Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad*

Zhi-Hao Liu(刘志昊)[1,2,3,†] and Han-Wu Chen(陈汉武)[1,2,‡]

[1] School of Computer Science and Engineering, Southeast University, Nanjing 211189, China
[2] Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, Nanjing 211189, China
[3] Center for Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia

(Received 18 November 2015; revised manuscript received 31 March 2016; published online 25 June 2016)

The security of quantum broadcast communication (QBC) and authentication protocol based on Greenberger–Horne–Zeilinger (GHZ) state and quantum one-time pad is analyzed. It is shown that there are some security issues in this protocol. Firstly, an external eavesdropper can take the intercept–measure–resend attack strategy to eavesdrop on 0.369 bit of every bit of the identity string of each receiver without being detected. Meanwhile, 0.524 bit of every bit of the secret message can be eavesdropped on without being detected. Secondly, an inner receiver can take the intercept–measure–resend attack strategy to eavesdrop on half of the identity string of the other's definitely without being checked. In addition, an alternative attack called the CNOT-operation attack is discussed. As for the multi-party QBC protocol, the attack efficiency increases with the increase of the number of users. Finally, the QBC protocol is improved to a secure one.

Keywords: cryptanalysis, quantum broadcast communication, information leakage, intercept–measure–resend attack, CNOT-operation attack

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a, 03.65.Ud **DOI:** 10.1088/1674-1056/25/8/080308

1. Introduction

As one of the most developed branches of quantum cryptography, quantum key distribution (QKD) discusses the problem of how to distribute a secret key between two remote users with the quantum manner. The pioneers Bennett and Brassard[1] designed the first QKD protocol in 1984, where four nonorthogonal single-photon states were used. Afterward, Ekert[2] put forward another novel QKD protocol by using Einstein–Podolsky–Rosen (EPR) pairs in 1991, in which Bell inequality was for the first time used to evaluate the security of the quantum channel. In the next year, Bennett *et al.*[3] proposed a new QKD protocol based on two nonorthogonal single-photon states with unconditional security. After that, QKD[4–11] received much attention and fruitful achievement in both theoretical and experimental aspects. In recent years, another branch of quantum cryptography called quantum direct communication (QDC) was put forward. Different from QKD, QDC allows the sender to transmit directly the secret or the deterministic key (instead of a random key) to the receiver in a deterministic and secure manner. Compared with that in QKD, the security demands in QDC are more rigorous because the information transmitted is the meaningful secret instead of a random key, which cannot be eavesdropped. This means the information cannot be leaked out whether the eavesdropper would be discovered or not in QDC. In general, QDC can be divided into two categories: quantum secure direct communication (QSDC)[12–26] and deterministic secure quantum communication (DSQC).[27–35] The difference between QSDC and DSQC is that there are some classical bits communicated to assist the receiver to decrypt the secret in DSQC, while in QSDC there is not. Quantum broadcast communication (QBC)[36–38] as a special kind of QDC was put forward several years ago, which involves a sender and multiple receivers. For QBC, a sender broadcasts a secret message to a set of receivers with the quantum manner, and every receiver can get the same message.

Recently, Chang *et al.*[39] put forward a novel QBC and authentication protocol with a quantum one-time pad based on the Greenberger–Horne–Zeilinger (GHZ) state. For the sake of convenience, we refer to this QBC protocol as the QBC-CXZY protocol later. It was shown that one bit of information could be broadcasted from the sender to the receivers at the cost of a GHZ state consumed. The classical exclusive-or (XOR) operation serving as a one-time-pad was used to forbid the eavesdroppers to eavesdrop on the secret transmitted by the sender. Eavesdropping detection and identity authentication were implemented at the same time based on previously shared identity strings. It was claimed that the identity strings could be reused with unconditional security and no hash function or

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61502101 and 61170321), the Natural Science Foundation of Jiangsu Province, China (Grant No. BK20140651), the Research Fund for the Doctoral Program of Higher Education, China (Grant No. 20110092110024), and the Project Funded by PAPD and CICAEET.

†Corresponding author. E-mail: lzh@seu.edu.cn
‡Corresponding author. E-mail: hw_chen@seu.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

local unitary operation was used. However, if considering this protocol carefully, one can find that it in fact has some security issues. An eavesdropper can take the intercept–measure–resend attack strategy to eavesdrop on some information of the identity strings of the receivers and the secret message without being detected. Moreover, one receiver can take the intercept–measure–resend attack more efficiently than the external eavesdropper to eavesdrop on the other's identity string without being detected. As for the multi-party QBC-CXZY protocol, the attack efficiency increases with the increase of the number of users. In the following context, we will cryptanalyze the QBC-CXZY protocol from the viewpoint of information theory.

2. Description of the QBC-CXZY protocol

Suppose that the sender Alice wants to broadcast her secret message to two receivers Bob and Charlie. Bob and Charlie have the secret N-bit strings ID_B and ID_C representing their identities respectively. Alice shares ID_B and ID_C with Bob and Charlie respectively. The QBC-CXZY protocol consists of the following steps.

Step 1 Alice prepares N ordered three-particle GHZ states to transmit the secret message. Each of them is in the state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}. \tag{1}$$

Then, Alice takes particles 1, 2, and 3 from each state to construct three ordered sequences S_1, S_2, and S_3, which are expressed as the following forms: $\{P_1(1), P_2(1), \ldots, P_N(1)\}$, $\{P_1(2), P_2(2), \ldots, P_N(2)\}$, and $\{P_1(3), P_2(3), \ldots, P_N(3)\}$ respectively.

Step 2 According to ID_B and ID_C, Alice prepares two N-qubit sequences S_{IDB} and S_{IDC}. The rule is that she randomly prepares the i-th qubit of S_{IDB} (S_{IDC}) in one of the two states in Z-basis $\{|0\rangle, |1\rangle\}$ if the i-th bit of ID_B (ID_C) is 0; otherwise, she randomly prepares the qubit in one of the two states in the X-basis $\{|\pm\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)\}$.

Step 3 According to ID_B and ID_C, Alice mixes S_{IDB} and S_{IDC} to S_2 and S_3 to form S'_2 and S'_3 respectively. The rule is that if the i-th bit of ID_B is 0, Alice puts the i-th particle of S_{IDB} behind the i-th particle in S_2; otherwise, she puts the i-th particle of S_{IDB} before the i-th particle in S_2. In the same way, S_{IDC} is mixed into S_3 to form S'_3. After that, Alice transmits S'_2 and S'_3 to Bob and Charlie respectively.

Step 4 After Bob and Charlie receive S'_2 and S'_3, they extract S_{IDB} and S_{IDC} according to ID_B and ID_C, and then measure the particles in each sequence using the right bases respectively.

Step 5 According to the respective measurement results of S_{IDB} and S_{IDC}, Bob and Charlie generate the classical bit sequences D_B and D_C respectively. That is, states $|0\rangle$ and $|+\rangle$ both represent classical bit 0, and states $|1\rangle$ and $|-\rangle$ represent classical bit 1. After that, Bob and Charlie publicly announce D_B and D_C respectively. Then, Alice compares Bob's and Charlie's results with the initial states of S_{IDB} and S_{IDC} respectively. If the error rates are low enough, Alice believes that Bob and Charlie are legal and no eavesdropping exists, and thus the communication goes on. Otherwise Alice interrupts it.

Step 6 Bob and Charlie respectively measure particles in S_2 and S_3 with Z-basis in order to get the ordered classical bit sequences C_{S2} and C_{S3} with the rule that the states $|0\rangle$ and $|1\rangle$ correspond to classical bits 0 and 1 respectively.

Step 7 Alice measures the particles in S_1 in order with Z-basis and constructs the ordered classical string C_{S1}. Assume that the secret message Alice wants to send is M, then Alice encrypts it with C_{S1} bit-by-bit by exclusive-or (XOR) operation to get C ($C = M \oplus C_{S1}$). After that, Alice publishes C.

Step 8 According to C_{S2} and C_{S3}, Bob and Charlie decrypt C to get the secret message M by XOR operation. That is, $M = C \oplus C_{S2} = C \oplus C_{S3}$.

Step 9 Two receivers Bob and Charlie store and deal with the secret message M.

Step 10 Alice, Bob and Charlie continue to the second transmission.

In the QBC-CXZY protocol, there are some obvious features. Firstly, the security of the protocol completely depends on the security of the identities, because eavesdropping check and identity authentication are implemented at the same time. Secondly, only Z-basis measurement is used to decrypt the secret message, so if an eavesdropper (Eve) happens to make a Z-basis measurement on a transmitted particle which comes from a GHZ state, there is no error introduced.

3. Cryptanalysis of the QBC-CXZY protocol

3.1. An external eavesdropper eavesdropping on the identity strings of the receivers and the secret message

Now we consider the situation that an external eavesdropper (Eve) eavesdrops on some information of the identity strings of the receivers (ID_B and ID_C) and the secret message without bringing any error. The attack strategy is described as follows.

i) In Step 3 of the QBC-CXZY protocol, when Alice transmits the sequences S'_2 and S'_3 to Bob and Charlie, Eve intercepts them, and measures the particles labeled even in each sequence with Z-basis to get two classical sequences E_2 and E_3 respectively. Here, classical bit 0 in E_2 and E_3 represents the measurement result $|0\rangle$ and classical bit 1 represents $|1\rangle$. After that, Eve prepares two sequences according to E_2 and E_3 and resends them to Bob and Charlie respectively. Obviously, there is no error introduced by her action. The reason is as follows. On the one hand, if one bit of ID_B (ID_C) is 0, then the corresponding particle Eve has measured is a decoy particle and it inevitably stays in Z-basis according to the Steps 2 and 3 of the QBC-CXZY protocol. So measuring this particle with Z-basis cannot bring error. On the other hand, if one bit of ID_B (ID_C) is 1, the corresponding particle she has measured is inevitably from a GHZ state according to Steps 2 and 3 of the QBC-CXZY protocol. However, even if she has measured this

particle with Z-basis, her action still cannot bring error, because she knows Bob (Charlie) will measure the particle with Z-basis in the Step 6.

ii) Eve waits for Bob and Charlie in Step 5 to publish the classical strings D_B and D_C which denote the measurement results of decoy sequences S_{IDB} and S_{IDC} respectively. Then Eve compares the classical strings E_2 and E_3 she has gotten in Step 1, with the classical strings D_B and D_C she has gotten from Bob's and Charlie's announcements.

Rule 1 If a couple of the corresponding bits from D_B and E_2 are different, she can immediately deduce that she has measured a particle from S_2, which means $ID_B = 1$. This is because if $ID_B = 0$, then she has measured a particle from S_{IDB} according to the rule that S_{IDB} is mixed into S_2 in the Step 3 of the QBC-CXZY protocol, and thus D_B must be identical to E_2. Similarly, if a couple of the corresponding bits from D_C and E_3 are different, Eve can immediately deduce that she has measured a particle from S_3, which means $ID_C = 1$;

Rule 2 If Eve has deduced that some bit of ID_B (ID_C) is 1, she can immediately infer that the corresponding bit of C_{S2} is equal to that of E_2 (the corresponding bit of C_{S3} is equal to that of E_3). This is because if some bit of ID_B (ID_C) is 1, Eve knows the particle she has measured is from S_2 (S_3) but this does not bring any error. That is to say, Eve gets C_{S2} (C_{S3}) in this situation;

Rule 3 If Eve has inferred some bit of $ID_B\,(ID_C)$ is equal to 1, but the corresponding bits of $C_{S2}\,(C_{S3})$ and $E_3\,(E_2)$ are not equal, then Eve can deduce that the corresponding bit of $ID_C\,(ID_B)$ is equal to 0 according to the rule that S_{IDC} (S_{IDB}) is mixed into S_3 (S_2) in Step 3 of the QBC-CXZY protocol;

Rule 4 In other cases, Eve cannot infer the direct values of ID_B, ID_C, and $C_{S2}\,(C_{S3})$, but this does not mean they are useless from the viewpoint of information theory because the posterior probability distributions of the bits of ID_B, ID_C, and $C_{S2}\,(C_{S3})$ may be changed.

To understand the above rules more unambiguously, we can refer to Table 1. Now we will take the 10th row of Table 1 as an example to explain how Eve can deduce C'_{S2} (C'_{S3}) where $C'_{S2}\,(C'_{S3})$ represents the classical bit string about $C_{S2}\,(C_{S3})$ that Eve can deduce. Because $D_C \neq E_3$, Eve can deduce ID_C is equal to 1 (Rule 1). Thus Eve knows that she has measured the particle from S_3 without bringing any error. This means $C'_{S2} = C'_{S3} = E_3 = 0$ (Rule 2). As a result, Eve can deduce the corresponding bit of the secret by $M = C \oplus C'_{S2} = C \oplus C'_{S3}$.

Table 1. Using D_B, D_C, E_2, and E_3 to deduce ID'_B, ID'_C, and $C'_{S2}\,(C'_{S3})$.

ID_B	ID_C	S_2 (S_3)	S_{IDB}	S_{IDC}	D_B	D_C	E_2	E_3	ID'_B	ID'_C	$C'_{S2}\,(C'_{S3})$
0	0	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	N	N	N
0	0	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	1	0	1	N	N	N
0	0	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	1	0	1	0	N	N	N
0	0	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	1	1	1	1	N	N	N
0	0	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	N	N	N
0	0	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	0	1	0	1	N	N	N
0	0	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	1	0	1	0	N	N	N
0	0	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	1	1	1	1	N	N	N
0	1	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	0	0	0	0	N	N	N
0	1	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	0	1	0	0	N	1	0
0	1	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	1	0	1	0	N	N	N
0	1	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	1	1	1	0	0	1	0
0	1	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	0	0	0	1	0	1	1
0	1	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	0	1	0	1	N	N	N
0	1	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	1	0	1	1	N	1	1
0	1	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	1	1	1	1	N	N	N
1	0	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	0	0	0	0	N	N	N
1	0	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	0	1	0	1	N	N	N
1	0	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	1	0	0	0	1	N	0
1	0	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	1	1	0	1	1	0	0
1	0	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	0	0	1	0	1	0	1
1	0	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	0	1	1	1	1	N	1
1	0	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	1	0	1	0	N	N	N
1	0	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	1	1	1	1	N	N	N
1	1	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	0	0	0	0	N	N	N
1	1	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	0	1	0	0	N	1	0
1	1	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	1	0	0	0	1	N	0
1	1	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	1	1	0	0	1	1	0
1	1	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	0	0	1	1	1	1	1
1	1	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	0	1	1	1	1	N	1
1	1	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	1	0	1	1	N	1	1
1	1	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	1	1	1	1	N	N	N

ID'_B represents the classical bit string about ID_B that Eve can deduce;
ID'_C represents the classical bit string about ID_C that Eve can deduce;
$C'_{S2}\,(C'_{S3})$ represents the classical bit string about $C_{S2}\,(C_{S3})$ that Eve can deduce;
N represents that Eve cannot deduce the value confidently.

Without loss of generality, we assume that the probabilities that classical bits 0 and 1 occur are identical in every identity string. It means that states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ have the same probabilities to be prepared for the decoy states. In addition, it is easily known that if measuring the particle 2 (3) from a GHZ state, one has the identical probability to get the results $|0\rangle$ and $|1\rangle$. This means in Table 1 the result that every row expresses has the same probability to appear.

It can be easily found that Eve has the probability of $5/16$ to obtain the bits of $ID_B\,(ID_C)$ definitely. Furthermore, we can calculate the average quantity of information Eve can gain about every bit of ID_B (denoting by $I_{\mathrm{Eve}\to ID_B}$).

$$\begin{aligned} I_{\mathrm{Eve}\to ID_B} &= 1+\frac{5}{32}\times\left(\frac{3}{5}\log\frac{3}{5}+\frac{2}{5}\log\frac{2}{5}\right)\times 2 \\ &\quad+\frac{4}{32}\times\left(\frac{3}{4}\log\frac{3}{4}+\frac{1}{4}\log\frac{1}{4}\right)\times 2 \\ &\quad+\frac{2}{32}\times\left(\frac{1}{2}\log\frac{1}{2}+\frac{1}{2}\log\frac{1}{2}\right)\times 2 \\ &\approx 0.369. \end{aligned} \tag{2}$$

Similarly, the average quantity of information Eve can gain about every bit of ID_C (denoting by $I_{\mathrm{Eve}\to ID_C}$) is also 0.369.

From Table 1, one can easily see that Eve has the probability of $7/16$ to get the bits of $C_{S2}\,(C_{S3})$ definitely. This means that Eve has the ability to get $7/16$ of the secret message definitely according to the equalities $M = C\oplus C_{S2} = C\oplus C_{S3}$. Moreover, one can calculate the quantity of information Eve can gain about every bit of the secret message on average (denoting by $I_{\mathrm{Eve}\to M}$).

$$\begin{aligned} I_{\mathrm{Eve}\to M} &= 1+\frac{5}{32}\times\left(\frac{4}{5}\log\frac{4}{5}+\frac{1}{5}\log\frac{1}{5}\right)\times 2 \\ &\quad+\frac{4}{32}\times\left(\frac{1}{2}\log\frac{1}{2}+\frac{1}{2}\log\frac{1}{2}\right)\times 2 \\ &\approx 0.524. \end{aligned} \tag{3}$$

So far, we have put forward an attack strategy for an external eavesdropper to get some information of ID_B and ID_C and the secret message M without being detected.

3.2. One receiver eavesdropping on the other's identity string

If a receiver acts as an eavesdropper to eavesdrop on the other's identity string, his attack obviously is more efficient because he has more resources and knowledge than the external eavesdropper. Here we take Bob as an example to eavesdrop on Charlie's identity string ID_C. The situation that Charlie eavesdrops on Bob's identity string ID_B is the same. The attack strategy is described as follows.

1) In Step 3 of the QBC-CXZY protocol, when Alice transmits the sequence S'_3 to Charlie, Bob intercepts it, and measures the particles labeled even with Z-basis. Meanwhile, he records classical bit 0 to express $|0\rangle$ and classical bit 1 to express $|1\rangle$. As a result, he can obtain one classical sequence which we denote by E_3. After that, Bob prepares a new particle sequence according to E_3 and resends this sequence to Charlie. Obviously, there is no error introduced by his action. The reason is as follows. On the one hand, if some bit of ID_C is 0, the particle (from sequence S'_3) he has measured is a decoy particle which inevitably stays in Z-basis according to Steps 2 and 3 of the QBC-CXZY protocol, so measuring this particle with Z-basis cannot bring error. On the other hand, if some bit of ID_C is 1, the particle he has measured is from the GHZ state according to Steps 2 and 3 of the QBC-CXZY protocol. However, he also knows Charlie will measure the particle with Z-basis in the Step 6, which means that Bob measuring this particle cannot bring error too.

2) Bob waits for Charlie to publish the classical string D_C which denotes the measurement results of decoy particles in the Step 5. Then Bob compares the classical strings E_3 he has acquired in Step 1) with D_C and C_{S2}. Note that he gets C_{S2} by measuring the sequence S_2.

Rule 1 If a couple of the corresponding bits from D_C and E_3 are different, Bob can immediately deduce that he has measured a particle from S_3, that is to say, $ID_C = 1$. The reason is that if $ID_C = 0$, then he has measured a decoy particle from S_{IDC} according to Steps 2 and 3 of the QBC-CXZY protocol, and thus he knows that D_C must be identical to E_3.

Rule 2 If a couple of the corresponding bits from $C_{S2}\,(C_{S3})$ and E_3 are different, Bob can immediately deduce that he has measured a decoy particle from S_{IDC}, that is to say, $ID_C = 0$. This is because if $ID_C = 1$, then he has measured a particle from S_3, and he knows that $C_{S2}\,(C_{S3})$ must be identical to E_3.

To understand the above rules more unambiguously, we can refer to Table 2. Let us take the second row of Table 2 as an example. Because $E_3 \neq C_{S2}$, Bob can deduce that $ID'_C = 0$.

Table 2. Using $C_{S2}\,(C_{S3})$, D_C, and E_3 to deduce ID'_C. In this table, ID'_C represents the classical bit string about ID_C that Eve can deduce; N represents that Eve cannot deduce the value confidently.

ID_C	$S_2\,(S_3)$	S_{IDC}	$C_{S2}\,(C_{S3})$	D_C	E_3	ID'_C
0	$\|0\rangle$	$\|0\rangle$	0	0	0	N
0	$\|0\rangle$	$\|1\rangle$	0	1	1	0
0	$\|1\rangle$	$\|0\rangle$	1	0	0	0
0	$\|1\rangle$	$\|1\rangle$	1	1	1	N
1	$\|0\rangle$	$\|+\rangle$	0	0	0	N
1	$\|0\rangle$	$\|-\rangle$	0	1	0	1
1	$\|1\rangle$	$\|+\rangle$	1	0	1	1
1	$\|1\rangle$	$\|-\rangle$	1	1	1	N

Without loss of generality, we assume again that the probabilities that classical bits 0 and 1 occur are identical in every identity string. It means that states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ have the same probabilities to be prepared for the decoy states. In addition, it is easily known that if measuring the particle 2 (3) from a GHZ state with Z-basis, one has the identical probability to get results $|0\rangle$ and $|1\rangle$. This means in Table 2 the result that every row expresses has the same probability to appear.

From Table 2, one can easily see that Bob has the probability of $1/2$ to get the bits of the identity string ID_C definitely. That is to say, the quantity of information Bob can gain about every bit of the secret message on average is $1/2$. Since $1/2 > 0.369$, it shows that an inner receiver is more efficient than an external eavesdroppers to attack the identity string of the other receiver.

4. Discussion

4.1. An alternative attack strategy

As described above, Eve can make an intercept–measure–resend attack strategy to attack every particle labeled even in each traveling sequence. Actually, Eve can exploit an alternative strategy to attack the QBC-CXZY protocol (we call it the CNOT-operation attack). The concrete steps are as follows. Eve prepares an ancilla sequence in which each ancilla initially stays in $|0\rangle$. When a GHZ particle labeled even passes by, she performs a CNOT operation on this particle and an ancilla with the particle as the control qubit and the ancilla as the target, where

$$\mathrm{CNOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|. \quad (4)$$

Then she measures each ancilla with Z-basis. The following steps are the same as described in Subsection 3.1. Also, one receiver can use this alternative strategy to eavesdrop on the other's identity string as described in Subsection 3.2.

4.2. Cryptanalysis of the multi-party QBC-CXZY protocol

As for the multi-party QBC-CXZY protocol, an external eavesdropper can use the same attack strategy to eavesdrop on the receivers' identity strings and the secret. The attack efficiency increases with the increase of the number of users. Now we will explain the reason in the following. For any i $(2 \le i \le n)$, according to the knowledge of information theory, we have

$$\begin{aligned} & I(ID_i; D_2, E_2, D_3, E_3, \ldots, D_n, E_n) \\ \ge\ & I(ID_i; D_2, E_2, D_3, E_3, \ldots, D_{n-1}, E_{n-1}) \\ \ge\ & \cdots \ge I(ID_i; D_2, E_2, D_3, E_3) = 0.369, \end{aligned} \quad (5)$$

i.e.,

$$I^{(n)}_{\mathrm{Eve}\to ID_i} \ge I^{(n-1)}_{\mathrm{Eve}\to ID_i} \ge \ldots \ge I^{(3)}_{\mathrm{Eve}\to ID_i} = 0.369. \quad (6)$$

Here, ID_i, D_j, E_j $(2 \le j \le n)$ represents the identity string of the i-th receiver (we let the sender be the first user), the classical bit string the j-th user can get by measuring the received decoy particles, and the classical bit string Eve can get by measuring the particles labeled even in the traveling sequence sent to the j-th user. $I(X;Y)$ denotes the mutual information between X and Y.

Similarly, the following inequalities hold.

$$\begin{aligned} & I(C_S; D_2, E_2, D_3, E_3, \ldots, D_n, E_n) \\ \ge\ & I(C_S; D_2, E_2, D_3, E_3, \ldots, D_{n-1}, E_{n-1}) \\ \ge\ & \cdots \ge I(C_S; D_2, E_2, D_3, E_3) = 0.524, \end{aligned} \quad (7)$$

i.e.,

$$I^{(n)}_{\mathrm{Eve}\to M} \ge I^{(n-1)}_{\mathrm{Eve}\to M} \ge \cdots \ge I^{(3)}_{\mathrm{Eve}\to M} = 0.524. \quad (8)$$

Here C_S is the classical bit string each receiver can get by measuring the received multi-qubit GHZ particles from the sender. Since $I(C_S; D_j, E_j) \ge 1/4$, one can easily know that

$$I^{(n)}_{\mathrm{Eve}\to M} \ge 1 - \left(\frac{3}{4}\right)^{n-1}, \quad (9)$$

which means that

$$\lim_{n\to\infty}\left(I^{(n)}_{\mathrm{Eve}\to M}\right) = 1. \quad (10)$$

In particular, when $n \ge 17$, $I^{(n)}_{\mathrm{Eve}\to M} \ge 0.99$. It means that when the number of the users is not less than 17, Eve can get at least 0.99 bit of every bit of the secret message. So far, we have explained the reason why the attack efficiency increases with the increase of the number of users.

5. Improvement of the QBC-CXZY protocol

The reason why an external eavesdropper or an inner user can successfully make an intercept–measure–resend attack is that the identity strings of the receivers are used not only to prepare the decoy particles but also to determine how the decoy particles are mixed into the information carrier particles. That is to say, the identity strings are repeatedly used. This is not allowed in secure communication. Whether the particles labeled even in every traveling sequence are decoy particles or information carrier particles, they all will be measured with Z-basis according to the rules that the decoy particles are prepared and they are inserted into the information carrier particles. So Eve can use this drawback to make an attack without bringing any error. Therefore, to improve the QBC-CXZY protocol, every identity string should be used only once. So, Steps 3 and 4 of the QBC-CXZY protocol are changed as follows.

Step R3 Alice randomly mixes S_{IDB} and S_{IDC} to S_2 and S_3 to form S'_2 and S'_3 respectively. Apart from Alice, no one else knows how S_{IDB} and S_{IDC} are mixed into S_2 and S_3. After that, Alice transmits S'_2 and S'_3 to Bob and Charlie respectively.

Step R4 After Bob and Charlie receive S'_2 and S'_3, Alice publishes the information about which particles in S'_2 and S'_3 are decoy particles. That is, Alice tells Bob and Charlie which particles compose S_{IDB} and S_{IDC} respectively. Bob and Charlie extract S_{IDB} and S_{IDC} according to Alice's announcement, and then they measure the particles in each sequence using the right bases respectively.

Note that, before Alice, Bob, and Charlie start a new communication, they will probably have to update the identity strings.

Now if an external eavesdropper or an inner receiver still exploits the intercept–measure–resend attack strategy to attack the particles labeled even in every traveling sequence, she (he) will introduce some errors. This is because the particles labeled even in each traveling sequence are not always staying in Z-basis or measured by the corresponding receiver with Z-basis.

6. Conclusion

In summary, we find that there are some security issues about the QBC-CXZY protocol. An eavesdropper can take the intercept–measure–resend attack strategy to eavesdrop on some information of the identity strings of the receivers and the secret message by measuring the particles labeled even in every traveling sequence with Z-basis without bringing any error. The reason why Eve can use this strategy to successfully attack is that whether the particles labeled even are decoy particles or information carrier particles, they all will be measured with Z-basis. This is really a serious drawback. Of course, an inner receiver can also take the intercept–measure–resend attack more efficiently than the external eavesdropper to eavesdrop on the other's identity string without being detected. In addition, an alternative attack called the CNOT-operation attack is discussed. As for the multi-party QBC-CXZY protocol, the attack efficiency increases with the increase of the number of users. Finally, the QBC-CXZY protocol is improved to a secure one. In a word, more attention should be paid to the security of the quantum secure communication in order to design really secure quantum communication protocols.

References

[1] Bennett C H and Brassard G 1984 *IEEE International Conference on Computers, Systems & Signal Processing*, December 10–12, Bangalore, India, p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[5] Bruβ D 1998 *Phys. Rev. Lett.* **81** 3018
[6] Wang X B 2004 *Phys. Rev. Lett.* **92** 077902
[7] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[8] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[9] Noh T G 2009 *Phys. Rev. Lett.* **103** 230501
[10] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X, Guan J Y, Yang D X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X F, Chen T Y, Zhang Q and Pan J W 2014 *Phys. Rev. Lett.* **113** 190501
[11] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[12] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[13] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[14] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[15] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[16] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[17] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett. A* 359
[18] Long G L, Deng F G, Wang C and Li X H 2007 *Front. Phys. China* **2** 251
[19] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev. A* **78** 064304
[20] Dong L, Xiu X M, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 1688
[21] Cao W F, Yang Y G and Wen Q Y 2010 *Sci. China: Phys. Mech. Astron.* **53** 1271
[22] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. China: Phys. Mech. Astron.* **54** 942
[23] Liu Z H, Chen H W, Liu W J, Xu J, Wang D and Li Z Q 2013 *Quantum Infor. Process.* **12** 587
[24] Hong C H, Heo J, Lim J I and Yang H J 2014 *Chin. Phys. B* **23** 090309
[25] Li X H 2015 *Acta Phys. Sin.* **64** 0160307 (in Chinese)
[26] Mi S C, Wang T J, Jin G S and Wang C 2015 *IEEE Photon. J.* **7** 7600108
[27] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol. A* **101** 357
[28] Yan F L and Zhang X Q 2004 *Eur. Phys. J. B* **41** 75
[29] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[30] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P and Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354
[31] Man Z X, Xia Y J and An N B 2006 *J. Phys. B: At. Mol. Opt. Phys.* **39** 3855
[32] Xiu X M, Dong H K, Dong L, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 2457
[33] Quan D X, Pei C X, Liu D and Zhao N 2010 *Acta Phys. Sin.* **59** 2493 (in Chinese)
[34] Liu Z H, Chen H W, Liu W J, Xu J and Li Z Q 2012 *Sci. China-Inf. Sci.* **55** 360
[35] Liu Z H, Chen H W, Wang D and Xue X L 2014 *Int. J. Theor. Phys.* **53** 2118
[36] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 23
[37] Wang J, Zhang Q and Tang C J 2007 *Chin. Phys.* **16** 1868
[38] Yang Y G, Wang Y H and Wen Q Y 2010 *Chin. Phys. B* **19** 070304
[39] Chang Y, Xu C X, Zhang S B and Yan L L 2014 *Chin. Phys. B* **23** 010305