International Journal of Theoretical Physics (2018) 57: 3716–3726
https://doi.org/10.1007/s10773-018-3884-2

Multiparty Quantum Key Agreement with Four-Qubit Symmetric W State

Sha-Sha Wang[1] · Guang-Bao Xu[1] · Xiang-Qian Liang[1] · Yu-Liang Wu[1]

Received: 20 March 2018 / Accepted: 3 September 2018 / Published online: 10 September 2018

Abstract
Based on four-qubit symmetric W state, the delayed measurement, decoy photos method, block transmission technique and the dense coding method, a multi-party quantum key agreement protocol is proposed. By utilizing the delayed measurement and decoy photos method, the fairness and security of the protocol are ensured. That is, the final generation key can be got fairly by m participants and the outside eavesdropper (includes Trojan-horse attacks, Measure-resend attack, Intercept-resend attack and Entangle-measure attack) and the dishonest participants attacks can be resisted in this protocol. By utilizing block transmission technique and the dense coding method, the efficiency of the protocol is improved. The efficiency analysis shows that the proposed protocol is more efficient than other multi-party QKA protocols.

Keywords Quantum key agreement · Multi-party · Quantum cryptography · W state

1 Introduction

With the development of quantum algorithm, the security of classical key agreement schemes based on computational complexity is confronted with severe challenges, especially since Shor [1] proposed two algorithms for quantum computation: discrete logarithms and factoring. Quantum cryptography is based on quantum mechanics, and its security is guaranteed by the fundamental principles of quantum mechanics. The main task of quantum

✉ Xiang-Qian Liang
xiangqian.liang@163.com

Sha-Sha Wang
wss20180118@163.com

Guang-Bao Xu
xu_guangbao@163.com

Yu-Liang Wu
1099646448@qq.com

[1] College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao, 266590, Shandong, China

cryptography is the quantum key distribution (QKD) which only one participant decides the private key and distributes it to the other ones. The first quantum key distribution protocol (QKD) was proposed by Bennett and Brassard in 1984 [2]. The BB84 is based upon a single particle carrier and non-orthogonal states which is easy to implement. In addition, BB84 utilized uncertainty principle and non-cloning theorem to ensure the security of QKD. Then, Shor et al. [3] proposed a protocol that proved the security of BB84 in 2000. In 1991, Ekert et al. [4] defined the delayed measurement at the first time. It is generally accepted that only non-orthogonal states can be used to design quantum cryptographic protocols because orthogonal states can be precisely cloned. However, Goldenberg et al. [5] proposed a protocol based on orthogonal states in 1995. Quantum cryptography had drawn considerable attention, and it has been developed quickly since the QKD protocols were proposed. Therefore, far many different types of quantum cryptographic protocols have been proposed, including quantum key agreement [7–25], quantum secure direct communication [26–28], quantum secret sharing [29, 30], quantum key distribution [31–34], quantum signature [35–38] and so on.

Different from QKD, the QKA allows two or more parties to generate the shared key, and no one can determine the generated key alone. In 1976, Diffie and Hellman [6] presented the first key agreement protocol that involves two parties. Zhou et al. [7] first put forward a QKA protocol based on quantum teleportation in 2004. However, in 2009, Zhou et al.'s protocol was pointed out the existence of security defects by Tsai et al. [8]. That is, a participant can determine the shared key alone without being detected completely. In 2010, Chong and Hwang [9] proposed a QKA protocol based on BB84 that enables two participants to consult a shared key, and no one can determine the shared key alone. In 2011, Chong et al. [10] proposed a improvement QKA protocol based on maximally entangled states, and pointed out two security loopholes of Hsueh and Chen protocol [11]: (1) dishonest user can decide the shared key alone fully; (2) an eavesdropper can get the shared key without being detected. And they proposed a possible solution to avoid these attacks. In 2016, He and Ma [13] proposed a QKA based on four-particle entangled states about two parties. Since each particle was transmitted only once in quantum channel, the protocol can resist the Trojan horse attacks. But these QKA protocols [7–16] only involved two parties and can not to extend the multi-party case. Next, let us to focus on multi-party QKA protocols. In 2013, Shi and Zhong [18] first proposed a multi-party QKA protocol based on entanglement swapping. Unfortunately, Liu et al. [19] pointed out that Shi et al.'s protocol [18] is not secure that dishonest participant can completely determine the shared key. At the same time, Liu et al. [19] proposed a multi-party QKA with single particles which was the first safe multi-party QKA protocol. But, Sun et al. [20] pointed out that Liu et al.'s protocol is inefficient. And Sun et al. [20] proposed the improvements on Liu et al.'s protocol. The photo efficiency of Sun et al.'s protocol can be improved to $\frac{1}{N(k+1)}$, and the security is also improved. In 2014, Xu et al. [23] proposed a novel multiparty quantum key agreement protocol with GHZ states. In 2016, Liu et al. [25] pointed out that Xu et al.'s protocol is unjust that the participants can control the shared key to a certain degree since performing the eavesdropping detection. In view of this problem, Gu et al. [39] proposed improvement on Xu et al.'s protocol in 2017. In 2014, Huang et al. [21] first presented QKA protocol with blocks of EPR pairs and single-particle measurements. Chitra Shukl et al. [22] proposed protocols of quantum key agreement merely utilizing Bell states and Bell measurement the same year. However, Zhu et al. [24] pointed out Chitra Shukl et al.'s [22] protocol that the three-party protocol is not secure, and put forward a scheme to improve the three-party protocol in 2015. Recently, some multi-party quantum key agreement protocols [18–20, 23, 25, 40–44] were proposed.

In this paper, we put forward a multi-party quantum key agreement protocol with four-qubit symmetric W state. The shared key is generated by all participants; neither party can decide the shared key alone. The outsider eavesdropper and dishonest participants cannot obtain the shared key without introducing any error. This protocol is more efficient than other multi-party QKA protocols.

The rest of the paper is organized as follows. Section 2, we introduce our three-party and multi-party QKA protocol with four-qubit symmetric W state. Section 3, we give the security analysis. Section 4, efficiency analysis is discussed. Section 5, a short conclusion is given.

2 The Presented Multi-party Quantum key Agreement Protocol

First, we introduce the four Pauli gates:

$$\sigma^0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|,$$
$$\sigma^1 = X = |0\rangle\langle 1| + |1\rangle\langle 0|,$$
$$\sigma^2 = Z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$
$$\sigma^3 = iY = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

Then, the four-qubit symmetric W state can be depicted as:

$$|\varphi_a\rangle_{1234} = \tfrac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)_{1234},$$

where the subscripts 1, 2, 3, 4 denote the first particle, the second particle, the third particle and the fourth particle of the cluster states, respectively.
Assume that the initial state is $|\varphi_a\rangle_{1234} = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)_{1234}$. When we perform unitary operation $\sigma^i (i = 0, 1, 2, 3)$ on qubit 3 and qubit 4, the cluster state $|\varphi_a\rangle_{1234}$ will be transformed into one of the following four cluster states [45]:

$$\begin{aligned}
|\varphi_a\rangle_{1234} &= \tfrac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)_{1234},\\
|\varphi_b\rangle_{1234} &= \tfrac{1}{2}(|0000\rangle - |0011\rangle - |0101\rangle - |1001\rangle)_{1234},\\
|\varphi_c\rangle_{1234} &= \tfrac{1}{2}(|0011\rangle + |0000\rangle + |0110\rangle + |1010\rangle)_{1234},\\
|\varphi_d\rangle_{1234} &= \tfrac{1}{2}(|0010\rangle - |0001\rangle - |0111\rangle - |1011\rangle)_{1234}.
\end{aligned}$$

As shown in Table 1. In order to unify a secret key, let us to define the following encoding rules:

$$|\varphi_a\rangle_{1234} : 00, |\varphi_b\rangle_{1234} : 01, |\varphi_c\rangle_{1234} : 10, |\varphi_d\rangle_{1234} : 11.$$

Table 1 shows the relationship of the unitary operations and the transformed states on the qubit 3 and qubit 4 of cluster state $|\varphi_a\rangle_{1234}$

Initial state	Unitary operation	Final state	Agreement key
$\|\varphi_a\rangle_{1234}$	$\sigma^0\sigma^0$	$\|\varphi_a\rangle_{1234}$	00
	$\sigma^0\sigma^3$	$\|\varphi_b\rangle_{1234}$	01
	$\sigma^1\sigma^0$	$\|\varphi_c\rangle_{1234}$	10
	$\sigma^1\sigma^3$	$\|\varphi_d\rangle_{1234}$	11

2.1 The Three-Party Quantum Key Agreement Protocol

Suppose that three participants want to generate a shared key K. They are P_1, P_2 and P_3. First, P_1, P_2 and P_3 generate the bit strings K_1, K_2 and K_3 randomly as their secret keys, respectively.

$$K_1 = (k_1^1, k_1^2, \ldots, k_1^s, \ldots, k_1^n),$$
$$K_2 = (k_2^1, k_2^2, \ldots, k_2^s, \ldots, k_2^n),$$
$$K_3 = (k_3^1, k_3^2, \ldots, k_3^s, \ldots, k_3^n).$$

Therefore, the shared key $K = K_1 \oplus K_2 \oplus K_3 = (k_1^1 \oplus k_2^1 \oplus k_3^1, k_1^2 \oplus k_2^2 \oplus k_3^2, \ldots, k_1^s \oplus k_2^s \oplus k_3^s, \ldots, k_1^n \oplus k_2^n \oplus k_3^n)$. Where $k_1^s, k_2^s, k_3^s \in \{0, 1\}, s = 1, 2, \ldots, n$ represent s^{th} private information of $P_i (i = 1, 2, 3)$. $\oplus$ denotes the addition module 2, and n is the length of secret bit string. P_i indicates i^{th} participant. Next, we describe the three-party quantum key agreement protocol.

1 The participant $P_i (i = 1, 2, 3)$ prepares $|\varphi_a\rangle_{1234}^{\otimes \frac{n}{2}}$, respectively. P_i divides these states into four sequences S_i^1, S_i^2, S_i^3 and S_i^4. Here, the sequence $S_i^l (l = 1, 2, 3, 4; i = 1, 2, 3)$ is composed of l^{th} particle of the $|\varphi_a\rangle_{1234}^{\otimes \frac{n}{2}}$. $S_i^l = (s_i^{l,1}, s_i^{l,2}, \ldots, s_i^{l,j}, \ldots, s_i^{l,\frac{n}{2}})$, $s_i^{l,j} (l = 1, 2, 3, 4; 1 \le j \le \frac{n}{2}; i = 1, 2, 3)$ denotes j^{th} particle of S_i^l. Then P_i prepares $\frac{n}{2}$ decoy photos respectively which are randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

2 The participant P_i randomly inserts these decoy photos into the two sequences S_i^3 and S_i^4, respectively. Then, P_i obtains the new sequence $S_i^{t'} (t = 3, 4; i = 1, 2, 3)$. Subsequently, P_i applies permutation operator $(\prod_{\frac{n}{2}})_{P_i}$ on $S_i^{t'}$ to create the new sequence $(\prod_{\frac{n}{2}})_{P_i} S_i^{t'} = S_i^{t''} (t = 3, 4; i = 1, 2, 3)$, and sends $S_i^{t''} (t = 3, 4; i = 1, 2, 3)$ to P_{i+1}. Here, $+$ denotes the addition module 3, i.e., $i + 1 = (i + 1) \bmod 3$.

3 After P_i confirms that P_{i+1} has received the $S_i^{t''}$. P_i announces the permutation operator $(\prod_{\frac{n}{2}})_{P_i}$. Then, P_i announces the positions and the corresponding bases of the decoy photos. Later, P_{i+1} measures the decoy photos by utilizing the correct bases. P_{i+1} publishes half of the measurement results randomly after the measurement. Then P_i publishes the initial states of the left half of the decoy photos. At last, they check whether the measurement results and the initial states are consistent. If they are consistent, P_i and P_{i+1} declare that S_i^3 and S_i^4 are secure; otherwise, they discard the protocol.

4 If all sequences $S_i^t (t = 3, 4)$ are secure. P_{i+1} performs unitary operations $\sigma^{k_{i+1}^{2j-1}}$ and $\sigma^{3k_{i+1}^{2j}}$ on $s_i^{3,j}$ and $s_i^{4,j}$ respectively according to his secret keys k_{i+1}^{2j-1} and k_{i+1}^{2j}, where $j = 1, 2, 3, \ldots, \frac{n}{2}$. Then, they can get the two sequences $S_{i,i+1}^3$ and $S_{i,i+1}^4$. Then, he applies the decoy photos and permutation operator method that described in step 2 to generate the new sequence $S_{i,i+1}^{t''} (t = 3, 4)$ and sends it to the next participant P_{i+2}.

5 The step is similar to step 3. After P_{i+1} confirms that P_{i+2} has received the $S_{i,i+1}^{t''} (t = 3, 4)$, P_{i+1} announces the permutation operator $(\prod_{\frac{n}{2}})_{P_{i+1}}$. Subsequently, P_{i+1} announces the positions and the corresponding bases of the decoy photos. Later, P_{i+2} measures the decoy photos by utilizing the correct bases. P_{i+2} publishes half of

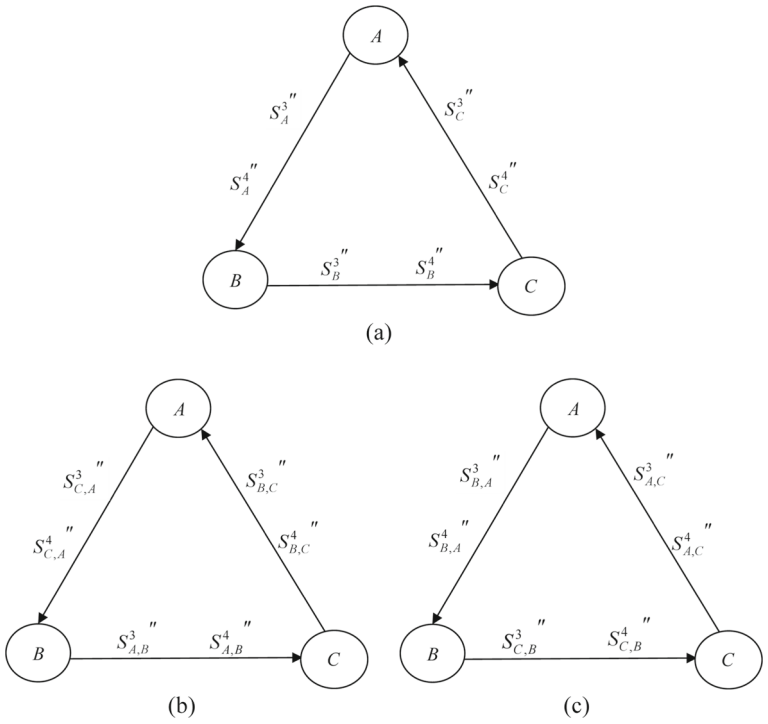

Fig. 1 The three-party quantum key agreement protocol steps of transmitting photons

the measurement results randomly after the measurement. Then P_{i+1} publishes the left half of the initial decoy photos. At last, they check whether the measurement results and the initial states are consistent. If they are consistent, P_{i+1} and P_{i+2} declare that $S^t_{i,i+1}(t = 3, 4)$ is secure; otherwise, they discard the protocol.

6 The step is similar to step 4. If all the sequences $S^t_{i,i+1}(t = 3, 4)$ are secure. P_{i+2} performs unitary operations $\sigma^{k^{2j-1}_{i+2}}$ and $\sigma^{3k^{2j}_{i+2}}$ on j^{th} particle of sequences $S^3_{i,i+1}$ and $S^4_{i,i+1}$ respectively according to his secret key k^{2j-1}_{i+2} and k^{2j}_{i+2}. Then, they can get two sequences $S^3_{i,i+2}$ and $S^4_{i,i+2}$. Then, he applies the decoy photos and permutation operator method that described in step (2) to generate the new sequence $S^{t''}_{i,i+2}(t = 3, 4)$ and sends it to the next participant P_i. Figure 1 shows the steps of transmitting photons.

7 When P_i receives the two sequences $S^{3''}_{i,i+2}$ and $S^{4''}_{i,i+2}$, he detects eavesdropping with P_{i+2}. If all the sequences $S^t_{i,i+2}(t = 3, 4)$ are secure, Then P_i can obtain the two sequences $S^3_{i,i+2}$ and $S^4_{i,i+2}$. By performing W basis measurement on j^{th} W state, P_i can get a measurement result. By Table 2, P_i can get the key $K_{i+1} \oplus K_{i+2}$. Then P_i an generate the final shared key $K = K_i \oplus K_{i+1} \oplus K_{i+2}$.

Table 2 shows the relationship of the unitary operations and the transformed states on the qubits 3 and 4 of cluster state $|\varphi_a\rangle_{1234}$, $|\varphi_b\rangle_{1234}$, $|\varphi_c\rangle_{1234}$ and $|\varphi_d\rangle_{1234}$

Initial state	K_{i+1}	The first operation	The first state	K_{i+2}	The second operation	Final state	$K_{i+1} \oplus K_{i+2}$
$\|\varphi_a\rangle_{1234}$	00	$\sigma^0\sigma^0$	$\|\varphi_a\rangle_{1234}$	00	$\sigma^0\sigma^0$	$\|\varphi_a\rangle_{1234}$	00
				01	$\sigma^0\sigma^3$	$\|\varphi_b\rangle_{1234}$	01
				10	$\sigma^1\sigma^0$	$\|\varphi_c\rangle_{1234}$	10
				11	$\sigma^1\sigma^3$	$\|\varphi_d\rangle_{1234}$	11
	01	$\sigma^0\sigma^3$	$\|\varphi_b\rangle_{1234}$	00	$\sigma^0\sigma^0$	$\|\varphi_b\rangle_{1234}$	01
				01	$\sigma^0\sigma^3$	$\|\varphi_a\rangle_{1234}$	00
				10	$\sigma^1\sigma^0$	$\|\varphi_d\rangle_{1234}$	11
				11	$\sigma^1\sigma^3$	$\|\varphi_c\rangle_{1234}$	10
	10	$\sigma^1\sigma^0$	$\|\varphi_c\rangle_{1234}$	00	$\sigma^0\sigma^0$	$\|\varphi_c\rangle_{1234}$	10
				01	$\sigma^0\sigma^3$	$\|\varphi_d\rangle_{1234}$	11
				10	$\sigma^1\sigma^0$	$\|\varphi_a\rangle_{1234}$	00
				11	$\sigma^1\sigma^3$	$\|\varphi_b\rangle_{1234}$	01
	11	$\sigma^1\sigma^3$	$\|\varphi_d\rangle_{1234}$	00	$\sigma^0\sigma^0$	$\|\varphi_d\rangle_{1234}$	11
				01	$\sigma^0\sigma^3$	$\|\varphi_c\rangle_{1234}$	10
				10	$\sigma^1\sigma^0$	$\|\varphi_b\rangle_{1234}$	01
				11	$\sigma^1\sigma^3$	$\|\varphi_a\rangle_{1234}$	00

2.2 The Multi-Party Quantum key Agreement Protocol

Suppose that m participants $P_1, P_2, \ldots, P_m$ want to generate a shared key K. They possess their own secret bit strings $K_1, K_2, \ldots, K_m$, respectively. Therefore, the shared key $K = K_1 \oplus K_2 \oplus \cdots \oplus K_m$, wherein neither party can decide the shared key alone.

$$
\begin{aligned}
&K_1 = (k_1^1, \ldots, k_1^s, \ldots, k_1^n),\\
&\vdots\\
&K_i = (k_i^1, \ldots, k_i^s, \ldots, k_i^n),\\
&\vdots\\
&K_m = (k_m^1, \ldots, k_m^s, \ldots, k_m^n).
\end{aligned}
$$

(1) Preparation: The participant $P_i (i = 1, 2, \ldots, m)$ prepares $|\varphi_a\rangle_{1234}^{\otimes \frac{n}{2}}$, respectively. P_i divides these states into four sequences S_i^1, S_i^2, S_i^3 and S_i^4. $S_i^l = (s_i^{l,1}, s_i^{l,2}, \ldots, s_i^{l,j}, \ldots, s_i^{l,\frac{n}{2}})(l = 1, 2, 3, 4; 1 \le j \le \frac{n}{2}; i = 1, 2, \ldots, m)$, $s_i^{l,j}$ denotes j^{th} particle of S_i^l. Then he prepares $\frac{n}{2}$ decoy states which are randomly in four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

(2) Transmission: Similar to the second step in the three party agreement. P_i sends $S_i^{t''} (i = 3, 4)$ to P_{i+1}. Here, $+$ denotes the addition module m, i.e., $i + 1 = (i + 1) \bmod m$.

(3) Detection: Similar to the third step in the three party agreement. If they are consistent, P_i and P_{i+1} declare that $S_i^t (t = 3, 4)$ is secure; otherwise, they discard the protocol.

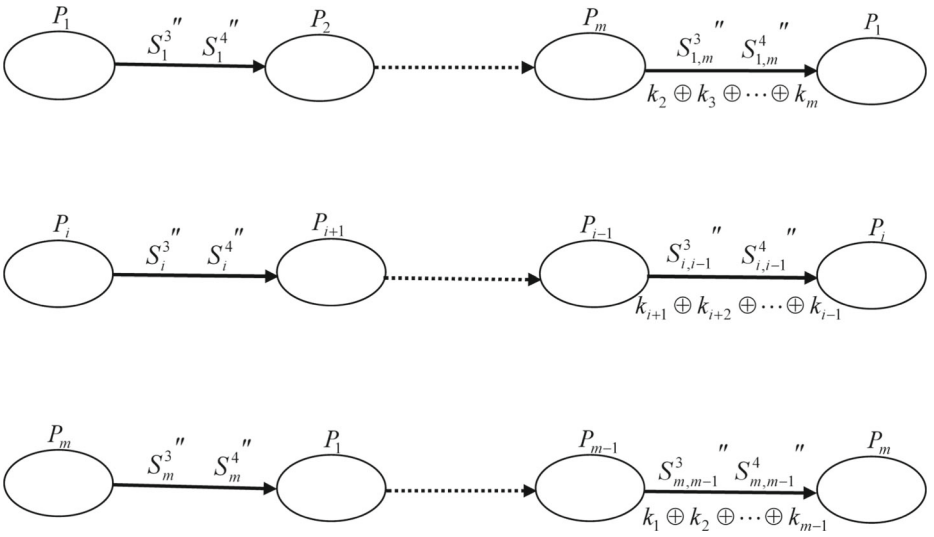

Fig. 2 The multi-party quantum key agreement protocol steps of transmitting photons

(4) Encoding: If all sequences $S_i^t (t = 3, 4)$ are secure. P_{i+1} performs unitary operations $\sigma^{k_{i+1}^{2j-1}}$ and $\sigma^{3k_{i+1}^{2j}}$ on j^{th} particle of sequences S_i^3 and S_i^4 respectively according to his secret keys k_{i+1}^{2j-1} and k_{i+1}^{2j}, where $j = 1, 2, \ldots, \frac{n}{2}$. Therefore, they can get two sequences $S_{i,i+1}^3$ and $S_{i,i+1}^4$. Then, P_{i+1} applies the decoy photos and permutation operator method that described in step (2) to generate the new sequence $S_{i,i+1}^{t''}(t = 3, 4)$ and sends it to the next participant P_{i+2}.

(5) The participants $P_{i+2}, \ldots, P_{i-1}$ perform the permutation operator, eavesdropping check and message encoding processes sequentially, just like steps (3) and (4). As shown in Fig. 2.

(6) When P_i receives two sequences $S_{i,i-1}^{3''}$ and $S_{i,i-1}^{4''}$, he detects eavesdropping with P_{i-1}. If all the sequences $S_{i,i-1}^t (t = 3, 4)$ are secure, Then P_i can obtain two sequences $S_{i,i-1}^3$ and $S_{i,i-1}^4$. By performing W basis measurement on j^{th} W state, P_i can get a measurement result. By Table 1, P_i can get the key $K_i' = \underset{j,j\neq i}{\oplus} K_j$. Then P_i can generate the final shared key $K = K_i \oplus K_i'$.

3 Security Analysis

3.1 Participant Attack

Participant attack is a normal attack mode in the protocols that participants do not trust each other. Without loss of generality, we assume that P_i is the dishonest participant. If P_i gets

the final key K ahead of time, where K is the bitwise of all parties. P_i wants to change the final shared key K to K^*. Then P_i encodes $K^* \oplus K \oplus K_i$ as his secret key instead of K_i when he performs the protocol. Other parties will regard K^* as the final shared key because of $K^* \oplus K \oplus K = K^*$. Thus, the multi-party agreement has a defect of fairness in this situation. To avoid the above unfairness, we demand that all participants must check eavesdropping. If all the sequences $S_i^t (t = 3, 4)$ are secure, they perform unitary operation by their own secret key in our protocol. Therefore, nobody can get the final shared key ahead of time, and all participants get the final generation key simultaneously. The dishonest participant P_i has no ability to change the final generate key as she expected. Therefore, it is impossible that a dishonest participant determines the final key alone by encoding a false secret to others.

3.2 Outsider Attack

Supposed that the outsider attacker is Eve. There are four kinds of attacks that Eve may use, including Trojan-horse attacks, Measure-resend attack, Intercept-resend attack and Entangle-measure.

3.2.1 Trojan-horse Attacks

Because our quantum protocol delivers the same photon more than once, it may be attacked by the Trojan horse attacks, such as the invisible-photon eavesdropping (IPE) attack and the delay-photon attack. A number of circular quantum transmission debated [47–50]. To avoid this type of attacks, participants can install a wavelength filter and the photon number splitters (PNS: 50/50). The photon number splitter (PNS: 50/50) which is used for dividing each signal into two pieces, should be introduced to defeat the delay-photon attack. If a multi-photon signal has an irrational high rate, an attack can be detected.

3.2.2 Measure-resend Attack

Eve may implement the measure-resend attack on the sequences $S_i^{t''}, S_{i,i+1}^{t''}, \ldots, S_{i,i-1}^{t''} (t = 3, 4)$ in steps (2), (4) and (5), respectively. Because Eve does not know the positions and the corresponding measurement bases of the decoy photos. The states of decoy photons will change when Eve performs measurement. Eve can be detected with the probability $1 - (\frac{3}{4})^{\frac{n}{2}}$ when the participants perform eavesdropping detection in step (3).

3.2.3 Intercept-resend Attack

First, Eve needs to forge some sequences. When Eve intercepts the sequences $S_i^{t''}, S_{i,i+1}^{t''}, \ldots, S_{i,i-1}^{t''} (t = 3, 4)$ in step (2), step (4) and step (5), she can send the forged sequences instead of $S_i^{t''}, S_{i,i+1}^{t''}, \ldots, S_{i,i-1}^{t''} (t = 3, 4)$ to the next participant. However, Eve cannot obtain any information about the decoy photos before $P_i, P_{i+1}, \ldots, P_{i-1}$ announce the positions and the corresponding bases of the decoy photos. Therefore, when the participants perform eavesdropping detection, Eve can be detected. Furthermore, Eve's attack can be found with the probability of $1 - (\frac{1}{2})^{\frac{n}{2}}$ when $\frac{n}{2}$ decoy photos are used for detecting this attack.

3.2.4 Entangle-measure Attack

Decoy photons are used for eavesdropping detection in the protocol. The decoy photons are $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. Eve can only select a set of orthogonal bases to detect them, but she cannot distinguish which are the target photons and the decoy photons. Therefore, any eavesdropper will expose themselves by changing the quantum state. Without loss of generality, suppose the eavesdropper uses the operation $\hat{U}_E$, and prepares an auxiliary system $|\varepsilon\rangle_E$. We can get the following equations:

$$\begin{aligned}
\hat{U}_E|0\rangle|\varepsilon\rangle_E &= a|0\rangle|\varepsilon_{00}\rangle_E + b|1\rangle|\varepsilon_{01}\rangle_E,\\
\hat{U}_E|1\rangle|\varepsilon\rangle_E &= c|0\rangle|\varepsilon_{10}\rangle_E + d|1\rangle|\varepsilon_{11}\rangle_E,\\
\hat{U}_E|+\rangle|\varepsilon\rangle_E &= \frac{1}{\sqrt{2}}(a|0\rangle|\varepsilon_{00}\rangle_E + b|1\rangle|\varepsilon_{01}\rangle_E + c|0\rangle|\varepsilon_{10}\rangle_E + d|1\rangle|\varepsilon_{11}\rangle_E)\\
&= \frac{1}{2}[|+\rangle(a|\varepsilon_{00}\rangle_E + b|\varepsilon_{01}\rangle_E + c|\varepsilon_{10}\rangle_E + d|\varepsilon_{11}\rangle_E) +\\
&\quad |-\rangle(a|\varepsilon_{00}\rangle_E - b|\varepsilon_{01}\rangle_E + c|\varepsilon_{10}\rangle_E - d|\varepsilon_{11}\rangle_E)],\\
\hat{U}_E|-\rangle|\varepsilon\rangle_E &= \frac{1}{\sqrt{2}}(a|0\rangle|\varepsilon_{00}\rangle_E + b|1\rangle|\varepsilon_{01}\rangle_E - c|0\rangle|\varepsilon_{10}\rangle_E - d|1\rangle|\varepsilon_{11}\rangle_E)\\
&= \frac{1}{2}[|+\rangle(a|\varepsilon_{00}\rangle_E + b|\varepsilon_{01}\rangle_E - c|\varepsilon_{10}\rangle_E - d|\varepsilon_{11}\rangle_E) +\\
&\quad |-\rangle(a|\varepsilon_{00}\rangle_E - b|\varepsilon_{01}\rangle_E - c|\varepsilon_{10}\rangle_E + d|\varepsilon_{11}\rangle_E)].
\end{aligned}$$

where $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$. $|\varepsilon\rangle_E$ is the initial state of the ancilla E. $\{|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle\}$ are pure ancilla states uniquely determined by $\hat{U}_E$, so $|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle$ must satisfy $\hat{U}_E\hat{U}_E^+ = I$, i.e.:

$$\begin{aligned}
\langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle &= 1,\\
\langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle &= 1,\\
\langle\varepsilon_{00}|\varepsilon_{01}\rangle + \langle\varepsilon_{10}|\varepsilon_{11}\rangle &= 0,\\
\langle\varepsilon_{01}|\varepsilon_{00}\rangle + \langle\varepsilon_{11}|\varepsilon_{10}\rangle &= 0.
\end{aligned}$$

If Eve don't to introduce error in the eavesdropping check, the $\hat{U}_E|0\rangle|\varepsilon\rangle_E$, $\hat{U}_E|1\rangle|\varepsilon\rangle_E$, $\hat{U}_E|+\rangle|\varepsilon\rangle_E$, $\hat{U}_E|-\rangle|\varepsilon\rangle_E$ can be denoted the following equations:

$$\begin{aligned}
\hat{U}_E|0\rangle|\varepsilon\rangle_E &= a|0\rangle|\varepsilon_{00}\rangle_E,\\
\hat{U}_E|1\rangle|\varepsilon\rangle_E &= d|1\rangle|\varepsilon_{11}\rangle_E,\\
\hat{U}_E|+\rangle|\varepsilon\rangle_E &= \tfrac{1}{2}|+\rangle(a|\varepsilon_{00}\rangle_E + b|\varepsilon_{01}\rangle_E + c|\varepsilon_{10}\rangle_E + d|\varepsilon_{11}\rangle_E),\\
\hat{U}_E|-\rangle|\varepsilon\rangle_E &= \tfrac{1}{2}|-\rangle(a|\varepsilon_{00}\rangle_E - b|\varepsilon_{01}\rangle_E - c|\varepsilon_{10}\rangle_E + d|\varepsilon_{11}\rangle_E).
\end{aligned}$$

Therefore, we can get the equations:

$$\begin{aligned}
b|1\rangle|\varepsilon_{01}\rangle_E &= 0,\\
c|0\rangle|\varepsilon_{10}\rangle_E &= 0,\\
a|\varepsilon_{00}\rangle_E - b|\varepsilon_{01}\rangle_E + c|\varepsilon_{10}\rangle_E - d|\varepsilon_{11}\rangle_E &= 0,\\
a|\varepsilon_{00}\rangle_E + b|\varepsilon_{01}\rangle_E - c|\varepsilon_{10}\rangle_E - d|\varepsilon_{11}\rangle_E &= 0.
\end{aligned}$$

Then, we can get $a = d = 1, b = c = 0, |\varepsilon_{00}\rangle_E = |\varepsilon_{11}\rangle_E$. If Eve don't to introduce error in the eavesdropping check, she cannot obtain any useful information. Therefore, the protocol can resist the outsider attack.

Table 3 Comparison between proposed multi-party QKA protocols and ours

QKA protocol	Quantum resource	Particle type	Decoy states	Qubit efficiency
Liu et al.'s protocol [19]	Single photons	circle-type	Yes	$\frac{1}{2m(m-1)}$
Xu et al.'s protocol [23]	GHZ states	tree-type	No	$\frac{1}{2m(m-1)}$
Our protocol	W states	circle-type	Yes	$\frac{1}{2m}$

4 Efficiency Analysis

In this chapter, we will discuss the qubit efficiency of this protocol. A well-known measure of efficiency of secure quantum communication is known as qubit efficiency introduced by Cabello [46], which is given as

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

where c denotes the length of transmitted message bits (the length of the final key), q is the number of the used qubits, and b is the number of classical bits exchanged for decoding of the message (classical communication used for checking of eavesdropping is not counted). Hence, the qubit efficiency of our protocol can be computed $\eta = \frac{n}{(2\cdot\frac{n}{2}+2\cdot\frac{n}{2})m} = \frac{1}{2m}$, where m is the number of participants. Table 3 shows that our protocol is more efficient than other multi-party QKA protocols.

5 Conclusion

In this paper, we present a multi-party quantum key agreement with four-qubit symmetric W state. By using the delayed measurement and decoy photos method, the security and fairness of the protocol are ensured. The m participants can get the final generation key fairly. And the result of security analysis shows that our protocol is safe in resisting both participant and outsider attacks. By utilizing block transmission technique and the dense coding method, the efficiency of the protocol is improved. Finally, we estimate its qubit efficiency. The efficiency analysis shows that the proposed protocol is more efficient than other multi-party QKA protocols.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61402265) and the Fund for Postdoctoral Application Research Project of Qingdao (01020120607).

References

1. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE Press, New York (1994)
2. Bennett, C.H., Brassard, G.: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. pp. 175–179, Ban-galore (1984)
3. Shor, P.W., Preskill, J.: Phys. Rev. Lett. **85**, 441 (2000)
4. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
5. Goldenberg, L., Vaidman, L.: Phys. Rev. Lett. **75**, 1239 (1995)
6. Diffie, W., Hellman, M.: IEEE Trans. Inf. Theory. **22**, 644–654 (1976)
7. Zhou, N., Zeng, G., Xiong, J.: Electron. Lett. **40**, 1149 (2004)

8. Tsai, C., Hwang, T.: Technical report, C-S-I-E, NCKU, Taiwan (2009)
9. Chong, S.K., Hwang, T.: Opt. Commun. **283**, 1192–1195 (2010)
10. Chong, S.K., Tsai, C.W., Hwang, T.: Int. J. Theor. Phys. **50**, 1793–1802 (2011)
11. Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information Security Conference, pp. 236–242. National Taiwan University of Science and Technology, Taipei (2004)
12. Shen, D., Ma, W., Wang, L.: Quantum Inf. Process. **13**, 2313–2324 (2014)
13. He, Y.F., Ma, W.P.: Mod. Phys. Lett. B **30**, 26 (2016)
14. He, Y.F., Ma, W.P.: Quantum Inf. Process. **15**, 5023–5035 (2016)
15. He, Y.F., Ma, W.P.: Int. J. Quantum Inf. **15**, 3 (2017)
16. He, Y.F., Ma, W.P.: Mod. Phys. Lett. **31**, 3 (2017)
17. 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, pp. 210C213, National Chiao Tung University, Hsinchu (2010)
18. Shi, R.H., Zhong, H.: Quantum Inf. Process. **12**, 921–932 (2013)
19. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Quantum Inf. Process. **12**, 1797–1805 (2013)
20. Sun, Z., Wang, B., Li, Q., Long, D.: Quantum Inf. Process. **12**, 3411 (2013)
21. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum Inf. Process. **13**, 649–663 (2014)
22. Chitra, S., Nasir, A., Anirban, P.: Quantum Inf. Process. **13**, 2391–2405 (2014)
23. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Quantum Inf. Process. **13**, 2587–2594 (2014)
24. Zhu, Z.C., Hu, A.Q., Fu, A.M.: Quantum Inf. Process. **14**, 4245–4254 (2015)
25. Liu, B., Xiao, D., Jia, H.Y., Liu, R.Z.: Quantum Inf. Process. **15**, 2113–2124 (2016)
26. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
27. Sun, Z.W., Du, R.G., Long, D.Y.: Int. J. Quantum Inf. **10**, 1250008 (2012)
28. Sun, Z.W., Du, R.G., Long, D.Y.: Int. J. Theor. Phys. **51**, 1946–1952 (2012)
29. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
30. Du, R.G., Sun, Z.W., Wang, B.H., Long, D.Y.: Int. J. Theor. Phys. **51**, 2727–2736 (2012)
31. Hwang, W.Y.: Phys. Rev. Lett. **91**, 057901 (2003)
32. Lo, H.K., Ma, X.F., Chen, K.: Phys. Rev. Lett. **94**, 230504 (2005)
33. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Phys. Rev. Lett. **88**, 127902 (2002)
34. Lo, H.K., Curty, M., Qi, B.: Phys. Rev. Lett. **108**, 130503 (2012)
35. Guo, W., Xie, S.C., Zhang, J.Z.: Int. J. Theor. Phys. **56**, 1708–1718 (2017)
36. Shao, A.X., Zhang, J.Z., Xie, S.C.: Int. J. Theor. Phys. **55**, 5216–5224 (2016)
37. Guo, W., Zhang, J.Z., Li, Y.P., An, W.: Int. J. Theor. Phys. **55**, 3524–3536 (2016)
38. Tian, J.H., Zhang, J.Z., Li, Y.P.: Int. J. Theor. Phys. **55**, 809–816 (2016)
39. Gu, J., Hwang, T.: Int. J. Theor. Phys. **56**, 3108–3116 (2017)
40. Wang, P., Sun, Z.W., Sun, X.Q.: Quantum Inf. Process. **16**, 170 (2017)
41. Cai, B.B., Guo, G.D., Lin, S.: Int. J. Theor. Phys. **56**, 1039–1051 (2017)
42. Wang, L.L., Ma, W.P.: Quantum. Inf. Process. **16**, 130 (2017)
43. Sun, Z.W., Yu, J.P., Wang, P.: Quantum. Inf. Process., 15, 373–384 (2016)
44. Sun, Z.W., Huang, J.W., Wang, P.: Quantum Inf. Process. **15**, 2101–2111 (2016)
45. Shukla, V., Kothari, C., Banerjee, A., Pathak, A.: Phys. Lett. A **377**, 518–527 (2013)
46. Cabello, A.: Phys. Rev. Lett. **85**, 5633–5638 (2000)
47. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.: Phys. Rev. A **72**, 044302 (2005)
48. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006)
49. Cai, Q.Y.: Phys. Lett. A **351**, 23–25 (2006)
50. Lin, J., Hwang, T.: Quantum Inf. Process. **12**, 685 (2013)