Quantum key agreement protocols based on multi-particle entangled states

Guo Ji-Hong (1342440634@qq.com)
Sichuan Normal University

Jia-Xin Xie
Sichuan Normal University

Ming-Qiang Bai
Sichuan Normal University

Zhi-Wen Mo
Sichuan Normal University

Research Article

Keywords: Quantum key agreement, four-particle Ω states, six-particle entangled states, qubit e

Posted Date: April 20th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1404068/v1

Noname manuscript No.
(will be inserted by the editor)

Quantum key agreement protocols based on multi-particle entangled states

Ji-Hong Guo[1,2,3] · Jia-Xin Xie[1,2,3] · Ming-Qiang Bai[1,2,3] · Zhi-Wen Mo[1,2,3,*]

Received: date / Accepted: date

Abstract Multi-particle entanglement is an important physical resource in quantum information processing, and the larger the number of particles in the entangled states, the more quantum superiority it can show in quantum communication and quantum computing. This paper proposes two quantum key agreement protocols using Ω states and six-particle entangled states. Both protocols ensure that two participants can fairly establish a final key through the measurement correlation for multi-particle entangled states. Since the protocols only use Bell measurements and Z-basis measurements, they are more easily achieved using current technology. From the perspective of security analysis, the protocols can resist participant attacks and external attacks. Finally, compared with some exising quantum key agreement protocols, our protocols can achieve higher qubit efficiency.

Keywords Quantum key agreement · four-particle Ω states · six-particle entangled states · qubit efficiency

1 Introduction

Quantum cryptography is a promising new field. Different from classical cryptography, the security of quantum cryptography is not based on the complexity of mathematical problems, but the basic principles of quantum mechanics. Therefore, it is unconditionally safe in theory. At present, many differ-

✉ Zhi-Wen Mo
E-mail: mozhiwen@263.net

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

ent types of quantum cryptography protocols have been proposed, including quantum key distribution (QKD)[1–4], quantum secret sharing (QSS)[5–8], quantum secure direct communication (QSDC)[9–11] and quantum key agreement (QKA)[12, 13] etc. In the QKA protocols, each participant contributes equally to the common key, and no party can determine this common key alone until key agreement is completed. In quantum secure communication, temporary conversations and realize authentication in the network need to be established. QKA technology can solve these problems, making it possible to establish a common key in a complex quantum network. Thus, QKA has important significance in quantum cryptography.

Using quantum teleportation, Zhou et al. [12] proposed the first QKA protocol in 2004, which has attracted a lot of attention from scholars. However, Tsai et al. [14] thought it cannot be called a fair QKA protocol because dishonest participants can decide the shared keys independently. In 2010, using the well known BB84 protocol, a successful two-party QKA protocol was proposed by Chong et al. [15], which can achieve high qubit efficiency through unitary transformation and delay measurement technology. Later, many QKA protocols[13, 16–18] have been proposed. But most of the above protocols are based on single particles or Bell states. In fact, multi-particle entangled states have more general composition and properties than single particles or Bell states, and are an indispensable and important resource for quantum information science towards applications. Therefore, many QKA protocols that exploit the entanglement of multi-particle have been proposed one after another recently. For example, using four-particle cluster states, a more efficient QKA protocol was designed by Shen et al. [19] in 2014. Then, He and Ma[20] put forward a two-party QKA protocol based on four-particle cluster states. Unfortunately, these protocols often need to pay a high price in the measurement of quantum states. For example, the protocols of both He et al. [20] and Shen et al. [21] use measurement basis of four-particle clusters, which are difficult to implement based on current technology.

In order to solve the problem of excessive measurement difficulty of QKA protocol using multi-particle entanglement, this paper proposes two new QKA protocols utilizing Ω states and six-particle entangled states, respectively. The new QKA protocols only use Bell measurements and single-particle measurements, it is easier to implement. Compared with the existing QKA protocols exploiting multi-particle entanglement correlations, our protocols are more efficient. Moreover, security analysis proves our protocols can resist participant attacks and external attacks.

The rest of the article is structured as follows. Section 2 describes some basics and specific steps of the protocols, and shows the negotiation process in the form of a graph. In Section 3, which mainly proves the security of the protocols. The qubit efficiency of the protocols is calculated in Section 4. Finally, in Section 5, the summarize and a short outlook is given.

2 Two QKA protocols based on Ω states and six-particle entangled states

2.1 A QKA protocol based on Ω states

Firstly, some basics will be drawn out. The four Pauli operators are represented as the following four forms of U-operations. $U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_{01} = |0\rangle\langle 1| + |1\rangle\langle 0|$, $U_{10} = |0\rangle\langle 0| - |1\rangle\langle 1|$, $U_{11} = |0\rangle\langle 1| - |1\rangle\langle 0|$. The four Bell states are defined as follows: $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The initial Bell states will change when $U_{i_1 i_2}(i_1, i_2 = 0, 1)$ operations are applied to the second particle of Bell states, and the transformation between the four Bell states and the corresponding U operations is shown in **Table** 1.

Table 1 Transformation between the four U-operations and the four Bell states

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

In this protocol, the following four-particle entangled Ω[22] state is used as the quantum source, that is

$$\begin{aligned} |\Omega\rangle_{1234} =& \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)_{1234} \\ =& \frac{1}{\sqrt{2}}(|0\rangle_1|\phi^+\rangle_{23}|0\rangle_4 + |1\rangle_1|\phi^-\rangle_{23}|1\rangle_4). \end{aligned} \tag{1}$$

According to Eq.(1), when we measured with Bell basis for particles 2 and 3 and with Z basis for particles 1 and 4, respectively. The state $|\Omega\rangle_{1234}$ will collapse to states $|0\rangle_1|\phi^+\rangle_{23}|0\rangle_4$, $|1\rangle_1|\phi^-\rangle_{23}|1\rangle_4$ with the probability $\frac{1}{2}$, respectively.

Alice and Bob randomly generate $2n$ bits of key information:

$$K_A = K_A^1 \| K_A^2 \| \ldots \| K_A^n,$$

$$K_B = K_B^1 \| K_B^2 \| \ldots \| K_B^n,$$

where $K_A^i, K_B^i \in \{00, 01, 10, 11\}$, $i = 1, 2, \ldots, n$, and $\|$ is the concatenation symbol. Negotiated common key $K = (K_A^1 \| K_B^1) \| (K_A^2 \| K_B^2) \| \ldots \| (K_A^n \| K_B^n)$. The negotiation steps are as follows.

Step 1 Alice prepares n $|\Omega\rangle_{1234}$ states and divides all particles into four sequences S_1, S_2, S_3 and S_4, where S_i corresponds to the sequence consisting of the i-th particle in all $|\Omega\rangle_{1234}$ states, respectively. To perform the first security detection, Alice randomly selects enough decoy particles from particles

$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to insert into the sequences S_1, S_4 and obtains sequences S_1^*, S_4^*. Then, Alice sends S_1^* and S_4^* to Bob and retains sequences S_2 and S_3.

Step 2 When Bob obtains sequences S_1^* and S_4^*, Alice tells Bob where the decoy particles are located in the sequences, and the measurement basis needed to measure them. Then, Bob uses the X-basis or Z-basis to measure the corresponding decoy particles and tells Alice his measurements. Based on these measurements and the initial states of the corresponding decoy particles, Alice is able to calculate the error rate between them. Since Alice and Bob set a suitable threshold in advance, Alice compares the error rate calculated above with this threshold. If the difference is within a certain range, it indicates that the protocol is in a safe condition. Otherwise, the protocol is terminated and restarted.

Step 3 After security detection, Bob discards the decoy states and returns to sequences S_1 and S_4. For the particles in the sequences S_2 and S_3, Alice uses Bell basis to measure, while for the particles in S_1 and S_4, Bob also uses the Z-basis to measure. According to Bob's measurements of the particles in the sequences S_1 and S_4, Alice and Bob can specify the corresponding coding rules: $|00\rangle \to 00$, $|01\rangle \to 01$, $|10\rangle \to 10$, $|11\rangle \to 11$. After their measurements of Ω states, Alice knows Bob's measurement result $H_B = H_B^1 \| H_B^2 \| \ldots \| H_B^n$, $H_B^i \in \{00, 01, 10, 11\}$, where H_B^i corresponds to each of Bob's measurements, respectively. Also, Bob knows the form of the Bell states that Alice possesses.

Step 4 Alice encodes her key $K_A^i (i = 1, 2, \ldots, n)$ into a series of operators $U_{i_1 i_2}$ that act on the $i - th$ particle in the sequence S_3, then obtains the sequence S_3^*, where the subscripts $i_1 i_2$ corresponds to the values of $K_A^i (i = 1, 2, \ldots, n)$. Then, in order to prevent arbitrary external eavesdroppers from knowing the true order of the sequence S_2, Alice performs a permutation operation $\prod_n$ on S_2 to obtain a randomized sequence S_2^*. Alice randomly selects enough decoy particles from particles $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to insert into the sequences S_2^*, S_3^* and obtains sequences S_2^{**}, S_3^{**}. Finally, she sends S_2^{**} and S_3^{**} to Bob.

Step 5 After Bob receives sequences S_2^{**} and S_3^{**}, Alice and Bob perform the second security testing. The second security testing is the same as the first security testing. If the difference is within a certain range, it indicates that the protocol is in a safe condition. Otherwise, the protocol is terminated and restarted.

Step 6 Bob publicly announces to Alice that the value of H_B^*, where $H_B^* = K_B \oplus H_B = (K_B^1 \| H_B^1) \oplus (K_B^2 \| H_B^2) \oplus \ldots \oplus (K_B^n \| H_B^n)$. Since the value of H_B^* is known, Alice is able to obtain the final key by calculating $K = K_A \oplus H_B^* \oplus H_B$.

Step 7 After Alice and Bob ending their two security detection, Alice publicly announces the permutation operation $\prod_n$. In order to obtain the sequence S_2, Bob only needs to perform a inverse operation $\prod_n^*$ on sequence S_2^*. Then Bob uses the Bell basis to measure the corresponding particles, and based on the measurements and the initial Bell states constituted by the particles in the sequences S_2 and S_3. Bob is able to infer the $U_{i_1 i_2}$ operator used, and can calculate K_A and K.

2.2 A QKA protocol based on six-particle entangled states

The six-particle entangled state[23] used in the protocol is depicted as:

$$
\begin{aligned}
|\Psi\rangle_{123456} =& \frac{1}{\sqrt{32}}[|000000\rangle + |111111\rangle + |000011\rangle + |111100\rangle + |000101\rangle \\
&+ |111010\rangle + |000110\rangle + |111001\rangle + |001001\rangle + |110110\rangle \\
&+ |001111\rangle + |110000\rangle + |010001\rangle + |101110\rangle + |010010\rangle \\
&+ |101101\rangle + |011000\rangle + |100111\rangle + |011101\rangle + |100010\rangle \\
&- (|001010\rangle + |110101\rangle + |001100\rangle + |110011\rangle + |010100\rangle \\
&+ |101011\rangle + |010111\rangle + |101000\rangle + |011011\rangle + |100100\rangle \\
&+ |011110\rangle + |100001\rangle)]_{123456} \\
=& \frac{1}{2}(|\phi^-\rangle_{16}|\phi^+\rangle_{25}|\phi^-\rangle_{34} + |\psi^-\rangle_{16}|\phi^-\rangle_{25}|\psi^+\rangle_{34} \\
&+ |\phi^+\rangle_{16}|\psi^-\rangle_{25}|\psi^-\rangle_{34} + |\psi^+\rangle_{16}|\psi^+\rangle_{25}|\phi^+\rangle_{34}).
\end{aligned} \tag{2}
$$

According to Eq.(2), when we perform Bell measurements on particles 1, 6; 2, 5; 3, 4 in the state $|\Psi\rangle_{123456}$, respectively, the state $|\Psi\rangle_{123456}$ will collapse to $|\phi^-\rangle_{16}|\phi^+\rangle_{25}|\phi^-\rangle_{34}$, $|\psi^-\rangle_{16}|\phi^-\rangle_{25}|\psi^+\rangle_{34}$, $|\phi^+\rangle_{16}|\psi^-\rangle_{25}|\psi^-\rangle_{34}$, $|\psi^+\rangle_{16}|\psi^+\rangle_{25}|\phi^+\rangle_{34}$ with probability $\frac{1}{4}$, respectively.

Similar to the first protocol, Alice and Bob agree on the following steps in order to get a shared key K.

Step 1 Firstly, Alice prepares n six-particle entangled states $|\Psi\rangle_{123456}$ and divides them into six sequences $S_i (i = 1, 2, \ldots, 6)$, where S_i corresponds to the sequence consisting of the i-th particle in all $|\Psi\rangle_{123456}$ states. Alice randomly selects enough decoy particles from particles $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to insert into the sequences S_3, S_4 and obtains sequences S_3^*, S_4^*. Then Alice sends S_3^* and S_4^* to Bob and retains sequences S_1, S_6 and S_2, S_5.

Step 2 When Bob receives sequences S_3^* and S_4^*, Alice tells Bob where the decoy particles are located in the sequences, and the measurement basis are needed to measure them. As with **Step** 2 of the previous protocol, if the difference is within a certain range, it indicates that the protocol is in a safe condition. Otherwise, the protocol is terminated and restarted.

Step 3 After security detection, Bob discards the decoy states and returns to sequences S_3 and S_4. For the particles in the sequences S_1, S_6 and S_2, S_5, Alice uses Bell basis to measure, while for the particles in sequences S_3 and S_4, Bob also uses the Bell basis to measure. According to Bob's measurements of the particles in the sequences S_3 and S_4, Alice and Bob can specify the corresponding coding rules: $|\phi^+\rangle_{34} \to 00$, $|\phi^-\rangle_{34} \to 01$, $|\psi^+\rangle_{34} \to 10$, $|\psi^-\rangle_{34} \to 11$. After their measurements of the $|\Psi\rangle_{123456}$ states, Alice knows Bob's measurement result $H_B = H_B^1 \| H_B^2 \| \ldots \| H_B^n$, $H_B^i \in \{00, 01, 10, 11\}$, where H_B^i corresponds to each of Bob's measurements, respectively. Also, Bob knows that the initial Bell states consisting of the particles in the sequences S_1, S_6 and S_2, S_5, respectively.

Step 4 Alice encodes her key $K_A^i (i = 1, 2, \ldots, n)$ into a series of operators $U_{i_1 i_2}$ that act on the i^{th} particle in the sequence S_6 to obtain the sequence S_6^*. The subscripts $i_1 i_2$ corresponds to the values of $K_A^i (i = 1, 2, \ldots, n)$. Then, in order to prevent arbitrary external eavesdroppers from knowing the true order of the sequence S_1, Alice performs a operation $\prod_n$ on S_1 to obtain a new sequence S_1^*. Then, Alice selects enough decoy particles from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts sequences S_1^* and S_6^* to obtain two new sequences S_1^{**} and S_6^{**}. Finally, she sends two sequences S_1^{**} and S_6^{**} to Bob.

Step 5 After Bob receives sequences S_1^{**} and S_6^{**}, As with **Step** 5 of the previous protocol. The second security testing is the same as the first security testing. If the detection result is within the initially specified threshold, the protocol continues. Otherwise, the protocol fails and starts over.

Step 6 Similar to **Step** 6 of the previous protocol, Alice gets the final shared key by a simple heterogeneous operation, i.e. $K = K_A \oplus H_B \oplus K_B^*$.

Step 7 After the second security detection, Alice publicly announces the permutation operation $\prod_n$. In order to obtain the sequence S_1, Bob only needs to perform the inverse operation $\prod_n^*$ on sequence S_1^*. Next, for the particles in sequences S_1 and S_6^*, Bob uses the Bell basis to measure the corresponding particles, and compares the measurement results and the initial Bell states constituted by the particles in the sequences S_1 and S_6. Bob can deduce K_A and calculate the shared key K.

For convenience, **Fig.** 1 mainly shows the transmission process between Alice and Bob in both protocols.

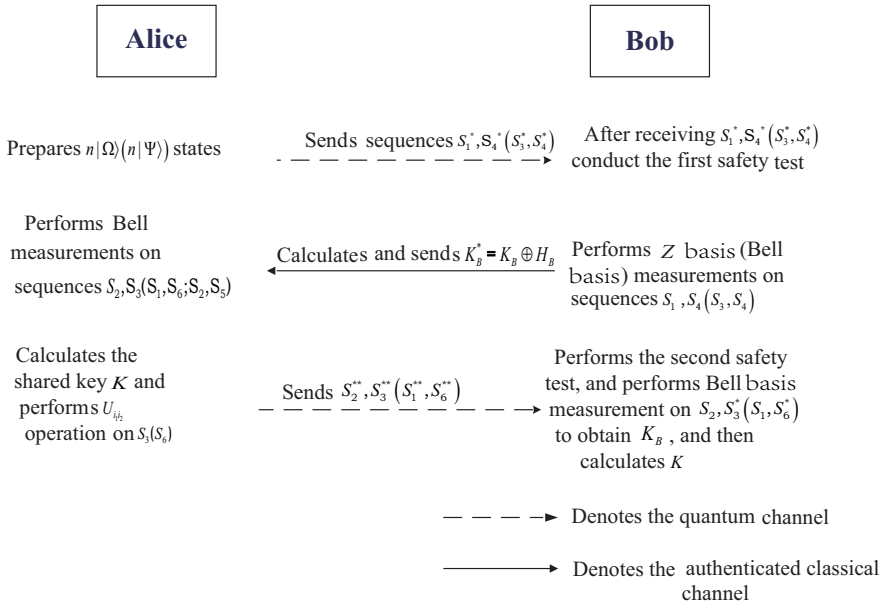

Fig. 1 The specific process of quantum key agreement between the two parties

3 Security Analysis

For the QKA protocol, it is essential to discuss its security. The QKA protocol mainly involves two kinds of attacks, which are participant attacks and outsider attacks. Participant attacks are mainly the impact on protocol security caused when Alice and Bob are dishonest during communication, respectively. The outsider attacks are some attacks that a malicious eavesdropper Eve performs in order to steal useful information. These attacks are divided into intercept-resend attack, trojan-horse attack, measure-resend attack, and entangle-measure attack. In this section, taking the first protocol as an example, the details are discussed below.

Participant attacks

When Alice is a dishonest participant, he only can modify K_A according to K_B. Since K_A is encrypted by $U_{i_1 i_2}$ operation and sent to Bob, Alice can know Bob's key K_B. So Alice cannot modify K_A optionally. Therefore, Alice cannot decide on this shared key K alone. When Bob is an illegitimate participant, Bob is able to obtain Alice's key by measurement. According to the principle of measurement[24], Bob can decode Alice's key only after he has declared his own key. Thus, Bob cannot modify his key K_B according to K_A. In a word, both Alice and Bob are able to resist participant attacks.

Trojan-horse attack

These two protocols are two separate one-way QKA protocols. All particles are transmitted only once in the channels, so the trojan-horse attacker Eve cannot steal useful information from the particles sequences. In other words, both protocols are resistant to this attack.

Intercept-resend attack

When Eve is an external eavesdropper who wants to perform an intercept-resend attack, he intercepts S_1^* and S_4^* firstly, then sends the prepared sequences to Bob. However, Eve does not know the location of decoy particles and measurement basis used in the sequences S_1^* and S_4^*. So the sequences intercepted by Eve cannot successfully pass the first security detection. Similarly, when Eve intercepts S_2^{**} and S_3^{**}, his malicious behavior will also be found in the second security detection. It is easy to conclude that the probability of an Eve attack being detected is $1-\frac{1}{2^m}$, where m refers to the number of decoy particles used in each security detection. With the increasing of the value of m, the probability of Eve being found approaches to 1.

Measure-resend attack

When the particles in the sequences S_1^*, S_4^*, S_2^{**} and S_3^{**} are attacked by Eve. Before the eavesdropping detection, Eve does not know which particles belong to the decoy particles and which belong to the initial particles in the sequences, and the measurement basis used. Thus, the measurement of Eve will affect the status of decoy particles in S_1^*, S_4^*, S_2^{**} and S_3^{**}. When Eve performs an attack, he has a probability of $\frac{1}{2}$ to choose either the X basis or the Z basis. Assuming he chooses the Z basis to measure the particles $|+\rangle$, $|-\rangle$, he will have a probability of $\frac{1}{4}$ to succeed. Thus, in the first and second

security tests, Eve attacks fail with probability $1-(\frac{3}{4})^m$, where m denotes the number of decoy particles used in the detection.

Entangle-measure attack

When Eve has entangled the transport particles in the sequences S_1^*, S_4^*, S_2^{**} and S_3^{**}, then the transport particles are sent to Alice. When the protocol is over, the corresponding auxiliary particles can be measured to extract useful information. However, all decoy particles are randomly inserted and this behavior of Eve will be acted on some decoy particles. Eve's unitary operation $\widehat{U}$ should satisfy

$$\widehat{U}(|0\rangle|E\rangle) = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \tag{3}$$

$$\widehat{U}(|1\rangle|E\rangle) = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle \tag{4}$$

$$\begin{aligned}\widehat{U}(|+\rangle|E\rangle) =& \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle + c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle)\\ =& \frac{1}{2}[|+\rangle(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle + c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle)+\\ & |-\rangle(a|0\rangle|e_{00}\rangle - b|1\rangle|e_{01}\rangle + c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle)]\end{aligned} \tag{5}$$

$$\begin{aligned}\widehat{U}(|-\rangle|E\rangle) =& \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle - c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle)\\ =& \frac{1}{2}[|+\rangle(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle - c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle)+\\ & |-\rangle(a|0\rangle|e_{00}\rangle - b|1\rangle|e_{01}\rangle - c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle)].\end{aligned} \tag{6}$$

In Eq.(3)-(6), where a, b, c, d are the complex coefficients of the corresponding states, and they must satisfy $|a|^2+|b|^2=1$, $|c|^2+|d|^2=1$. To avoid introducing errors, the unitary operation $\widehat{U}$ in Eq. (3)-(6) satisfy the following two conditions: $b=c=0$, $a=d=1$. However, when the above conditions are satisfied, there is $|e_{00}\rangle = |e_{11}\rangle$. At this point, since Eve is unable to distinguish $|e_{00}\rangle$ and $|e_{11}\rangle$, Eve can't get the useful information by observing auxiliary particles. Therefore, Eve cannot successfully perform entangle-measure attack.

4 Efficiency Analysis

In QKA protocol, Cabello's[25] method is used to evaluate qubit efficiency which is defined as

$$\eta = \frac{c}{q+b} \tag{7}$$

, where c is the length of the shared key generated by Alice and Bob, q is the number of qubits used in the whole protocol, and b is the number of classical bits used by Bob to decode Alice's key. In the first (second) QKA protocol proposed, the number of classical bits negotiated is $c=4n$, and the total

number of qubits used in the protocol is $q = 4n+2m+2m$ ($q = 6n+2m+2m$). Bob decodes Alice's key by U-transformations, so the value of b is $2n$. Based on the above analysis, the qubit efficiency of these two protocols are as follows: $\eta_1 = \frac{4n}{4n+2m+2m+2n}$ ($\eta_2 = \frac{4n}{6n+2m+2m+2n}$). In general, when $m = n$, $\eta_1 = \frac{2}{5} = 40\%$, $\eta_2 = \frac{4}{12} = 33.33\%$, The comparison between our protocols and some other QKA protocols is shown in the **Table** 2. Obviously, these two protocols have higher qubit efficiency.

Table 2 Comparison of our protocols and some exising QKA protocols

QKA protocol	Quantum resource	Measurement basis	Efficiency
Chitra's[17]	Bell states	Bell basis	14.29%
Huang's[18]	Bell states	Single particles	25.00%
He's[20]	Four-particle cluster states	Single particles	26.67%
Shen's[21]	Four-particle cluster states	Single particles	33.33%
He's[26]	GHZ states	Bell basis and single particles	33.33%
Yang's[27]	Four-particle cluster states	Cluster basis	30.77%
Ours 1	Four-qubit states	Bell basis and single particles	40.00%
Ours 2	Six-qubit states	Bell basis	33.33%

5 Conclusion

It has been a challenge to design efficient QKA protocols using multi-particle entangled states. In this manuscript, by using Ω states and six-particle entangled states, two new QKA protocols are proposed respectively. By comparing with other QKA protocols that utilize multi-particle entangled states, our QKA protocols only use Bell measurements and Z basis measurements, which are easy to implement based on the existing technology. Security analysis demonstrates that our protocols are resistant to participant attacks and external attacks. The qubit efficiency of these two protocols is also analyzed. The efficiency of the first protocol is up to 40% and the second one up to 33.33%, which is higher than currently proposed QKA protocols. The protocols in this paper are secure only on the ideal channel, however, they are not immune to interference from noise. The errors introduced by noise still reduce the information transmission efficiency of the protocol. Thus, the design of QKA protocol under noise channel has great research significance. At present, some anti-noise protocols[28–31] have been proposed one after another, but these protocols are inefficient. Therefore, how to design noise-immune and efficient QKA protocols may be an important direction we should consider in the future.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No.11671284), Sichuan Science Foundation and Technology Program (Grant No.2020YFG0290).

Author contributions
In fact, all of the authors' contributions to this paper are important. The specific contributions are as follows. The first author played a major role in the conceptualization and writing of the article. The second author worked mainly on the overall framework and language of the article. The third and fourth authors mainly guided the article in terms of its core ideas and expertise.

Data availability
The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

1. T.Y. Wang, Q.Y. Wen, X.B. Chen, Optics Communications **283**(24), 5261 (2010). DOI https://doi.org/10.1016/j.optcom.2010.07.022. URL https://www.sciencedirect.com/science/article/pii/S0030401810007583
2. C.W. Tsai, S.K. Chong, T. Hwang, Optics Communications **283**(24), 5285 (2010). DOI https://doi.org/10.1016/j.optcom.2010.07.076. URL https://www.sciencedirect.com/science/article/pii/S0030401810008345
3. F.G. Deng, G.L. Long, Physical Review A **68**, 042315 (2003). DOI 10.1103/PhysRevA.68.042315. URL https://link.aps.org/doi/10.1103/PhysRevA.68.042315
4. M. Bourennane, A. Karlsson, G. Björk, Physical Review A **64**, 012306 (2001). DOI 10.1103/PhysRevA.64.012306. URL https://link.aps.org/doi/10.1103/PhysRevA.64.012306
5. L. Xiao, L.G. Lu, F.G. Deng, J.W. Pan, Physical Review A **69**, 052307 (2004). DOI 10.1103/PhysRevA.69.052307. URL https://link.aps.org/doi/10.1103/PhysRevA.69.052307
6. C.R. Hsieh, T. Hwang, Communications in Theoretical Physics **54**(6), 1019 (2010). DOI 10.1088/0253-6102/54/6/13. URL https://doi.org/10.1088/0253-6102/54/6/13
7. Y.G. Yang, Y. Wang, H.P. Chai, Y.W. Teng, H. Zhang, Optics Communications **284**(13), 3479 (2011). DOI https://doi.org/10.1016/j.optcom.2011.03.017. URL https://www.sciencedirect.com/science/article/pii/S0030401811002884
8. Y.M. Li, K.S. Zhang, K.C. Peng, Physics Letters A **324**(5/6), 420 (2004). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=12778221&lang=zh-cn&site=ehost-live
9. X.R. Yin, W.P. Ma, W.Y. Liu, D.S. Shen, Quantum Information Processing **12**(9), 3093 (2013). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=89518916&lang=zh-cn&site=ehost-live
10. F.L. Yan, X.Q. Zhang, European Physical Journal. B, Condensed Matter **41**(1), 75 (2004). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=14665042&lang=zh-cn&site=ehost-live
11. J. Wang, Q. Zhang, C. Tang, Physics Letters A **358**(4), 256 (2006). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=22219063&lang=zh-cn&site=ehost-live
12. N. Zhou, G. Zeng, J. Xiong, Electronics Letters (Institution of Engineering & Technology) **40**(18), 1149 (2004). URL https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14329439&lang=zh-cn&site=ehost-live
13. S.K. Chong, C.W. Tsai, T. Hwang, International Journal of Theoretical Physics **50**(6), 1793 (2011). DOI 10.1007/s10773-011-0691-4. URL https://doi.org/10.1007/s10773-011-0691-4
14. C.W. Tsai, S.K. Chong, T. Hwang, Nephron Clinical Practice pp. 47–49 (2010)
15. S.K. Chong, T. Hwang, Optics Communications **283**(6), 1192 (2010). DOI https://doi.org/10.1016/j.optcom.2009.11.007. URL https://www.sciencedirect.com/science/article/pii/S0030401809011316

16. R.H. Shi, H. Zhong, Quantum Information Processing **12**(2), 921 (2013). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=84695721&lang=zh-cn&site=ehost-live
17. S. Chitra, A. Nasir, P. Anirban, Quantum Information Processing **13**(11), 2391 (2014). DOI 10.1007/s11128-014-0784-0. URL https://doi.org/10.1007/s11128-014-0784-0
18. W. Huang, Q.Y. Wen, B. Liu, F. Gao, Y. Sun, Quantum Information Processing **13**(3), 649 (2014). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=94231656&lang=zh-cn&site=ehost-live
19. S.S. Wang, G.B. Xu, X.Q. Liang, Y.L. Wu, International Journal of Theoretical Physics **57**(12), 3716 (2018). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=132696541&lang=pt-br&site=ehost-live
20. Y.F. He, W.P. Ma, Quantum Information Processing **14**(9), 3483 (2015)
21. D.S. Shen, W.P. Ma, L.L. Wang, Quantum Information Processing **13**(10), 2313 (2014). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=97942738&lang=zh-cn&site=ehost-live
22. H.R. Pang, J.L. Ping, F. Wang, Communications in Theoretical Physics **38**(4), 424 (2002). DOI 10.1088/0253-6102/38/4/424. URL http://dx.doi.org/10.1088/0253-6102/38/4/424
23. A. Borras, A.R. Plastino, J. Batle, C. Zander, M. Casas, A. Plastino, Journal of Physics: A Mathematical Theoretical **40**(44), 13407 (2007). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=44660236&lang=zh-cn&site=ehost-live
24. G.F. Deng, G.L. Long, Y. Wang, L. Xiao, **21**(11), 2097 (2004). DOI 10.1088/0256-307x/21/11/007. URL https://doi.org/10.1088/0256-307x/21/11/007
25. A. Cabello, Physical Review Letters **85**, 5635 (2000). DOI 10.1103/PhysRevLett.85.5635. URL https://link.aps.org/doi/10.1103/PhysRevLett.85.5635
26. Y.F. He, W.P. Ma, International Journal of Quantum Information **14**(1), 1 (2016). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=115610139&lang=zh-cn&site=ehost-live
27. Y.G. Yang, B.R. Li, S.Y. Kang, X.B. Chen, Y.H. Zhou, W.M. Shi, Quantum Information Processing **18**(3), 1 (2019). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=135041050&lang=zh-cn&site=ehost-live
28. Y.H. Zhou, M.F. Wang, W.M. Shi, Y.G. Yang, J. Zhang, Quantum Information Processing **19**(3), 100 (2020). DOI 10.1007/s11128-020-2593-y. URL https://doi.org/10.1007/s11128-020-2593-y
29. H. Gao, X.G. Chen, S.R. Qian, Quantum Information Processing **17**(6), 1 (2018). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=129928283&lang=pt-br&site=ehost-live
30. Y.G. Yang, S. Gao, D. Li, Y.H. Zhou, W.M. Shi, Quantum Information Processing **18**(3), 1 (2019). URL https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=135041039&lang=zh-cn&site=ehost-live
31. S.S. Wang, D.H. Jiang, G.B. Xu, Y.H. Zhang, X.Q. Liang, Quantum Information Processing **18**(6), 190 (2019). DOI 10.1007/s11128-019-2305-7. URL https://doi.org/10.1007/s11128-019-2305-7