EasyChair Preprint

№ 2053

SS1: Quantum key agreement via non-maximally entangled Bell states

Taichao Li and Min Jiang

November 29, 2019

Quantum key agreement via non-maximally entangled Bell states

Taichao Li[1], Min Jiang[1,2*]
1. School of Electronics & Information Engineering, Soochow University, Suzhou 215006, People′s Republic of China
2. Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai, 200240, People′s Republic of China
E-mail: jiangmin08@suda.edu.cn

***Abstract*—In this paper, we propose one new quantum key agreement (QKA) protocol using non-maximally entangled Bell states with positive operator-valued measurement (POVM). It is designed for multi-party QKA by non-maximally entangled Bell states with POVM. Since Bell states and single particle can be obtained by various physical systems, thus, our protocol is feasible based on the current technology. It is secure against the outsider and participant attack. Further, it is shown that the shared key is decided by all participants. Therefore, it could guarantee the security and fairness.**

Keywords—quantum key agreement, multi-party key agreement, positive operator-valued measurement, non-maximally entangled Bell state

Ⅰ. INTRODUCTION

With the development of quantum information technology, quantum cryptography has drawn more and more attention [1-2]. Its security is guaranteed by the principles of quantum mechanics, rather than the assumption of computational complexity. Therefore, quantum cryptographic protocols can theoretically provide unconditional security. Many kinds of quantum cryptographic protocols have been proposed, such as quantum key distribution (QKD), quantum secret sharing (QSS), quantum secure direct communication (QSDC), quantum signature (QS) and so on.

Recently, quantum key agreement (QKA) has attracted lots of attention. Different from QKD, QKA is aimed to distribute the shared key among two or more parties in a secure manner where each party contributes its part to the shared key, and the shared key should not be determined fully by any subset alone. In 2004, Zhou et al. [3] proposed the first QKA protocol which contained two parties and utilized the quantum teleportation technique. Almost simultaneously Hsueh and Chen [4] proposed another QKA protocol based on Bell pairs. However, in 2009, Tsai et al. [5] found that it could not resist participant attack since a participant could determine the final shared key alone without being detected. Later, Tsai et al. [6] showed that the protocol proposed by Hsueh and Chen did not qualify as a protocol of QKA. In 2010, Chong et al. [7] proposed a QKA protocol based on the BB84 protocol, which utilized a delayed measurement technique. It was the first successful QKA protocol. However, above QKA protocols only involved two-party case. In 2013, Shi et al. [8] presented a multi-party QKA (MQKA) protocol by using the entanglement swapping technique. In the same year, Liu et al. [9] pointed out that Shi et al.'s protocol was not a fair QKA protocol and then put forward another MQKA protocol with single particle. Later, a MQKA protocol with Bell state and Bell state measurement was proposed by Shukla et al. [10]. However, their protocol's efficiency was low. To improve the qubit efficiency of Liu's MQKA protocol, Sun et al. [11] presented a new multi-party QKA protocol. However, it could not achieve privacy and fairness, which was shown by Huang et al. [12]. Latter Min et al. [13] put forward a multi-party QKA protocol with G-Like states and Bell states, which demonstrated a high efficiency. Recently, Yang et al. [14] gave a new quantum key agreement protocols based on Bell states. In addition, many other different QKA protocols have been proposed based on multipartite entangled state, such as cluster states, brown states and W states [15-17].

Although several QKA schemes based on Bell states have been proposed, these schemes have yet to be improved in terms of the efficiency, quantum and classical resource consumption. However, in a real environment, due to decoherence and noise maximally entangled channels readily evolve into non-maximally entangled states. The common solutions to this problem are quantum distillation [18] and local filtering [19]. However, they inevitably increase operational complexity. So far, there have been many quantum communication schemes reported where non-maximally entangled states are used directly, such as probabilistic quantum teleportation, secure quantum dialogue, probabilistic remote state preparation, quantum state sharing and so on.

In this paper, multi-party QKA protocol is proposed based on non-maximally entangled Bell states. The fairness means that the final key needs to be determined by all participants. The security is ensured by the decoy particles method. Security analysis indicates that these two protocols can resist the dishonest participant and outside eavesdropper attacks.

The rest of this paper is organized as follows. In Section 2, we firstly introduce how to distinguish four non-maximally entangled Bell states with known parameters and give detailed procedures of quantum key agreement protocols, respectively. In Section 3, we prove that our QKA protocol is safe against both external and participant attacks. Finally, we summarize and discuss our QKA protocol in Section 4.

Ⅱ. HOW TO DISTINGUISH FOUR NON-MAXIMALLY ENTANGLED BELL STATES

A non-maximally entangled Bell state is written as $|\varphi_0\rangle_{AB}=(a|00\rangle+b|11\rangle)_{AB}$, where two coefficients *a* and b are known and they all satisfy the normalization condition $|a|^2+|b|^2=1$. The subscripts A and B label the corresponding particles in the Bell state. Z basis $\{|0\rangle,|1\rangle\}$ and X basis $\{|+\rangle=1/\sqrt{2}(|0\rangle+|1\rangle),|-\rangle=1/\sqrt{2}(|0\rangle-|1\rangle)\}$ are two orthogonal bases of one qubit, which can be used as decoy states. To change the state of a qubit, one may apply one of four Pauli operations as follows

$$\begin{aligned} I&=\begin{pmatrix}1&0\\0&1\end{pmatrix},\sigma_X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\\ i\sigma_Y&=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\sigma_Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}. \end{aligned} \tag{1}$$

We also introduce two unitary gates CNOT and Hadamard as follows

$$CNOT=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}, \tag{2}$$

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}. \tag{3}$$

We study from $|\varphi_0\rangle_{AB}$ and perform Pauli operations U^B on the second particle of $|\varphi_0\rangle_{AB}$, respectively, which result in the following four non-orthogonal Bell states

$$\begin{aligned} |\varphi_0\rangle_{AB}&=I_B\otimes|\varphi_0\rangle_{AB}=(a|00\rangle+b|11\rangle)_{AB},\\ |\varphi_1\rangle_{AB}&=(\sigma_X)_B\otimes|\varphi_0\rangle_{AB}=(a|01\rangle+b|10\rangle)_{AB},\\ |\varphi_2\rangle_{AB}&=(i\sigma_Y)_B\otimes|\varphi_0\rangle_{AB}=(a|01\rangle-b|10\rangle)_{AB},\\ |\varphi_3\rangle_{AB}&=(\sigma_Z)_B\otimes|\varphi_0\rangle_{AB}=(a|00\rangle-b|11\rangle)_{AB}. \end{aligned} \tag{4}$$

TABLE Ⅰ. THE RESULTING AGREEMENT KEY AFTER A UNITARY OPERATION APPLIED ON A PARTICLE

Unitary operation U^B	Final state	Agreement key
I^B	$\|\varphi_0\rangle$	00
$(\sigma_X)^B$	$\|\varphi_1\rangle$	01
$(i\sigma_Y)^B$	$\|\varphi_2\rangle$	10
$(\sigma_Z)^B$	$\|\varphi_3\rangle$	11

Note that above four Bell states are non-orthogonal. Therefore, they cannot be distinguished by orthogonal projection measurements. However, it is possible to use POVM to distinguish them with a certain probability.

First, we perform unitary operation as $U_{AB}=CNOT_{A,B}$ on particle B, where particle A is the controlling party, and the controlled party is particle B. The transformation formula is as follows:

$$\begin{aligned} |\varphi_0\rangle_{AB}&=U_{AB}\otimes|0\rangle_B\otimes I_B(a|0\rangle+b|1\rangle)_A,\\ |\varphi_1\rangle_{AB}&=U_{AB}\otimes|0\rangle_B\otimes(\sigma_X)_B(a|0\rangle-b|1\rangle)_A,\\ |\varphi_2\rangle_{AB}&=U_{AB}\otimes|1\rangle_B\otimes(i\sigma_Y)_B(a|0\rangle+b|1\rangle)_A,\\ |\varphi_3\rangle_{AB}&=U_{AB}\otimes|1\rangle_B\otimes(\sigma_Z)_B(a|0\rangle-b|1\rangle)_A. \end{aligned} \tag{5}$$

By observation, if we only make single particle measurement on particle B, we cannot distinguish above four states. It is possible to use POVM to distinguish the state of particle A as follows

$$\begin{aligned} |\phi_0\rangle&=(a|0\rangle+b|1\rangle)_A,\\ |\phi_1\rangle&=(a|0\rangle-b|1\rangle)_A. \end{aligned} \tag{6}$$

Since the parameters a and b are known, we can introduce one set of POVM measurement operators to measure particle A.

$$P_i=\frac{1}{x}|\psi_i\rangle\langle\psi_i|,i=0,1; \tag{7}$$

$$P_2=1-\frac{1}{x}\sum_{i=0}^{1}|\psi_i\rangle\langle\psi_i|, \tag{8}$$

where

$$\begin{aligned} |\psi_0\rangle&=F(\frac{1}{a}|0\rangle+\frac{1}{b}b|1\rangle),\\ |\psi_1\rangle&=F(\frac{1}{a}|0\rangle-\frac{1}{b}|1\rangle). \end{aligned} \tag{9}$$

with

$$F=\frac{1}{\sqrt{\frac{1}{a^2}+\frac{1}{b^2}}}. \tag{10}$$

x is a coefficient associated with *a and b*, which makes P_2 a positive operator. We can write these operators P_0,P_1,P_2 in the matrix form as

$$P_0=\frac{F^2}{x}\begin{bmatrix}\frac{1}{a^2}&\frac{1}{ab}\\\frac{1}{ab}&\frac{1}{b^2}\end{bmatrix}, \tag{11}$$

$$P_1=\frac{F^2}{x}\begin{bmatrix}\frac{1}{a^2}&-\frac{1}{ab}\\-\frac{1}{ab}&\frac{1}{b^2}\end{bmatrix}, \tag{12}$$

$$P_2=\begin{bmatrix}1-\frac{2F^2}{xa^2} & 0\\ 0 & 1-\frac{2F^2}{xb^2}\end{bmatrix}. \tag{13}$$

Apparently, it is required that all diagonal elements of P_2 are non-negative such that the minimum value of x is $x_{\min}=\frac{2F^2}{\mu^2}, \mu=\min\{a,b\}$. Since only when the measurement result of particle A obtained is not P_2, we can use POVM to discriminate above four Bell states, the probability of success for POVM can be calculated as

$$\eta={}_1\langle\psi_0|P_0|\psi_0\rangle_1=\frac{4a^2b^2}{x}. \tag{14}$$

Therefore, when we combine the state of particle B and the POVM result of particle A, it is possible to distinguish above four Bell states as shown in Table II.

TABLE Ⅱ. THE MEASURING RESULT OF POVM WITH THE CORRESPONDING FINAL STATE

State of B_j	result of POVM	State of A_j	Final state	Agreement key
$\|0\rangle_{B_j}$	P_0	$(a_i\|0\rangle+b_i\|1\rangle)_{A_j}$	$\|\varphi_0\rangle_{A_jB_j}$	00
	P_1	$(a_i\|0\rangle-b_i\|1\rangle)_{A_j}$	$\|\varphi_1\rangle_{A_jB_j}$	01
	P_2		fail	null
$\|1\rangle_{B_j}$	P_0	$(a_i\|0\rangle+b_i\|1\rangle)_{A_j}$	$\|\varphi_2\rangle_{A_jB_j}$	10
	P_1	$(a_i\|0\rangle-b_i\|1\rangle)_{A_j}$	$\|\varphi_3\rangle_{A_jB_j}$	11
	P_2		fail	null

For example, if the state of particle 2 is $|0\rangle_B$ and the POVM result of particle A is P_0, according to equation (5), the corresponding Bell state is $|\varphi_0\rangle_{AB}$. Then the joint encoding operation of all the other participants is I_B in Table 1. However, if the outcome of POVM is P_2, no information about the identity of the Bell states can be obtained. That is to say, although there is such a situation that cannot be judged, the advantage of POVM is that the measurement never makes a wrong judgment, thereby ensuring the accuracy and reliability of the judgment result.

Ⅲ. QUANTUM KEY AGREEMENT PROTOCOL VIA NON-MAXIMALLY ENTANGLED BELL STATES

Now, let us describe our QKA protocol via non-maximally entangled Bell states with known parameters as follows. Suppose there are M participants $T_i(i=0,1,\cdots,M-1)$ who have passed quantum identity authentication [20]. All participants are expected to negotiate a shared key with length n. Each participant T_i should have a private key K_i with length $2l$ as $K_i=(k_{i,1},k_{i,2},\cdots,k_{i,2l})$.

Note that $2l$ is an integer and $2l\geq\left\lceil n/\prod_{i=1}^{M}p_i\right\rceil$, where p_i is the success probability of POVM for each participant. The generated raw key sequence with length l is

$$K'=(k_{0,1}\oplus k_{1,1}\oplus\cdots\oplus k_{M-1,1},k_{0,2}\oplus k_{1,2}\oplus \cdots\oplus k_{M-1,2},\cdots,k_{0,2l}\oplus k_{1,2l}\oplus\cdots\oplus k_{M-1,2l}). \tag{15}$$

The final negotiation key expected by all participants is

$$K=(k_{0,1}\oplus k_{1,1}\oplus\cdots\oplus k_{M-1,1},k_{0,2}\oplus k_{1,2}\oplus \cdots\oplus k_{M-1,2},\cdots,k_{0,n}\oplus k_{1,n}\oplus\cdots\oplus k_{M-1,n}). \tag{16}$$

Step 1: To generate an n-bit quantum agreement key, each participant $T_i(i=0,1,\cdots,M-1)$ prepares l non-maximally entangled Bell states as $|\varphi 0\rangle_{AB}=(a_i|00\rangle+b_i|11\rangle)_{AB}^{\otimes l}$,where the coefficients a_i and b_i are known and satisfy the normalization condition $|a_i|^2+|b_i|^2=1$. Then, each participant denotes the l ordered Bell states with $\{[A_1,B_1],[A_2,B_2],\cdots[A_l,B_l]\}$, where the subscripts denote two particles of each Bell state. Then T_i picks up each particle from each Bell state orderly to compose two subsequences $S_i^1=\{A_1,A_2,\cdots,A_j,\cdots,A_l\}$ and $S_{i,i\oplus1}^2=\{B_1,B_2,\cdots,B_j,\cdots,B_l\}$.

Step 2: T_i prepares enough decoy particles, which are randomly chosen from four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ and randomly inserts them into two sequences $S_{i,i\oplus1}^2$ to obtain two new sequences $S_{i,i\oplus1}^{2*}$. The purpose of adding decoy states to the particle sequences that to be sent is to detect whether there are eavesdroppers in the communication and to ensure information security. Then T_i sends both $S_{i,i\oplus1}^{2*}$ to his next participant $T_{i\oplus1}$ over the quantum channel.

Step 3: After confirming that $T_{i\oplus1}$ has received the sequences $S_{i,i\oplus1}^{2*}$, T_i and $T_{i\oplus1}$ begin to check eavesdropping. Firstly, T_i announces the positions of decoy particles and their corresponding measurement bases $\{|0\rangle,|1\rangle\}$ or $\{1/\sqrt{2}(|0\rangle+|1\rangle),1/\sqrt{2}(|0\rangle-|1\rangle)\}$, and then $T_{i\oplus1}$ measures the decoy particles in the correct bases and informs T_i of his measurement results. By comparing measurement results and the initial states of the decoy particles, T_i can compute the error rate. If it does not exceed the threshold, they claim that sequences $S_{i,i\oplus1}^{2*}$ are secure and continue to the next step; otherwise, they abandon this communication and restart from step 1.

Step 4: If all sequences are secure, $T_{i\oplus1}$ firstly discards the decoy particles from the mixed particles to recover the initial sequences $S_{i,i\oplus1}^2$. According to his encrypted key sequence $K_{i\oplus1}=(k_{i\oplus1,1},k_{i\oplus1,2},\cdots,k_{i\oplus1,2l-1},k_{i\oplus1,2l})$, $T_{i\oplus1}$ implements the encoding operations. Following the relationship between the encoding positions, secret keys and the encoding unitary operations given in Table 1, $T_{i\oplus1}$ performs unitary operations $U_j^2(j\in\{1,2,\cdots,l\})$ onto particles B_j in the sequences $S_{i,i\oplus1}^2$

respectively. Then, $T_{i\oplus 1}$ makes use of the decoy method described in step 2 to generate a new sequences $S_{i,i\oplus 1}^{2*}$, and sends them to his next participant $T_{i\oplus 2}$.

Step 5: Other participants $T_{i\oplus 2}, T_{i\oplus 3}, \cdots, T_{i\oplus(i-1)}$ check the security and encode messages in the same way as in step 3 and step 4 sequentially. If all sequences are safe after eavesdropping, they encode the corresponding particles of each sequence with their secret keys and insert the decoy particles randomly in the sequences and send them to the next participant. Otherwise, they go back to step 1 and restart our protocol.

Step 6: After receiving the final particle sequence $S_{i,i\oplus 1}^{2}$ and safety verification, T_i performs encoding operations on the particles B_j in the sequences $S_{i,i\oplus 1}^{2}$ and carries out $U_{12} = CNOT_{A_j,B_j}$ operation. Then he performs single-bit measurement on particles $\{B_1, B_2, \cdots, B_j, \cdots, B_l\}$ and the POVM operations on the particles $\{A_1, A_2, \cdots, A_j, \cdots, A_l\}$. In this way, T_i will get the final state containing all encoding operations. Following by the coding rules in Table 1, he can obtain a joint encryption key as K'. Since all other participants perform same operation as T_i at the same time and all participants can get the joint encryption key K'.Finally, each participant announces successful positions of their POVMs in the sequence K'. Note that when all participants have carried out the POVMs, only partial sub-keys selected from the common successful locations in the raw key sequence K' are considered to be the final negotiated key K

$$K=(k_{0,1}\oplus k_{1,1}\oplus\cdots\oplus k_{M-1,1}, k_{0,2}\oplus k_{1,2}\oplus \cdots\oplus k_{M-1,2}, \cdots, k_{0,n}\oplus k_{1,n}\oplus\cdots\oplus k_{M-1,n}). \quad (17)$$

In the above QKA protocol, *m* participants generate an agreement key respectively which only known to themselves, and the final negotiated key *K* cannot be determined by any part of them alone. The participants insert special decoy particles in bases X and Z, in order to prevent a kind participant and outsider attack. In this way, they can achieve both outsider and mutual eavesdropping checking. The detailed security analysis will be given in next section.

Ⅳ. SECURITY ANALYSIS OF OUR QUANTUM KEY AGREEMENT PROTOCOL

In this section, we prove the security of the proposed protocol, and we consider both outsider attack and participant attack.

A. Outsider Attack

The security of the proposed protocols mainly depends on the process for setting up the quantum channels. To set up the secure quantum channels, we use the decoy-particle technique as the references.

Suppose that there is an outside eavesdropper and he can intercept the particle sequences transmitted from one party to the other, and resend the fake sequences prepared by herself (himself) to the corresponding receiver (i.e. the intercept-resend attack). In our proposed QKA protocol, the sender and the corresponding receiver need to accomplish an honesty check before they execute the next step. That is, the sender randomly inserts some decoy particles in the transmitted sequences, requires the receiver to measure them later, and checks their measurement results. In fact, if the eavesdropper takes an intercept-resend attack, he does not know which are decoy particles in the transmitted sequences and which are initial states of the decoy particles. Since each decoy particle is randomly in one of the four states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$, the probability of not being detected is $(1/4)^t$, where *t* is the number of decoy particles in the transmitted sequences. In fact, if any outside eavesdropper is to eavesdrop in transmitting the particle sequences, she must inevitably introduce errors and be detected during the honesty check.

In addition, even if an outside eavesdropper can obtain all classical information transmitted to $S_{i,i\oplus 1}^{2}$ in our multi-party QKA protocols, she (he) doesn't know K_i and the original Bell states of all parties. Thus, the eavesdropper cannot obtain any secret information about the shared key without K_i by the *ith* secret equation,

$$K' = (k_{0,1}\oplus k_{1,1}\oplus\cdots\oplus k_{M-1,1}, k_{0,2}\oplus k_{1,2}\oplus \cdots\oplus k_{M-1,2}, \cdots, k_{0,l}\oplus k_{1,l}\oplus\cdots\oplus k_{M-1,l}). \quad (18)$$

B. Participant Attack

As described in the specific process of our protocol, we can infer they all have similar participant attack strategies. The first participant attack was proposed by Gao et al. [21]. Since a dishonest participant already knows part information of a shared key, the danger of the participant attack cannot be underestimated. The main methods to prevent attacks from dishonest participants are quantum authentication techniques and delayed measurement technique, which can successfully detect dishonest participants before implementing the key agreement protocol. Without loss of generality, we assume that there are dishonest participants. Consider the dishonest participant T_i who wishes to decide the final key by himself and he can do it in two ways. Suppose that once T_i obtains the shared key beforehand, he can control the shared key by selecting corresponding unitary operations. However, our QKA protocol requires neighboring participants to perform eavesdropping checks in sequence. Only when sequences $S_{i,i\oplus 1}^{2*}$ are safe, participants are allowed to encode with their keys. Since all participants perform operations in parallel and obtain the final key at the same time, the chance of a participant getting the negotiated key in advance is very small. In addition, if a dishonest participant wishes to destroy the quantum key agreement protocol, he can perform different encoding operations on particles from different participants. All participants make single-bit measurement and POVM on their own particles, then publish the right position of POVM at the same time respectively. Once the test keys are inconsistent, it is proved that there are some dishonest participants and the existing key sequence is not secure.

Ⅴ. CONCLUSIONS

In this paper, we propose one quantum key agreement protocol via non-maximally entangled Bell states with known parameters, which has the advantage of flexibility due to the weakening requirements on channels. In our protocol, it is the first time to negotiate a key among multi-participants using non-maximally entangled Bell states at the cost of obtaining an original key which is longer than the final agreement key. In this scheme, each participant performs one unitary operation on the same particle sequences with an encrypted key sequence. Then, by performing POVMs, they can negotiate a raw key with the single-bit measurement. Finally, all participants announce the successful locations of their POVMs in the raw key and select the sub-keys of the common location as the final agreement key. Our QKA protocol ensures that each participant contributes equally to the final key, it can also withstand typical outsider and participant attacks. What's more, current technology can generate Bell states and single particles. Therefore, our protocol is feasible with real physical devices.

ACKNOWLEDGMENT

This work is supported by the Tang Scholar project of Soochow University, the National Natural Science Foundation of China (No. 61473199 and 61873162), in part by the Suzhou key industry technology innovation project (No. SYG201808) and the project supported by Key Laboratory of System Control and Information Processing, Ministry of Education, China (Grant No.Scip201804).

REFERENCES

[1] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74, 145-195 (2001)

[2] Liu, B., Gao, F., Wen, Q.Y.: Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J. Quant. Electron. 47, 1389–1390 (2011)

[3] Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. 40, 1149–1150 (2004)

[4] Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information Security Conference, National Taiwan University of Science and Technology, Taipei, pp. 236–242 (2004)

[5] Tsai, C.W., Hwang, T.: On "Quantum key agreement protocol", Technical Report, C-S-I-E, NCKU. Taiwan, R.O.C. (2009)

[6] Tsai, C.W., Chong S.K., Hwang, T.: Comment on quantum key agreement protocol with maximally entangled states. In: Proceedings of the 20th Cryptology and Information Security Conference (CISC 2010), pp. 210–213. National Chiao Tung University, Hsinchu, Taiwan, 27–28 May (2010)

[7] Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. 283, 1192–1195 (2010)

[8] Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. 12, 921–932 (2013)

[9] Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. 12, 1797–1805 (2013)

[10] Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. 13, 2391–2405 (2014)

[11] Sun, Z.W., Zhang, C., Wang, B.H., Li, Q., Long, D.Y.: Improvements on "Multiparty quantum key agreement with single particles". Quantum Inf. Process. 12, 3411–3420 (2013)

[12] Huang, W., Wen, Q.Y., Liu, B., Su, Q., Gao, F.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. Quantum Inf. Process. 13, 1651–1657 (2014)

[13] Min, S.Q., Chen, H.Y., Gong, L.H.: Novel multi-party quantum key agreement protocol with g-like states and bell states. Int. J. Theor. Phys. 57, 1811–1822 (2018)

[14] Yang, Y.G., Li, B.R., Li, D., Zhou, Y.H.: New quantum key agreement protocols based on Bell states. Quantum Inf. Process. 18, 322 (2019)

[15] Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process. 15, 373–384 (2016)

[16] Cai, T., Jiang, M., Cao, G.: Multi-party quantum key agreement with five-qubit brown states. Quantum Inf. Process. 17, 103 (2018)

[17] Wang, S.-S., Xu, G.-B., Liang, X.-Q., Wu, Y.-L.: Multiparty quantum key agreement with four-qubit symmetric W state. Int. J. Theor. Phys. 57(12), 3716–3726 (2018)

[18] Bennett, C.H., Brassard, G., Popescu, S., et al.: Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Phys. Rev. Lett. 76(5), 722-725 (1996)

[19] Gisin, N.: Hidden quantum nonlocality revealed by local filters. Phys. Lett. A 210 (3), 151-156 (1996)

[20] Zawadzki, P.: Quantum identity authentication without entanglement. Quantum Inf. Process. 18, 7 (2019)

[21] Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum information & computation. 7 (4), 329-334 (2007)