secret identity information and the measurement correlation property of Bell states. Moreover, they can negotiate session keys fairly with the entanglement exchange relations of Bell states. The new mutual authentication quantum key agreement protocol is proved to be unconditionally secure and has good performance.

Keywords Quantum cryptography · Quantum key agreement · Mutual authentication · Unconditional security · Qubit efficiency

1 Introduction

Based on quantum mechanics principles, quantum key agreement (QKA) [1, 2] can realize unconditional secure communication by providing encryption and decryption keys for "one-time-one pad" cryptosystem. It is new and different information protection technology from quantum key distribution (QKD) [3–6]. Unlike QKD, which allows one party to decide the key independently and sends it to the other party, QKA requires all participants to jointly and fairly establish a shared key. Therefore, QKA is more suitable for practical needs.

At present, QKA are widely concerned [7–10] since the first QKA protocol [7] was given in 2004. The first QKA protocol mainly uses the idea of quantum teleportation.

✉ Ye-Feng He
yefenghe2008@hotmail.com ; yefenghe2008@vip.sina.com

[1] School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Subsequently, several new QKA protocols were proposed. Most of them cannot resist the participant attack [9] or the controlled-Not attack [10]. One successful two-party QKA protocol was proposed by Chong and Hwang in 2010 [11]. Now, there have been many new successful QKA protocols including two-party QKA [11–13] and multi-party QKA [13–18]. These QKA protocols mainly use single particles or Bell states as quantum sources. Subsequently, researchers also put forward some QKA protocols based on four-particle cluster states [1, 19, 20]. Since the security of QKA protocols will also be adversely affected by channel noise, researchers have spent more energy on the study of the QKA protocols [2, 21, 22] against collective noise. In order to adapt to different application environments, researchers also proposed controlled quantum key agreement protocols [23] and semi-quantum key agreement protocols [24]. On the other hand, in practical application, the attackers often want to disguise themselves as participants to obtain shared keys, that is, to implement man-in-the-middle attacks on QKA protocols. Thus, the QKA protocols should first authenticate the identities of the participants before key negotiation. This is very important for the QKA protocols to be applied safely. Unlike the classical mutual authentication key agreement protocols, which have been studied more, the research on mutual authentication quantum key agreement (MAQKA) is still less. In 2021, Zhu et al.[25] and Ma et al.[26] proposed a MAQKA protocol, respectively. Since then, such MAQKA protocols have also attracted more attention from researchers.

In this paper, we propose a new MAQKA protocol based on Bell states. It can not only generate shared keys fairly, but also authenticate participants' identities before negotiating keys. The participants can authenticate each other's identity according to whether they can choose the correct measurement bases with their shared secret identity information. They generate shared secret keys by using the entanglement swapping property of Bell states. The security analysis shows that the authentication process of the MAQKA protocol can resist forgery attacks and is unconditionally secure, and the key agreement process of the MAQKA protocol can resist external attacks and participant attacks. Compared with the two existing MAQKA protocols, the new MAQKA protocol has higher quantum bit efficiency, and it can realize identity authentication and key negotiation without the participation of trusted or semi-trusted third party, thus reducing the communication complexity.

The rest of this paper is organized as follows. In Sect. 3, we present a new MAQKA protocol. Section 3 gives its security analysis and performance analysis. Finally, a conclusion is given in Sect. 4.

2 The mutual authentication quantum key agreement protocol

A hash function $H(x)$ outputting an n-bit value is used in our MAQKA protocol. Moreover, the mutual identity authentication needs a secret identity information K_{AB}, which is shared by Alice and Bob in advance. If Alice and Bob want to negotiate a session key, they must first authenticate each other's identity and then negotiate the key after passing the identity authentication. See Fig. 1 and the following specific steps for details of the MAQKA protocol. In Fig 1(c), the square symbol denotes

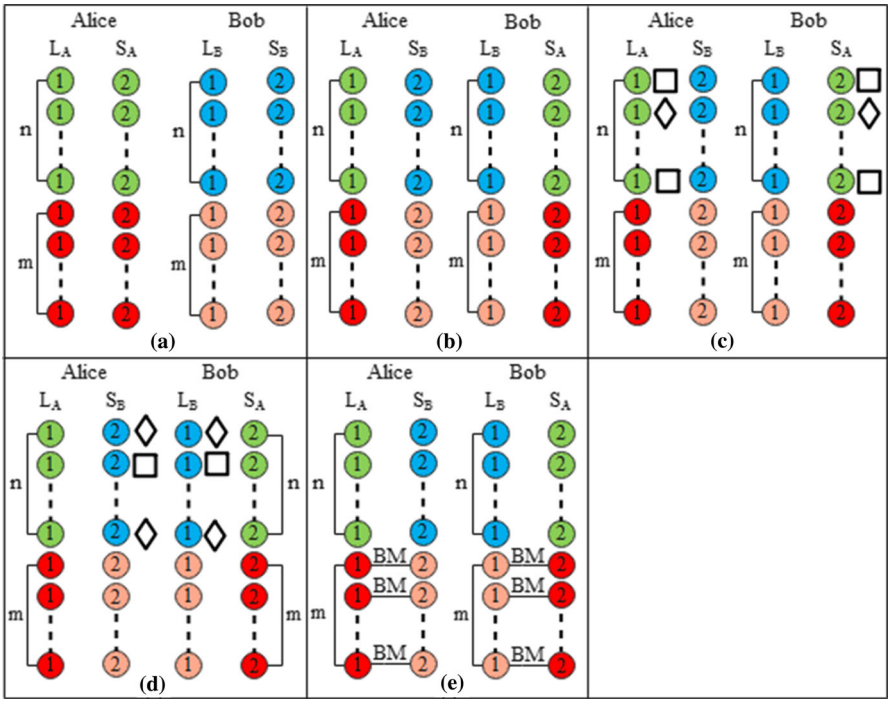

Fig. 1 The process of MAQKA protocol without considering decoy states. **a** Bell states preparation. **b** Bell states transmission. **c** Bob's identity authentication. **d** Alice's identity authentication. **e** Key negotiation

the measurement with Z-base, the diamond symbol denotes the measurement with X-base, and BM denotes Bell measurement here.

Step 1. **Bell states preparation and transmission:** Alice and Bob prepare $n+m$ Bell states $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$, respectively. Alice records the first-particle sequence of $n+m$ Bell states as $L_A = L_A^{(1)} L_A^{(2)} \cdots L_A^{(n+m)}$ and the second-particle sequence as $S_A = S_A^{(1)} S_A^{(2)} \cdots S_A^{(n+m)}$. Similarly, Bob gets the sequences $L_B = L_B^{(1)} L_B^{(2)} \cdots L_B^{(n+m)}$ and $S_B = S_B^{(1)} S_B^{(2)} \cdots S_B^{(n+m)}$. From the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, Alice and Bob randomly select some decoy states and insert their sequences S_A and S_B at random. Alice sends the new sequence S'_A to Bob, and Bob sends the new sequence S'_B to Alice. Moreover, they all keep the sequences L_A and L_B themselves.

Step 2. **Eavesdropping detection:** For the sequence S'_A, Alice announces the positions and measurement bases of the decoy states. With the correct bases, Bob measures the decoy photons and sends the measurement results to Alice. Then Alice computes the error rate and determines whether the channel is safe or not. For the sequence S'_B, similar work is required. If the channels are safe, they continue to execute the protocol. Otherwise, they terminate the protocol and restart.

Step 3. **Mutual authentication:** After eavesdropping detection, the sequences S'_A and S'_B have been restored to the sequences S_A and S_B. Since the methods of authenticating Alice and Bob are completely similar, we only take Bob's identity authentication as an example. It is carried out in the following three steps.

Table 1 The relationship among the hash value $\overline{K}_{AB}$, the measurement results of the sequence L_A and the coding sequence R_A

The hash value $\overline{K}_{AB}$	The measurement results of the sequence L_A	The coding sequence R_A
0101	$\|0\rangle, \|+\rangle, \|0\rangle, \|+\rangle$	0000
0101	$\|1\rangle, \|+\rangle, \|0\rangle, \|+\rangle$	1000
0101	$\|0\rangle, \|+\rangle, \|1\rangle, \|+\rangle$	0010
0101	$\|1\rangle, \|+\rangle, \|1\rangle, \|+\rangle$	1010
0101	$\|0\rangle, \|-\rangle, \|0\rangle, \|+\rangle$	0100
0101	$\|0\rangle, \|+\rangle, \|0\rangle, \|-\rangle$	0001
0101	$\|0\rangle, \|-\rangle, \|0\rangle, \|-\rangle$	0101
0101	$\|1\rangle, \|-\rangle, \|0\rangle, \|+\rangle$	1100
0101	$\|1\rangle, \|+\rangle, \|0\rangle, \|-\rangle$	1001
0101	$\|1\rangle, \|-\rangle, \|0\rangle, \|-\rangle$	1101
0101	$\|0\rangle, \|-\rangle, \|1\rangle, \|+\rangle$	0110
0101	$\|0\rangle, \|+\rangle, \|1\rangle, \|-\rangle$	0011
0101	$\|0\rangle, \|-\rangle, \|1\rangle, \|-\rangle$	0111
0101	$\|1\rangle, \|-\rangle, \|1\rangle, \|+\rangle$	1110
0101	$\|1\rangle, \|+\rangle, \|1\rangle, \|-\rangle$	1011
0101	$\|1\rangle, \|-\rangle, \|1\rangle, \|-\rangle$	1111

(a) Alice randomly selects a number r and makes it public. Then she computes $\overline{K}_{AB} = H(K_{AB}||r)$, which is expressed as $\overline{K}_{AB} = \overline{K}_{AB}^{(1)}\overline{K}_{AB}^{(2)}\cdots\overline{K}_{AB}^{(n)}$. According to the value of $\overline{K}_{AB}^{(i)}$, she chooses the measurement bases to measure the particle $L_A^{(i)}$ in the sequence L_A, where $i = 1, 2, \cdots, n$. If $\overline{K}_{AB}^{(i)} = 0$, Alice chooses Z-basis $\{|0\rangle, |1\rangle\}$ as the measurement base; if $\overline{K}_{AB}^{(i)} = 1$, Alice chooses X-basis $\{|+\rangle, |-\rangle\}$ as the measurement base. When Alice finishes measuring all the first n particles in the sequence L_A, she codes the measurement results as $R_A = R_A^{(1)}R_A^{(2)}\cdots R_A^{(n)}$. The coding rule she uses is: If the quantum state is $|0\rangle$ or $|+\rangle$, then $R_A^{(i)} = 0$; if the quantum state is $|1\rangle$ or $|-\rangle$, then $R_A^{(i)} = 1$.

For example, Alice prepares six Bell states in Step 1, that is, the Bell state sequence is $|\phi^+\rangle|\phi^+\rangle|\phi^+\rangle|\phi^+\rangle|\phi^+\rangle|\phi^+\rangle$. If the hash value $\overline{K}_{AB}$ she calculates in this step is 0101, the measurement bases she chooses are $ZXZX$. However, there may be 16 different measurement results for the first four particles of the sequence L_A, corresponding to 16 different coding sequences R_A. See Table 1 for details. Moreover, the probability of each result is 1/16. However, when Alice completes the measurement in this step, the first four quantum states of her sequence L_A will inevitably collapse to one of these 16 kinds.

(b) According to the key K_{AB} and the random number r, Bob computes the hash value $\overline{K}'_{AB} = H(K_{AB}||r)$, which is recorded as $\overline{K}'_{AB} = \overline{K}'^{(1)}_{AB}\overline{K}'^{(2)}_{AB}\cdots\overline{K}'^{(n)}_{AB}$. After that, Bob selects his measurement bases in terms of the value $\overline{K}'_{AB}$. If $\overline{K}'^{(i)}_{AB} = 0$, his measurement base is $\{|0\rangle, |1\rangle\}$. If $\overline{K}'^{(i)}_{AB} = 1$, his measurement base is $\{|+\rangle, |-\rangle\}$. After

Bob has measured all the first n particles in the sequence S_A, his measurement results are coded as the sequence $R'_A = R'^{(1)}_A R'^{(2)}_A \cdots R'^{(n)}_A$. Bob's coding rule is exactly the same as Alice's coding rule for the sequence L_A. Then the sequence R'_A is announced by Bob.

(c) By comparing the values of R_A and R'_A, Alice judges whether Bob's identity is correct. Continue with the above example of Step 3(a). When $\overline{K}_{AB} = 0101$, since there are 16 different measurement results for the sequence L_A, then the sequence S_A will collapse to 16 different state sequences. However, according to the measurement correlation property of Bell states, the quantum states of the sequence L_A and the sequence S_A correspond to the same. That is, if the measurement results of the sequence L_A are $|1\rangle|+\rangle|0\rangle|+\rangle$, then the quantum states of the sequence S_A after collapsing in Step 3(a) are also $|1\rangle|+\rangle|0\rangle|+\rangle$. Therefore, when the measurement bases of Bob and Alice are consistent, the measurement results of the sequence S_A are consistent with those of the sequence L_A.

It is worth noting that the first n particles of L_B and S_B are also used to detect the identity of Alice. Therefore, only the last m particles are left in the four sequences L_A, S_A, L_B and S_B, which are re-marked as $L^*_A = L^{(n+1)}_A L^{(n+2)}_A \cdots L^{(n+m)}_A$, $S^*_A = S^{(n+1)}_A S^{(n+2)}_A \cdots S^{(n+m)}_A$, $L^*_B = L^{(n+1)}_B L^{(n+2)}_B \cdots L^{(n+m)}_B$ and $S^*_B = S^{(n+1)}_B S^{(n+2)}_B \cdots S^{(n+m)}_B$. Moreover, the two sequences L^*_A and S^*_B are in Alice's hands, the other two sequences L^*_B and S^*_A are in Bob's hands.

Step 4. **Key negotiation:** After the mutual authentication between Alice and Bob is successful, they negotiate the session key together. Alice performs Bell measurements on the corresponding m pairs of particles in the sequences L^*_A and S^*_B. At the same time, Bob performs Bell measurements on the corresponding m pairs of particles in the sequences L^*_B and S^*_A. According to the entanglement exchange relation of Bell states $|\phi^+\rangle$, that is,

$$\begin{aligned}|\phi^+\rangle_{12}|\phi^+\rangle_{34} = \frac{1}{2}(&|\phi^+\rangle_{14}|\phi^+\rangle_{23} + |\phi^-\rangle_{14}|\phi^-\rangle_{23} \\ &+|\psi^+\rangle_{14}|\psi^+\rangle_{23} + |\psi^-\rangle_{14}|\psi^-\rangle_{23}),\end{aligned} \tag{1}$$

we know that the measurement results of Alice and Bob are equal. And, for each Bell measurement, they will get the states $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, or $|\psi^-\rangle$ with a $1/4$ probability. Alice and Bob negotiate a session key encoding rule, that is, $|\phi^+\rangle$ corresponds to 00, $|\phi^-\rangle$ corresponds to 01, $|\psi^+\rangle$ corresponds to 10, and $|\psi^-\rangle$ corresponds to 11. Therefore, after encoding their m measurement results, they can get a binary sequence K with a length of $2m$. The sequence K is the session key negotiated by both parties.

3 Security analysis and performance analysis

3.1 Security analysis of mutual authentication

In the following, let us analyze the security of mutual authentication from three aspects.

Correctness: According to the description and examples of the mutual authentication, it judges whether Bob's identity is correct or not by comparing the gap between R_A and R'_A. If Bob's identity is correct, he must own K_{AB} and can calculate the correct value $\overline{K}'_{AB} = H(K_{AB}||r)$. Moreover, he has $\overline{K}'_{AB} = \overline{K}_{AB}$. Therefore, Alice and Bob choose the same measurement bases. According to the measurement correlation property of Bell states, the measurement results of the sequence S_A are consistent with those of the sequence L_A. That is, there is $R_A = R'_A$ when Bob's identity is correct.

For example: When $\overline{K}_{AB} = 0101$, Alice chooses the measurement bases $ZXZX$. According to Table 1, we easily know that Alice's measurement results are one of 16 cases. If Alice's measurement results are $L_A = L_A^{(1)} L_A^{(2)} L_A^{(3)} L_A^{(4)} = |1\rangle|+\rangle|0\rangle|+\rangle$, then her coding sequence is $R_A = R_A^{(1)} R_A^{(2)} R_A^{(3)} R_A^{(4)} = 1000$. Since there is $\overline{K}'_{AB} = \overline{K}_{AB}$ for correct Bob's identity, the measurement bases chosen by Bob are exactly the same as those chosen by Alice. For the sequence S_A, Bob's measurement results are also $|1\rangle|+\rangle|0\rangle|+\rangle$. So his coding sequence is also $R'_A = 1000$, that is, $R_A = R'_A$. Therefore, Bob can pass the identity authentication by using his correct identity information.

Forgery attack: If Charlie wants to authenticate herself as Bob, she must not know K_{AB}. So she cannot get the right $\overline{K}'_{AB}$ and cannot choose the right measurement bases. For every particle of the sequence S_A, she can only choose one randomly between two measurement bases Z and X. Moreover, the corresponding probability is $1/2$. If the measurement bases of Charlie and Alice are consistent, then Charlie's measurement results must be correct. Continue to use the previous example, if Alice's measurement results are $L_A = L_A^{(1)} L_A^{(2)} L_A^{(3)} L_A^{(4)} = |1\rangle|+\rangle|0\rangle|+\rangle$, then the sequence S_A must collapse to $S_A = S_A^{(1)} S_A^{(2)} S_A^{(3)} S_A^{(4)} = |1\rangle|+\rangle|0\rangle|+\rangle$. For $S_A^{(1)} = |1\rangle$, Charlie can choose two possible measurement bases Z and X with a probability of $1/2$. If Charlie chooses Z base for measuring the particle $S_A^{(1)}$, then her measurement result must be $|1\rangle$. However, if Charlie chooses X base for her measurement, she must obtain one of two measurement results $|+\rangle$ or $|-\rangle$. Since $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$, the probability of each result is $1/2$. When Charlie's measurement result is $|-\rangle$, her code is $R_A'^{(1)} = 1$ and $R_A'^{(1)} = R_A^{(1)}$. When Charlie's measurement result is $|+\rangle$, her code is $R_A'^{(1)} = 0$ and $R_A'^{(1)} \neq R_A^{(1)}$. Therefore, Charlie's probability of getting $R_A'^{(i)} = R_A^{(i)}$ is $\frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. For n long sequence $S_A = S_A^{(1)} S_A^{(2)} \cdots S_A^{(n)}$, the successful probability of her forgery attack is $(\frac{3}{4})^n$. If n approaches ∞, the value $(\frac{3}{4})^n$ approaches 0. Therefore, her identity forgery attack fails.

Unconditional security: The mutual authentication has used the hash function $H(x)$. The hash values are used to determine the measurement bases of Alice and Bob. In Step.3(c), Bob publishes the corresponding coding sequence R'_A after measuring the sequence S_A. However, an attacker cannot get Bob's measurement bases from the value R'_A. Because the coding rules stipulate that both $|0\rangle$ and $|+\rangle$ are coded as "0," both $|1\rangle$ and $|-\rangle$ are coded as "1." For the value $R'_A = 0000$, the sequence S_A is one of 16 cases. See Table 2 for details. Therefore, there are 16 kinds of possible measurement base sequences, which correspond to 16 kinds of different hash value sequences $\overline{K}'_{AB}$. Thus, the attacker does not know the hash values $\overline{K}'_{AB}$ ($\overline{K}'_{AB} = H(K_{AB}||r) = \overline{K}_{AB}$). So he

Table 2 The relationship among the hash value $\overline{K}'_{AB}$, the sequence S_A and the coding sequence R'_A

The hash value $\overline{K}'_{AB}$	The sequence S_A	The coding sequence R'_A
0000	$\|0\rangle, \|0\rangle, \|0\rangle, \|0\rangle$	0000
1000	$\|+\rangle, \|0\rangle, \|0\rangle, \|0\rangle$	0000
0100	$\|0\rangle, \|+\rangle, \|0\rangle, \|0\rangle$	0000
0010	$\|0\rangle, \|0\rangle, \|+\rangle, \|0\rangle$	0000
0001	$\|0\rangle, \|0\rangle, \|0\rangle, \|+\rangle$	0000
1100	$\|+\rangle, \|+\rangle, \|0\rangle, \|0\rangle$	0000
1010	$\|+\rangle, \|0\rangle, \|+\rangle, \|0\rangle$	0000
1001	$\|+\rangle, \|0\rangle, \|0\rangle, \|+\rangle$	0000
0101	$\|0\rangle, \|+\rangle, \|0\rangle, \|+\rangle$	0000
0011	$\|0\rangle, \|0\rangle, \|+\rangle, \|+\rangle$	0000
0110	$\|0\rangle, \|+\rangle, \|+\rangle, \|0\rangle$	0000
0111	$\|0\rangle, \|+\rangle, \|+\rangle, \|+\rangle$	0000
1011	$\|+\rangle, \|0\rangle, \|+\rangle, \|+\rangle$	0000
1101	$\|+\rangle, \|+\rangle, \|0\rangle, \|+\rangle$	0000
1110	$\|+\rangle, \|+\rangle, \|+\rangle, \|0\rangle$	0000
1111	$\|+\rangle, \|+\rangle, \|+\rangle, \|+\rangle$	0000

can't compute the secret identity information K_{AB}. In fact, our mutual authentication does not use the computational complexity security of hash function $H(x)$, such as one-way property and anti-collision property. For each identity authentication, we only use the information compression ability of hash function $H(x)$. Moreover, the hash value $\overline{K}'_{AB}$ ($\overline{K}_{AB}$) is different for each different r. Thus, our mutual authentication is still unconditionally secure.

3.2 Security analysis of key negotiation

Now, we show that the key negotiation is secure against both participant and external attacks.

First, we consider participant attacks. The secret key negotiation of this MAQKA protocol is realized by the entanglement exchange of Bell states. The entanglement exchange relations of Bell states ensure that the key negotiated by both parties are equal and random. Neither Alice nor Bob can change this randomness, so neither can control the shared key independently. That is, neither Alice nor Bob can successfully carry out the participant attack.

Second, we consider external attacks. The key agreement here also faces four types of attacks, including Trojan horse attacks, intercept-resend attack, measure-resend attack and entangle-measure attack [1, 2]. Since all the sequences in the channel are transmitted only once, this MAQKA protocol is naturally immune to two kinds of Trojan horse attacks [27, 28]. Moreover, there are decoy particles inserted in all transmission sequences. All the decoy particles are chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ which form two different orthogonal bases. These decoy states are used to

Table 3 Comparison between our MAQKA protocol and the existed MAQKA protocols

the MAQKA protocols	Quantum resource	Qubit efficiency (%) of key negotiation	Qubit efficiency (%) of the protocol
ZWL protocol[25]	GHZ-like states	25	8.33
MHLZ protocol[26]	five-qubit genuinely entangled states	7.7	6.67
our protocol	Bell states	33.33	16.67

detect channel security, which ensures the security of both the transmitted sequences S'_A and S'_B. That is, the security detection of Step.2 can find all the attacks such as intercept-resend attack, measure-resend attack and entangle-measure attack. The security detection probability can be referred to the references [1, 2]. On the other hand, the entanglement exchange of Bell states makes key negotiation free of information leakage [29].

Thus, the key negotiation of our MAQKA protocol is also unconditionally secure since it is also based on quantum mechanics principles [3, 30, 31].

3.3 Performance analysis

Then we discuss the performance of new MAQKA protocol which is mainly characterized by quantum bit efficiency $\eta = \frac{c}{q+b}$[32]. For the parameters c, q and b, they represent the shared key bits, the qubits and the classical bits for decoding the partial secret keys, respectively. If we only want to calculate the quantum bit efficiency of key negotiation phase, we may not consider the consumption of quantum states for identity mutual authentication. In our MAQKA protocol, the length of the shared key is $2m$, the number of Bell states used to negotiate the shared key is also $2m$ and the number of the classical bits is 0. When calculating the specific value of quantum bit efficiency, it can be assumed that the number of decoy states and transmitted particles is equal. Thus, there are also $2m$ decoy states and the qubit efficiency of our MAQKA protocol is $\eta = \frac{2m}{4m+2m} = \frac{1}{3} \approx 33.33\%$. When we want to calculate the quantum bit efficiency of the whole MAQKA protocol, the consumption of quantum states for identity mutual authentication is considered. There are $2n$ Bell states needed for identity mutual authentication in our MAQKA protocol. Similarly, we also assume that we need the same number of decoy states for the mutual authentication phase. Then the number of decoy states is also $2n$. So the qubit efficiency of our whole protocol is $\eta' = \frac{2m}{4(n+m)+2(n+m)}$. When n is equal to m, the qubit efficiency η' is equal to $1/6$, which is approximately 16.67%. In a similar way, we calculate the overall efficiency of the existing two MAQKA protocols. Compared with the existing MAQKA protocols (see Table 3), our MAQKA protocol has great advantages in qubit efficiency.

In the new MAQKA protocol, Bell states are used as quantum resource, which are easier to realize with the existing technology than three-particle entangled states [25] and five-particle entangled states [26]. For the measurement basis, our protocol uses the single-particle measurement basis and Bell basis to measure the corresponding quantum states. So its realizing difficulty of particle measurement is very close to that

of the existing two protocols. Because ZWL protocol [25] only uses single-particle measurements, MHLZ protocol [26] uses single-particle measurements and Bell measurements. Further, the implementation of this MAQKA protocol can be completed without the help of a trusted or semi-trusted third party, which makes its steps relatively simpler and it less communication traffic. Moreover, two participants of the MAQKA protocol only needs once quantum communication and fewer classical communication. However, both ZWL [25] and MHLZ [26] protocols require the participation of the third party to achieve mutual authentication and key negotiation. And MHLZ protocol [26] requires more quantum communication and classical communication.

4 Conclusion

Based on Bell states, we design a two-party MAQKA protocol which can realize mutual authentication and key negotiation without the participation of trusted or semi-trusted third party. Compared with the existing MAQKA protocols, the new MAQKA protocol not only reduces the complexity of its steps, but also reduces the communication between participants. It uses the secret identity information and the measurement correlation property of Bell states to realize mutual identity authentication. It uses the entanglement swapping property of Bell states to realize key negotiation. We also show that the new MAQKA protocol is unconditionally secure. More specifically, its identity authentication can resist forgery attacks; its key negotiation resist external attacks and participant attacks. Moreover, it has higher quantum bit efficiency. Therefore, it is more suitable for practical application.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 61802302) and the Basic Research Project of Natural Science of Shaanxi Province (Grant No. 2021JM-462).

Data Availability Statement All data supporting the findings of this study are available within the article.

References

1. He, Y.F., Ma, W.P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**, 3483–3498 (2015)
2. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**, 5023–5035 (2016)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International conference on computers, systems and signal Processing, Bangalore, India, pp. 175-179. (1984)
4. He, Y.F., Ma, W.P.: The decoy-state measurement-device-independent quantum key distribution with heralded single-photon source. Int. J. Theor. Phys. **59**, 908–917 (2020)
5. He, Y.F., Ma, W.P.: The enhanced measurement-device-independent quantum key distribution with heralded pair coherent state. Mod. Phys. Lett. B **34**, 2050063 (2020)
6. He, Y.F., Ma, W.P.: Measurement-device-independent quantum key distribution protocols against collective noise. Mod. Phys. Lett. B **35**, 2150195 (2021)
7. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149–1150 (2004)
8. Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information security conference (ISC 2004), pp. 236-242. National Taiwan University of Science and Technology, Taipei 10-11 June (2004)

9. Tsai, C.W., Hwang, T.: On "quantum key agreement protocol.". Taiwan. R.O.C, Technical Report, C-S-I-E, NCKU (2009)
10. 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 (CISC 2010), pp. 210-213. National Chiao Tung University, Hsinchu, 27-28 May (2010)
11. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
12. 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)
13. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with Bell states and Bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
14. 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)
15. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
16. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. **52**, 3915–3921 (2013)
17. Sun, Z.W., Zhang, C., Wang, B.H., Li, Q., Long, D.Y.: Improvements on "Multiparty quantum key agreement with single particles.". Quantum Inf. Process. **12**, 3411–3420 (2013)
18. 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)
19. 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)
20. Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process. **15**, 373–384 (2016)
21. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single-particle measurements. Quantum Inf. Process. **13**, 649–663 (2014)
22. He, Y.F., Ma, W.P.: Two quantum key agreement protocols immune to collective noise. Int. J. Theor. Phys. **56**, 328–338 (2017)
23. Das, A., Nandi, S., Sazim, S., Agrawal, P.: Resource state structure for controlled quantum key distribution. Eur. Phys. J. D. **74**, 91 (2020)
24. Zhou, N.R., Zhu, K.N., Wang, Y.Q.: Three-party semi-quantum key agreement protocol. Int. J. Theor. Phys. **59**, 663–676 (2020)
25. Zhu, H.F., Wang, C.N., Li, Z.X.: Semi-honest three-party mutual authentication quantum key agreement protocol based on GHZ-like state. Int. J. Theor. Phys. **60**, 293–303 (2021)
26. Ma, X.Y., Hur, J.B., Li, Z.X., Zhu, H.F.: Quantum mutual authentication key agreement scheme using five-qubit entanglement towards different realm architecture. Int. J. Theor. Phys. **60**, 1933–1948 (2021)
27. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
28. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
29. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Comment on: Three-party quantum secure direct communication based on GHZ states. Phys. Lett. A **372**, 3333–3336 (2008)
30. Xu, G.B., Jiang, D.H.: Novel methods to construct nonlocal sets of orthogonal product states in an arbitrary bipartite high-dimensional system. Quantum Inf. process. **20**, 128 (2021)
31. Wang, T.Y., Wang, X.X., Cai, X.Q., et al.: Analysis of efficient and secure dynamic quantum secret sharing protocol based on Bell states. Quantum Inf. Process. **20**, 7 (2021)
32. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000)