 CMC, vol.57, no.3, pp.621-633, 2018

Analysis and Improvement of an Efficient Controlled Quantum Secure Direct Communication and Authentication Protocol

Jifeng Zhong[1, *], Zhihao Liu[2, 3, *] and Juan Xu[4]

Abstract: The controlled quantum secure direct communication (CQSDC) with authentication protocol based on four particle cluster states via quantum one-time pad and local unitary operations is cryptanalyzed. It is found that there are some serious security issues in this protocol. An eavesdropper (Eve) can eavesdrop on some information of the identity strings of the receiver and the controller without being detected by the selective-CNOT-operation (SCNO) attack. By the same attack, Eve can also steal some information of the secret message that the sender transmits. In addition, the receiver can take the same kind of attack to eavesdrop on some information of the secret message out of the control of the controller. This means that the requirements of CQSDC are not satisfied. At last, we improve the original CQSDC protocol to a secure one.

Keywords: Quantum cryptography, controlled quantum secure direct communication, selective-CNOT-operation attack.

1 Introduction

Now we have entered into the era of cloud computing and big data. The security of data becomes more and more important. The most efficient way is to encrypt the data with a private key. Although the one-time pad cryptosystem is with, but how to distribute a key with the proven security is really hard in classical cryptography. On the contrary, the proven secure key distribution problem can be effectively solved by the quantum manner [Bennett and Brassard (1984); Gisin, Ribordy, Tittel et al. (2002); Lo, Curty and Tamaki (2014)]. In fact, there is a new secure communication way called as the quantum secure direct communication (QSDC) [Deng, Long and Liu (2003); Deng and Long (2004); Wang, Deng, Liu et al. (2005); Long, Deng, Wang et al. (2007); Liu, Chen, Liu et al. (2012); Liu, Chen, Liu et al. (2013); Li (2015)] where the secret message is communicated directly without being encrypted by a private key in advance. With the development of QSDC, many researchers put forward a new kind of QSDC, which is usually called the controlled QSDC

[1] Navigation College, Jimei University, Xiamen, 361021, China.

[2] School of Computer Science and Engineering, Southeast University, Nanjing, 211189, China.

[3] Key Laboratory of Computer Network and Information Integration, Southeast University, Ministry of Education, Nanjing, 211189, China.

[4] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada, N2L3G1.

[*] Corresponding Authors: Jifeng Zhong. Email: jfzhong0618@163.com;

Zhihao Liu. Email: liuzhtopic@163.com.

(CQSDC) [Wang, Zhang and Tang (2006); Hassanpour and Houshmand (2014); Tan and Zhang (2016)]. In CQSDC, at least one additional user, the controller, is introduced besides the sender and the receiver to control the communication. If the controller does not permit the sender and the receiver to exchange the secret message, the receiver cannot gain any useful information of the secret message. If and only if the controller permits the sender and the receiver to exchange the secret message, the receiver can obtain the sender's secret message. We can summarize the basic requirements of CQSDC. Firstly, the CQSDC protocol should be secure against the external eavesdropper. Secondly, the receiver cannot gain any useful information about the secret message before the controller's permission.

As the contrary side of cryptography, cryptanalysis is also an important and interesting branch of cryptology, which usually be viewed as the art of code breaking in quantum cryptology. In 2005, Lo et al. [Lo and Ko (2005)] said that "breaking cryptographic systems is as important as building them". It assesses whether a cryptographic protocol is secure or not. For example, it assesses whether a cryptographic protocol has some potential loopholes, if so, it tries to mend these loopholes. Thus, cryptanalysis makes people to put forward more and more secure cryptographic protocols. Up to now, people have proposed many kinds of attack strategies, such as the denial-of-service (DoS) attack [Cai (2003)], the (partially) intercept-measure-resend attack [Liu, Chen, Wang et al. (2014); Liu, Chen and Liu (2016)], the correlation-extractability (CE) attack and its general case [Gao, Wen and Zhu (2007); Song and Zhang (2007); Gao, Qin, Wen et al. (2010); Qin, Gao and Guo (2010); Liu, Chen, Liu et al. (2011)], the teleportation attack [Gao, Wen and Zhu (2008)], the entanglement attack [Liu, Chen, Wang et al. (2014)], the different initial state attack [Yen, Horng, Goan et al. (2009); Liu and Chen (2018)] and so on.

Recently, a novel CQSDC with authentication protocol [Nanvakenari and Houshmand (2017)] was proposed by using four particle cluster states via quantum one-time pad and local unitary operations. In every transmission, the fourth qubit of each cluster state was used as controller's permission, and the same qubit and the first qubit of the same cluster state are utilized to deduce two classical bits of information. Since only single particle measurement was needed, it was easier to implement and less expensive. The authors also claimed that the protocol was secure and feasible against both of the inside and the outside attacks. They thought the receiver's and the controller's identity strings were reusable with unconditional security since they did not announce positions and bases of decoy particles. However, it can be found that there are some security problems if this protocol is deeply taken into account. Some information of the receiver's and the controller's identity strings can be stolen without being detected by the selective-CNOT-operation (SCNO) attack from an eavesdropper (Eve). Furthermore, she can eavesdrop on some information of the sender's secret message with the same attack. In addition, the receiver can take the same kind of attack to eavesdrop on some information of the secret message out of the control of the controller. This means that the requirements of CQSDC are not satisfied. Finally, the original CQSDC protocol is improved to a secure one.

2 The original CQSDC protocol

There are three users: Alice, Bob and Charlie who are the sender, the receiver, and the controller respectively. Bob has the secret N -bit identity string ID_B, and Charlie has the

secret N -bit identity string ID_C . Alice shares ID_B and ID_C with Bob and Charlie respectively, but Bob and Charlie do not share their identity strings. The original CQSDC protocol [Nanvakenari and Houshmand (2017)] is described as follows.

Step (1): Alice prepares an ordered sequence with N number of four particle cluster states, each of which is staying in

$$\left|P_n\right\rangle = \frac{1}{2}\left(\left|0000\right\rangle + \left|0011\right\rangle + \left|1100\right\rangle + \left|1111\right\rangle\right)_{b_n t_n k_n c_n}, \tag{1}$$

where b_n , t_n , k_n , c_n are four correlated particles in the n -th cluster state. Then, Alice constructs the ordered B and C sequences by particles b_n and c_n respectively. The remaining particles t_n and k_n construct the ordered A sequence $[t_1, k_1, t_2, k_2, \cdots, t_N, k_N]$. For convenience, we also denote the two subsequences $[t_1, t_2, \cdots, t_N]$ and $[k_1, k_2, \cdots, k_N]$ by the A_t sequence and the A_k sequence respectively.

Step (2): If a bit of ID_B is 0, Alice performs the unitary operation U_0 on the corresponding particle in the C sequence, otherwise the unitary operation U_1 is performed, where $U_0 = I = \left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|$ and $U_1 = i\sigma_y = \left|0\right\rangle\left\langle 1\right| - \left|1\right\rangle\left\langle 0\right|$. Thus, we get a new ordered sequence, C_U .

Step (3): Alice measures the A sequence in Z basis and gets an ordered classical bit sequence T_A which denotes $[T_{AT1}, T_{AK1}, T_{AT2}, T_{AK2}, \cdots, T_{ATN}, T_{AKN}]$. Similarly, T_A can be divided into two subsequences T_{AT} and T_{AK} which denote $[T_{AT1}, T_{AT2}, \cdots, T_{ATN}]$ and $[T_{AK1}, T_{AK2}, \cdots, T_{AKN}]$ respectively. For convenience, we let T_A be expressed as $T_{AT}T_{AK}$.

Step (4): If a bit of T_{AK} is 0, Alice performs U_0 on the corresponding particle in the B sequence; otherwise U_1 is performed. Thus, we get a new ordered sequence, B_U .

Step (5): Alice prepares two decoy N -qubit sequences S_{IDB} and S_{IDC} according to ID_B and ID_C , respectively. The rule to prepare a qubit is that: the i -th qubit of S_{IDB} (S_{IDC}) is prepared in Z basis if the i -th bit of ID_B (ID_C) is 0; otherwise, it is prepared in X basis.

Step (6): Alice mixes S_{IDB} and S_{IDC} into B_U and C_U to form B_U' and C_U' respectively according to the following rule. The rule is: Alice puts the i -th qubit of S_{IDB} (S_{IDC}) just behind the i -th particle in B_U (C_U) if the i -th bit of ID_B (ID_C) is 0; otherwise, she puts the i -th particle in B_U (C_U) just behind the i -th qubit of ID_B (ID_C). After that, Alice transmits B_U' and C_U' to Bob and Charlie respectively.

Step (7): After Bob and Charlie receive B_U' and C_U' , they extract S_{IDB} and S_{IDC} according to ID_B and ID_C respectively. Then Bob and Charlie measure each particle in

S_{IDB} and S_{IDC} with the right bases respectively. According to the measurement results, Bob and Charlie construct classical number sequences M_B and M_C respectively. The rule is that, states $|0\rangle$ and $|+\rangle$ are both represented as classical bit 0, and states $|1\rangle$ and $|-\rangle$ as classical bit 1. After that, Bob and Charlie publicly announce M_B and M_C respectively.

Step (8): According to S_{IDB} and S_{IDC}, Alice constructs two classical bit sequences M'_B and M'_C respectively. Under the ideal condition, the two equalities $M'_B = M_B$ and $M'_C = M_C$ must hold if there is no eavesdropping. Therefore, by comparison, Alice believes that there is no eavesdropping and Bob and Charlie are legal if the error rate is low enough. Then the communication continues. Otherwise, it will be stopped.

Step (9): If the controller Charlie permits the receiver Bob to read out the secret message from the sender Alice, he measures every particle in C_U with Z basis. According to the measurement result, he will form a classical bit string called T_{CU}. The rule is that the measurement result $|0\rangle$ corresponds to classical bit 0 while $|1\rangle$ corresponds to classical bit 1 respectively. Then Charlie announces the classical bit string T_{CU}.

Step (10): Bob measures every particle in B_U with Z basis. According to the measurement result, he will form a classical bit string called T_{BU}. The rule is the same as Charlie's.

Step (11): Alice prepares the secret message M which is expressed as $[M_{11}, M_{21}, M_{12}, M_{22}, \cdots, M_{1N}, M_{2N}]$. Similarly, M is divided into two subsequences M_1 and M_2 which denote $[M_{11}, M_{12}, \cdots, M_{1N}]$ and $[M_{21}, M_{22}, \cdots, M_{2N}]$ respectively. For convenience, we let M be expressed as $M_1 M_2$. Then Alice encrypts it with $T_{AT}T_{AK}$ bit by bit using XOR operation to get E_1E_2 ($E_1E_2 = M_1M_2 \oplus T_{AT}T_{AK}$). After that, Alice publishes E_1E_2.

Step (12): Bob obtains T_C according to T_{CU} and ID_B. That is, $T_C = ID_B \oplus T_{CU}$.

Step (13): Bob obtains T_B according to T_C and T_{BU}. That is, $T_B = T_{BU} \oplus T_C$.

Step (14): According to T_B and T_C, Bob reads out the secret message M_1M_2 by XOR operation from E_1E_2. That is, $M_1M_2 = T_BT_C \oplus E_1E_2$.

In this CQSDC protocol, we can find some obvious drawbacks. Firstly, the security of the identities determines the security of the protocol, because the identities are used to identity authentication as well as eavesdropping check at the same time. Secondly, inder to decrypt the secret message, there is only one kind of measurement is performed on

information carrier particles, so there is no error introduced if an eavesdropper happens to make the same measurement on an information carrier particle.

3 Cryptanalysis of the original CQSDC protocol

3.1 Eavesdropping on the identity strings of the receiver and the controller with the SCNO attack

We find that Eve can take the so-called attack strategy, the SCNO attack strategy [Liu, Chen and Liu (2016)] to successfully steal some information of the receiver's identity string (ID_B) and the controller's identity string (ID_C). In this strategy, only some selected particles not all the travelling particles are attacked. The detailed idea can be described as follows. At first, an ancilla sequence each of which initially stays in $|0\rangle$ is prepared by Eve. When every even particle in the travel sequence passes by, a CNOT operation is performed on this particle and an ancilla with this particle as the control qubit and the ancilla as the target, where $CNOT = \sum_{i,j=0}^{1} |i, j\rangle\langle i, i \oplus j|$. Then she will manipulate each ancilla to continue to attack. Let us take the case that Eve eavesdrops on ID_B as an example. We can describe the detailed attack strategy in the followings.

Step (a): Eve prepares an ancilla sequence, and makes each particle of the sequence initially stay in $|0\rangle$. When the sequence B'_U is transmitted from Alice to Bob in Step (6) of the CQSDC protocol, Eve chooses the even particles to attack. That is, if the particle is in the odd position, Eve just let this particle pass by, but if it is a particle in the even position, Eve captures it, makes one CNOT operation on this particle and an ancilla (Here, Eve lets the particle be the control qubit and the ancilla be the target qubit), and then releases the particle but measures the ancilla with Z basis. In consequence, she will obtain one classical bit sequence F_U according to the measurement result. The rule is that: the measurement result $|0\rangle$ is expressed by classical bit 0 and measurement result $|1\rangle$ is expressed by classical bit 1. It is easy to find the Eve's action will not introduce any error. Here we will give the detailed reasons. For one thing, if one bit of ID_B is 0, one can easily know that the particle Eve will measure in her attack is a decoy particle which inevitably stays in Z basis in line with Step (5) and Step (6) of the CQSDC protocol, so it can be successfully copied by a CNOT operation without bringing error. For another thing, if one bit of ID_B is 1, one can easily know that the particle Eve will measure in her attack is a cluster state particle. According to Step (10), it will be measured with Z basis. Obviously, Eve's CNOT operation acting on this particle and an ancilla in the state $|0\rangle$ does not change the Z basis measurement result on this particle but makes the ancilla has the same measurement result, so measuring the ancilla with Z basis does not introduce error too.

To understand Step (a) more explicitly, an example will be taken. We suppose ID_B is a five-bit string "00111" which is the same as that in Fig. 1 of the original CQSDC protocol [Nanvakenari and Houshmand (2017)], and ID_B, S_{IDB} and B_U be expressed as " $ID_{B1}ID_{B2}ID_{B3}ID_{B4}ID_{B5}$ ", " $S_{IDB1}S_{IDB2}S_{IDB3}S_{IDB4}S_{IDB5}$ ", " $B_{U1}B_{U2}B_{U3}B_{U4}B_{U5}$ " respectively. Obviously, S_{IDB1} and S_{IDB2} are in Z basis while S_{IDB3}, S_{IDB4} and S_{IDB5} are in X basis. Then the sequence B_U' can be expressed as " $B_{U1}S_{IDB1}B_{U2}S_{IDB2}S_{IDB3}B_{U3}S_{IDB4}B_{U4}S_{IDB5}B_{U5}$ ". The particles labeled even in this sequence are $S_{IDB1}, S_{IDB2}, B_{U3}, B_{U4}, B_{U5}$ respectively. We have known that S_{IDB1} and S_{IDB2} are in Z basis, so their states can be copied into the ancillas by CNOT operations. At the same time, we can deduce that B_{U3}, B_{U4}, B_{U5} will be measured with Z basis by the receiver Bob in Step (10). As we know, a CNOT operation on each of these particles and an ancilla in the state $|0\rangle$ does not change the Z basis measurement results on this particles but makes the ancillas has the same measurement results, so there is no error introduced if the ancilla is measured with Z basis. Therefore, Eve measures the ancillas with Z basis do not introduce any error. Meanwhile, she gets one corresponding classical sequence F_B which we express it as " $F_{B1}F_{B2}F_{B3}F_{B4}F_{B5}$ ". One possible case of F_B is "01001".

Step (b): Eve gains the classical string M_B after Bob's announcement in Step (7). Then She compares the classical strings F_B and M_B. (We let M_B be expressed as " $M_{B1}M_{B2}M_{B3}M_{B4}M_{B5}$ "). One possible case of M_B is "01010".

i. Eve can immediately deduce that the corresponding bit of ID_B is 1 (For example, Eve can deduce the fourth and the fifth bits of ID_B are 1), if a couple of the corresponding bits from F_B and M_B are different (In the above example, $F_{B4} \neq M_{B4}$ and $F_{B5} \neq M_{B5}$),. Now we explain the reason. If it is 0, then according to the rule to insert decoy particles, we know that Eve has measured the copy of the decoy particle in Z basis in the SCNO attack. Thus, the two classical bits of F_B and M_B must be identical.

ii. Eve indeed cannot simply deduce the definite value of ID_B, if a couple of the corresponding bits from F_B and M_B are identical, but this is of great meaning. In fact, the probability distribution of every bit of ID_B is not the same as the initial distribution. For example, if $F_B = M_B$, Eve can deduce the probability that $ID_B = 0$ is 2/3 while the prior probability is 1/2. We can refer to Tab. 1 to understand the above rules more unambiguously. From Tab. 1, we know that Eve has the probability of 1/4 to gain the precise outcomes which means the corresponding bits of ID_B are 1. If $M_B = F_B$, there is the probability of 2/3 to deduce $ID_B = 0$ and the probability of 1/3 to deduce $ID_B = 1$; if $M_B \neq F_B$, then

$ID_B = 1.$

So, the average quantity of information of every bit of ID_B that Eve can gain (denoting by $I_{Eve \to ID_B}$) is 0.311.

$$I_{Eve \to ID_B} = H(ID_B) - H(ID_B | M_B F_B) = 0.311 \quad (2)$$

So far, we have put forward the SCNO attack strategy for Eve to eavesdrop on some information of the receiver's identity string. Similarly, Eve or Bob can take the same attack strategy to eavesdrop on some information of the controller's identity string.

Table 1: Using M_B and F_B to deduce ID'_B, T'_{BU} and $ID'_B \oplus T'_{BU}$

ID_B	B_U	S_{IDB}	M_B	F_B	ID'_B	T'_{BU}	$ID'_B \oplus T'_{BU}$
0	$\|0\rangle$	$\|0\rangle$	0	0	(2,1)	(2,1)	(1,2)
0	$\|0\rangle$	$\|1\rangle$	1	1	(2,1)	(1,2)	(2,1)
0	$\|1\rangle$	$\|0\rangle$	0	0	(2,1)	(2,1)	(1,2)
0	$\|1\rangle$	$\|1\rangle$	1	1	(2,1)	(1,2)	(2,1)
1	$\|0\rangle$	$\|+\rangle$	0	0	(2,1)	(2,1)	(1,2)
1	$\|0\rangle$	$\|-\rangle$	1	0	1	0	1
1	$\|1\rangle$	$\|+\rangle$	0	1	1	1	0
1	$\|1\rangle$	$\|-\rangle$	1	1	(2,1)	(1,2)	(2,1)

ID'_B means the bit string that Eve can be deduced from ID_B;

T'_{BU} means the bit string that Eve can be deduced from T_{BU};

(a, b) in the last three columns represents the probability of bit 0 is a/3, and the probability of bit 1 is b/3.

3.2 Eavesdropping on the secret message with the SCNO attack

If Eve wants to get some information of the secret message, she will continue to Step (c).

Step (c): Eve gains T_{CU} from Charlie in Step (9), and E_1 as well as E_2 from Alice in Step (11). As we know, $T_B = T_{AT}$, $T_C = T_{AK}$, $T_{BU} = T_B \oplus T_{AK}$, $T_{CU} = T_C \oplus ID_B$, $E_1 = M_1 \oplus T_{AT}$ and $E_2 = M_2 \oplus T_{AK}$. So, the secret messages M_1 and M_2 can be decoded by

$$M_1 = E_1 \oplus T_{AT} = E_1 \oplus ID_B \oplus T_{BU} \oplus T_{CU}, \quad (3)$$

and

$$M_2 = E_2 \oplus T_{AK} = E_2 \oplus ID_B \oplus T_{CU}, \tag{4}$$

respectively. Since Eve can get E_1 and T_{CU} from the public classical channel, if she can also gain some information of $ID_B \oplus T_{BU}$, she will get some information of M_1. If $M_B F_B = 00$, there is the probability of 1/3 to deduce $ID_B \oplus T_{BU} = 0$ and the probability of 2/3 to deduce $ID_B \oplus T_{BU} = 1$; If $M_B F_B = 11$, there is the probability of 2/3 to deduce $ID_B \oplus T_{BU} = 0$ and the probability of 1/3 to deduce $ID_B \oplus T_{BU} = 1$; If $M_B F_B = 10$, then $ID_B \oplus T_{BU} = 1$; If $M_B F_B = 01$, then $ID_B \oplus T_{BU} = 0$. There is the probability of $1/4$ for Eve to get the precise value of $ID_B \oplus T_{BU}$. This means that Eve is able to eavesdrop on $1/4$ of the secret message M_1 in a determinate way.

Therefore, the average quantity of information of every bit of the secret message M_1 that Eve can gain (denoting by $I_{Eve \to M_1}$) is 0.311 if she only intends to acquire some information of M_1.

$$\begin{aligned} I_{Eve \to M_1} &= H(M_1) - H(M_1 | M_B F_B) \\ &= H(M_1) - H(ID_B \oplus T_{BU} | M_B F_B) = 0.311 \end{aligned} \tag{5}$$

Similarly, Eve can gain 0.311 bit of information about every bit of the secret message M_2 if she only intends to acquire some information of M_2.

If Eve eavesdrops on the secret messages M_1 and M_2 together, we find she can get more information than the sum of $I_{Eve \to M_1}$ and $I_{Eve \to M_2}$. This is because M_1 and M_2 are correlated after encryption. If $M_B F_B = 00$, there is the probability of 1/3 to deduce $(ID_B, ID_B \oplus T_{BU}) = (0,0)$, $(ID_B, ID_B \oplus T_{BU}) = (0,1)$ and $(ID_B, ID_B \oplus T_{BU}) = (1,1)$ respectively; If $M_B F_B = 11$, there is the probability of 1/3 to deduce $(ID_B, ID_B \oplus T_{BU}) = (0,0)$, $(ID_B, ID_B \oplus T_{BU}) = (0,1)$ and $(ID_B, ID_B \oplus T_{BU}) = (1,0)$ respectively; If $M_B F_B = 10$, then $(ID_B, ID_B \oplus T_{BU}) = (1,1)$; If $M_B F_B = 01$, then $(ID_B, ID_B \oplus T_{BU}) = (1,0)$. There is the probability of $1/4$ for to eavesdrop on the precise value of $(ID_B, ID_B \oplus T_{BU})$. This means that Eve is able to get $1/4$ of the secret message $M_1 M_2$ in a determinate way. Actually, the average quantity of information of every couple of the corresponding bits of the secret message M_1 and M_2 that Eve can gain (denoting by $I_{Eve \to M_1 M_2}$) is 0.811.

$$\begin{aligned} I_{Eve \to M_1 M_2} &= H(M_1 M_2) - H(M_1 M_2 | M_B F_B) \\ &= 0.811 \end{aligned} \tag{6}$$

So far, we have presented the so-called SCNO attack which Eve can take to eavesdrop on some information of the secret message without being detected by the two users, Alice and Bob.

3.3 The receiver eavesdropping on some information of the secret message without the controller's permission by the SCNO attack

It is well known that a CQSDC protocol must satisfies the basic security requirement that the receiver cannot obtain any information about the secret message without the permission of the controller. However, the original CQSDC protocol does not satisfy this requirement. The receiver Bob indeed can eavesdrop on some information of the secret message without Charlie's permission if he acts like an eavesdropper as described in the above. Here, Bob's purpose is to deduce some information of the secret message without Charlie's permission on basis of some information of T_{CU} is deduced at first.

Since Bob knows ID_B and T_{BU} . He also knows E_1E_2 after Alice's announcement. Therefore, he can deduce some information of the secret message M_1M_2 without Charlie's permission once he applies the SCNO attack strategy to get some information of T_{CU} . By taking the SCNO attack, we can calculate the average quantity of information of every couple of the corresponding bits of the secret message that Bob can eavesdrop on without Charlie's permission (denoting by $I_{Bob\to M_1M_2}$).

$$\begin{aligned} I_{Bob\to M_1M_2} &= H(M_1M_2) - H(M_1M_2 \mid M_C F_C) \\ &= H(M_1M_2) - H(T_{CU} \mid M_C F_C) \\ &= 1.311 \end{aligned} \tag{7}$$

4 Improvement of the original CQSDC protocol

We can summarize the reasons that Eve can successfully attack each even particle in every traveling sequence by the SCNO attack without introducing error is that: These particles are either decoy particles or information carrier particles, but every of them is measured with the same basis, Z basis. This is determined by the rules that Alice prepares the decoy particles and then mixes them into the information carrier particles. In each running of the CQSDC protocol, each identity string is used twice, one for determining the bases of the decoy particles, and the other for determining how the decoy particles are mixed into information carrier particles. This is indeed a drawback. Eve can ingeniously utilize this drawback to take an effective attack but does not introduce any error. To avoid the identity strings to be reused twice in each running, we can change the protocol a little.

Step (R1): Alice prepares an ordered sequence of N number of four particle cluster states, and makes each of them stay in the state $|P_n\rangle$. Then, Alice constructs the ordered B and C sequences by particles b_n and c_n from each state respectively. The remaining particles t_n and k_n construct the ordered A sequence $[t_1, k_1, t_2, k_2, \cdots, t_N, k_N]$. For

convenience, we also denote the two subsequences $[t_1, t_2, \cdots, t_N]$ and $[k_1, k_2, \cdots, k_N]$ by the A_t sequence and the A_k sequence respectively.

Step (R2): Alice performs the unitary operation U_0 on the corresponding particle in the C sequence if a bit of ID_B is 0, otherwise the unitary operation U_1 will be performed. In consequence, a new ordered sequence can be obtained. We call it C_U.

Step (R3): Alice measures the A sequence in Z basis and gets an ordered classical bit sequence T_A which denotes $[T_{AT1}, T_{AK1}, T_{AT2}, T_{AK2}, \cdots, T_{ATN}, T_{AKN}]$. Similarly, T_A can divide into two subsequences T_{AT} and T_{AK} which denote $[T_{AT1}, T_{AT2}, \cdots, T_{ATN}]$ and $[T_{AK1}, T_{AK2}, \cdots, T_{AKN}]$ respectively. For convenience, we let T_A be expressed as $T_{AT}T_{AK}$.

Step (R4): If a bit of T_{AK} is 0, Alice performs U_0 on the corresponding particle in the B sequence; otherwise U_1 is performed. In consequence, a new ordered sequence can be obtained. We call it B_U.

Step (R5): In line with ID_B and ID_C, Alice prepares two ordered sequences with N qubits, S_{IDB} and S_{IDC} respectively. The rule to prepare a qubit is that: The i-th qubit of S_{IDB} (S_{IDC}) is prepared in Z basis if the i-th bit of ID_B (ID_C) is 0; otherwise, it is prepared in X basis.

Step (R6): Alice prepares two random bit strings RID_B and RID_C. According to RID_B and RID_C, Alice mixes S_{IDB} and S_{IDC} into B_U and C_U to form B'_U and C'_U respectively. The rule is: Alice places the i-th qubit of S_{IDB} (S_{IDC}) just behind the i-th particle of B_U (C_U) if the i-th bit of RID_B (RID_C) is 0; or else, the i-th qubit of ID_B (ID_C) is placed before the i-th particle in B_U (C_U). After that, Alice transmits B'_U and C'_U to Bob and Charlie respectively.

Step (R7): After Bob and Charlie receive B'_U and C'_U, Alice publicly announces the two bit strings RID_B and RID_C. After that, Bob and Charlie extract S_{IDB} and S_{IDC} according to RID_B and RID_C respectively. Then Bob and Charlie measure S_{IDB} and S_{IDC} with the right bases according to ID_B and ID_C respectively. In line with the measurement outcomes, Bob and Charlie respectively construct classical bit sequences M_B and M_C. The rule is: Classical bit 0 expresses both states $|0\rangle$ and, and classical bit 1 expresses both states $|1\rangle$ and $|-\rangle$. Afterward, Bob and Charlie announce M_B and M_C respectively.

Step (R8): In line with S_{IDB} and S_{IDC}, Alice generates two classical bit sequences M'_B and M'_C respectively. Then M'_B is compared with M_B, and M'_C is compared with M_C. Under the ideal condition, the two equalities $M'_B = M_B$ and $M'_C = M_C$ must hold if there is no eavesdropping. Therefore, by comparison, Alice believes that there is no eavesdropping and Bob and Charlie are legal if the error rate is low enough. Then the communication continues. Otherwise, it will be stopped.

Step (R9): If the controller Charlie permits the receiver Bob to read out the secret message from the sender Alice, he measures every particle in C_U with Z basis. According to the measurement result, he will form a classical bit string called T_{CU}. The rule is that the measurement result $|0\rangle$ corresponds to classical bit 0 while $|1\rangle$ corresponds to classical bit 1 respectively. Then Charlie announces the classical bit string T_{CU}.

Step (R10): Bob measures every particle in B_U with Z basis. According to the measurement result, he will form a classical bit string called T_{BU}. The rule is the same as Charlie's.

Step (R11): Assume that the secret message Alice wants to send is M which expresses as $[M_{11}, M_{21}, M_{12}, M_{22}, \cdots, M_{1N}, M_{2N}]$. Similarly, M is divided into two subsequences M_1 and M_2 which denote $[M_{11}, M_{12}, \cdots, M_{1N}]$ and $[M_{21}, M_{22}, \cdots, M_{2N}]$ respectively. For convenience, we let M be expressed as $M_1 M_2$. Then Alice encrypts it with $T_{AT}T_{AK}$ bit by bit using XOR operation to get E_1E_2 ($E_1E_2 = M_1M_2 \oplus T_{AT}T_{AK}$). After that, Alice publishes E_1E_2.

Step (R12): Bob obtains T_C according to T_{CU} and ID_B. That is, $T_C = ID_B \oplus T_{CU}$.

Step (R13): Bob obtains T_B according to T_C and T_{BU}. That is, $T_B = T_{BU} \oplus T_C$.

Step (R14): According to T_B and T_C, Bob reads out the secret message M_1M_2 by XOR operation from E_1E_2. That is, $M_1M_2 = T_BT_C \oplus E_1E_2$.

In the improved protocol, the identity strings are only used once to determine the bases of decoy particles. In addition, the decoy particles which are regularly inserted into the corresponding information carriers according to the identity strings are randomly mixed into the corresponding information carriers. As a result, the particles labeled even in each traveling sequence are not always staying in Z basis or measured by Z basis. Therefore, if an attacker still takes the SCNO attack strategy, some errors will be inevitably introduced, which will lead to the stopping of the communication before the secret message is transmitted. This indicates that the improved CQSDC protocol is secure.

5 Conclusion

To sum up, the CQSDC with authentication protocol [Nanvakenari and Houshmand (2017)] is cryptanalyzed. We find that some security issues exist in it. By the Eve's SCNO attack, some information of the receiver's and the controller's identity strings can be eavesdropped on without being checked. Thus, she can successfully eavesdrop on some information of the secret message the sender transmits. In addition, the receiver can take the SCNO attack to eavesdrop on some information about the secret message without the controller's permission. This does not satisfy the basic security requirement of CQSDC. At last, the original CQSDC protocol is improved to a secure one.

Acknowledgement: This work was supported by National Natural Science Foundation of China (Grant No. 61502101), the Six Talent Peaks Project of Jiangsu Province (Grant No. XYDXX-003), Scientific Research Foundation of the science and Technology Department of Fujian Province (Grant No. JK2015023), and Shangda Li Education Foundation of Jimei University (Grant No. ZC2013010).

References

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems & Signal Processing*, pp. 175-179.

Cai, Q. Y. (2003): The "ping-pong" protocol can be attacked without eavesdropping. *Physical Review Letters*, vol. 91, no. 10.

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

Deng, F. G.; Long, G. L.; Liu, X. S. (2003): Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Physical Review A*, vol. 68, no. 4.

Gao, F.; Qin, S. J.; Wen, Q. Y.; Zhu, F. C. (2010): Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. *Optics Communications*, vol. 283, no. 1, pp. 192-195.

Gao, F.; Wen, Q. Y.; Zhu, F. C. (2007): Comment on: "Quantum exam". *Physics Letters A*, vol. 360, no. 6, pp. 748-750.

G**ao, F.; Wen, Q. Y.; Zhu, F. C.** (2008): Teleportation attack on the QSDC protocol with a random basis and order. *Chinese Physics B*, vol. 17, no. 9, pp. 3189-3193.

Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. (2002): Quantum cryptography. *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195.

Hassanpour, S.; Houshmand, M. (2014): Efficient controlled quantum secure direct communication based on GHZ-like states. *Quantum Information Processing*, vol. 14, no. 2, pp. 739-753.

Li, X. H. (2015): Quantum secure direct communication. *Acta Physica Sinica*, vol. 64.

Liu, Z. H.; Chen, H. W.; Liu, W. J.; Xu, J.; Li, Z. Q. (2011): Analyzing and revising a two-way protocol for quantum cryptography with a nonmaximally entangled qubit pair. *International Journal of Quantum Information*, vol. 9, no. 5, pp. 1329-1339.

Liu, Z. H.; Chen, H. W.; Liu, W. J. (2016): Cryptanalysis of controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *International Journal of Theoretical Physics*, vol. 55, no. 10, pp. 4564-4576.

Liu, Z. H.; Chen, H. W.; Liu, W. J.; Xu, J.; Wang, D. et al. (2013): Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states. *Quantum Information Processing*, vol. 12, no. 1, pp. 587-599.

Liu, Z. H.; Chen, H. W.; Liu, W. J.; Xu, J.; Li, Z. Q. (2012): Deterministic secure quantum communication without unitary operation based on high-dimensional entanglement swapping. *Science China-Information Sciences*, vol. 55, no. 2, pp. 360-367.

Liu, Z. H.; Chen, H. W.; Wang, D.; Li, W. Q. (2014): Cryptanalysis and improvement of three-particle deterministic secure and high bit-rate direct quantum communication protocol. *Quantum Information Processing*, vol. 13, no. 6, pp. 1345-1351.

Lo, H. K.; Curty, M.; Tamaki, K. (2014): Secure quantum key distribution. *Nature Photonics*, vol. 8, no. 8, pp. 595-604.

Lo, H. K.; Ko, T. M. (2005): Some attacks on quantum-based cryptographic protocols. *Quantum Information & Computation*, vol. 5, no. 1, pp. 41-48.

Long, G. L.; Deng, F. G.; Wang, C.; Li, X. H.; Wen, K. et al. (2007): Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China*, vol. 2, no. 3, pp. 251-272.

Nanvakenari, M.; Houshmand, M. (2017): An efficient controlled quantum secure direct communication and authentication by using four particle cluster states. *International Journal of Quantum Information*, vol. 15, no. 1.

Qin, S. J.; Gao, F.; Guo, F. Z.; Wen, Q. Y. (2010): Comment on "two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair". *Physical Review A*, vol. 82.

Song, J; Zhang, S. (2007): Comment on: "Quantum exam". *Physics Letters A*, vol. 360, no. 6, pp. 746-747.

Tan, X.; Zhang, X. (2016): Controlled quantum secure direct communication by entanglement distillation or generalized measurement. *Quantum Information Processing*, vol. 15, no. 5, pp. 2137-2154.

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.

Wang, J.; Zhang, Q.; Tang, C. J. (2006): Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. *Optics Communications*, vol. 266, pp. 732-737.

Yen, C. A.; Horng, S. J.; Goan, H. S.; Kao, T. W.; Chou, Y. H. (2009): Quantum direct communication with mutual authentication. *Quantum Information & Computation*, vol. 9, no. 5, pp. 376-394.