Int J Theor Phys (2016) 55:1920–1929
DOI 10.1007/s10773-015-2831-8

Multi-Party Quantum Key Agreement by an Entangled Six-Qubit State

Zhiwei Sun[1,2] · Cai Zhang[3] · Ping Wang[2] · Jianping Yu[1,2] · Yong Zhang[1] · Dongyang Long[3]

Received: 10 June 2015 / Accepted: 29 September 2015 / Published online: 14 October 2015

Abstract Since the first quantum key agreement protocol based on Bell state was presented by Zhou et al., much attention has focused on it, which is based on entangled states and product states. In this paper, we propose a multi-party quantum key agreement protocol, in which the genuinely maximally entangled six-qubit states are used. The presented protocol allows participants to share a secret key and preserves the following advantages. First, the outcome of the protocol is influenced by all parties; Second, the presented protocol is fairness, i.e., no one can determine the shared key alone; Third, outside eavesdroppers cannot gain the generated key without introducing any error. The security analysis shows that our protocol can resist both outside attacks and inside attacks.

Keywords Quantum key agreement · Genuinely maximally entangled six-qubit state

1 Introduction

Key agreement, also called key exchange, is a cryptographical primitive which allows two participants to interact with each other so that they can share a secret key. The shared

✉ Ping Wang
wangping@szu.edu.cn

Zhiwei Sun
sunzhiwei1986@gmail.com

[1] ATR Key Laboratory of National Defense Technology, Shenzhen University, ShenZhen, Guangdong, 518060, People's Republic of China

[2] College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, 518060, People's Republic of China

[3] School of Information Science and Technology, Sun Yat-sen University, Guangzhou, 510006, People's Republic of China

key can be used for a secret-key cryptosystem or authentication protocols. These protocols allow parties to share secret keys freely and securely over insecure channel without the need for a previously-established shared secret. Different from the key distribution, in which one party distributes a secret key to the other ones, all involved parties in a key agreement protocol can equally influence the outcome of the protocol, and no one can decide the shared key alone. In other words, in addition to have the same ability of resisting adversaries from the outside world as the key distribution protocol does, a secure key agreement protocol is also required to prevent the participant attacks, i.e., the dishonest party may try to determine the secret key alone. The first practical solution to the key agreement problem was the Deffie-Hellman exponential key exchange in 1976 [1]. Since the pioneering work of Diffie and Hellman, a number of work began to consider the multiparty key agreement. Multiparty key agreement can be seen as a generalization of two-party key agreement. The first multiparty key agreement was proposed by Ingemarsson et al. in 1982 [2], which is a nature extension of the classical Diffe-Hellman key agreement protocol. However, key agreement protocols become increasingly vulnerable with more powerful quantum computation [3, 4] since their security is mostly based on the computation complexity.

On the other hand, quantum cryptography, which is based on the principle of quantum mechanical to perform cryptographic tasks, can provide unconditional security [5]. A lot of attention has focused on the quantum cryptography, and it has been developed quickly since the quantum key distribution protocol (BB84) was proposed by Bennett and Brassard in 1984 [6], such as quantum key distribution [7–11], quantum secret sharing [12–15], quantum secure direct communication [16–26], quantum private comparison [27–32], quantum signature [33, 34] and quantum oblivious transfer [35].

Quantum key agreement (QKA), a new branch of quantum cryptography, was first proposed by Zhou et al. in 2004 [36], which utilizes quantum mechanics to guarantee its security. In their protocol, the quantum teleportation technique [37] was used to generate a secret key over public channels. However, there are some attacks on Zhou et al.'s protocol, e.g., a party can fully determine the shared key alone, i.e., it is not a fair QKA [38], and it is susceptible to the participant attack [39]. Later, Chong and Hwang [40] proposed a new QKA protocol based on BB84 protocol, in which the technique of delayed measurement and the authenticated classical channel were used. Recently, Huang et al.[41] considered the QKA protocol in the collective noise channels. However, only two participants were involved in the above QKA protocols. Recently, an extension of the two-party quantum key agreement was proposed by Shi and Zhong [42], which is based on EPR pairs and entanglement swapping. Unfortunately, Liu et al. [43] found that their protocol was not a fair QKA because a dishonest participant can determine the secret key independently, and they presented a secure multiparty QKA protocol with single particles. Later, the efficiency of their protocol was improved [44].

In this paper, we propose a multi-party quantum key agreement (MQKA) protocol utilizing the genuinely maximally entangled six-qubit state [45] (we call it BPB state for short hereafter). The presented protocol allows participants to share a secret key and preserves the following advantages. The outcome of the protocol is influenced by all parties; no one can determine the shared key alone. And both outside eavesdroppers and inside participants cannot influence the generated key without introducing any error.

The rest of this paper is organized as follows. Section 2 analyzes the structure of the BPB state and shows the excellent properties which are useful for designing our protocol. In Section 3, we present our MQKA protocol by using the BPB state. Then, the security analysis is given in Section 4. Section 5 gives a short conclusion.

2 The Genuinely Maximally Entangled Six-Qubit State

Quantum entanglement, as a physical resource, plays a key role in many applications such as quantum teleportation [37], quantum dense coding [9], quantum key distribution [7], quantum secret sharing [46, 47]. By using a numeric searching program, Borras et al.[45] found the BPB state, which is

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

We denote this six-qubit state by Ψ_{6qb}. From the above formula, we can see that Ψ_{6qb} includes 32 terms, each of which has even $|0\rangle$ and equal coefficient.

To show the entangled property of Ψ_{6qb}, we can rewrite it as

$$\begin{aligned}\Psi_{6qb} &= \frac{1}{2}(|\Phi^+\rangle_{12}|\Phi^+\rangle_{36}|\Phi^+\rangle_{45} + |\Phi^-\rangle_{12}|\Psi^-\rangle_{36}|\Psi^+\rangle_{45} \\ &+ |\Psi^-\rangle_{12}|\Psi^+\rangle_{36}|\Phi^-\rangle_{45} + |\Psi^+\rangle_{12}|\Phi^-\rangle_{36}|\Psi^-\rangle_{45}) \quad (2) \\ &= \frac{1}{2}(-|\Phi^-\rangle_{13}|\Phi^-\rangle_{24}|\Phi^+\rangle_{56} + |\Phi^+\rangle_{13}|\Psi^+\rangle_{24}|\Psi^+\rangle_{56} \\ &- |\Psi^+\rangle_{13}|\Psi^-\rangle_{24}|\Phi^-\rangle_{56} - |\Psi^-\rangle_{13}|\Phi^+\rangle_{24}|\Psi^-\rangle_{56}) \quad (3) \\ &= \frac{1}{2}(|\Phi^-\rangle_{14}|\Phi^+\rangle_{26}|\Phi^-\rangle_{35} + |\Phi^+\rangle_{14}|\Psi^+\rangle_{26}|\Psi^+\rangle_{35} \\ &+ |\Psi^-\rangle_{14}|\Psi^-\rangle_{26}|\Phi^+\rangle_{35} + |\Psi^+\rangle_{14}|\Phi^-\rangle_{26}|\Psi^-\rangle_{35}) \quad (4) \\ &= \frac{1}{2}(|\Phi^+\rangle_{15}|\Phi^+\rangle_{23}|\Phi^+\rangle_{46} + |\Phi^-\rangle_{15}|\Psi^+\rangle_{23}|\Psi^-\rangle_{46} \\ &+ |\Psi^+\rangle_{15}|\Psi^-\rangle_{23}|\Phi^-\rangle_{46} + |\Psi^-\rangle_{15}|\Phi^-\rangle_{23}|\Psi^+\rangle_{46}) \quad (5) \\ &= \frac{1}{2}(|\Phi^-\rangle_{16}|\Phi^+\rangle_{25}|\Phi^-\rangle_{34} + |\Phi^+\rangle_{16}|\Psi^-\rangle_{25}|\Psi^-\rangle_{34} \\ &+ |\Psi^+\rangle_{16}|\Psi^+\rangle_{25}|\Phi^+\rangle_{34} + |\Psi^-\rangle_{16}|\Phi^-\rangle_{25}|\Psi^+\rangle_{34}) \quad (6) \end{aligned}$$

From the above (2–6), it is obvious to see that the other four qubits will collapse to the tensor product of two pairs of EPR when any two qubits of Ψ_{6qb} are measured with the Bell Basis $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$. The Ψ_{6qb} can also be rewritten as

$$\begin{aligned}\Psi_{6qb} = \frac{1}{4}[&|\Phi^+\rangle_{12}(\ |\Phi^+\rangle_{34}\ |\Phi^+\rangle_{65} + |\Phi^-\rangle_{34}|\Phi^-\rangle_{65}\\ &+\ |\Psi^+\rangle_{34}\ |\Psi^+\rangle_{65} + |\Psi^-\rangle_{34}|\Psi^-\rangle_{65})\\ &+|\Phi^-\rangle_{12}(-\ |\Phi^+\rangle_{34}\ |\Phi^-\rangle_{65} + |\Phi^-\rangle_{34}|\Phi^+\rangle_{65}\\ &-\ |\Psi^+\rangle_{34}\ |\Psi^-\rangle_{65} + |\Psi^-\rangle_{34}|\Psi^+\rangle_{65})\\ &+|\Psi^+\rangle_{12}(\ |\Phi^+\rangle_{34}\ |\Psi^+\rangle_{65} + |\Phi^-\rangle_{34}|\Psi^-\rangle_{65}\\ &-\ |\Psi^+\rangle_{34}\ |\Phi^+\rangle_{65} - |\Psi^-\rangle_{34}|\Phi^-\rangle_{65})\\ &+|\Psi^-\rangle_{12}(-\ |\Phi^+\rangle_{34}\ |\Psi^-\rangle_{65} + |\Phi^-\rangle_{34}|\Psi^+\rangle_{65}\\ &+\ |\Psi^+\rangle_{34}\ |\Phi^-\rangle_{65} - |\Psi^-\rangle_{34}|\Phi^+\rangle_{65})] \end{aligned} \tag{7}$$

On the other hand, we know that when one of the Pauli unitary operators $\{I, \sigma_X, i\sigma_Y, \sigma_Z\}$ is applied to one particle of a Bell state, it will be transformed into another Bell state. For instance,

$$\begin{aligned}(I \otimes I)|\Phi^+\rangle &= |\Phi^+\rangle\\ (\sigma_Z \otimes I)|\Phi^+\rangle &= |\Phi^-\rangle\\ (\sigma_X \otimes I)|\Phi^+\rangle &= |\Psi^+\rangle\\ (i\sigma_Y \otimes I)|\Phi^+\rangle &= |\Psi^-\rangle \end{aligned} \tag{8}$$

Local unitary transformation will not change the entanglement of quantum state, so Ψ_{6qb} will be changed into another BPB state. Let us agree on the following encoding:

$$\begin{aligned}|\Phi^+\rangle &: 00, \quad |\Phi^-\rangle : 01\\ |\Psi^+\rangle &: 10, \quad |\Psi^-\rangle : 11 \end{aligned} \tag{9}$$

$$\begin{aligned}I &: 00, \quad \sigma_Z : 01\\ \sigma_X &: 10, \quad i\sigma_Y : 11 \end{aligned} \tag{10}$$

We denote the encoding of x as $Encod(x)$ where $x \in \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle, I, \sigma_Z, \sigma_X, i\sigma_Y\}$. For example, $Encod(|\Phi^-\rangle) = 01$ and $Encod(\sigma_Z) = 01$. We can let $Encod(y) = Encod(-y)$ ($y \in \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$) because the measurement outcome of $-y$ will be y with certainty if it is measured with Bell basis. Actually, we can say that y and $-y$ are the same up to a global phase factor -1.

After the above encoding (9–10) , the (7) tells us that if we measure particle 1,2 , particle 3,4 and particle 6,5 with Bell basis, respectively, then the responding measurement outcomes R_{12}, R_{34} and R_{65} satisfy the following equation:

$$Encod(R_{12}) \oplus Encod(R_{34}) \oplus Encod(R_{65}) = 00 \tag{11}$$

Furthermore, if unitary operators U_1, U_2 and U_3 ($U_1, U_2, U_3 \in \{I, \sigma_Z, \sigma_X, i\sigma_Y\}$) are applied to particle 1, particle 3 and particle 6, respectively, and then particle 1,2 , particle 3,4 and particle 6,5 are measured with Bell basis, respectively, the measurement outcomes R'_{12}, R'_{34} and R'_{65} satisfy the following equation:

$$\begin{aligned}&Encod(U_1) \oplus Encod(U_2) \oplus Encod(U_3)\\ &= Encod(R'_{12}) \oplus Encod(R'_{34}) \oplus Encod(R'_{65}) \end{aligned} \tag{12}$$

3 The Presented Multi-Party Quantum Key Agreement Protocol

In this section, we introduce our MQKA protocol, in which the participants can share a secret key. In our protocol, we assume that the classic channel is authenticated. Suppose that n participants, $P_0, \cdots, P_{n-1}$, have secret bit strings $K_0, \cdots, K_{n-1}$, respectively. They want to derive a secret key $K = K_0 \oplus \cdots \oplus K_{n-1}$. Here, $\oplus$ denotes the addition module 2.

$$\begin{aligned} K_0 &= (k_{0L}, k_{0(L-1)}, \ldots, k_{01}) \\ &\cdots \\ K_i &= (k_{iL}, k_{i(L-1)}, \ldots, k_{i1}) \\ &\cdots \\ K_{n-1} &= (k_{(n-1)L}, k_{(n-1)(L-1)}, \ldots, k_{(n-1)1}) \\ K_0 \oplus \ldots \oplus K_{n-1} &= (k_{0L} \oplus \ldots \oplus k_{(n-1)L}, \ldots, k_{01} \oplus \ldots \oplus k_{(n-1)1}) \end{aligned} \tag{13}$$

where L is even (for simplicity) and represents the length of secret bit string.

The presented multi-party quantum key agreement protocol can be described as follows.

(S1) For each P_i, he first prepares $\frac{L}{2}$ BPB state Ψ_{6qb}, where $i \in \{0, \cdots, n-1\}$. Then he picks up the particles 3, 4 (particles 6, 5) from each Ψ_{6qb} to form an ordered sequence S_{34} (S_{65}). After that P_i prepares some decoy particles, each of which is in one of the quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. He randomly inserts the decoy particles into the sequence S_{34} (S_{65}) to form a new sequence S^*_{34} (S^*_{65}). Note that only P_i know the initial states and positions of the d decoy particles. Then, P_i transmits S^*_{34} (S^*_{65}) to $P_{(i-1)modn}$ ($P_{(i+1)modn}$), and only keeps particles 1, 2 in his lab. For simplicity, let us denote $P_{(i-1)modn}$ and $P_{(i+1)modn}$ as P_{i-1} and P_{i+1}, respectively.

(S2) Confirming that P_{i-1} and P_{i+1} have received all the particles of S^*_{34} and S^*_{65}, respectively. P_i announces the positions and the bases of the decoy particles to P_{i-1} and P_{i+1}, respectively. In the following, P_{i-1} and P_{i+1} measure the decoy particles in the correct bases according to P_i's announcement and randomly publish half of their measurement outcomes. Then P_i announces the initial states of the left half of the decoy particles. At last, they check whether the initial states and the measurement results are consistent. If they are not consistent, this protocol will be aborted and repeat the step (1). Otherwise, the protocol will go to the next step.

(S3) P_{i-1} and P_{i+1} remove the particles of the sample states. Then they perform operation $U_{P_{i-1}}$ and $U_{P_{i+1}}$ ($U_{P_{i-1}}, U_{P_{i+1}} \in \{I, \sigma_X, \sigma_Y, \sigma_Z\}$) on the particle 3 and particle 6 of each Ψ_{6qb} of the ordered sequence according to their input and the encoding agreement (10), respectively. For example, if the $jth\left(j = 1, 2, \ldots, \frac{L}{2}\right)$ two bits of the input of P_{i-1} and P_{i+1} are 11 and 01, respectively. P_{i-1} and P_{i+1} will perform operation$i\sigma_Y$ and σ_Z on the particle 3 and particle 6 of the jth BPB state Ψ_{6qb} respectively.

(S4) If all the participants have finished steps (1)–(3), then they go to the next step.

(S5) P_{i-1} and P_{i+1} randomly insert the decoy states into the encoded particle sequence S_{34} and particle S_{65} respectively by the decoy method described in step (1) and step (2), and then send them to P_{i-2} and P_{i+2}, respectively.

(S6) The participants carry out the protocol similar to steps (2)–(5) until participants $P_{i-\frac{n-1}{2}}$ and $P_{i+\frac{n-1}{2}}$ have sent the encoded particle sequences to P_i if the security checking of quantum channels is passed.

(S7) If all the participants have finished steps (1)–(6), then they go to the next step.

(S8) After confirming that P_i has received the sequence from $P_{i-\frac{n-1}{2}}$ and $P_{i+\frac{n-1}{2}}$, they announce the positions and the corresponding bases of the decoy particles. Then for each of the decoy particles, P_i measures the decoy particles in the correct bases . After that, he asks $P_{i-\frac{n-1}{2}}$ and $P_{i+\frac{n-1}{2}}$ to announce the initial states of the decoy particles respectively. At last, he checks whether the initial states and the measurement results are consistent. If there are consistent with each other, they continue to the next step; otherwise, they abort this protocol and restart from step (1).

(S9) After receiving the encoded particle sequence S_{34} and particle sequence S_{65}, P_i performs unitary operation U_{P_i} on the particle 1 of each Ψ_{6qb} of the ordered sequence according to his input and the encoding agreement (10), then he measures particles 1,2, particles 3,4 and particles 6,5 of the $jth\Psi_{6qb}\left(j=1,2,\ldots,\frac{L}{2}\right)$ with the Bell basis. Then he will obtain the final key. Suppose their measurement outcomes of the jth Ψ_{6qb} are R_{12}^j, R_{34}^j and R_{65}^j, then he will get the final key of the jth two bits $K^j = Encod\left(R_{12}^j\right) \oplus Encod\left(R_{34}^j\right) \oplus Encod\left(R_{65}^j\right)$.

4 Analysis of the Presented Protocol

In this section, we will prove that our protocol is secure. Generally speaking, the security analysis of quantum key agreement protocol is more complex than quantum key distribution (QKD) [5, 6, 48–50] and quantum secure direct communication (QSDC) [17, 18, 51–54] because the attacks from all participants have to be considered in quantum key agreement protocols. In other words, the outside eavesdroppers try to obtain the shared key. While, some participants may try to determine the shared key alone. Therefore, the security of quantum key agreement protocol is to prevent both outside and participant attacks. For clarity, we assume that the party P_i starts the protocol.

4.1 Outside Attacks

In our protocol, we use the decoy particles to prevent the eavesdropping. This idea is derived from the quantum key distribution protocol [6]. In decoy-state method, besides target states, several other non-orthogonal states as decoy states are used. Since eavesdropper cannot distinguish between the target states and the decoy states, she has to apply the same strategy to all of them. As a result, any eavesdropping attempt by eavesdropper will inevitably modify the photon statistic and expose her [55–57]. Therefore, any eavesdropping will be discovered in the protocol by using the decoy-state method. Without loss of generality, the most general operation U_E Eve employed is to cause the intercepted photons to interact coherently with an auxiliary quantum system $|E\rangle$. Then she sends the operated photons to the receivers. Suppose that U_E satisfies the following conditions.

$$U_E|0\rangle|E\rangle = a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle, \tag{14}$$

$$U_E|1\rangle|E\rangle = c|0\rangle|E_{10}\rangle + d|1\rangle|E_{11}\rangle, \tag{15}$$

where $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$. If Eve introduces no error in the eavesdropping check, the general operation U_E must satisfy the following conditions.

$$\begin{aligned} U_E|0\rangle|E\rangle &= a|0\rangle|E_{00}\rangle, \\ U_E|1\rangle|E\rangle &= d|1\rangle|E_{11}\rangle, \end{aligned} \tag{16}$$

$$\begin{aligned} U_E|+\rangle|E\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle + c|0\rangle|E_{10}\rangle + d|1\rangle|E_{11}\rangle) \\ &= \frac{1}{2}(|+\rangle(a|E_{00}\rangle + b|E_{01}\rangle + c|E_{10}\rangle + d|E_{11}\rangle)) \\ &+ \frac{1}{2}(|-\rangle(a|E_{00}\rangle - b|E_{01}\rangle + c|E_{10}\rangle - d|E_{11}\rangle)) \\ &= \frac{1}{2}(|+\rangle(a|E_{00}\rangle + b|E_{01}\rangle + c|E_{10}\rangle + d|E_{11}\rangle)) \end{aligned} \tag{17}$$

$$\begin{aligned} U_E|-\rangle|E\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle - c|0\rangle|E_{10}\rangle - d|1\rangle|E_{11}\rangle) \\ &= \frac{1}{2}(|+\rangle(a|E_{00}\rangle + b|E_{01}\rangle - c|E_{10}\rangle - d|E_{11}\rangle)) \\ &+ \frac{1}{2}(|-\rangle(a|E_{00}\rangle - b|E_{01}\rangle - c|E_{10}\rangle + d|E_{11}\rangle)) \\ &= \frac{1}{2}(|-\rangle(a|E_{00}\rangle - b|E_{01}\rangle - c|E_{10}\rangle + d|E_{11}\rangle)). \end{aligned} \tag{18}$$

From the above (16), (17) and (18), we have the following Eqs.

$$b|E_{01}\rangle = 0 \tag{19}$$

$$c|E_{10}\rangle = 0 \tag{20}$$

$$a|E_{00}\rangle - b|E_{01}\rangle + c|E_{10}\rangle - d|E_{11}\rangle = 0 \tag{21}$$

$$a|E_{00}\rangle + b|E_{01}\rangle - c|E_{10}\rangle - d|E_{11}\rangle = 0. \tag{22}$$

Here 0 denote a column zero vector. Further, we can get $a = d = 1$, $b = c = 0$ and $|E_{00}\rangle = |E_{11}\rangle$. Therefore, we have $U_E\Psi_{6qb}|E\rangle = \Psi_{6qb}|E^{'}\rangle$, i.e., Eve introduce no error in the eavesdropping only when her ancillary state and the target photon are product states. So outside eavesdroppers cannot obtain the shared key without being detected.

Since our protocol transmits the same photons more than once, it may suffer from the Trojan horse attacks. Such kind of circular quantum transmission has been discussed [58–62]. To prevent this type of attacks, participants can install a special quantum optical device such as the wavelength quantum filter and the photon number splitters (PNS) to detect an attack. According to Refs. [58–62], Eve's invisible photons can be filtered out by using the wavelength quantum filter, and the PNS can split each legitimate photon to discover the delay photons. If there is an irrational high rate of multi-photon signal, then the attack can be detected. As pointed out in Ref. [60], this kind of Trojan horse attack is not an exploit of a weakness of the protocol in itself, but rather an exploit of a weakness in certain imperfect implementations. Without the imperfection of the single-photon detectors, this kind of Trojan horse attack will not exist any longer.

4.2 Participant Attack

Generally speaking, the participant is the most powerful attacker in the multi-party computation protocols [63]. If the presented QKA protocol is secure for the dishonest participants, it is also secure for any eavesdropper.

Because of the decoy-photon technique, eavesdropper's several kinds of outsider attacks, such as the intercept-resend attack, measurement-resend attack, entanglement-measure attack and the denial-of-service attack can be detected. Notice that if P_i is the first one that

finishes the protocol, then he will be the first one that gets the shared key. Then he can decide the final key alone. For example, suppose P_i has already obtain the shared key k, where k is the bitwise of $P_0, \cdots, P_{n-1}$'s keys. Then P_i encodes $k' \oplus k \oplus k_i$ as his secret key, instead of k_i, when other participants as senders carry out their protocol, where k' is the key that P_i desired and k_i is P_i's secret key. Therefore, other participants will accept k' as the final shared key. Thus, this protocol is not a fair key agreement in this situation. To avoid this unfairness, all the participant cannot execute the steps (8)-(9) until all the other participants have accomplished the steps (1)-(9). Then P_i has no chance to know the share key ahead of the others. Then this attack can be avoided automatically. Notice that the decoy-state method is also used to detect the dishonest of P_i in the presented protocol.

4.3 Security Analysis Over Noisy Quantum Channel

The security of our protocol is analyzed under the condition that all quantum channels are noiseless. Since it is hard to build perfect quantum channels in a practical transmission process, the success probability of quantum communication would be decreased under noisy conditions. In this subsection, we show that our protocol is still secure over noisy quantum channel.

Eve may intercept the particles sent from P_i to P_{i-1} and P_{i+1}. She then performs intercept-resend attack or entangle-measure attack, and forwards these tampered particles to P_{i-1} and P_{i+1} through an ideal channel (supposed that she has the ability to establish an ideal quantum channel). Eve tries to cover up her attack by the way that it seems for honest participants that the error induced by her attack just like the the noise of the quantum channel. We have learned that the quantum bit error rate of noise (ϵ) is roughly between 2 % and 8.9 % depending on the different channel situations. The above attacks will not be detected if the eavesdropper detection rate of our protocol is smaller than ϵ. Fortunately, the detection rate using the decoy method in our protocol is 25 % which is greater than ϵ. Therefore, the presented protocol will be secure even in the noisy quantum channel.

4.4 Efficiency Analysis

Here, the particle efficiency is defined as $\eta = c/q$, where, c denotes the length of the final secret key, and q is the number of the transmitted qubits on the quantum channel. In order to generate 2 bits of shared key, each party has to prepare a BPB state and enough decoy particles in our protocol. Hence, the qubit efficiency of our protocol can be computed, $\eta = \frac{2}{(2\kappa+4)n} = \frac{1}{(\kappa+1)n}$, where κ is the detection rate and n is the number of the participants. While, the qubit efficiency of the improved MQKA in Ref. [44] is $\frac{1}{(\kappa+1)n}$. Hence, our new protocol is as efficient as it.

5 Conclusions

We present a multi-party quantum key agreement protocol based on the genuinely maximally entangled six-qubit state. In our protocol, participants can agree on a key and no one can determine the shared key alone. We have also shown that it is secure against both outside and participant attacks. Up to now, dealing with a BPB state is far more involved than the counterparts involving two or three particles, so our protocol may be difficult to realize

physically. However, utilizing multi-particle entanglement to constructing quantum cryptography protocols is important in theory, and further research on applications of multi-qubit entanglement is need in the future.

Acknowledgments The authors would like to thank anonymous referees for very useful comments. This work is supported by the National Natural Science Foundation of China (No.61272013, No. 61402293 and No.61171072), the Key Program for Technology and Innovation of College in Guangdong Province (No. CXZD1143), Natural Science Foundation of Guangdong Province (No. S2013040011789), Shenzhen Technology Plan (No. JCYJ20150324141711665, No. JCYJ20150324141711694, No. JCYJ20150324141711562 and No. JCYJ20130401095947219), Natural Science Foundation of SZU(No. 201435), Innovative Research Team of Shenzhen University, and Postdoctoral Science Foundation of China (No. 2015M572360).

References

1. Diffie, W., Hellman, M.: IEEE Trans. Inf. Theory **22**(6), 644 (1976)
2. Ingemarsson, I., Tang, D., Wong, C.: Trans. IEEE Inf. Theory **28**(5), 714 (1982)
3. Grover, L.K.: In Proceedings of 28th Annual ACM Symposium on Theory of Computing (1996), pp. 212C219
4. Shor, P.W.: In Proceedings of 35th Annual Symposium on the Foundation of Computer Science (1994), pp. 124C134
5. Shor, P.W., Preskill, J.: Phys. Rev. Lett. **85**(2), 441 (2000)
6. Bennett, C.H., Brassard, G.: In Proceedings of IEEE International Conference on Com- puter, System and Signal (1984), pp. 175C179
7. Bennett, C.H., Wiesner, S.J.: Phys. Rev. Lett. **69**(20), 2881 (1992)
8. Goldenberg, L., Vaidman, L.: Phys. Rev. Lett. **75**(7), 1239 (1995)
9. Deng, F.G., Long, G.L.: Phys. Rev. A **70**, 012311 (2004)
10. Zhang, C.-M., Song, X.-T., Treeviriyanupab, P., Li, M., Wang, C., Li, H.-W., Yin, Z.-Q., Chen, W., Han, Z.-F.: Sci. Bullet **59**, 2825–2828 (2014)
11. Zhang, C.X., Guo, B.H., Cheng, G.M., Guo, J.J., Fan, R.H.: Sci. China: Phys. Mech. Astron. **57**, 2043–2048 (2014)
12. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
13. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)
14. Gottesman, D.: Phys. Rev. A **61**, 042311 (2000)
15. Zhang, Z.j., Li, Y., Man, Z.x.: Phys. Rev. A **71**, 044301 (2005)
16. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
17. Wang, C. et al.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
18. Wang, T.J., Li, T., Du, F.F., Deng, F.G.: Chin. Phys. Lett. **28**, 040305 (2011)
19. Gu, B. et al.: Sci. China Phys. Mech. Astron **54**, 942–947 (2011)
20. Gu, B. et al.: Chin. Phys. B **20**, 100309 (2011)
21. Sun, Z.W., Du, R.G., Long, D.Y.: Int. J. Quantum Inf. **10**(01) (2012)
22. Sun, Z.W., Du, R.G., Long, D.Y.: Int. J. Theor. Phys. **51**, 1946 (2012)
23. Ren, B.C. et al.: Eur. Phys. J. D **67**, 30 (2013)
24. Chang, Y., Xu, C., Zhang, S., Yan, L.: Sci. Bullet **58**, 4571–4576 (2013)
25. Chang, Y., Xu, C., Zhang, S., Yan, L. Sci. Bullet **59**, 2541–2546 (2014)
26. Zou, X.F., Qiu, D.W.: Sci. China Phys. Mech. Astron **57**, 1696–1702 (2014)
27. Yang, Y.G., Wen, Q.Y.: J. Phys. A. Math. Theor. **42**(5), 055305 (2009)
28. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: Opt. Commun. **283**(7), 1561 (2010)
29. Wen, L., Yong Bin, W., Zheng Tao, J.: Opt. Commun. **284**(12), 3160 (2011)
30. Hsin Yi, T., Jason, L., Tzonelih, H.: Quantum Inf. Process **11**(2), 373 (2012)
31. Sun, Z.W., Long, D.Y.: Int. J. Theor. Phys. **52**, 212 (2013)
32. Sun, Z., Yu, J., Wang, P., Xu, L., Wu, C.: Quantum Inf. Process **14**(6), 2125–2133 (2015)
33. Zeng, G., Keitel, C.H.: Phys. Rev. A **65**, 042312 (2002)
34. Li, Q., Chan, W.H., Long, D.Y.: Phys. Rev. A **79**, 054307 (2009)
35. Sun, Z., Yu, J., Wang, P., Xu, L.: Phys. Rev. A **91**, 052303 (2015)
36. Zhou, N., Zeng, G., Xiong, J.: Electron. Lett. **40**(18), 1149 (2004)

37. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Phys. Rev. Lett. **70**(13), 1895 (1993)
38. Tsai, C., Hwang, T.: Technical Report, C-S-I-E, NCKU, Taiwan, ROC (2009)
39. Song Kong, C., Chia Wei, T., Tzonelih, H.: Int. J. Theor. Phys. **50**(6), 1793 (2011)
40. Song Kong, C., Tzonelih, H.: Opt. Commun. **283**(6), 1192 (2010)
41. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum Inf. Process. **13**(3), 649 (2014)
42. Shi, R.H., Zhong, H.: Quantum Inf. Process. **12**(2), 921 (2013)
43. Liu, B., Gao, F., Huang, W., Wen, Q.y.: Quantum Inf. Process. **12**(4), 1797 (2013)
44. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Quantum Inf. Process. **12**(11), 3411 (2013)
45. Borras, A., Plastino, A., Batle, J., Zander, C., Casas, M., Plastino, A.: J. Phys. A. Math. Theor. **40**(44), 13407 (2007)
46. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**(3), 648 (1999)
47. Long, Y., Qiu, D., Long, D.: J. Phys. A. Math. Theor. **45**(19) (2012)
48. Lo, H.K., Chau, H.F.: Science **283**(5410), 2050 (1999)
49. He, G.P.: J. Phys. A, Math. Theor, 44 (2011)
50. Furrer, F., Franz, T., Berta, M., Leverrier, A., Scholz, V.B., Tomamichel, M., Werner, R.F.: Phys. Rev. Lett. **109**(10) (2012)
51. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**(4), 042317 (2003)
52. Gao, T., Yan, Y.L., Wang, Z.X.: J. Phys. A. Math. Gen. **38**(25), 5761 (2005)
53. Zhu, S.L., Qiao-Yan, W., Fei, G., Fu, C.: Phys. Rev. A **78**(6), 064304 (2008)
54. Liu, D., Chen, J.L., Jiang, W.: Int. J. Theor. Phys. **51**(9), 2923 (2012)
55. Hwang, W.Y.: Phys. Rev. Lett. **91**, 057901 (2003)
56. Li, C.Y. et al.: Chin. Phys. Lett. **22**, 1049 (2005)
57. Li, C.Y. et al.: Chin. Phys. Lett. **23**, 2896 (2006)
58. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.j.: Phys. Rev. A **72**, 044302 (2005)
59. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006)
60. Cai, Q.Y.: Phys. Lett. A **351**, 23 (2006)
61. Lin, J., Yang, C.W., Tsai, C.W., Hwang, T.: Int. J. Theor. Phys. **52**(1), 156 (2013)
62. Lin, J., Hwang, T.: Quantum Inf. Process **12**(1), 685 (2013)
63. Goldreich, O.: Foundations of Cryptography: Volume 2, Basic Applications Cambridge university press (2009)