frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 25 March 2025
DOI 10.3389/fphy.2025.1563674

OPEN ACCESS

EDITED BY
Ming Yang,
Anhui University, China

REVIEWED BY
Tianyu Ye,
Zhejiang Gongshang University, China
Hao Cao,
Anhui Science and Technology University, China

*CORRESPONDENCE
Songfeng Lu,
lusongfeng@hust.edu.cn

†These authors have contributed equally to this work.

RECEIVED 20 January 2025
ACCEPTED 03 March 2025
PUBLISHED 25 March 2025

CITATION
Yang H, Yi Z, Lu S and Wang M (2025) Mutual authentication quantum key agreement protocol with single-particle measurement. *Front. Phys.* 13:1563674. doi: 10.3389/fphy.2025.1563674

Mutual authentication quantum key agreement protocol with single-particle measurement

Hao Yang[1†], Zepu Yi[1†], Songfeng Lu[1,2*] and Mu Wang[3]

[1]Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, China, [2]Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen, China, [3]The NanHua Affiliated Hospital, Clinical Research Institute, Hengyang Medical School, University of South China, Hengyang, China

In this paper, a mutual authentication quantum key agreement protocol with single-particle measurement is proposed. The participants can authenticate each other's identity through their secret identity information and the entanglement property of Bell states. After the authentication phase, the participants can negotiate a private key with equal contribution. We prove that the proposed scheme is unconditional security. In comparison to the previous mutual authentication quantum key agreement protocols, the proposed method utilizes Bell states as the quantum resource states in both the identity authentication and key agreement stages. It requires single-particle measurement without the need for Bell measurements or the involvement of trusted or semi-trusted other participants. Additionally, our proposed scheme demonstrates significant advantages in terms of qubit efficiency.

KEYWORDS

quantum cryptography, quantum key agreement, mutual authentication, unconditional security, bell states, single particle measurement

1 Introduction

As one of the important branches of cryptography, key agreement allows all the participants to contribute equally to generating a negotiated key, where any nontrivial subset cannot privately determine the negotiated key. Since the first key agreement protocol was proposed by Diffie and Hellman in 1976 [1], many key agreement protocols have been proposed [2–5]. However, with the rapid development of quantum computing and quantum computers, the classical cryptography schemes based on the complexity of mathematical algorithms will be seriously endangered. Different from classical cryptography, quantum cryptography is theoretically unconditionally secure. For this reason, quantum cryptography has garnered widespread attention from numerous cryptography researchers and has gradually evolved into a popular research direction in the field of cryptography.

Quantum cryptography encompasses various branches, such as quantum key distribution (QKD) [6–8], quantum key agreement (QKA) [9, 10], quantum secure direct communication (QSDC) [11–13], quantum secret sharing (QSS) [14, 15], quantum signature (QS) [16–18], quantum private query (QPQ) [19–21], quantum private comparison (QPC), [22–24]. Currently, quantum key agreement is a novel and highly significant research topic that has attracted considerable attention within the academic sphere.

In 2004, Zhou et al. [9], achieved the first QKA protocol by utilizing quantum teleportation, thereby pioneering the application of quantum technology in key negotiation. However, Tsai et al. [25] identified a critical flaw in Zhou et al.'s protocol, wherein a participant could unilaterally determine the shared key. Subsequently, in the same year, Hsueh et al. [26] proposed a QKA scheme using unitary operations and single photons. Nevertheless, Tsai et al. [27] pointed out that this scheme lacked sufficient security, as an attacker could acquire the shared key through controlled attacks without detection. In 2010, Chong et al. [10] successfully proposed an efficient two-party QKA protocol, building upon the foundation of the BB84 protocol. This QKA protocol primarily leverages unitary operations and delayed measurement techniques. Subsequently, numerous research efforts have been proposed to enhance the QKA protocol from various perspectives, such as multi-party QKA [28–32], improved communication efficiency [33–37], enhanced security [38, 39], and against noise environments [34, 40–44], semi-quantum capabilities [45–50].

However, the aforementioned QKA protocols lack the capability to authenticate the identities of the involved parties. In practical settings, attackers often attempt to impersonate participants to gain access to the shared key and carry out man-in-the-middle attacks on the QKA protocol. To counteract this attack, it is crucial to authenticate the identity of the key negotiators before the key establishment process, which holds significant importance for ensuring the security of the QKA protocol. In 2021, Zhu et al. [51] proposed a semi-honest three-party mutual authentication quantum key agreement (MAQKA) scheme based on three-particle entangled states, which requires a semi-honest third party to assist two key negotiators in achieving mutual authentication and key agreement. In the same year, Ma et al. [52] presented a MAQKA protocol based on five-particle entangled states, involving four participants and relying on two users to assist the other two users in achieving identity authentication and key agreement. However, this scheme exhibits relatively low qubit efficiency. In 2022, He et al. [53] presented a novel MAQKA protocol based on Bell states, which improves qubit efficiency and achieves the identity authentication and key agreement without relying on a trusted or semi-trusted third party.

In this paper, we propose a mutual authentication quantum key agreement protocol with single-particle measurement. The protocol utilizes Bell entangled states as the quantum source, enabling identity verification of participants before key agreement and against potential attacks. Compared to the previous MAQKA schemes, our proposed protocol has significant improvements in terms of quantum sources, auxiliary requirements from other participants, measurement bases, and qubit efficiency.

The rest of the paper is organized as follows. In Section 2, the proposed two-party mutual authentication quantum key agreement protocol is described in detail. In Section 3, we provide concrete examples. In Section 4, we analyze its security. In Section 5, we discuss the performance of our scheme and provide a conclusion.

2 The proposed mutual authentication quantum key agreement protocol

Two participants Alice and Bob want to authenticate their identity and negotiate a key. We assume that Alice and Bob need a secret identity information K_{AB} through a secure channel in advance [53–55]. Two hash functions $H_1(x)$ outputting m-bit value and $H_2(x)$ outputting n-bit value are used. The process is described as follows.

Step 1: Bell sates preparation and transmission. Alice prepares m + n Bell states all in $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where m denotes the number of the authentication particles, n denotes the number of the information particles. Alice records the first particles as qubit sequence $S_A = \{S_A^1, S_A^2, \ldots, S_A^{m+n}\}$, the second particles as qubit sequence $S_B = \{S_B^1, S_B^2, \ldots, S_B^{m+n}\}$. Alice randomly inserts some decoy states into the qubit sequence S_B. These particles form a new sequence S_{DB}, where the decoy states are random in the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Alice sends the qubit sequence S_{DB} to Bob, and keeps the qubit sequence S_A.

Step 2: Eavesdropping detection. After Bob received S_{DB}, Alice publishes the positions and the measurement bases of the decoy states. Bob measures the decoy states and publishes the results. Alice calculates the error rate and determines whether the quantum channel is safe or not. If the quantum channel is safe, the protocol continues. Otherwise, the protocol aborts.

Step 3: Mutual authentication. After the eavesdropping detection, the qubit sequence S_{DB} has been restored as the sequence S_B. For the qubit sequence S_A (S_B), we use the first m particles as the authentication sequence L_A (L_B) and the last n particles as the information particles R_A (R_B), where $L_A = \{L_A^1, L_A^2, \ldots, L_A^m\}$, $L_B = \{L_B^1, L_B^2, \ldots, L_B^m\}$, $R_A = \{R_A^1, R_A^2, \ldots, R_A^n\}$, $R_B = \{R_B^1, R_B^2, \ldots, R_B^n\}$. Bob generates two random numbers r_1, r_2 and publishes them. Alice and Bob calculate the value $K_{auth} = H_1(K_{AB} \| r_1)$, where $K_{auth} = \{K_{auth}^1, K_{auth}^2, \ldots, K_{auth}^m\}$, $K_{auth}^i \in \{0,1\}$, $i \in \{1,2,\ldots,m\}$. Then, according to the value of K_{auth}, Alice and Bob choose the measurement bases to measure the particles L_A and L_B. For the i-th particle L_A^i (L_B^i), if the value of $K_{auth}^i = 0$, Alice (Bob) chooses $Z = \{|0\rangle, |1\rangle\}$ to measure the particle L_A^i (L_B^i). If the value of $K_{auth}^i = 1$, Alice (Bob) chooses $X = \{|+\rangle, |-\rangle\}$ to measure the particle L_A^i (L_B^i). After measuring the particles L_A^i (L_B^i), Alice (Bob) obtains the measurement results L_{MA}^i (L_{MB}^i) and encodes the measurement results as L_{EA}^i (L_{EB}^i). If the measurement result of L_{MA}^i (L_{MB}^i) is 0 or $|+\rangle$, take the value of L_{EA}^i (L_{EB}^i) as 0. If the measurement result of L_{MA}^i (L_{MB}^i) is $|1\rangle$ or $|-\rangle$, take the value of L_{EA}^i (L_{EB}^i) as 1. Next, Alice announces the value of L_{EA}^i at the position corresponding to an odd number i, where $i \in \{1,2,\ldots,m\}$. Bob can judge whether Alice's identity is legal. Obviously, Alice's identity is correct when $L_{EA}^i = L_{EB}^i$. Otherwise, Alice' identity is illegal. Similarly, Bob announces the value of L_{EB}^j at the position corresponding to an even number j, where $j \in \{1,2,\ldots,m\}$. Alice can judge whether Bob's identity is legal. Obviously, Bob's identity is correct when $L_{EA}^j = L_{EB}^j$. Table 1 shows the process of the mutual authentication phase when the identities of Alice and Bob are legal.

Step 4: Key negotiation. After the mutual authentication phase, Alice and Bob negotiate a session key together. They calculate the value $K_{info} = H_2(K_{AB} \| r_2)$, where $K_{info} = \{K_{info}^1, K_{info}^2, \ldots, K_{info}^n\}$, $K_{info}^i \in \{0,1\}$, $i \in \{1,2,\ldots,n\}$. Then, according to the value of K_{info}, Alice and Bob choose

TABLE 1 The process of the mutual authentication phase when the identifies of Alice and Bob are legal.

The initialstate	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$
The value of K^i_{auth}	0	1	1	0	1	1	0	0
The chosen measurement basis of L^i_A	Z	X	X	Z	X	X	Z	Z
The measurement result L^i_{MA}	0	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	0
The value of L^i_{EA}	0	0	1	1	0	1	1	0
The chosen measurement basis of L^i_B	Z	X	X	Z	X	X	Z	Z
The measurement result L^i_{MB}	0	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	0
The value of L^i_{EB}	0	0	1	1	0	1	1	0
The correctness (Yes/No)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TABLE 2 The process of the key negotiation phase.

The initialState	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle$
The value of K^i_{info}	1	0	1	0	0	1	1	0
The chosen measurement basis of R^i_A	X	Z	X	Z	Z	X	X	Z
The measurement result R^i_{MA}	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	0	$\|+\rangle$	$\|-\rangle$	0
The chosen measurement basis of R^i_B	X	Z	X	Z	Z	X	X	Z
The measurement result R^i_{MB}	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	0	$\|+\rangle$	$\|-\rangle$	0
The value of K^i	1	1	0	1	0	0	1	0

the measurement bases to measure owned particles R_A and R_B. For the i-th particle R^i_A (R^i_B), if the value of $K^i_{info} = 0$, Alice (Bob) chooses $Z = \{|0\rangle, |1\rangle\}$ to measure the particle R^i_A (R^i_B). If the value of $K^i_{info} = 1$, Alice (Bob) chooses $X = \{|+\rangle, |-\rangle\}$ to measure the particle R^i_A (R^i_B). Obviously, there are four kinds of different measurement results $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ of R^i_A (R^i_B). For the measurement results R^i_{MA} (R^i_{MB}), Alice and Bob negotiate an encoding rule, that is, 0 and $|+\rangle$ correspond to 0, $|1\rangle$ and $|-\rangle$ correspond to 1. According to the encoding rule and the measurement results R^i_{MA}, R^i_{MB}, Alice and Bob can obtain the negotiated key $K = \{K^1, K^2, \ldots, K^n\}$. The key K is negotiated by both parties. Table 2 shows the process of the key negotiation phase.

As shown in Figure 1, the flowchart depicts the mechanism of the proposed protocol.

3 Examples

In this section, we provide concrete examples of our scheme to help readers better understand it. For simplicity, we have omitted the steps involved in eavesdropping detection.

Step 1: Bell states preparation and transmission. Alice prepares 16 Bell states all in $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + 11)$. Alice records the first particles as qubit sequence $S_A = \{S^1_A, S^2_A, \ldots, S^{16}_A\}$, the second particles as qubit sequence $S_B = \{S^1_B, S^2_B, \ldots, S^{16}_B\}$. Alice sends the qubit sequence S_B to Bob, and keeps the qubit sequence S_A.

Step 2: Mutual authentication. For the qubit sequence S_A (S_B), we use the particles $\{S^1_A, S^2_A, \ldots, S^8_A\}$ ($\{S^1_B, S^2_B, \ldots, S^8_B\}$) as the authentication sequence L_A (L_B) and the particles $\{S^9_A, S^{10}_A, \ldots, S^{16}_A\}$ ($\{S^9_B, S^{10}_B, \ldots, S^{16}_B\}$) as the information particles R_A (R_B), where $L_A = \{L^1_A, L^2_A, \ldots, L^8_A\}$, $L_B = \{L^1_B, L^2_B, \ldots, L^8_B\}$, $R_A = \{R^1_A, R^2_A, \ldots, R^8_A\}$, $R_B = \{R^1_B, R^2_B, \ldots, R^8_B\}$. Bob generates two random numbers r_1, r_2 and publishes them. Alice and Bob calculate the value $K_{\text{auth}} = H_1(K_{\text{AB}} \| r_1) = 01101100$. Then, according to the value of K_{auth}, Alice and Bob choose the measurement bases $ZXXZXXZZ$ to measure the particles L_A and L_B. After measuring the particles L_A (L_B), Alice (Bob) obtains the measurement results $L_{MA} = \{|0\rangle, |+\rangle, |-\rangle, |1\rangle, |+\rangle, |-\rangle, |1\rangle, |0\rangle\}$ ($L_{MB} = \{|0\rangle|, |+\rangle, |-\rangle, |1\rangle, |+\rangle, |-\rangle, |1\rangle, |0\rangle\}$) and encodes the measurement results as $L_{EA} = 00110110$ ($L_{EB} = 00110110$). Next, Alice announces the value of $L^1_{EA}L^3_{EA}L^5_{EA}L^7_{EA} = 0101$. Obviously, since $L^1_{EB}L^3_{EB}L^5_{EB}L^7_{EB} =$

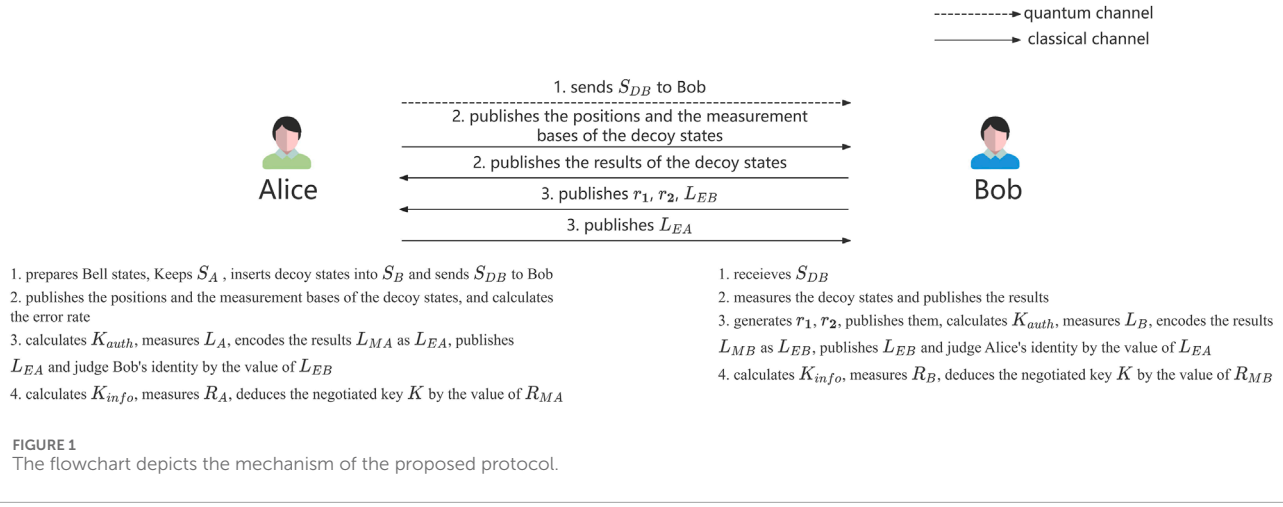

FIGURE 1
The flowchart depicts the mechanism of the proposed protocol.

$L^1_{EA}L^3_{EA}L^5_{EA}L^7_{EA} = 0101$, Bob can judge that Alice is legal. Similarly, Bob announces the value of $L^2_{EB}L^4_{EB}L^6_{EB}L^8_{EB} = 0110$. Since $L^2_{EA}L^4_{EA}L^6_{EA}L^8_{EA} = L^2_{EB}L^4_{EB}L^6_{EB}L^8_{EB} = 0110$, Alice can judge that Bob is legal.

Step 3: Key negotiation. After the mutual authentication phase, Alice and Bob negotiate a session key together. They calculate the value $K_{info} = H_2(K_{AB}\|r_2) = 10100110$. Then, according to the value of K_{info}, Alice and Bob choose the measurement bases $XZXZZXXZ$ to measure owned particles R_A and R_B. For the measurement results $R_{MA} = \{|-\rangle, |1\rangle, |+\rangle, |1\rangle, |0\rangle, |+\rangle, |-\rangle, |0\rangle\}$, Alice can obtain the negotiated key $K = 11010010$. Similarly, For the measurement results $R_{MB} = \{|-\rangle, |1\rangle, |+\rangle, |1\rangle, |0\rangle, |+\rangle, |-\rangle, |0\rangle\}$, Bob can obtain the negotiated key $K = 11010010$.

4 Security analysis

4.1 Security analysis of mutual authentication phase

We analyze the security of mutual authentication phase from the following aspects.

Correctness: According to the process of the mutual authentication, Alice (Bob) can judge that the identity of Bob (Alice) is legal. If the identities of Alice and Bob are correct, they must have K_{AB} and calculate the correct value of $K_{auth} = H_1(K_{AB}\|r_1)$. Then, they measure owned authentication parties L_A, L_B, and obtain the measurement results L_{MA}, L_{MB}. Alice and Bob encodes their measurement results and get L_{EA}, L_{EB}. According to the property of Bell state, the value must satisfy $L_{EA} = L_{EB}$ when the identities of Alice and Bob are correct. For examples, suppose that the initial prepared states are $S = \{|\varphi^+\rangle, |\varphi^+\rangle, |\varphi^+\rangle, |\varphi^+\rangle, |\varphi^+\rangle, |\varphi^+\rangle, |\varphi^+\rangle, |\varphi^+\rangle\}$. Alice holds the first qubit sequence $L_A = \{L^1_A, L^2_A, \ldots, L^8_A\}$, Bob holds the second qubit sequence $L_B = \{L^1_B, L^2_B, \ldots, L^8_B\}$. The hash value $K_{auth} = 01101100$, corresponding to the measurement bases $ZXXZXXZZ$. When the measurement results $L^1_A L^3_A L^5_A L^7_A = |0\rangle|-\rangle|+\rangle|1\rangle$, the corresponding encoding value $L^1_{EA}L^3_{EA}L^5_{EA}L^7_{EA} = 0101$. Alice publishes the value $L^1_{EA}L^3_{EA}L^5_{EA}L^7_{EA}$. As the measurement bases Bob selected are the same Alice, Bob's measurement results must satisfy $L^1_B L^3_B L^5_B L^7_B = |0\rangle|-\rangle|+\rangle|1\rangle$. Then, Bob gets the value $L^1_{EB}L^3_{EB}L^5_{EB}L^7_{EB} = 0101$, and judges Alice's identity is correct by $L^1_{EA}L^3_{EA}L^5_{EA}L^7_{EA} = L^1_{EB}L^3_{EB}L^5_{EB}L^7_{EB}$. Similarly, when the measurement results $L^2_B L^4_B L^6_B L^8_B = |+\rangle|1\rangle|-\rangle|0\rangle$, the corresponding encoding value $L^2_{EB}L^4_{EB}L^6_{EB}L^8_{EB} = 0110$. Bob publishes the value $L^2_{EB}L^4_{EB}L^6_{EB}L^8_{EB}$. According to the property of Bell state, Alice's measurement results must satisfy $L^2_A L^4_A L^6_A L^8_A = |+\rangle|1\rangle|-\rangle|0\rangle$. Then, Alice gets the value $L^2_{EA}L^4_{EA}L^6_{EA}L^8_{EA} = 0110$, and judges Bob's identity is correct by $L^2_{EB}L^4_{EB}L^6_{EB}L^8_{EB} = L^2_{EA}L^4_{EA}L^6_{EA}L^8_{EA}$.

Forgery attack: If charlie wants to disguise herself as Alice, she must get the correct value of L_{EA}. In order to get L_{EA}, she should obtain the measurement results L_{MA} of the particles L_A. However, she cannot get the right K_{auth} and choose the right measurement bases. For each particle of L_A, she can only randomly selects measurement basis $Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$, where the probability of each measurement basis is $\frac{1}{2}$. Continue to use the previous example, for the first particle L^1_A, L^1_B, the initial system state is $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + 11\rangle)$, $K^1_{auth} = 0$, the correct choosed basis is $Z = \{|0\rangle, |1\rangle\}$, the correct measurement results $L^1_{MA} = 0$, $L^1_{MB} = 0$ and the correct encoding value $L^1_{EA} = 0$, $L^1_{EB} = 0$. Form the aspect of Charlie, Charlie may choose the measurement basis $Z = \{0, 1\}$ to measurement the particle L^1_A with a probability of $\frac{1}{2}$, and obtain the correct measurement result 0 and the correct encoding value 0. Meanwhile, Charlie may choose the measurement basis $X = \{|+\rangle, |-\rangle\}$ to measurement the particle L^1_A with a probability of $\frac{1}{2}$. Since $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$, the probability of each result is $\frac{1}{2}$. When Charlie's measurement result is $|+\rangle$, she can obtain the correct encoding value 0. When Charlie's measurement result is $|-\rangle$, she can obtain the false encoding value 1. Thereby, for each particle, Charlie gets the correct encoding value is $\frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. Evidently, with the number of the authentication particles increases, the probability will converge to 0.

Unconditional security: In our scheme, the value of the hash function $H_1(x)$ is used to determine the measurement bases of Alice and Bob. In Step 3, Alice publishes the corresponding encoding value of L_{EA} after measuring the particles L_A. However, an attacker cannot obtain any useful information from L_{EA}. For example,

TABLE 3 The correlation among the encoding value L_{EA}, the hash value K_{auth}, the chosen measurement bases, the measurement results L_{MB}.

The encoding value L_{EA}	The value of K_{auth}	The chosen measurement bases	The measurement results L_{MB}
0110	0000	*ZZZZ*	$\|0\rangle\|1\rangle\|1\rangle\|0\rangle$
0110	0001	*ZZZX*	$\|0\rangle\|1\rangle\|1\rangle\|+\rangle$
0110	0010	*ZZXZ*	$\|0\rangle\|1\rangle\|-\rangle\|0\rangle$
0110	0011	*ZZXX*	$\|0\rangle\|1\rangle\|-\rangle\|+\rangle$
0110	0100	*ZXZZ*	$\|0\rangle\|-\rangle\|1\rangle\|0\rangle$
0110	0101	*ZXZX*	$\|0\rangle\|-\rangle\|1\rangle\|+\rangle$
0110	0110	*ZXXZ*	$\|0\rangle\|-\rangle\|-\rangle\|0\rangle$
0110	0111	*ZXXX*	$\|0\rangle\|-\rangle\|-\rangle\|1\rangle$
0110	1000	*XZZZ*	$\|+\rangle\|1\rangle\|1\rangle\|0\rangle$
0110	1001	*XZZX*	$\|+\rangle\|1\rangle\|1\rangle\|+\rangle$
0110	1010	*XZXZ*	$\|+\rangle\|1\rangle\|-\rangle\|0\rangle$
0110	1011	*XZXX*	$\|+\rangle\|1\rangle\|-\rangle\|+\rangle$
0110	1100	*XXZZ*	$\|+\rangle\|-\rangle\|1\rangle\|0\rangle$
0110	1101	*XXZX*	$\|+\rangle\|-\rangle\|1\rangle\|+\rangle$
0110	1110	*XXXZ*	$\|+\rangle\|-\rangle\|-\rangle\|0\rangle$
0110	1111	*XXXX*	$\|+\rangle\|-\rangle\|-\rangle\|+\rangle$

when $L_{EA} = 0110$, there are 16 kinds of possible hash value K_{auth}, which corresponds to 16 kinds of different measurement bases and measurement results L_{MB}, as shown in Table 3. Therefore, the attacker cannot know the hash value K_{auth} ($K_{auth} = H_1(K_{AB}\|r_1)$) and infer the private identity information K_{AB}. Actually, we merely use the information compression ability of the hash function $H_1(x)$, instead of the one-way property and anti-collision property of the hash function. Thereby, for each different random number r_1, the hash value K_{auth} is different. Thus, our mutual authentication scheme is still unconditional security.

4.2 Security analysis of key negotiation phase

In this part, we analyze the participant attacks and the external attacks.

The participant attacks: The private key negotiation of our scheme is realized by the property of Bell states. The entanglement characteristic of Bell states ensures that the key negotiated by both parties is equal and random. Neither Alice nor Bob can change this randomness, so neither of them can independently control the private key. That is, they cannot successfully launch this attack.

The external attacks: Here, we consider four kinds of external attacks, including Trojan horse attacks, intercept-resend attack, measure-resend attack, and entangle-measure attack. As all the quantum states are transmitted only once, our scheme is naturally immune to the invisible photon eavesdropping Trojan horse attack [56] and the delay-photon Trojan horse attack [57]. Furthermore, in our scheme, we employ decoy states to detect the channel security, thereby ensuring the security of the transmitted qubit sequence S_{DB}. By randomly selecting decoy states from two different orthogonal bases, our scheme enables the detection of all types of attacks, such as intercept-resend attack, measure-resend attack, and entangled-measure attack, during the eavesdropping detection in Step 2. The probability of security verification can be referenced from the reference [40]. Besides, as our scheme only publishes the encoding value, the entanglement property of Bell state ensures no information leakage in the key negotiation [58].

It should be noted that we use the information compression ability of the hash function $H_2(x)$ to determine the measurement bases of the information particles R_A, R_B. For each different random number r_2, the hash value K_{info} is different.

Thereby, the key negotiation of our scheme is unconditional security.

5 Discussions and conclusion

In this section, we discuss the performance of our scheme, and provide a conclusion.

TABLE 4 Comparison between our protocol and the previous MAQKA protocols.

The MAQKA protocols	Quantum resource states	Other participants (Yes/No)	Measurement bases	Qubit efficiency of key negotiation	Qubit efficiency of the protocol
Protocol [51]	GHZ-like states	Yes	Z basis, X basis	25%	8.33%
Protocol [52]	five-qubit entangled states	Yes	Z basis, X basis, Bell-basis	7.7%	6.67%
Protocol [53]	Bell states	No	Z basis, X basis, Bell-basis	25%	14.29%
Our protocol	Bell states	No	Z basis, X basis	25%	14.29%

As pointed in the reference [59], the qubit efficiency is defined as $\eta = \frac{f}{q+c}$, where f, q, c are the number of bits of the negotiated key, the consumed qubits, the classical bits needed for the classical communication, respectively. Suppose that the number of the decoy states is equal to the number of the transmitted qubits, and the length of pre-shared identity information K_{AB} is n. Here, we consider the qubit efficiency in two cases, one of which includes the authentication part, and the other does not. First, we consider the qubit efficiency without authentication phase. The length of the negotiated key is n, the number of the consumed decoy states is n, the number of the consumed Bell states is also n, and the number of the classical bits is n. We can obtain $f = n$, $q = 2n + n$, $c = n$. Therefore, the qubit efficiency of the key negotiation phase is $\eta = \frac{n}{2n+n+n} = \frac{1}{4} \approx 25\%$. Second, we consider the qubit efficiency including the authentication phase. The authentication phase consumes the number of m Bell states, and the number of m decoy states. Thereby, the qubit efficiency including the authentication phase is $\bar{\eta} = \frac{n}{2(m+n)+m+n+n}$. When n is the same as m, the qubit efficiency $\bar{\eta} \approx 14.29\%$. In comparison to the existing MAQKA protocol, as illustrated in Table 4, our MAQKA protocol demonstrates great advantages.

In our protocol, from the perspective of the quantum source, our scheme utilizes Bell states, which are easier to implement with existing technology compared to three-particle entangled states [51] and five-particle entangled states [52]. Unlike scheme [52] that necessitates the involvement of a trusted or semi-trusted third party, and scheme [52] that relies on the assistance of two additional participants, our approach does not require auxiliary support from other participants. Furthermore, our scheme only requires single-particle measurement (Z basis, X basis), without the need for Bell measurements as in schemes [52] and [53]. In terms of qubit efficiency, our scheme exhibits significant improvements compared to [51] and [52]. It is evident that our scheme is more feasible to implement in realistic scenarios.

In this paper, we propose a mutual authentication quantum key agreement protocol with single-particle measurement. By utilizing the secret identity information and the entanglement property of Bell states, our protocol enables mutual identity authentication to be realized. After the authentication phase, the participants can negotiate a private key with equal contribution. We prove that our scheme is unconditionally secure and can resist potential attacks. In contrast to the previous MAQKA schemes, our proposed protocol has significant improvements in terms of quantum sources, assistance requirements from other participants, measurement bases, and qubit efficiency.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

HY: Writing–original draft, Writing–review and editing. ZY: Writing–original draft, Writing–review and editing. SL: Writing–review and editing. MW: Writing–review and editing.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. This work is supported by the Major Research Plan of Hubei Province under Grant/Award NO. 2023BAA027; the Key Research & Development Plan of Hubei Province of China under Grant No. 2024BAB049 and the project of Science, Technology and Innovation Commission of Shenzhen Municipality of China under Grant No. GJHZ20240218114659027.

Acknowledgments

We are deeply grateful to all the authors for their steadfast guidance and support throughout the entire research process. Their valuable insights and encouragement are crucial in shaping the direction and quality of this research.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

References

1. Diffie W, Hellman M. New directions in cryptography. *IEEE Trans Inf Theor* (1976) 22:644–54. doi:10.1109/tit.1976.1055638

2. Steiner M, Tsudik G, Waidner M. CLIQUES: a new approach to group key agreement. In: *Proceedings of the 18th international conference on distributed computing systems*. Amsterdam, Netherlands (1998). p. 380–7. doi:10.1109/ICDCS.1998.679745

3. Steiner M, Tsudik G, Waidner M. Key agreement in dynamic peer groups. *IEEE Trans Parallel Distrib Syst* (2000) 11:769–80. doi:10.1109/71.877936

4. Pieprzyk J, Li CH. Multiparty key agreement protocols. *IEEE Proc Comput Digital Tech* (2000) 147:229–36. doi:10.1049/ip-cdt:20000531

5. Ateniese G, Steiner M, Tsudik G. New multiparty authentication services and key agreement protocols. *IEEE J Sel Areas Commun* (2000) 18(4):628–39. doi:10.1109/49.839937

6. Bennett CH, Brassard G. Quantum cryptography: public-key distribution and coin tossing. In: *Proceedings of IEEE international conference on computers. Systems and signal processing*. Bangalore, India (1984). p. 175–9.

7. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett* (1992) 68:3121–4. doi:10.1103/physrevlett.68.3121

8. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. *Phys Rev Lett* (2007) 99(14):140501. doi:10.1103/physrevlett.99.140501

9. Zhou N, Zeng G, Xiong J. Quantum key agreement protocol. *Electron Lett* (2004) 40(18):1149–50. doi:10.1049/el:20045183

10. Chong SK, Hwang T. Quantum key agreement protocol based on BB84. *Opt Commun* (2010) 283:1192–5. doi:10.1016/j.optcom.2009.11.007

11. Zhang W, Ding D-S, Sheng Y-B, Zhou L, Shi B-S, Guo G-C. Quantum secure direct communication with quantum memory. *Phys Rev Lett* (2017) 118(22):220501. doi:10.1103/physrevlett.118.220501

12. Panda SS, Yasir PA, Chandrashekar C. Quantum direct communication protocol using recurrence in k-cycle quantum walks. *Phys Rev A* (2023) 107(2):022611. doi:10.1103/physreva.107.022611

13. Hong YP, Zhou L, Zhong W, Sheng YB. Measurement-device-independent three-party quantum secure direct communication. *Quant Inform Process* (2023) 22:111. doi:10.1007/s11128-023-03853-1

14. Hillery M, Buek V, Berthiaume A. Quantum secret sharing. *Phys Rev A* (1999) 59:1829–34. doi:10.1103/physreva.59.1829

15. Senthoor K, Sarvepalli PK. Theory of communication efficient quantum secret sharing. *IEEE Trans Inf Theor* (2022) 68(5):3164–86. doi:10.1109/tit.2021.3139839

16. Gottesman D, Chuang I. Quantum digital signatures. *arXiv:quant-ph/0105032* (2001). doi:10.48550/arXiv.quant-ph/0105032

17. Collins RJ, Donaldson RJ, Dunjko V, Wallden P, Clarke PJ, Andersson E, et al. Realization of quantum digital signatures without the requirement of quantum memory. *Phys Rev Lett* (2014) 113:040502. doi:10.1103/physrevlett.113.040502

18. Yin HL, Fu Y, Chen ZB. Practical quantum digital signature. *Phys Rev A* (2016) 93:032316. doi:10.1103/physreva.93.032316

19. Giovannetti V, Lloyd S, Maccone L. Quantum private queries. *Phys Rev Lett* (2008) 100(23):230502. doi:10.1103/physrevlett.100.230502

20. Gao F, Qin SJ, Huang W, Wen QY. Quantum private query: a new kind of practical quantum cryptographic protocol. *Sci China Phys Mech Astron* (2019) 62(7):70301. doi:10.1007/s11433-018-9324-6

21. Yang H, Xiao M. Multi-user quantum private query. *Quan Inf. Process.* (2020) 19:253. doi:10.1007/s11128-020-02732-3

22. Yang YG, Cao WF, Wen QY. Secure quantum private comparison. *Phys Scr* (2009) 80(6):065002. doi:10.1088/0031-8949/80/06/065002

23. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A: Math Theor* (2009) 42(5):055305. doi:10.1088/1751-8113/42/5/055305

24. Geng MJ, Chen Y, Xu TJ, Ye TY. Single-state semiquantum private comparison based on bell states. *EPJ Quan Technol.* (2022) 9(36):36. doi:10.1140/epjqt/s40507-022-00156-9

25. Tsai C, Hwang T. On quantum key agreement protocol. Technical Report, C-S-I-E, NCKU, Taiwan ROC (2009)

26. Hsueh CC, Chen CY. Quantum key agreement protocol with maximally entangled states. In: *Proceedings of the 14th information security conference (ISC 2004)*. Taipei, Taiwan: National Taiwan University of Science and Technology (2004). p. 236â€–242.

27. Tsai CW, Chong SK, Hwang T. Comment on quantum key agreement protocol with maximally entangled states. In: *Proceedings of the 20th cryptology and information security conference (CISC 2010)*. Hsinchu, Taiwan: National Chiao Tung University (2010). p. 210–3.

28. Shi RH, Zhong H. Multi-party quantum key agreement with bell states and bell measurements. *Quan Inf Process* (2013) 12:921–32. doi:10.1007/s11128-012-0443-2

29. Xu GB, Wen QY, Gao F, Qin SJ. Novel multiparty quantum key agreement protocol with GHZ states. *Quan Inf Process* (2014) 13:2587–94. doi:10.1007/s11128-014-0816-9

30. Yang H, Lu S, Zhu J, Wu J, Zhou Q, Li T. A tree-type multiparty quantum key agreement protocol against collusive attacks. *Int J Theor Phys* (2023) 62:7. doi:10.1007/s10773-022-05265-w

31. Liu B, Gao F, Huang W, Wen Q. Multiparty quantum key agreement with single particles. *Quan Inf. Process.* (2013) 12(4):1797–805. doi:10.1007/s11128-012-0492-6

32. Sun Z, Yu J, Wang P. Efficient multi-party quantum key agreement by cluster states. *Quan Inf Process* (2016) 15:373–84. doi:10.1007/s11128-015-1155-1

33. He YF, Ma WP. Quantum key agreement protocols with four-qubit cluster states. *Quan Inf Process* (2015) 14:3483–98. doi:10.1007/s11128-015-1060-7

34. Yang YG, Li BR, Li D, Zhou YH, Shi WM. New quantum key agreement protocols based on Bell states. *Quan Inf Process* (2019) 18:322. doi:10.1007/s11128-019-2434-z

35. Yang YG, Gao S, Li D, Zhou YH, Shi WM. Two-party quantum key agreement over a collective noisy channel. *Quan Inf Process* (2019) 18:74. doi:10.1007/s11128-019-2187-8

36. Huang X, Zhang SB, Chang Y, Qiu C, Liu DM, Hou M. Quantum key agreement protocol based on quantum search algorithm. *Int J Theor Phys* (2021) 60:838–47. doi:10.1007/s10773-020-04703-x

37. Zhao XQ, Wan H, Li LZ. High-efficient quantum key agreement protocol with entanglement measure. *Int J Theor Phys* (2022) 61:183. doi:10.1007/s10773-022-05166-y

38. Zhu ZC, Hu AQ, Fu AM. Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. *Quan Inf. Process.* (2015) 14:4245–54. doi:10.1007/s11128-015-1110-1

39. Yang YG, Huang RC, Xu GB, Zhou YH, Shi WM, Li D. Measurement-device-independent quantum key agreement based on entanglement swapping. *Quan Inf Process* (2023) 22:438. doi:10.1007/s11128-023-04189-6

40. He YF, Ma WP. Two-party quantum key agreement against collective noise. *Quan Inf Process* (2016) 15:5023–35. doi:10.1007/s11128-016-1436-3

41. Gao H, Chen XG, Qian SR. Two-party quantum key agreement protocols under collective noise channel. *Quan Inf Process* (2018) 17:140. doi:10.1007/s11128-018-1910-1

42. Zhou YH, Wang MF, Shi WM, Yang YG, Zhang J. Two-party quantum key agreement against collective noisy channel. *Quan Inf Process* (2020) 19:100. doi:10.1007/s11128-020-2593-y

43. Li L, Zhou RG, Zhang XX. Three-party quantum key agreement protocol based on logical four-particle Cluster state to resist collective noise. *Quan Inf Process* (2023) 22:453. doi:10.1007/s11128-023-04206-8

44. Mu Q, Liu J, Wang Q, Li G, Sun W. Two-layer multiparty quantum key agreement protocol with collective detection. *Int J Theor Phys* (2024) 63:56. doi:10.1007/s10773-024-05564-4

45. Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quan Inf. Process.* (2017) 16:295. doi:10.1007/s11128-017-1736-2

46. Liu WJ, Chen ZY, Ji S, Wang HB, Zhang J. Multi-party semi-quantum key agreement with delegating quantum computation. *Int J Theor Phys* (2017) 56:3164–74. doi:10.1007/s10773-017-3484-6

47. Li HH, Gong LH, Zhou NR. New semi-quantum key agreement protocol based on high-dimensional single-particle states. *Chin Phys B* (2020) 29(11):110304. doi:10.1088/1674-1056/abaedd

48. Xu TJ, Gan ZG, Ye TY. Multiparty semiquantum key agreement with d-level single-particle states. *Physica A: Stat Mech its Appl* (2023) 625:128991. doi:10.1016/j.physa.2023.128991

49. Yi HM, Zhou RG, Xu RQ. Semi-quantum key agreement protocol using W states. *Int J Theor Phys* (2023) 62:212. doi:10.1007/s10773-023-05467-w

50. Hong WL, Bai CM, Zhang SJ, Liu L. Multiparty semi-quantum key agreement protocol based on multiparticle entangled states. *Laser Phys Lett* (2024) 21:125212. doi:10.1088/1612-202x/ad8cc5

51. Zhu H, Wang C, Li Z. Semi-honest three-party mutual authentication quantum key agreement protocol based on GHZ-like state. *Int J Theor Phys* (2021) 60:293–303. doi:10.1007/s10773-020-04692-x

52. Ma X, Hur J, Li Z, Zhu H. Quantum mutual authentication key agreement scheme using five-qubit entanglement towards different realm architecture. *Int J Theor Phys* (2021) 60:1933–48. doi:10.1007/s10773-021-04812-1

53. He YF, Pang Y, Di M. Mutual authentication quantum key agreement protocol based on Bell states. *Quan Inf Process* (2022) 21:290. doi:10.1007/s11128-022-03640-4

54. Zhang L, Han ZW, Ma QM, Li LL. Authenticated quantum key agreement based on cluster states against collective noise. *Phys Scr* (2024) 99:075104. doi:10.1088/1402-4896/ad514c

55. Zhang L, Han ZW, Li TH, Ma QY, Li LL. Authenticated multi-party quantum key agreement protocol based on cluster states. *Laser Phys* (2024) 34:095205. doi:10.1088/1555-6611/ad6d52

56. Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A* (2006) 351(12):23–5. doi:10.1016/j.physleta.2005.10.050

57. Li XH, Deng FG, Zhou HY. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys Rev A* (2006) 74:054302. doi:10.1103/physreva.74.054302

58. Gao F, Qin SJ, Wen QY, Zhu FC. Comment on: three-party quantum secure direct communication based on GHZ states. *Phys Lett A* (2008) 372:3333–6. doi:10.1016/j.physleta.2008.01.043

59. Cabello A. Quantum key distribution in the Holevo limit. *Phys Rev Lett* (2000) 85:5635–8. doi:10.1103/physrevlett.85.5635