Copyright © 2019 Tech Science Press CMC, vol.58, no.3, pp.809-827, 2019

Controlled Secure Direct Communication Protocol *via* the Three-Qubit Partially Entangled Set of States

Gang Xu[1, 2, *], Ke Xiao[1, *], Zongpeng Li[3], Xin-Xin Niu[2, 4] and Michael Ryan[5]

Abstract: In this paper, we first re-examine the previous protocol of controlled quantum secure direct communication of Zhang et al.'s scheme, which was found insecure under two kinds of attacks, fake entangled particles attack and disentanglement attack. Then, by changing the party of the preparation of cluster states and using unitary operations, we present an improved protocol which can avoid these two kinds of attacks. Moreover, the protocol is proposed using the three-qubit partially entangled set of states. It is more efficient by only using three particles rather than four or even more to transmit one bit secret information. Given our using state is much easier to prepare for multiqubit states and our protocol needs less measurement resource, it makes this protocol more convenient from an applied point of view.

Keywords: Controlled secure direct communication, cluster state, three-qubit partially entangled state, entanglement swapping.

1 Introduction

Since the Bennett and Brassard's original article [Bennett and Brassard (1984)] was published, quantum key distribution (QKD) has an approach using quantum mechanics [Jiang, Jiang and Ling (2014)] principles for the participants of communication to share a private key with unconditional security.

With the development of quantum cryptography [Wei, Chen, Niu et al. (2015)] and network communication, security of communication is widely concerned [Chen, Tang, Xu et al. (2018); Chen, Sun, Xu et al. (2017); Xu, Chen, Li et al. (2015); Xu, Chen, Dou

[1] School of Information Science and Technology, North China University of Technology, Beijing, 100144, China.

[2] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[3] School of Computer Science, Wuhan University, Hubei, 430072, China.

[4] Guizhou Provincial Key Laboratory of Public Big Data, GuiZhou University, Guiyang, Guizhou, 550025, China.

[5] School of Computing, Dublin City University, Dublin 9, Ireland.

[*] Corresponding Authors: Gang Xu. Email: gangxu_bupt@163.com;
Ke Xiao. Email: xiaoke@ncut.edu.cn

CMC. doi:10.32604/cmc.2019.04400 www.techscience.com/cmc

et al. (2015); Xu, Chen, Dou et al. (2016)]. Different from QKD, quantum secure direct communication (QSDC) is another field of quantum cryptography. In 2002, Boström and Felbinger presented a ping-pong QSDC protocol using Einstein-Podolsky-Rosen (EPR) state [Boström and Felbinger (2002)]. After that, a series of QSDC protocols [Deng and Long (2004); Wang, Deng, Li et al. (2005); Wang, Fang and Tane (2006); Cao, Yang and Wen (2010)] have been proposed.

Recently, the controlled quantum secure direct communication (CQSDC), a new kind of QSDC, has been proposed and has attracted much attention [Chen, Wang, Du et al. (2008); Chen, Wen, Guo et al. (2008); Gao, Yan and Wang (2005); Xia and Song (2007); Wang, Zhang and Tang (2006); Xia, Song and Song (2008); Zhang, Zhan and Zhang (2009); Chang, Lin, Zeng et al. (2012); Hassanpour and Houshmand (2015); Fang (2014)]. In CQSDC scheme, the receiver cannot get any secret information without the controller's admission. Besides that, if the number of controllers, senders or receivers is more than one, the protocol could also be deemed as a network protocol [Lu, Wang and Wang (2012); Lv and Wang (2017); Pang, Liu, Zhou et al. (2017); Li, Wang, Li et al. (2018); Li, Chen, Sun et al. (2016)]. By using partially entangled GHZ state, Chen et al. [Chen, Wang, Du et al. (2008)] proposed a CQSDC protocol, whose aim is to share the private quantum entanglement keys to encrypt and decrypt the secret information. Using W state, Chen et al. [Chen, Wen, Guo et al. (2008)] proposed a novel CQSDC protocol in which entanglement swapping is utilized and the quantum circuit of it is also put forward. However, W state is difficult to prepare under the conditions of the experiment for multiqubit states. Chang et al. [Chang, Lin and Zeng (2012)] proposed a CQSDC protocol using single photons to carry dealer's information. And they declared that if any eavesdropper wants to steal dealer's information, the lawful participants will discover it and abort their transmission. Hassanpour et al. [Hassanpour and Houshmand (2015)] proposed a CQSDC protocol based on GHZ-like state. In their scheme, the receiver can obtain two-secret bits using entanglement swapping, which guarantees the security of the process. Fang [Fang (2014)] proposed a CQSDC protocol based on EPR pair entanglement swapping to complete the communication, five-particle cluster state is utilized in this protocol to achieve eavesdropping detection which makes the detection probability more than 88%.

A secure CQSDC protocol must meet two needs. First, an outside eavesdropper cannot obtain any information about the transmitted state. Second, if the controller(s) doesn't permit, the receiver cannot obtain the secret information. In 2009, Zhang et al. [Zhang, Zhan and Zhang (2009)] designed a CQSDC protocol (the ZZZ protocol) with four particle cluster states using swapping quantum entanglement and local unitary operations. However, Yang et al. [Yang, Chai, Teng et al. (2011)] shown that the dishonest party Bob can give a special attack strategy. By using fake entangled particles, Bob can obtain Alice's secret information without the permission of the controller. Besides that, they gave a further improvement to resist their proposed attack. Then, Qin [Qin (2012)] analyzes the ZZZ protocol and found another special attack, disentanglement attack. Using this attack, the control function of Charlie in the ZZZ protocol [Zhang, Zhan and Zhang (2009)] can be eliminated by the receiver Bob without the knowledge of Charlie. In addition, this new attack is also valid for the improved scheme in Yang et al.'s protocol [Yang, Chai, Teng et al. (2011)]. However, Qin did not propose a further improved protocol. In conclusion, no effective protocol is proposed at last.

According to the above three papers, we further analyze the reasons why the ZZZ protocol cannot resist fake entangled particles attack and disentanglement attack. At last, we find out two reasons. On one hand, Bob prepares the four particle cluster states and he is the last one to measure his own particles in the detection of eavesdropping. Under this circumstance, he can prepare any state (fake entangled particles) which can be used to deceive Charlie, the controller, without being detected. On the other hand, he owns half particles of the four particle cluster states. And one of his two particles is equal to Alice's particle and another is equal to Charlie's. Then, Bob can measure the particle which is equal to Charlie's and get rid of the control of Charlie (disentanglement attack).

Considering these weaknesses, we investigate whether it is possible to make it secure by letting Charlie prepare the four particle cluster states and Alice be the last one to measure her particles. However, if we only change these of the protocol, it is still insecure under disentanglement attack. Thus, we can let Charlie perform some operations on the cluster states as secret information which is only known by him, and then Bob cannot use disentanglement attack to make Charlie out of the control of the communication. In summary, we propose a novel protocol with two versions of improvement in which the communication is secure under the above two attacks as well as some other attacks. What's more, without the permission of the controller, the secret information cannot be recovered by the receiver or any other.

Furthermore, based on three-qubit partially entangled set of states, we also investigate a new CQSDC protocol which has many distinct advantages compared with many previous protocols. First, our protocol uses less quantum resources to transmit the same information. In other words, the protocol [Chen, Wang, Du et al. (2008)] transmits one bit by using six particles, but in our protocol, one bit is transmitted only by using three particles. Second, our three-qubit partially entangled set of state is much easier to prepare than GHZ state in Wang et al.'s protocol [Wang, Zhang and Tang (2006)], W state [Xia, Song and Song (2008)] and four particle cluster state [Zhang, Zhan and Zhang (2009)]. Third, our protocol uses less effective measurements than the ZZZ protocol. In some sense, our protocol has a lower cost than the ZZZ protocol.

The rest of this paper is organized as follows. In Section 2, two new improved protocols are proposed. Then we analyze that our new improved protocol is secure under fake entangled particles attack and disentanglement attack. In Section 3, we give a new CQSDC protocol. Finally, the paper is ended up with a conclusion in Section 4.

2 The new improved CQSDC protocol

In this section, we propose a new improved CQSDC protocol which is secure under the fake entangled particles attack and disentanglement attack. In our improved protocol, it is Charlie rather than Bob who prepares four particle cluster states. In fact, Bob wants to remove Charlie's control and obtain Alice's secret freely. Yang et al. [Yang, Chai, Teng et al. (2011)] presented a fake entangled particles attack on the ZZZ protocol, in which Bob prepares two Bell states rather than a four-qubit cluster state. Then, Bob can obtain

Alice's secret information freely without Charlie's control. And they also gave an improvement to resist their fake entangled particles attack.

However, Qin [Qin (2012)] analyzed further and discovered another special attack, disentanglement attack. Using this attack, the control function of Charlie in the ZZZ protocol can be eliminated by the receiver Bob without the knowledge of Charlie. Moreover, this new attack is also valid for the improved scheme [Yang, Chai, Teng et al. (2011)]. But to our disappointment, Qin did not give a further improvement. Therefore, in the next part, we will give two new improvements to the ZZZ protocol.

2.1 Improvement for the ZZZ protocol

2.1.1 The first improvement

In this part, we will propose our first improvement of the ZZZ protocol. And we give a detailed description of our new improved protocol as follows.

(S1) Charlie prepares $N+m$ four-qubit states in $|\Psi\rangle_n = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{h_n t_n k_n c_n}$. Then he performs one of four kinds of operations U_1, U_2, U_3, U_4 on particles t_n and k_n, each with the probability of 1/4, where $U_1 = I \otimes I$, $U_2 = I \otimes \sigma_x$, $U_3 = \sigma_x \otimes I$ and $U_4 = \sigma_x \otimes \sigma_x$.

Therefore, he gets the following states

$$|\Psi_1\rangle_n = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{h_n t_n k_n c_n} \tag{1}$$

$$|\Psi_2\rangle_n = \frac{1}{2}(|0010\rangle + |0001\rangle + |1110\rangle - |1101\rangle)_{h_n t_n k_n c_n} \tag{2}$$

$$|\Psi_3\rangle_n = \frac{1}{2}(|0100\rangle + |0111\rangle + |1000\rangle - |1011\rangle)_{h_n t_n k_n c_n} \tag{3}$$

$$|\Psi_4\rangle_n = \frac{1}{2}(|0110\rangle + |0101\rangle + |1010\rangle - |1001\rangle)_{h_n t_n k_n c_n} \tag{4}$$

Charlie takes the particles h_n from each state to form an ordered particle sequence $[h_1, h_2, \ldots, h_{N+m}]$, and names it as the H sequence. Similarly, the remaining particles constitute T sequence $[t_1, t_2, \ldots, t_{N+m}]$, K sequence $[k_1, k_2, \ldots, k_{N+m}]$ and C sequence $[c_1, c_2, \ldots, c_{N+m}]$.

(S2) Charlie prepares three checking sequences, D_H, D_T and D_K for the analysis of the eavesdropping. These sequences are large enough. Let the number of particles in them be l. They are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, Charlie mingles D_H with H sequence to get H' sequence, D_T with T sequence to get T' sequence and D_K with K sequence to get K' sequence. And he also makes a record of the insertion positions and the measurement basis of the checking particles. Finally, Charlie sends H' sequence to Alice, T', K' sequence to Bob and holds C sequence.

(S3) Charlie confirms that Alice and Bob have received the travelling particles. Then, Charlie let Alice and Bob measure checking particles in H', T' and K', respectively. After that, he tells Alice and Bob the positions and the corresponding basis of D_H, D_T and D_K.

Alice and Bob measure their checking sequences with the corresponding basis announced by Charlie. Alice and Bob tell their measurement results to Charlie. Then, Charlie can determine the existence of the eavesdropping in the communication in accordance with Alice's and Bob's measurement results. If the error rate of the eavesdropping checking is higher than a set threshold, Charlie will restart the protocol. If not, they will carry out the next step.

(S4) Also, Alice and Bob need to check whether the state is four particle cluster state or not. Alice randomly selects *m* particles from her *H* sequence and performs randomly one of the two unitary operations $U_1' = I$ and $U_2' = i\sigma_y$ on each selected particle. Then she asks Charlie randomly to measure his corresponding particles using one of two measurement bases $\{|+\rangle, |-\rangle\}$ and $\{|0\rangle, |1\rangle\}$. Then Charlie informs his measuring results of Alice and Bob. Additionally, he must inform Bob of what operations he has performed on Bob's corresponding particles. According to Charlie's public information, Bob can first do the same operations $\{U_1, U_2, U_3, U_4\}$ on his particles and then take the Bell measurement or *Z*-basis on the corresponding particles and inform Alice of his measurement results. According to the measurement results of Bob and Charlie, Alice measures her particles and can determine whether the state is four particle cluster state or not.

In fact, after Alice's U_1' or U_2' operation and Bob's one of four operations, the state $|\psi_i\rangle_n\ (i = 1,2,3,4)$ will change into

$$\begin{aligned}U_1'|\psi\rangle_n &= |\psi\rangle_n = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{h_n t_n k_n c_n}\\ &= \frac{1}{2\sqrt{2}}\{|+\rangle_{c_n}[(|\phi^-\rangle + |\psi^+\rangle)_{t_n k_n}|+\rangle_{h_n} + (|\phi^+\rangle + |\psi^-\rangle)_{t_n k_n}|-\rangle_{h_n}]\\ &\quad + |-\rangle_{c_n}[(|\phi^+\rangle - |\psi^-\rangle)_{t_n k_n}|+\rangle_{h_n} + (|\phi^-\rangle - |\psi^+\rangle)_{t_n k_n}|-\rangle_{h_n}]\}\end{aligned} \tag{5}$$

$$\begin{aligned}U_2'|\psi\rangle_n &= |\psi\rangle_n = \frac{1}{2}(|0100\rangle - |1000\rangle - |1011\rangle - |0111\rangle)_{h_n t_n k_n c_n}\\ &= \frac{1}{2\sqrt{2}}\{|+\rangle_{c_n}[(|\phi^-\rangle + |\psi^+\rangle)_{t_n k_n}|-\rangle_{h_n} - (|\phi^+\rangle + |\psi^-\rangle)_{t_n k_n}|+\rangle_{h_n}]\\ &\quad + |-\rangle_{c_n}[(|\phi^+\rangle - |\psi^-\rangle)_{t_n k_n}|-\rangle_{h_n} - (|\phi^-\rangle - |\psi^+\rangle)_{t_n k_n}|+\rangle_{h_n}]\}\end{aligned} \tag{6}$$

Where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ are *X*-basis, $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ are Bell states.

If the error rate is higher than a set threshold, Alice can conclude that the states are not four-qubit cluster states and give up the communication.

(S5) Suppose Alice wants to transmit secret information to Bob. After confirming the security checking, Alice takes M_h set by way of two particles as encoding-decoding groups. Group 1 includes particles h_1 and h_2, group 2 includes particles h_3 and h_4 etc. Afterward, Alice announces the encoding-decoding groups in the M_h set.

(S6) After that Alice's announcement, Bob and Charlie form ordered encoding-decoding groups which consist of the corresponding particles in M_t, M_k set and M_c set, severally.

(S7) Alice requires Charlie to perform a Hadamard operation on each c_n in order in M_c set, and then Eqs. (1)-(4) will be transformed into the states

$$\begin{aligned}|\Psi_1{}^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|000\rangle+|001\rangle+|110\rangle-|111\rangle)_{h_nt_nk_n}|0\rangle_{c_n}\\ &+(|000\rangle-|001\rangle+|110\rangle+|111\rangle)_{h_nt_nk_n}|1\rangle_{c_n}]\end{aligned} \tag{7}$$

$$\begin{aligned}|\Psi_2{}^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|001\rangle+|000\rangle+|111\rangle-|110\rangle)_{h_nt_nk_n}|0\rangle_{c_n}\\ &+(|001\rangle-|000\rangle+|111\rangle+|110\rangle)_{h_nt_nk_n}|1\rangle_{c_n}]\end{aligned} \tag{8}$$

$$\begin{aligned}|\Psi_3{}^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|010\rangle+|011\rangle+|100\rangle-|101\rangle)_{h_nt_nk_n}|0\rangle_{c_n}\\ &+(|010\rangle-|011\rangle+|100\rangle+|101\rangle)_{h_nt_nk_n}|1\rangle_{c_n}]\end{aligned} \tag{9}$$

$$\begin{aligned}|\Psi_4{}^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|011\rangle+|010\rangle+|101\rangle-|100\rangle)_{h_nt_nk_n}|0\rangle_{c_n}\\ &+(|011\rangle-|010\rangle+|101\rangle+|100\rangle)_{h_nt_nk_n}|1\rangle_{c_n}]\end{aligned} \tag{10}$$

And then, Charlie measures particle c_n like the ZZZ protocol.

(S8) Charlie informs Bob of his measurement results and his operations on each particle in (S1). According to Charlie's information, Bob performs the same operations on the particles in his hand, the rest steps are the same as the steps (S7-S9) of the ZZZ protocol.

2.1.2 The second improvement

Our second improvement of the ZZZ protocol is similar with the first improvement. And we give a detailed description of our second improved protocol as follows.

(S1') Charlie prepares $N+m$ four-qubit states in $|\Psi\rangle_n = \frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{h_nt_nk_nc_n}$. Then he performs one of four kinds of operations U_1, U_2, U_3, U_4 on particles t_n and k_n, each with the probability of 1/4, where $U_1 = I \otimes \sigma_z$, $U_2 = I \otimes i\sigma_y$, $U_3 = \sigma_x \otimes I$ and $U_4 = \sigma_x \otimes \sigma_x$.

Therefore, he gets the following states

$$\left|\psi_1\right\rangle_n = \frac{1}{2}(\left|0000\right\rangle - \left|0011\right\rangle + \left|1100\right\rangle + \left|1111\right\rangle)_{h_n t_n k_n c_n} \tag{11}$$

$$\left|\psi_2\right\rangle_n = \frac{1}{2}(\left|0001\right\rangle - \left|0010\right\rangle - \left|1110\right\rangle - \left|1101\right\rangle)_{h_n t_n k_n c_n} \tag{12}$$

$$\left|\psi_3\right\rangle_n = \frac{1}{2}(\left|0100\right\rangle + \left|0111\right\rangle + \left|1000\right\rangle - \left|1011\right\rangle)_{h_n t_n k_n c_n} \tag{13}$$

$$\left|\psi_4\right\rangle_n = \frac{1}{2}(\left|0110\right\rangle + \left|0101\right\rangle + \left|1010\right\rangle - \left|1001\right\rangle)_{h_n t_n k_n c_n} \tag{14}$$

Charlie takes the particles h_n from each state to form an ordered particle sequence $[h_1, h_2, \ldots, h_{N+m}]$, and names it as the H sequence. Similarly, the remaining particles compose T sequence $[t_1, t_2, \ldots, t_{N+m}]$, K sequence $[k_1, k_2, \ldots, k_{N+m}]$ and C sequence $[c_1, c_2, \ldots, c_{N+m}]$.

(S2')-(S6') are the same as the steps (S2-S6) of the first improvement.

(S7') Alice requires Charlie to perform a Hadamard operation on each c_n in order in M_c set, and then Eqs. (11)-(14) will be turned into

$$\begin{aligned} |\Psi_1^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|000\rangle - |001\rangle + |110\rangle + |111\rangle)_{h_n t_n k_n} |0\rangle_{c_n} \\ &+(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{h_n t_n k_n} |1\rangle_{c_n}] \end{aligned} \tag{15}$$

$$\begin{aligned} |\Psi_2^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|000\rangle - |001\rangle - |111\rangle - |110\rangle)_{h_n t_n k_n} |0\rangle_{c_n} \\ &+(|110\rangle - |000\rangle - |001\rangle - |111\rangle)_{h_n t_n k_n} |1\rangle_{c_n}] \end{aligned} \tag{16}$$

$$\begin{aligned} |\Psi_3^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|010\rangle + |011\rangle + |100\rangle - |101\rangle)_{h_n t_n k_n} |0\rangle_{c_n} \\ &+(|010\rangle - |011\rangle + |100\rangle + |101\rangle)_{h_n t_n k_n} |1\rangle_{c_n}] \end{aligned} \tag{17}$$

$$\begin{aligned} |\Psi_4^+\rangle_n = \frac{1}{2\sqrt{2}}[&(|011\rangle + |010\rangle + |101\rangle - |100\rangle)_{h_n t_n k_n} |0\rangle_{c_n} \\ &+(|011\rangle - |010\rangle + |101\rangle + |100\rangle)_{h_n t_n k_n} |1\rangle_{c_n}] \end{aligned} \tag{18}$$

And then, Charlie measures particle c_n like the ZZZ protocol and tells Alice and Bob his measurement results.

(S8') Alice and Bob utilize the local operation $U_{nm}(n, m = 0,1)$ to encode secret information. Here, $U_{00} = I$, $U_{01} = \sigma_x$, $U_{10} = -i\sigma_y$ and $U_{11} = \sigma_z$. For convenience, let two cbit strings 00, 01, 10 and 11 correspond to them, severally. Alice uses local operation U_{nm} to encode two-bit on the encoding-decoding groups in M_c set. Later, Alice measures all the encoding-decoding groups with Bell bases and announces measurement results and the order of the encoding-decoding groups.

(S9’) Bob makes the Bell measurements on their corresponding particles in

M_t and M_k set, separately. As shown in Tab. 1, Bob can obtain Alice’s secret information when he receives Charlie’s and Alice’s measurement results. For example, suppose that Charlie’s state is $|\Psi_2\rangle_2$ and his measurement results are $|0\rangle_{c_1}$ and $|0\rangle_{c_2}$, then $|\Psi_2\rangle_1$ and $|\Psi_2\rangle_2$ will be collapsed into

$$|\eta^+\rangle_1 = \frac{1}{2\sqrt{2}}(|000\rangle - |001\rangle - |111\rangle - |110\rangle)_{h_n t_n k_n} \tag{19}$$

$$|\eta^+\rangle_2 = \frac{1}{2\sqrt{2}}(|000\rangle - |001\rangle - |111\rangle - |110\rangle)_{h_n t_n k_n} \tag{20}$$

If Alice performs a U_{00} operation on one particle of group 1, the state composed of particles $(h_1 t_1 k_1; h_2 t_2 k_2)$ is

$$\begin{aligned}
&U_{00}\left|\eta^+\right\rangle_1 \otimes \left|\eta^+\right\rangle_2 \\
&= \frac{1}{8}(\left|000\right\rangle - \left|001\right\rangle - \left|110\right\rangle - \left|111\right\rangle)_{h_1 t_1 k_1} \otimes (\left|000\right\rangle - \left|001\right\rangle - \left|110\right\rangle - \left|111\right\rangle)_{h_2 t_2 k_2} \\
&= \frac{1}{4\sqrt{2}}(\left|\Phi^+\right\rangle_{h_1 h_2}\left|\Phi^+\right\rangle_{t_1 t_2}\left|\Phi^+\right\rangle_{k_1 k_2} - \left|\Phi^+\right\rangle_{h_1 h_2}\left|\Phi^-\right\rangle_{t_1 t_2}\left|\Psi^+\right\rangle_{k_1 k_2} \\
&\quad - \left|\Phi^-\right\rangle_{h_1 h_2}\left|\Phi^+\right\rangle_{t_1 t_2}\left|\Psi^+\right\rangle_{k_1 k_2} + \left|\Phi^-\right\rangle_{h_1 h_2}\left|\Phi^-\right\rangle_{t_1 t_2}\left|\Phi^+\right\rangle_{k_1 k_2} \\
&\quad - \left|\Psi^+\right\rangle_{h_1 h_2}\left|\Psi^+\right\rangle_{t_1 t_2}\left|\Phi^-\right\rangle_{k_1 k_2} - \left|\Psi^+\right\rangle_{h_1 h_2}\left|\Psi^-\right\rangle_{t_1 t_2}\left|\Psi^-\right\rangle_{k_1 k_2} \\
&\quad - \left|\Psi^-\right\rangle_{h_1 h_2}\left|\Psi^+\right\rangle_{t_1 t_2}\left|\Psi^-\right\rangle_{k_1 k_2} - \left|\Psi^-\right\rangle_{h_1 h_2}\left|\Psi^-\right\rangle_{t_1 t_2}\left|\Phi^-\right\rangle_{k_1 k_2})
\end{aligned} \tag{21}$$

But there is one more point that we need to notice, that is, the Eq. (12) of the ZZZ protocol is written wrong, and it should be written as follows.

$$\begin{aligned}
U_{00}\left|\xi_1^+\right\rangle_1 \otimes \left|\xi_1^+\right\rangle_2 &= \frac{1}{8}(\left|000\right\rangle + \left|001\right\rangle + \left|110\right\rangle - \left|111\right\rangle)_{h_1 t_1 k_1} \otimes (\left|000\right\rangle + \left|001\right\rangle + \left|110\right\rangle - \left|111\right\rangle)_{h_2 t_2 k_2} \\
&= \frac{1}{4\sqrt{2}}(\left|\Phi^+\right\rangle_{h_1 h_2}\left|\Phi^+\right\rangle_{t_1 t_2}\left|\Phi^+\right\rangle_{k_1 k_2} + \left|\Phi^+\right\rangle_{h_1 h_2}\left|\Phi^-\right\rangle_{t_1 t_2}\left|\Psi^+\right\rangle_{k_1 k_2} \\
&\quad + \left|\Phi^-\right\rangle_{h_1 h_2}\left|\Phi^+\right\rangle_{t_1 t_2}\left|\Psi^+\right\rangle_{k_1 k_2} + \left|\Phi^-\right\rangle_{h_1 h_2}\left|\Phi^-\right\rangle_{t_1 t_2}\left|\Phi^+\right\rangle_{k_1 k_2} \\
&\quad + \left|\Psi^+\right\rangle_{h_1 h_2}\left|\Psi^+\right\rangle_{t_1 t_2}\left|\Phi^-\right\rangle_{k_1 k_2} - \left|\Psi^+\right\rangle_{h_1 h_2}\left|\Psi^-\right\rangle_{t_1 t_2}\left|\Psi^-\right\rangle_{k_1 k_2} \\
&\quad - \left|\Psi^-\right\rangle_{h_1 h_2}\left|\Psi^+\right\rangle_{t_1 t_2}\left|\Psi^-\right\rangle_{k_1 k_2} + \left|\Psi^-\right\rangle_{h_1 h_2}\left|\Psi^-\right\rangle_{t_1 t_2}\left|\Phi^-\right\rangle_{k_1 k_2})
\end{aligned} \tag{22}$$

Table 1: Alice's and Bob's measurement results according to the unitary operation U_{nm} and the initial states

$\boldsymbol{U_{00}}$	$\boldsymbol{U_{01}}$	$\boldsymbol{U_{10}}$	$\boldsymbol{U_{11}}$
$\lvert\eta^{+}\rangle_1\otimes\lvert\eta^{+}\rangle_2$	$\lvert\mu^{+}\rangle_1\otimes\lvert\eta^{+}\rangle_2$	$\lvert\mu^{-}\rangle_1\otimes\lvert\eta^{+}\rangle_2$	$\lvert\eta^{-}\rangle_1\otimes\lvert\eta^{+}\rangle_2$
$\phi_u^+\phi_v^+\phi_w^+$	$\phi_u^+\psi_v^+\phi_w^-$	$\phi_u^+\psi_v^+\psi_w^-$	$\phi_u^+\phi_v^+\phi_w^-$
$\phi_u^+\phi_v^-\psi_w^+$	$\phi_u^+\psi_v^-\psi_w^-$	$\phi_u^+\psi_v^-\phi_w^-$	$\phi_u^+\phi_v^-\psi_w^-$
$\phi_u^-\phi_v^+\psi_w^+$	$\phi_u^-\psi_v^+\psi_w^-$	$\phi_u^-\psi_v^+\phi_w^-$	$\phi_u^-\phi_v^+\psi_w^-$
$\phi_u^-\phi_v^-\phi_w^+$	$\phi_u^-\psi_v^-\phi_w^-$	$\phi_u^-\psi_v^-\psi_w^-$	$\phi_u^-\phi_v^-\phi_w^-$
$\psi_u^+\psi_v^+\phi_w^-$	$\psi_u^+\phi_v^+\phi_w^+$	$\psi_u^+\phi_v^+\psi_w^+$	$\psi_u^+\psi_v^+\phi_w^+$
$\psi_u^+\psi_v^-\psi_w^-$	$\psi_u^+\phi_v^-\psi_w^+$	$\psi_u^+\phi_v^-\phi_w^+$	$\psi_u^+\psi_v^-\psi_w^+$
$\psi_u^-\psi_v^+\psi_w^-$	$\psi_u^-\phi_v^+\psi_w^+$	$\psi_u^-\phi_v^+\phi_w^+$	$\psi_u^-\psi_v^+\psi_w^+$
$\psi_u^-\psi_v^-\phi_w^-$	$\psi_u^-\phi_v^-\phi_w^+$	$\psi_u^-\phi_v^-\psi_w^+$	$\psi_u^-\psi_v^-\phi_w^+$

2.3 Security analysis

Mathematics provides some important tools [Dong, Zhang, Zhang et al. (2014)] to analyze and solve practical problems. The security of our protocol could be proved in theory and by mathematics. In this section, we will show that our protocol is secure under fake entangled particles attack and disentanglement attack which the original ZZZ protocol cannot resist.

Case1: The fake entangled particles attack. In our new proposed CQSDC protocol, it is Charlie rather than Bob who prepares the four particle cluster state, so it is impossible for Bob to prepare two Bell states in Yang et al.'s protocol [Yang, Chai, Teng et al. (2011)] to deliver fake entangled particles attack on Charlie. That is to say, Bob cannot prepare fake entangled particles to deceive Charlie with the attempt of getting rid of control of Charlie. However, chances are that Charlie may prepare two entangled states instead of four particle cluster state to obtain Alice secret information. In this condition, Charlie sends one entangled state to Bob and shares one entangled state with Alice. But in the check of four particle cluster state, Alice and Bob can conclude that error rate is higher than a set threshold. For Charlie does not know Alice's operations, he can guess wrong with the possibility of 1/2. And there are *m* cluster states, therefore he has the possibility of to guess all right, which is impossible when *m* is large enough.

Case2: The disentanglement attack. As Qin [Qin (2012)] has pointed out, if Bob wants to get rid of Charlie's control, he can measure every particle in K sequence using $\{\lvert 0\rangle, \lvert 1\rangle\}$ basis. However, in our protocol, Charlie performs four kinds of unitary operations. In our first improvement, if Bob measures K sequence, then he will not know what the state collapses into. If the state is $\left|\Psi_1\right\rangle_n$, it can be rewritten as follows.

$$\left|\Psi_1\right\rangle_n = \frac{1}{2}\{(\left|00\right\rangle + \left|11\right\rangle)_{h_n t_n}\left|00\right\rangle_{k_n c_n} + (\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|11\right\rangle_{k_n c_n}\} \tag{23}$$

When Bob's measurement outcome is $\left|0\right\rangle$, the cluster state after the measurement immediately collapses into $\left|\varphi_1^{\,0}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)_{h_n t_n}\left|0\right\rangle_{c_n}$.

Otherwise, the state collapses into $\left|\varphi_1^{\,1}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|1\right\rangle_{c_n}$. And if the state is $\left|\Psi_2\right\rangle_n$, the result will be different from the state $\left|\Psi_1\right\rangle_n$. When Bob's measurement result is $\left|0\right\rangle$, the state collapses into $\left|\varphi_2^{\,0}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|1\right\rangle_{c_n}$. Otherwise, the state will collapse into $\left|\varphi_2^{\,1}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)_{h_n t_n}\left|0\right\rangle_{c_n}$. And the rest states $\left|\Psi_3\right\rangle_n$ and $\left|\Psi_4\right\rangle_n$, we can see details in Tab. 2.

Table 2: Correlations among Bob's measurement results on K sequence, the states after Charlie's operations and the collapsed states

$\left|\Psi\right\rangle_n$ \ $\left|\varphi\right\rangle_k$	$\left|0\right\rangle$	$\left|1\right\rangle$
$\left|\Psi_1\right\rangle_n$	$\left|\phi_1^0\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)_{\mathrm{h_n t_n}}\left|0\right\rangle_{\mathrm{c_n}}$	$\left|\varphi_1^1\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|1\right\rangle_{c_n}$
$\left|\Psi_2\right\rangle_n$	$\left|\varphi_2^0\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|1\right\rangle_{c_n}$	$\left|\varphi_2^1\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)_{h_n t_n}\left|0\right\rangle_{c_n}$
$\left|\Psi_3\right\rangle_n$	$\left|\varphi_3^0\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)_{h_n t_n}\left|0\right\rangle_{c_n}$	$\left|\varphi_3^1\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle)_{h_n t_n}\left|1\right\rangle_{c_n}$
$\left|\Psi_4\right\rangle_n$	$\left|\varphi_4^0\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle)_{h_n t_n}\left|1\right\rangle_{c_n}$	$\left|\varphi_4^1\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)_{h_n t_n}\left|0\right\rangle_{c_n}$

It is apparent that Bob cannot know what the state will collapse into after his measurement on K sequence. Therefore, he cannot get rid of Charlie's control. In the second improvement, the four states can be rewritten as follows.

$$\left|\Psi_1\right\rangle_n = \frac{1}{2}\{(\left|00\right\rangle + \left|11\right\rangle)_{h_n t_n}\left|00\right\rangle_{k_n c_n} - (\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|11\right\rangle_{k_n c_n}\} \tag{24}$$

$$\left|\Psi_2\right\rangle_n = \frac{1}{2}\{(\left|00\right\rangle - \left|11\right\rangle)_{h_n t_n}\left|01\right\rangle_{k_n c_n} - (\left|00\right\rangle + \left|11\right\rangle)_{h_n t_n}\left|10\right\rangle_{k_n c_n}\} \tag{25}$$

$$\left|\Psi_3\right\rangle_n = \frac{1}{2}\{(\left|01\right\rangle + \left|10\right\rangle)_{h_n t_n}\left|00\right\rangle_{k_n c_n} + (\left|01\right\rangle - \left|10\right\rangle)_{h_n t_n}\left|11\right\rangle_{k_n c_n}\} \tag{26}$$

$$\left|\Psi_4\right\rangle_n = \frac{1}{2}\{(\left|01\right\rangle - \left|10\right\rangle)_{h_n t_n}\left|01\right\rangle_{k_n c_n} + (\left|01\right\rangle + \left|10\right\rangle)_{h_n t_n}\left|10\right\rangle_{k_n c_n}\} \tag{27}$$

And we can see, if Bob measures particle k_n before Charlie's measurement, he cannot know what the state will collapse into. So, he can't get rid of Charlie's control.

Case3: The out of control attack. Another attack strategy is that when the controller Charlie sends H sequence to Alice, Bob intercepts it and then sends Alice another particle sequence which prepared by himself in order to get out of Charlie's control. But in our protocol, Charlie inserts decoy particles randomly in H sequence in (S3), because Bob doesn't know the exact position and the original state of the decoy particles, he cannot prepare the right fake sequence, so our protocol can resist this kind of attack.

3 A New CQSDC protocol by using three-qubit partially entangled set of states

Without respect to the security of the ZZZ protocol, there still exist another two disadvantages in it. First, it is not easy to obtain a four-particle cluster state in real experimental setups. Second, the efficiency of the protocol is not high, because it uses four particles to transmit one bit secret information.

In this section, we will propose a new protocol by using the three-qubit partially entangled set of states. It is shown that our protocol can resist fake entangled particles attack and disentanglement attack. Moreover, our protocol uses three particles to transmit one bit secret information and three-qubit partially entangled states are also much easier to prepare.

This section is organized as follows. Subsection 3.1 is a detailed description of our new protocol. And in Subsection 3.2, we give the security analysis of our new proposed CQSDC protocol.

3.1 The process of new CQSDC protocol

In 2013, Kumar et al. [Kumar, Adhikari, Banerjee et al. (2013)] pointed out that they can prepare three-qubit partially entangled set of states from the generalized GHZ states. In the beginning, we prepare GHZ states.

$$\left|\psi\right\rangle_{123} = \sin\theta\left|000\right\rangle_{123} + \cos\theta\left|111\right\rangle_{123} \tag{28}$$

A Hadamard operation is applied on the third-qubit of the GHZ state, and we will get the following state

$$\left|\psi'\right\rangle_{123} = \frac{1}{\sqrt{2}}[\sin\theta\left|000\right\rangle_{123} + \sin\theta\left|001\right\rangle_{123} + \cos\theta\left|110\right\rangle_{123} - \cos\theta\left|111\right\rangle_{123}] \tag{29}$$

And we perform a CNOT operation on particles 2 and 3. Here, particle 3 is the control one and particle 2 is the target one. Finally, we obtain our communication channel

$$\begin{aligned}|\zeta\rangle_{123} &= CNOT_{23}|\psi'\rangle_{123}\\ &= CNOT_{23}\frac{1}{\sqrt{2}}[\sin\theta|000\rangle_{123}+\sin\theta|001\rangle_{123}+\cos\theta|110\rangle_{123}-\cos\theta|111\rangle_{123}] \\ &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle_{123}+\sin\theta|011\rangle_{123}+\cos\theta|110\rangle_{123}-\cos\theta|101\rangle_{123}].\end{aligned} \tag{30}$$

Next, we depict our protocol in detail as follows.

(S1) Charlie prepares $N+m$ three-qubit partially entangled states.

$$|\zeta\rangle_{c_na_nb_n} = \frac{1}{\sqrt{2}}[\sin\theta|000\rangle_{c_na_nb_n}+\sin\theta|011\rangle_{c_na_nb_n}+\cos\theta|110\rangle_{c_na_nb_n}-\cos\theta|101\rangle_{c_na_nb_n}] \tag{31}$$

Here, $n\in\{1, N+m\}$, c_n, a_n and b_n denote the three particles of the partially entangled state.

Charlie takes the particles c_n from each state to form an ordered particle sequence $[c_1, c_2, \ldots, c_{N+m}]$, and names it as the C sequence. Similarly, the remaining particles make up A sequence $[a_1, a_2, \ldots, a_{N+m}]$ and B sequence $[b_1, b_2, \ldots, b_{N+m}]$.

(S2) Charlie prepares two checking sequences, D_A and D_B for the analysis of the eavesdropping. These sequences are large enough. Let the number of particles in them be l. They are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, Charlie mingles D_A with A sequence to get A' sequence and D_B with B sequence to get B' sequence. And he also makes a record of the insertion positions and the measurement basis of the checking particles. Finally Charlie sends A' sequence to Alice, B' sequence to Bob and holds C sequence.

(S3) Alice and Bob confirm that they have received the travelling particles. Then, Charlie let Alice and Bob measure checking particles in A' and B'. He tells the positions and the corresponding basis of D_A to Alice and D_B to Bob, respectively.

Then, Alice and Bob measure their checking sequences with the corresponding basis announced by Charlie. After that, Alice and Bob notify Charlie of their measurement results. After that, Charlie can determine the existence of the eavesdropping in the communication according to Alice's and Bob's measurement results. If the error rate of is higher than a set threshold, Charlie will restart the protocol. Otherwise, they

.

$$\begin{aligned}|\zeta\rangle_{c_na_nb_n} &= \frac{1}{\sqrt{2}}[\sin\theta|000\rangle_{c_na_nb_n}+\sin\theta|011\rangle_{c_na_nb_n}+\cos\theta|110\rangle_{c_na_nb_n}-\cos\theta|101\rangle_{c_na_nb_n}]\\ &= \frac{1}{\sqrt{2}}[\sin\theta|0\rangle_{c_n}(|00\rangle+|11\rangle)_{a_nb_n}+\cos\theta|1\rangle_{c_n}(|10\rangle-|01\rangle)_{a_nb_n}] \\ &= \frac{1}{\sqrt{2}}[\sin\theta|0\rangle_{c_n}(|++\rangle+|--\rangle)_{a_nb_n}+\cos\theta|1\rangle_{c_n}(|+-\rangle-|-+\rangle)_{a_nb_n}]\end{aligned} \tag{32}$$

(S4) Alice and Bob check whether the state is the three-qubit partially entangled states or not. Alice asks Charlie to measure his particles using *Z*-basis, and then he publishes his measurement results. Then Alice and Bob randomly choose m positions and measure their corresponding particles. That is, Bob measures his particles in using one of two set of measurement basis $\{|+\rangle, |-\rangle\}$ and $\{|0\rangle, |1\rangle\}$. Then he informs his measurement basis and corresponding measurement results of Alice. According to Bob's announcement, Alice chooses the same measurement basis and measures her particles. Then she can determine whether they have shared the three-qubit partially entangled states. Here, we must note that if Charlie only prepares Bell states and does not prepare the three-qubit partially entangled states, can our protocol work? The answer is yes. Because Charlie still controls the protocol. If he does not publish his classical bits, then Alice and Bob do not know what states they share.

(S5) We suppose Alice wants to send some messages to Bob. In the (S4), if Charlie obtains the result $|0\rangle_c$, particles (a_n, b_n) will collapse into

$$|\delta\rangle_n^1 = \frac{1}{\sqrt{2}} \sin\theta(|00\rangle + |11\rangle)_{a_n b_n} \tag{33}$$

Otherwise, particles (a_n, b_n) will collapse into

$$|\delta\rangle_n^2 = \frac{1}{\sqrt{2}} \cos\theta(|10\rangle - |01\rangle)_{a_n b_n} \tag{34}$$

(S6) Alice and Bob use the local operation $U_{nm}(n,\ m = 0{,}1)$ to encode secret information. Here, $U_{00} = I$, $U_{01} = \sigma_x$, $U_{10} = -i\sigma_y$, and $U_{11} = \sigma_z$. let two cbit strings 00, 01, 10 and 11 correspond to them, severally.

Alice sets two particles as an encoding-decoding group, such as particles a_1 and a_2 as group 1, particles a_3 and a_4 as group 2, etc., and Bob sets his encoding-decoding group too.

Alice performs the operation U_{nm} on the encoding-decoding groups to encode her two-bit secret information. Then, she uses Bell bases to measure all the encoding-decoding groups and announces her measurement results and the group's order.

(S7) Bob measures his encoding-decoding groups using Bell basis too. Subsequently, he can get Alice's secret information after he knows Alice's and Charlie's measurement results. For example, we assume Charlie's measurement results are $|0\rangle_{c_1}$ and $|0\rangle_{c_2}$, then Alice's and Bob's particles collapse into the state

$$|\delta\rangle_1^1 = \frac{1}{\sqrt{2}} \sin\theta(|00\rangle + |11\rangle)_{a_1 b_1} \tag{35}$$

$$|\delta\rangle_2^1 = \frac{1}{\sqrt{2}} \sin\theta(|00\rangle + |11\rangle)_{a_2 b_2} \tag{36}$$

If Alice performs U_{00} on one particle of group 1, then the state composed particles $(a_1b_1; a_2b_2)$ is

$$\begin{aligned} &U_{00}\left|\delta\right\rangle_1^1 \otimes \left|\delta\right\rangle_2^1 \\ &\quad= \frac{1}{\sqrt{2}}\sin\theta(\left|00\right\rangle + \left|11\right\rangle)_{a_1b_1} \otimes \frac{1}{\sqrt{2}}\sin\theta(\left|00\right\rangle + \left|11\right\rangle)_{a_2b_2} \\ &\quad= \frac{1}{2}\sin^2\theta(\left|\phi^+\right\rangle_{a_1a_2}\left|\phi^+\right\rangle_{b_1b_2} + \left|\phi^-\right\rangle_{a_1a_2}\left|\phi^-\right\rangle_{b_1b_2} + \left|\psi^+\right\rangle_{a_1a_2}\left|\psi^+\right\rangle_{b_1b_2} + \left|\psi^-\right\rangle_{a_1a_2}\left|\psi^-\right\rangle_{b_1b_2}) \end{aligned} \tag{37}$$

If Alice's result of a Bell state measurement is $\left|\phi^+\right\rangle_{a_1a_2}$, it's easy to conclude that Bob's measurement result is $\left|\phi^+\right\rangle_{b_1b_2}$. Thus, Bob can obtain that Alice performs a U_{00} operation on one particle of group 1 and, therefore, extract the bits (00), and he can read the two-bit secret information.

3.2 Security analysis

In this section, we show our protocol is secure under some possible types of attacks as follows.

Case1: The intercept-and-resend attack. In our protocol, the eavesdropper doesn't know the exact position and the original state of the decoy particles, (e.g., $\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle$) since these particles are randomly inserted in the transmitted sequences (for instance, H' sequence, T' sequence, K' sequence). Therefore, if the eavesdropper try to measure and resend the particles, the probability to be detected will be $1-(3/4)^l$. Here, l denotes the number of decoy particles. If l is large enough, the eavesdropping detection probability $1-(3/4)^l$ is approximately 1.

Case2: The entangle-and-measure attack. An eavesdropper Eve may try to obtain the secret information between Alice and Bob. However, he does not know the positions and the states of the checking particles in the intercepted Charlie's sequence H'. For instance, Eve prepares some ancillary particles $E = \{\left|E_1\right\rangle, \left|E_2\right\rangle, \dots, \left|E_m\right\rangle\}$ and entangles these ancillary particles with the H' sequence via a unitary operation $\hat{U}$.

$$\hat{U}\left|0\right\rangle\left|E_i\right\rangle = \alpha\left|0\right\rangle\left|e_{00}\right\rangle + \beta\left|1\right\rangle\left|e_{01}\right\rangle \tag{38}$$

$$\hat{U}\left|1\right\rangle\left|E_i\right\rangle = \gamma\left|0\right\rangle\left|e_{10}\right\rangle + \delta\left|1\right\rangle\left|e_{11}\right\rangle \tag{39}$$

$$\begin{aligned} \hat{U}\left|+\right\rangle\left|E_i\right\rangle = \frac{1}{2}[&\left|+\right\rangle(\alpha\left|e_{00}\right\rangle + \beta\left|e_{01}\right\rangle + \gamma\left|e_{10}\right\rangle + \delta\left|e_{11}\right\rangle) + \\ &\left|-\right\rangle(\alpha\left|e_{00}\right\rangle - \beta\left|e_{01}\right\rangle + \gamma\left|e_{10}\right\rangle - \delta\left|e_{11}\right\rangle)] \end{aligned} \tag{40}$$

$$\hat{U}\left|-\right\rangle\left|E_i\right\rangle=\frac{1}{2}[\left|+\right\rangle(\alpha\left|e_{00}\right\rangle+\beta\left|e_{01}\right\rangle-\gamma\left|e_{10}\right\rangle-\delta\left|e_{11}\right\rangle)+ \\ \left|-\right\rangle(\alpha\left|e_{00}\right\rangle-\beta\left|e_{01}\right\rangle-\gamma\left|e_{10}\right\rangle+\delta\left|e_{11}\right\rangle)] \tag{41}$$

Here, we have $\hat{U}\hat{U}^{\dagger}=\hat{U}^{\dagger}\hat{U}=I$; $\left|E_i\right\rangle$ is the initial state of Eve's ancilla; $\left|e_{00}\right\rangle,\left|e_{01}\right\rangle,\left|e_{10}\right\rangle,\left|e_{11}\right\rangle$ are the four states determined by Eve and satisfied with $\left|\alpha^2\right|+\left|\beta^2\right|+\left|\gamma^2\right|+\left|\delta^2\right|=1$. If Alice's checking particles are $\left|0\right\rangle$ or $\left|1\right\rangle$, Eve has to set $\beta=\gamma=0$ in order to pass the security checking. Likewise, if they are $\left|+\right\rangle$ or $\left|-\right\rangle$, Eve has to set $\alpha\left|e_{00}\right\rangle-\beta\left|e_{01}\right\rangle+\gamma\left|e_{10}\right\rangle-\delta\left|e_{11}\right\rangle=\alpha\left|e_{00}\right\rangle+\beta\left|e_{01}\right\rangle-\gamma\left|e_{10}\right\rangle-\delta\left|e_{11}\right\rangle$=0, where 0 denotes a zero vector. In this case, Eve's attack will not be detected in the process of security checking. Nevertheless, if $\beta=\gamma=0$, then we know that $\alpha\left|e_{00}\right\rangle-\delta\left|e_{11}\right\rangle=0$. It also means that $\alpha\left|e_{00}\right\rangle=\delta\left|e_{11}\right\rangle$. In this situation, Eve cannot distinguish $\alpha\left|e_{00}\right\rangle$ from $\delta\left|e_{11}\right\rangle$. Hence, he also cannot measure these ancillas to obtain any useful information about Alice's secret information. Inversely, if Eve wants to distinguish ancillas (i.e., to make $\alpha\left|e_{00}\right\rangle\neq\delta\left|e_{11}\right\rangle$) to steal Alice's information, then he will disturb the checking particles and be further detected in the end.

Case3: The fake entangled particles attack. Because we only use three-particle states as a communication channel and the controller Charlie prepares states, Bob cannot prepare two entangled states instead of the three-qubit partially entangled set of states. However, chances are that Charlie may prepare other states instead of three-qubit partially entangled state to obtain Alice secret information. Under this condition, Charlie may send one particle to Bob and shares one entangled state with Alice. But in the check of the three-qubit partially entangled state, Alice and Bob can conclude that error rate is higher than a set threshold. Charlie does not know Alice's operations, so he can guess wrong with the possibility of 1/2. And there are *m* entangled states, therefore he has the possibility of $(1/2)^m$ to guess all right, which is impossible when *m* is large enough. Thus, fake entangled particles attack cannot work.

Case4: The disentanglement attack. Each of the three parties (Alice, Bob and Charlie) only has one particle of the three-qubit partially entangled state, so Bob cannot measure his particles to get rid of the control of Charlie, which means, using disentanglement attack is not effective. For example, we assume Charlie prepares three-qubit partially entangled state in (13).

$$\begin{aligned}\left|\zeta\right\rangle_{c_na_nb_n}&=\frac{1}{\sqrt{2}}[\sin\theta\left|000\right\rangle_{c_na_nb_n}+\sin\theta\left|011\right\rangle_{c_na_nb_n}+\cos\theta\left|110\right\rangle_{c_na_nb_n}-\cos\theta\left|101\right\rangle_{c_na_nb_n}]\\&=\frac{1}{\sqrt{2}}[(\sin\theta\left|00\right\rangle_{c_na_n}+\cos\theta\left|11\right\rangle_{c_na_n})\left|0\right\rangle_{b_n}+(\sin\theta\left|01\right\rangle_{c_na_n}-\cos\theta\left|10\right\rangle_{c_na_n})\left|1\right\rangle_{b_n}]\end{aligned} \tag{42}$$

After Bob measures his particles, if his measurement result is $\left|0\right\rangle_{b_n}$, particles ($c_n$, a_n) will collapse into the state

$$\frac{1}{\sqrt{2}}(\sin\theta|00\rangle_{c_n a_n}+\cos\theta|11\rangle_{c_n a_n}) \tag{43}$$

If his measurement results is $|1\rangle_{b_n}$, particles (c_n, a_n) will collapse into the state

$$\frac{1}{\sqrt{2}}(\sin\theta|01\rangle_{c_n a_n}-\cos\theta|10\rangle_{c_n a_n}) \tag{44}$$

We can conclude that Bob’s particles are no longer entangled with Alice’s, and he cannot get any secret information from Alice. Thus, disentanglement attack is not effective in this condition.

Case5: The modification attack. In this attack, the eavesdropper Eve may try to perform malicious modify operations on the particles which Charlie wants to send Alice or Bob. However, Charlie doesn’t know the positions of the decoy particles, so the modify operations will lead to the wrong measurement results of checking particles.

4 Conclusion

In this paper, we have analyzed the reasons why the ZZZ protocol is insecure under fake entangled particles attack and disentanglement attack. Firstly, it is the secret receiver Bob who prepares the four particles cluster state. So he can prepare other states which are beneficial to him. Moreover, he is the last one to measure his particles. Then, he can perfectly deceive the controller, Charlie, by preparing two fake entangled particles without being detected. Secondly, Bob has half particles of the states and one of his two particles is equivalent to Alice’s, another is equivalent to Charlie’s. So it is easy for Bob to measure his particle which is equivalent to Charlie’s to get rid of Charlie’s control. In essence, this happens because Charlie’s control information is not enough and Bob has too much power. Therefore, by making Bob powerless and Charlie have more control information, we have proposed a new improved secure protocol. In our new protocol, we have two versions of improvement, and both of them can prevent the two attack strategies we have mentioned above.

Besides, we have proposed a novel secure protocol using a more useful and practical state, the three-qubit partially entangled set of state. In our protocol, on one hand, it is impossible for Bob to carry out fake entangled particles attack, for he is not the one who prepares the three-qubit partially entangled set of states, and it is also impossible for Charlie to deliver fake entangled particles attack, for he will be detected by Alice and Bob in the detection of three-qubit partially entangled states. On the other hand, it is difficult for Bob to carry out disentanglement attack too. Because he has only one particle of the state, he cannot measure his particle to make Charlie out of control of their communication. We also analyze some other possible attacks and find out these attacks do not work. And also, we have pointed out that our protocol is easier and more secure to prepare the resource states. Moreover, efficiency in transmitting of secret information via a particle is higher than Chen et al.’s protocol [Chen, Wang, Du et al. (2008)]. In addition, our protocol needs less measurement resource, which makes this protocol more convenient from an applied point of view.

Acknowledgement: Project supported by NSFC (Grant Nos. 61671087, 61272514, 61170272, 61003287, 61571335, 61628209), the Fok Ying Tong Education Foundation (Grant No. 131067), the National Key R&D Program of China under Grant 2017YFB0802300, the Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ016) and Hubei Science Foundation (2016CFA030, 2017AAA125).

References

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 7-11.

Boström, K.; Felbinger, T. (2002): Deterministic secure direct communication using entanglement. *Physical Review Letters*, vol. 89, no. 18, 187902.

Cao, W. F.; Yang, Y. G.; Wen Q. Y. (2010): Quantum secure direct communication with cluster states. *Science China Physics, Mechanics and Astronomy*, vol. 53, no. 7, pp. 1271-1275.

Chang, W. L.; Lin, F. J.; Zeng, G. J.; Chou, Y. H. (2012): Controlled quantum secure direct communication based on single photons. *Advances in Intelligent Systems and Applications*, pp. 195-204.

Chen, X. B.; Tang, X.; Xu, G.; Dou, Z.; Chen, Y. L. et al. (2018): Cryptanalysis of secret sharing with a single d-level quantum system. *Quantum Information Processing*, vol. 17, no. 9, pp. 225.

Chen, X. B.; Sun, Y. R.; Xu, G.; Jia, H. Y.; Qu, Z. et al. (2017): Controlled bidirectional remote preparation of three-qubit state. *Quantum Information Processing*, vol. 16, no, 10, pp. 244.

Chen, X. B.; Wang, T. Y.; Du, J. Z.; Wen, Q. Y.; Zhu, F. C. (2008): Controlled quantum secure direct communication with quantum encryption. *International Journal of Quantum Information*, vol. 6, no. 3, pp. 543-551.

Chen, X. B.; Wen, Q. Y.; Guo, F. Z.; Sun, Y.; Xu, G. et al. (2008): Controlled quantum secure direct communication with W state. *International Journal of Quantum Information*, vol. 6, no. 4, pp. 899-906.

Deng, F. G.; Long, G. L. (2004): Secure direct communication with a quantum one-time pad. *Physical Review A*, vol. 69, no. 5, pp. 052319.

Dong, H. H.; Zhang, Y. F.; Zhang, Y. F.; Yin, B. S. (2014): Generalized bilinear differential operators, binary Bell polynomials, and exact periodic wave solution of Boiti-Leon-Manna-Pempinelli equation. *Abstract and Applied Analysis*, vol. 2014, 738609.

Fang, T. (2014): Controlled quantum secure direct communication protocol based on five-particle cluster state and EPR pair entanglement swapping. *17th International Conference on Network-Based Information Systems*, pp. 135-140.

Gao, T.; Yan, F. L.; Wang, Z. X. (2005): Controlled quantum teleportation and secure direct communication. *Chinese Physics*, vol. 14, no. 5, pp. 893.

Hassanpour, S; Houshmand, M. (2015): Efficient controlled quantum secure direct communication based on GHZ-like states. *Quantum Information Processing*, vol. 14, no. 2, pp. 739-753.

Jiang, T. S.; Jiang, Z. W.; Ling, S. T. (2014): An algebraic method for quaternion and complex Least Squares coneigen-problem in quantum mechanics. *Applied Mathematics and Computation*, vol. 249, pp. 222-228.

Kumar, A.; Adhikari, S.; Banerjee, S.; Roy, S. (2013): Optimal quantum communication using multiparticle partially entangled states. *Physical Review A*, vol. 87, no. 2, 022307.

Li, J.; Chen, X. B.; Sun, X. M.; Li, Z. P.; Yang, Y. X. (2016): Quantum network coding for multi-unicast problem based on 2*d* and 3*d* cluster states. *Science China Information Sciences*, vol. 59, no. 4, 042301.

Li, L.; Wang, Z.; Li, Y. X.; Shen. H.; Lu, J. W. (2018): Hopf bifurcation analysis of a complex-valued neural network model with discrete and distributed delays. *Applied Mathematics and Computation*, vol. 330, pp. 152-169.

Lv, W. S.; Wang, F. (2017): Adaptive tracking control for a class of uncertain nonlinear systems with infinite number of actuator failures using neural networks. *Advances in Difference Equations*, vol. 2017, pp. 374.

Lu, X.; Wang, H. X.; Wang, X. (2012): On Kalman smoothing for wireless sensor networks systems with multiplicative noises. *Journal of Applied Mathematics*, vol. 2012, 71750.

Pang, Z. H; Liu, G. P.; Zhou, D. H.; Sun D. H. (2017): Data-based predictive control for networked nonlinear systems with packet dropout and measurement noise. *Journal of Systems Science & Complexity*, vol. 30, no. 5, pp. 1072-1083.

Qin, S. J. (2012): Reexamining the security of controlled quantum secure direct communication by using four particle cluster states. *International Journal of Theoretical Physics*, vol. 51, no. 9, pp. 2714-2718.

Wang, C.; Deng, F. G.; Li, Y. S.; Liu, X. S.; Long, G. L. (2005): Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A*, vol. 71, no. 4, 044305.

Wang, G. Y.; Fang, X. M.; Tan, X. H. (2006): Quantum secure direct communication with cluster state. *Chinese Physics Letters*, vol. 23, no. 10, pp. 2658.

Wang, J.; Zhang, Q.; Tang, C. (2006): Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. *Optics Communications*, vol. 266, no. 2, pp. 732-737.

Wei, Z. H.; Chen, X. B.; Niu, X. X.; Yang, Y. X. (2015): The quantum steganography protocol via quantum noisy channels. *International Journal of Theoretical Physics*, vol. 54, no. 8, pp. 2505-2515.

Xia, Y.; Song, H. S. (2007): Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding. *Physics Letters A*, vol. 364, no. 2, pp. 117-122.

Xia, Y.; Song, J.; Song, H. S. (2008): Controlled secure quantum communication using pure entangled W class states. *Communications in Theoretical Physics*, vol. 49, no. 4, pp. 919.

Xu, G.; Chen, X. B.; Dou, Z.; Li, J. X.; Liu, X. et al. (2016): Novel criteria for deterministic remote state preparation via the entangled six-qubit state. *Entropy*, vol. 18, no. 7, pp. 267.

Xu, G.; Chen, X. B.; Duo, Z.; Yang, Y. X.; Li, Z. P. (2015): A novel protocol for multiparty quantum key management. *Quantum Information Processing*, vol. 14, no. 8, pp. 2959-2980.

Xu, G.; Chen, X. B.; Li, J.; Wang, C.; Yang, Y. X. et al. (2015): Network coding for quantum cooperative multicast. *Quantum Information Processing*, vol. 14, no. 11, pp. 4297-4322.

Yang, Y. G.; Chai, H. P.; Teng, Y. W.; Wen, Q. Y. (2011): Improving the security of controlled quantum secure direct communication by using four particle cluster states against an attack with fake entangled particles. *International Journal of Theoretical Physics*, vol. 50, no. 2, pp. 395-400.

Zhang, L. L.; Zhan, Y. B.; Zhang, Q. Y. (2009): Controlled quantum secure direct communication by using four particle cluster states. *International Journal of Theoretical Physics*, vol. 48, no. 10, pp. 2971-2976.