Vol 16 No 7, July 2007
1009-1963/2007/16(07)/1868-10

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Quantum broadcast communication*

Wang Jian(王 剑)†, Zhang Quan(张 权), and Tang Chao-Jing(唐朝京)

School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, *China*

(Received 23 August 2006; revised manuscript received 8 December 2006)

Broadcast encryption allows the sender to securely distribute his/her secret to a dynamically changing group of users over a broadcast channel. In this paper, we just take account of a simple broadcast communication task in quantum scenario, in which the central party broadcasts his secret to multi-receiver via quantum channel. We present three quantum broadcast communication schemes. The first scheme utilizes entanglement swapping and Greenberger–Horne–Zeilinger state to fulfil a task that the central party broadcasts the secret to a group of receivers who share a group key with him. In the second scheme, based on dense coding, the central party broadcasts the secret to multi-receiver, each of which shares an authentication key with him. The third scheme is a quantum broadcast communication scheme with quantum encryption, in which the central party can broadcast the secret to any subset of the legal receivers.

Keywords: quantum broadcast communication, quantum secure direct communication
PACC: 0367

1. Introduction

Quantum key distribution (QKD),[1−3] which provides a way for two legitimate parties to establish a private key with unconditional security, has progressed rapidly since the first QKD protocol was proposed by Bennett and Brassard in 1984.[1] With quantum mechanics, a good many of other quantum cryptography protocols have also been proposed and pursued, such as quantum secret sharing (QSS)[4−9] and quantum secure direct communication (QSDC).[10−24] QSS is the generalization of classical secret sharing to a quantum scenario. Many researches have been carried out in both theoretical and experimental aspects after the pioneering QSS scheme proposed by Hillery, Buzěk and Berthiaume in 1999.[4] Different from QKD, QSDC aims to transmit the secret message directly without first establishing a key to encrypt it. QSDC can be used in some special environments, which has been shown in Ref.[11,12]. The work on QSDC has attracted much attention. Boström and Felbinger[11] proposed a Ping–Pong protocol which is quasi-secure for secure direct communication if perfect quantum channel is used. Deng *et al*[12,13] put forward a two-step QSDC protocol using Einstein–Podolsky–Rosen (EPR) pairs and a QSDC scheme using batches of single photons which serves as quantum one-time pad cryptosystem. We proposed a multiparty controlled QSDC scheme using Greenberger–Horne–Zeilinger (GHZ) state and a QSDC scheme based on the order rearrangement of single photons.[17,18] Lee *et al*[23] presented two QSDC protocols with user authentication. Recently, some multiparty quantum direct communication schemes, which are used to fulfil the task that many users send each of their secrets to a central party, have been proposed.[25−28] Gao *et al*[26] proposed a QSDC scheme using GHZ states and entanglement swapping. In their scheme, the secret messages can be transmitted from two senders to a remote receiver. They also presented a simultaneous QSDC scheme between the central party and other M parties using GHZ states, in which the M parties can transmit each of their secret messages to the central party simultaneously.[27] Jin *et al*[28] put forward a simultaneous QSDC scheme by using GHZ states and dense coding.

Broadcast encryption involves a sender and multi-users (receivers).[29] The sender first encrypts his content and then transmits it to a dynamically changing set of users via insecure broadcasting channels. The broadcast encryption scheme ensures that only the privileged receivers can recover the content subscribed and the unauthorized users cannot learn anything. In this paper, we take account of a simple broadcast encryption task in a quantum scenario, called quantum broadcast communication (QBC), in which the central

*Project supported by the National Natural Science Foundation of China (Grant No 60472032).
†E-mail: jwang@nudt.edu.cn

party broadcasts his secret message to a group of legal receivers via quantum channel and no illegal receiver can obtain the central party's secret. We then consider a naive scheme that the sender first establishes a common key with multi-users and then encrypts the secret with the sharing key. Thus the multi-users can obtain the sender's secret by decrypting the cypher with the key. In the present schemes, we try to allow the sender to broadcast the secret to multi-users directly without first establishing a common key to encrypt it. We then present three QBC schemes based on the ideas in Refs.[23,27,28,30]. In scheme 1, a group of users share a group key with the central party. After authenticating the users, the central party broadcasts his secret message to them by using entanglement swapping.[31] In scheme 2, each user shares an authentication key with the central party. The central party first authenticates the users and then broadcasts the secret to them by using dense coding.[32] In scheme 3, based on quantum encryption,[30] the central party encrypts his secret message by performing controlled-NOT (CNOT) operation on the secret qubit and the particle in GHZ state and the designated users also use CNOT operation to decrypt the central party's secret.

QBC aims to broadcast the secret to legal multi-users directly. In our schemes, we suppose a trusted third party, Trent, broadcasts his secret to r legal users, Alice_1, Alice_2, ..., Alice_r. Similar to Ref.[23], Trent shares a secret identity number ID_i $(i = 1, 2, \ldots, r)$ and a secret hash function h_i $(i = 1, 2, \ldots, r)$ with each user. Trent broadcasts his secret to the users, only if their identities are legal. Here the hash function is

$$h : \{0,1\}^l \times \{0,1\}^m \to \{0,1\}^n, \tag{1}$$

where l, m and n denote the length of the identity number, the length of a counter and the length of authentication key, respectively. Thus the user's authentication key can be expressed as $\text{AK} = h(\text{ID},C)$, where C is the counter of calls on the user's hash function. When the authentication key is not long enough to satisfy the requirement of cryptographic task, the parties can increase the counter and then generate a new authentication key. We denote the authentication keys of Alice_1, Alice_2, ..., Alice_r's as $\text{AK}_{A_1} = h_{A_1}(\text{ID}_{A_1}, C_{A_1})$, $\text{AK}_{A_2} = h_{A_2}(\text{ID}_{A_2}, C_{A_2})$, ..., $\text{AK}_{A_r} = h_{A_r}(\text{ID}_{A_r}, C_{A_r})$.

We then give some relations which will be used in our schemes. The four Bell states and the eight three-particle GHZ states are defined as

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned} \tag{2}$$

and

$$\begin{aligned} |\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad |\Psi_2\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \\ |\Psi_3\rangle &= \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \quad |\Psi_4\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle), \\ |\Psi_5\rangle &= \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \quad |\Psi_6\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle), \\ |\Psi_7\rangle &= \frac{1}{\sqrt{2}}(|110\rangle + |001\rangle), \quad |\Psi_8\rangle = \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle), \end{aligned} \tag{3}$$

respectively. The four unitary operations, which can be encoded as two bits of classical information, are as follows:

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\ \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ \mathrm{i}\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0|, \\ \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|. \end{aligned} \tag{4}$$

Here the encoding is defined as $I \to 00$, $\sigma_x \to 01$, $\mathrm{i}\sigma_y \to 10$, $\sigma_z \to 11$. The Hadamard (H) operation is

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|). \quad (5)$$

2. Scheme 1: QBC using entanglement swapping

In scheme 1, Trent utilizes multi-particle GHZ states and entanglement swapping to realize quantum broadcast communication called QBC-ES. We first present the scheme with two users (Alice$_1$, Alice$_2$) and then generalize it to the case with many users (Alice$_1$, Alice$_2$, ..., Alice$_r$). In the scheme, Trent broadcasts his secret message to a group of users and all users have the same authentication key which we call group key (GK).

(S1) Trent prepares an ordered N three-particle GHZ states, each of which is in the state $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{TA_1A_2}$, where the subscripts T, A_1 and A_2 represent the three particles of each GHZ state. Trent takes particle T (A_1, A_2) from each state to form an ordered particle sequence, called T (A_1, A_2) sequence. For each GHZ state, Trent performs I or H operation on particles A_1 and A_2 according to the group key, GK. If the ith value of GK is 0 (1), he performs I (H) operation on particles A_1 and A_2. As we have described in Section 1, here GK= $h(ID, C)$. If GK is not long enough to reach N, new GK can be generated by increasing the counter until GK is not shorter than N. Trent also performs randomly one of the two operations $\{I, \mathrm{i}\sigma_y\}$ on particle A_1. He then sends A_1 and A_2 sequences to Alice$_1$ and Alice$_2$, respectively.

(S2) After receiving A_1 and A_2 sequences, Alice$_1$ and Alice$_2$ perform I or H operation on each of their particles according to GK. For example, if the ith value of GK is 0 (1), Alice$_1$ executes I (H) operation on particle A_1. They inform Trent that they have transformed their qubit by using unitary operation according to GK. Trent then authenticates the identities of the users and checks eavesdropping in the transmission line.

(S3) The procedure of authentication and eavesdropping check is as follows: (a) After hearing from the users, Trent selects randomly a sufficiently large subset from the ordered N GHZ states. (b) He measures the sampling particles in T sequence, in a random measuring basis, Z-basis($|0\rangle, |1\rangle$) or X-basis ($|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$). (c) Trent publishes the positions of the sampling particles and the measuring basis for each of the sampling particles. Alice$_1$ (Alice$_2$) measures the sampling particles in A_1 (A_2) sequence, in the same measuring basis as Trent. After measurements, the users publish their measurement results. (d) Trent can then authenticate the users and check the existence of eavesdropper by comparing their measurement results. If the users are legal and the channel is safe, their results should be completely correlated. Suppose Trent's operation performed on particle A_1 is I. When Trent performs Z-basis measurement on his particle, Alice$_1$ and Alice$_2$'s results should be $|00\rangle(|11\rangle)$, on the condition that Trent's result is $|0\rangle(|1\rangle)$. And Alice$_1$ and Alice$_2$'s result should be $|++\rangle$ or $|--\rangle$ ($|+-\rangle$ or $|-+\rangle$), if Trent performs X-basis measurement on his particle and obtains the result $|+\rangle(|-\rangle)$. Thus, if Trent confirms that the users are legal and there is no eavesdropping, they will continue to execute the next step. Otherwise, they will abort the communication.

(S4) After authenticating the users, Trent announces publicly his random operations on the particles in A_1 sequence and Alice$_1$ then performs the same operations on them. Trent divides the remaining GHZ states into M ordered groups, $\{\mathrm{P}(1)_{TA_1A_2}, \mathrm{Q}(1)_{T'A_1'A_2'}\}$, $\{\mathrm{P}(2)_{TA_1A_2}, \mathrm{Q}(2)_{T'A_1'A_2'}\}$, ..., $\{\mathrm{P}(M)_{TA_1A_2}, \mathrm{Q}(M)_{T'A_1'A_2'}\}$, where 1, 2, ..., M represent the order of the group and the subscripts T and T' (A_1, A_1' and A_2, A_2') denote Trent's (Alice$_1$'s and Alice$_2$'s) particles. Trent encodes his secret on each particle T by using one of the four operations $\{I, \sigma_x, \mathrm{i}\sigma_y, \sigma_z\}$. The parties agree that the four operations represent two-bit of classical message, as we have described in Section 1. Alice$_1$ generates an M-bit random string a_1. For each group, she performs one of the two unitary operations $\{I, \sigma_x\}$ on particle A_1 according to a_1. For example, if the ith value of a_1 is 0 (1), Alice$_1$ executes I (σ_x) operation on particle A_1. Here Alice$_1$ does not perform any operation on particle A_1'.

(S5) Alice$_1$ (Alice$_2$) measures particles A_1 and A_1' (A_2 and A_2') of each group in Bell basis. After measurements, Alice$_1$ publishes her measurement results, but Alice$_2$ does not do this directly. Referring to GK, Alice$_2$ transforms her result by using corresponding unitary operation. If the $(2i-1)$th and $2i$th values of GK are 00 (01, 10, 11), she performs I (σ_x, $\mathrm{i}\sigma_y$, σ_z) operation on her result and then publishes the

transformed result. If Alice$_2$'s result is $|\phi^+\rangle$ and the corresponding bits of GK are 01, the published result is $|\psi^+\rangle$.

(S6) Trent performs Bell basis measurement on particles T and T' of each group and publishes his measurement results. According to the published information, the users can obtain Trent's secret message. We then explain it in detail. The state of a group can be written as

$$\begin{aligned}|\Psi_1\rangle_{TA_1A_2}\otimes|\Psi_1\rangle_{T'A_1'A_2'} = \ & \frac{1}{2\sqrt{2}}(|\phi^+_{TT'}\rangle|\phi^+_{A_1A_1'}\rangle|\phi^+_{A_2A_2'}\rangle+|\phi^+_{TT'}\rangle|\phi^-_{A_1A_1'}\rangle|\phi^-_{A_2A_2'}\rangle+|\phi^-_{TT'}\rangle|\phi^+_{A_1A_1'}\rangle|\phi^-_{A_2A_2'}\rangle\\ &+|\phi^-_{TT'}\rangle|\phi^-_{A_1A_1'}\rangle|\phi^+_{A_2A_2'}\rangle+|\psi^+_{TT'}\rangle|\psi^+_{A_1A_1'}\rangle|\psi^+_{A_2A_2'}\rangle+|\psi^+_{TT'}\rangle|\psi^-_{A_1A_1'}\rangle|\psi^-_{A_2A_2'}\rangle\\ &+|\psi^-_{TT'}\rangle|\psi^+_{A_1A_1'}\rangle|\psi^-_{A_2A_2'}\rangle+|\psi^-_{TT'}\rangle|\psi^-_{A_1A_1'}\rangle|\psi^+_{A_2A_2'}\rangle).\end{aligned}\tag{6}$$

If Trent's encoding operation is σ_x which corresponds to secret bits 01 and Alice$_1$'s random operation is also σ_x corresponding to bit 1, $|\Psi_1\rangle_{TA_1A_2}$ is then transformed into $|\Psi_7\rangle_{TA_1A_2}$ and the state of the group becomes

$$\begin{aligned}|\Psi_7\rangle_{TA_1A_2}\otimes|\Psi_1\rangle_{T'A_1'A_2'} = \ & \frac{1}{2\sqrt{2}}(|\psi^+_{TT'}\rangle|\psi^+_{A_1A_1'}\rangle|\phi^+_{A_2A_2'}\rangle-|\psi^+_{TT'}\rangle|\psi^-_{A_1A_1'}\rangle|\phi^-_{A_2A_2'}\rangle\\ &-|\psi^-_{TT'}\rangle|\psi^+_{A_1A_1'}\rangle|\phi^-_{A_2A_2'}\rangle+|\psi^-_{TT'}\rangle|\psi^-_{A_1A_1'}\rangle|\phi^+_{A_2A_2'}\rangle+|\phi^+_{TT'}\rangle|\phi^+_{A_1A_1'}\rangle|\psi^+_{A_2A_2'}\rangle\\ &-|\phi^+_{TT'}\rangle|\phi^-_{A_1A_1'}\rangle|\psi^-_{A_2A_2'}\rangle-|\phi^-_{TT'}\rangle|\phi^+_{A_1A_1'}\rangle|\psi^-_{A_2A_2'}\rangle+|\phi^-_{TT'}\rangle|\phi^-_{A_1A_1'}\rangle|\psi^+_{A_2A_2'}\rangle).\end{aligned}\tag{7}$$

From the results of Trent and Alice$_1$, Alice$_2$ can deduce Trent's secret message because the three parties' results correspond to an exclusive state. For example, the results of Trent and Alice$_1$ are respectively $|\psi^-_{TT'}\rangle$ and $|\psi^-_{A_1A_1'}\rangle$ and Alice$_2$'s original result is $|\phi^+_{A_2A_2'}\rangle$. Referring to Eq.(7), the state of the group must be $|\Psi_7\rangle_{TA_1A_2}\otimes|\Psi_1\rangle_{T'A_1'A_2'}$. Alice$_2$ deduces that Trent's secret must be '01' because only the operation $\sigma_x\otimes\sigma_x$ applied on particles T and A_1 can transform the state $|\Psi_1\rangle$ into $|\Psi_7\rangle$. On the other hand, Alice$_1$ knows GK and she can deduce Alice$_2$'s original result according to the published result. Similarly, she can also obtain Trent's secret. Thus Trent broadcasts his secret to two legal users.

Now, let us discuss the security for the present scheme. The security requirement for the scheme is that no illegal user can obtain Trent's secret. As long as the procedure of authentication and eavesdropping check is secure, the whole scheme is secure. Anyone who has no GK cannot obtain Trent's secret message because it is impossible to deduce a definite result about the secret from the published results. We then discuss the security for the procedure of authentication and eavesdropping check.

At step (S1), Trent performs I or H operation on particles A_1 and A_2 according to GK which is only shared by the three parties. If the ith bit of GK is 0 or 1, the three-particle GHZ state becomes

$$|\Phi_1\rangle=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|\phi^+\rangle+|-\rangle|\phi^-\rangle)=\frac{1}{2}[|+\rangle(|++\rangle+|--\rangle)+|-\rangle(|+-\rangle+|-+\rangle)],\tag{8}$$

or

$$\begin{aligned}|\Phi_2\rangle \ &= \frac{1}{\sqrt{2}}(|0++\rangle+|1--\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|\phi^+\rangle+|-\rangle|\psi^+\rangle)\\ &= \frac{1}{2}[|+\rangle(|++\rangle+|--\rangle)+|-\rangle(|++\rangle-|--\rangle)].\end{aligned}\tag{9}$$

According to Eqs.(8) and (9), if an eavesdropper, Eve, intercepts particles A_1 and A_2 and makes a Bell basis measurement on them, she can obtain partial information of GK. However, Trent performs random I or $\mathrm{i}\sigma_y$

operation on particle A_1, which can prevent Eve from eavesdropping the information of GK. As a result of Trent's operation, there are four possible states $|\Phi_1\rangle, |\Phi_2\rangle$,

$$\begin{aligned} |\Phi_3\rangle &= \frac{1}{\sqrt{2}}(-|010\rangle + |101\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|\psi^-\rangle - |-\rangle|\psi^+\rangle) \\ &= \frac{1}{2}[|+\rangle(|-+\rangle - |+-\rangle) - |-\rangle(|++\rangle - |--\rangle)] \end{aligned} \tag{10}$$

and

$$\begin{aligned} |\Phi_4\rangle &= \frac{1}{\sqrt{2}}(|0-+\rangle - |1+-\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|\psi^-\rangle + |-\rangle|\phi^-\rangle) \\ &= \frac{1}{2}[|+\rangle(|-+\rangle - |+-\rangle) + |-\rangle(|+-\rangle + |-+\rangle)]. \end{aligned} \tag{11}$$

According to Eqs.(8)–(11), Eve cannot distinguish the four states by using Bell basis measurement. During the process of authentication and eavesdropping check, Trent measures his sampling particles in Z-basis or X-basis randomly and allows the users to measure their corresponding particles in the same measuring basis. Suppose Trent performs Z-basis measurement on his particle and Eve also measures particles A_1 and A_2 in Z-basis. Eve publishes her measurement result after measurements. If the state is $|\Phi_1\rangle$ or $|\Phi_3\rangle$, Eve will not introduce any error during the process of authentication and eavesdropping check. However, if the state is $|\Phi_2\rangle$ or $|\Phi_4\rangle$, Eve will obtain $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ each with probability 1/4 and the error rate introduced by her achieves 75%. Similarly, when Trent performs X-basis measurement and Eve measures particles A_1 and A_2 in the same measuring basis, if the state is $|\Phi_2\rangle$ or $|\Phi_4\rangle$, Eve will not introduce any error. But if the state is $|\Phi_1\rangle$ or $|\Phi_3\rangle$, Eve will obtain $|++\rangle, |+-\rangle, |-+\rangle$ and $|--\rangle$ each with probability 1/4 and the error rate introduced by her is 50%. Suppose Trent performs X-basis measurement and Eve measures particles A_1 and A_2 in Bell basis. When Eve's result is $|\phi^+\rangle(|\psi^-\rangle)$, her action will not be detected by Trent if she publishes the result $|++\rangle$ or $|--\rangle(|+-\rangle$ or $|-+\rangle)$. However, when her result is $|\phi^-\rangle$ $(|\psi^+\rangle)$, if the state is $|\Phi_4\rangle(|\Phi_3\rangle)$, Trent will detect Eve's eavesdropping. Similarly, if Trent performs Z-basis measurement and Eve executes Bell basis measurement, Eve's eavesdropping will also be detected by Trent with some probability.

According to Stinespring's dilation theorem, Eve's action can be realized by a unitary operation $\hat{E}$ on a large Hilbert space, $H_{A_1A_2} \otimes H_E$. Then the state of Trent, Alice$_1$ and Eve is

$$|\Phi\rangle = \sum_{T,A_1,A_2\in\{0,1\}} |\varepsilon_{T,A_1,A_2}\rangle|T\rangle|A_1A_2\rangle, \tag{12}$$

where $|\varepsilon\rangle$ denotes Eve's probe state and $|T\rangle$ and $|A_1A_2\rangle$ are states shared by Trent and the users. The condition for the states of Eve's probe is

$$\sum_{T,A_1,A_2\in\{0,1\}} \langle\varepsilon_{T,A_1,A_2}|\ \varepsilon_{T,A_1,A_2}\rangle = 1. \tag{13}$$

As Eve can eavesdrop particles A_1 and A_2, her action on the system can be written as

$$\begin{aligned} |\Phi\rangle = \ & \frac{1}{\sqrt{2}}[|0\rangle(\alpha_1|00\rangle|\varepsilon_{000}\rangle + \beta_1|01\rangle|\varepsilon_{001}\rangle \\ & +\gamma_1|10\rangle|\varepsilon_{010}\rangle + \delta_1|11\rangle|\varepsilon_{011}\rangle) + |1\rangle(\delta_2|11\rangle|\varepsilon_{100}\rangle \\ & +\gamma_2|10\rangle|\varepsilon_{101}\rangle + \beta_2|01\rangle|\varepsilon_{110}\rangle + \alpha_2|00\rangle|\varepsilon_{111}\rangle]. \end{aligned} \tag{14}$$

When the state is $|\Phi_1\rangle$, the error rate introduced by Eve is $\epsilon = 1 - |\alpha_1|^2 = 1 - |\delta_2|^2$. Here the complex numbers α, β, γ and δ must satisfy $\hat{E}\hat{E}^\dagger = I$.

We then generalize the three-party QBC-ES scheme to a multiparty one (more than three parties). Suppose Trent wants to broadcast his secret to a group of users, {Alice$_1$, Alice$_2$, ..., Alice$_r$}. He prepares an ordered N $(r+1)$-particle GHZ states

$$\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)_{T,A_1,\ldots,A_r}. \tag{15}$$

The details of the multiparty QBC-ES are very similar to those of three-party one. Trent performs I or H operation on particles A_1, A_2, ..., A_r according to the GK they share. He also performs randomly I or iσ_y operation on particles A_1, A_2, ..., $A_{(r-1)}$ and sends A_1, A_2, ..., A_r sequences to Alice$_1$, Alice$_2$, ..., Alice$_r$,

separately. After receiving the particles, each user performs I or H operation on their particles according to GK. Similar to step (S3), Trent authenticates the users and checks eavesdropping. If all users are legal, he announces publicly his operations on particles A_1, A_2, ..., $A_{(r-1)}$ and Alice$_1$, Alice$_2$, ..., Alice$_{(r-1)}$ execute the same operations on them. Trent divides all GHZ states into M ordered groups, $[\{\mathrm{P}(1)_{TA_1\ldots A_r}, \mathrm{Q}(1)_{T'A'_1\ldots A'_r}\}, \ldots, \{\mathrm{P}(M)_{TA_1\ldots A_r}, \mathrm{Q}(M)_{T'A'_1\ldots A'_r}\}]$. He encodes his secret on particles T by using one of the four operations, $\{I, \sigma_x, \mathrm{i}\sigma_y, \sigma_z\}$. Alice$_1$, Alice$_2$, ..., Alice$_{(r-1)}$ each perform randomly one of the two operations $\{I, \sigma_x\}$ on their particles. Each user measures particles A_i and A'_i $(i = 1, 2, \ldots, r)$ in Bell basis. After measurements, Alice$_1$, Alice$_2$, ..., Alice$_{(r-1)}$ publish their measurement results. Alice$_r$ first transforms her result according to GK and then publishes the transformed result. Trent also performs Bell basis measurement on particles T and T' of each group. Thus Trent broadcasts his secret to all legal users, Alice$_1$, Alice$_2$, ..., Alice$_{(r-1)}$ and Alice$_r$. The security for multiparty QBC-ES scheme is similar to that for three-party one. As long as the procedure of authentication and eavesdropping check is secure, the scheme is secure. Based on such method, we can also obtain a simultaneous multiparty quantum authentication scheme.[33]

3. Scheme 2: QBC based on dense coding

In scheme 1, Trent can only broadcast secret to a group of users who share a GK with him. Based on dense coding, we present a quantum broadcast communication scheme, called QBC-DC scheme, in which Trent broadcasts his secret to multi-users {Alice$_1$, Alice$_2$, ..., Alice$_r$} and each user shares an authentication key with Trent. We first present a three-party QBC-DC scheme and then generalize it to a multiparty one.

(S1) Trent prepares an ordered N three-particle GHZ states, each of which is randomly produced in one of the eight GHZ states $\{|\Psi_1\rangle_{TA_1A_2}, |\Psi_2\rangle_{TA_1A_2}, \ldots, |\Psi_8\rangle_{TA_1A_2}\}$, where the subscripts T, A_1 and A_2 represent the three particles of each GHZ state. He takes particle T from each of the GHZ states to form an ordered particle sequence, called T sequence. Similarly, the remaining partner particles compose A_1 sequence and A_2 sequence. Trent performs one of the two operations $\{I, H\}$ on each particle in A_1 sequence according to Alice$_1$'s authentication key, AK_{A_1}. Here $\mathrm{AK}_{A_1} = h_{A_1}(\mathrm{ID}_{A_1}, C_{A_1})$. That is, if the ith value of AK_{A_1} is 0 (1), he performs I (H) operation on particle A_1. Trent also executes I or H operation on particle A_2 according to Alice$_2$'s authentication key, AK_{A_2}. After doing these, he sends A_1 and A_2 sequences to Alice$_1$ and Alice$_2$, respectively.

(S2) Alice$_1$ (Alice$_2$) performs I or H operation on each of her particles according to AK_{A_1} (AK_{A_2}). For example, if the ith value of AK_{A_1} is 0 (1), I (H) operation is applied to particle A_1. After doing these, they inform Trent. Trent then authenticates the users and checks eavesdropping during the transmission of A_1 and A_2 sequences.

(S3) We then describe the procedure of authentication and eavesdropping check in detail. (a) Trent selects randomly a sufficiently large subset from the ordered GHZ states. (b) He measures the sampling particles in T sequence in Z-basis or X-basis randomly. (c) Trent announces publicly the positions of the sampling particles and the measuring basis for each of the sampling particles. Alice$_1$ and Alice$_2$ measure their sampling particles in the same basis as Trent. After measurements, the users publish their measurement results. (d) Trent can authenticate the users and check the existence of eavesdropper by comparing their measurement results. If the users are legal and the channel is safe, their results should be completely correlated. For example, the initial state is $|\Psi_1\rangle$. Suppose Trent performs Z-basis measurement on particle T. If Trent's result is $|0\rangle(|1\rangle)$, the users' results must be $|00\rangle(|11\rangle)$. If Trent performs X-basis measurement on his particle and obtains the result $|+\rangle(|-\rangle)$, the users' results should be $|++\rangle$ or $|--\rangle(|+-\rangle$ or $|-+\rangle)$. Then if any user is illegal, Trent will abandon the communication. Otherwise, they will continue to the next step.

(S4) Alice$_1$ and Alice$_2$ each generate a random string, a_1 and a_2. According to their random strings, they perform one of the two unitary operations $\{I, \mathrm{i}\sigma_y\}$ on particles A_1 and A_2, separately. For example, if the ith value of Alice$_1$'s random string is 0 (1), she performs I ($i\sigma_y$) operation on particle A_1. After their operations, they return A_1 and A_2 sequences to Trent.

(S5) Trent selects randomly a sufficiently large subset from the ordered GHZ states and performs randomly one of the four unitary operations $\{I, \sigma_x, \mathrm{i}\sigma_y, \sigma_z\}$ on each of the sampling particles in T sequence. He then encodes his secret message on the remaining

particles T by performing one of the four unitary operations on each of them. Trent measures particles T, A_1 and A_2 of each GHZ state in three-particle GHZ basis. He announces publicly the positions of the sampling particles and lets each user publish the information of the random operations on the sampling particles in A_1 and A_2 sequences. According to his measurement result, Trent can check the security for the transmission of the returned particle sequences. When the initial state is $|\Psi_1\rangle$, his result is $|\Psi_8\rangle$ and his operation on particle T is σ_x, he can deduce that Alice$_1$ and Alice$_2$'s operations are each iσ_y and I. He then compares his conclusion with the operations published by the users and can evaluate the security for the transmitting particles. If he confirms that there is no eavesdropping, he publishes his measurement results and the initial GHZ states he prepared. Alice$_1$ and Alice$_2$ can then obtain Trent's secret. For example, when the initial state is $|\Psi_1\rangle$ and Trent's operation is σ_x (corresponds to his secret 01), $|\Psi_1\rangle$ is transformed into $|\Psi_8\rangle$, if Alice$_1$ and Alice$_2$ perform iσ_y and I operations on particles A_1 and A_2, respectively. That is, $\sigma_x\otimes \mathrm{i}\sigma_y\otimes I|\Psi_1\rangle = |\Psi_8\rangle$. Referring to her operation performed on particle A_1 (A_2), Trent's result $|\Psi_8\rangle$ and the initial state $|\Psi_1\rangle$, Alice$_1$ (Alice$_2$) can obtain Trent's secret message 01.

The security for the three-party QBC-DC scheme is based on the security for the procedure of authentication and eavesdropping check. Trent prepares an ordered N GHZ states, each of which is in one of the eight GHZ states, and performs I or H operation on particles A_1 and A_2 according to each user's authentication key. For each initial state, there are four possible states after Trent's operations. For example, if the initial state is $|\Psi_1\rangle$, then the four possible states are

$$\begin{aligned}
|\Omega_1\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),\\
|\Omega_2\rangle &= \frac{1}{\sqrt{2}}(|0+0\rangle + |1-1\rangle)\\
&= \frac{1}{2}[|+\rangle(|\phi^-\rangle + |\psi^+\rangle) + |-\rangle(|\phi^+\rangle - |\psi^-\rangle)],\\
|\Omega_3\rangle &= \frac{1}{\sqrt{2}}(|00+\rangle + |11-\rangle)\\
&= \frac{1}{2}[|+\rangle(|\phi^-\rangle + |\psi^+\rangle) + |-\rangle(|\phi^+\rangle + |\psi^-\rangle)],\\
|\Omega_4\rangle &= \frac{1}{\sqrt{2}}(|0++\rangle + |1--\rangle). \qquad (16)
\end{aligned}$$

Eve has no information of the user's authentication key. If Eve intercepts particles A_1 and A_2 and performs Bell basis measurement on them, she cannot obtain the information of the user's authentication key because she cannot distinguish the four states. During the process of authentication and eavesdropping check, Trent performs randomly Z-basis or X-basis measurement on his particle. When Trent performs Z-basis measurement and Eve measures the intercepted particles in the same measuring basis as Trent, if the state is not $|\Omega_1\rangle$, it is possible for her to publish a wrong result after measurements. Similarly, whether Eve utilizes Z-basis, X-basis or Bell basis measurement, she will publish a wrong result with some probability and her action will be detected by Trent during the process of authentication and eavesdropping check. We can also describe Eve's effect on the system as Eq.(14). If the initial state is $|\Psi_5\rangle$, the error rate introduced by Eve is $\epsilon = 1 - |\gamma_1|^2$.

We then generalize the three-party QBC-DC scheme to a multiparty (more than three parties) one, in which Trent broadcasts his secret to r users {Alice$_1$, Alice$_2$, ..., Alice$_r$}. He prepares an ordered N GHZ states, each of which is random in one of the $2^{(r+1)}$ $(r+1)$-particle GHZ states

$$\frac{1}{\sqrt{2}}(|ij\ldots k\rangle + |\bar{i}\bar{j}\ldots\bar{k}\rangle)_{T,A_1,\ldots,A_r}, \qquad (17)$$

where $i, j, \ldots, k \in \{0, 1\}$ and $\bar{i}, \bar{j}, \ldots, \bar{k}$ are the counterparts of $i, j, \ldots, k$. The details of the multiparty QBC-DC are very similar to those of three-party one. Trent performs I or H operation on each particle in A_1 (A_2, ..., A_r) sequence according to AK$_{A_1}$ (AK$_{A_2}$, ..., AK$_{A_r}$). He then sends A_1, A_2, ..., A_r sequences to Alice$_1$, Alice$_2$, ..., Alice$_r$, respectively. After receiving the particle sequence, each user performs I or H operation on their particles according to their respective authentication key. Similar to step (S3) in the three-party QBC-DC scheme, Trent authenticates the users and checks eavesdropping. If any user is illegal, Trent will abort the communication. Otherwise, they will continue to the next step. Alice$_1$, Alice$_2$, ..., Alice$_r$ perform randomly I or iσ_y operation on their respective particles. After doing these, they return A_1, A_2, ..., A_r sequences to Trent. Trent first chooses a sufficiently large subset to check the security for the transmitting particles and performs randomly one of the four operations on the sampling particles in T sequence. He also encodes his secret on the remaining particles in T sequence by using the four operations. Trent measures each of the $(r+1)$-particle GHZ states in the $(r+1)$-particle GHZ basis. He publishes the positions of the sampling particles and lets the users announce publicly their operations

on the sampling particles. Trent can then check the security for the transmission of the returned particle sequences. If there is no eavesdropping, he publishes his measurement results and the initial $(r+1)$-particle GHZ states he prepared. Thus Trent broadcasts his secret to Alice$_1$, Alice$_2$, ..., Alice$_r$.

4. Scheme 3: QBC based on quantum encryption

In scheme 2, Trent broadcasts his secret to a group of designated users. We then present a QBC scheme with quantum encryption, called QBC-QE scheme, in which Trent can broadcast his secret to any subset of the users. The details of the QBC-QE scheme are as follows.

(S1) Trent prepares an ordered N $(r+1)$-particle GHZ states, each of which is in the state

$$\frac{1}{\sqrt{2}}(|00\ldots0\rangle+|11\ldots1\rangle)_{T,A_1,\ldots,A_r}. \tag{18}$$

The N particles T form T sequence and the N particles A_i $(i=1,2,\ldots,r)$ form A_i sequence. Trent performs one of the two operations $\{I,\ H\}$ on the particles in A_i sequence according to Alice$_i$'s authentication key. That is, if Alice$_i$'s AK_{A_i} is 0 (1), Trent performs I (H) operation on particle A_i. Trent sends A_1, A_2, ..., A_r sequences to Alice$_1$, Alice$_2$, ..., Alice$_r$, respectively.

(S2) Alice$_i$ $(i=1,2,\ldots,r)$ performs I or H operation on each of her particles according to AK_{A_i}. Similar to the method which is used at step (S3) in QBC-DC scheme, Trent authenticates the users and checks eavesdropping by performing random Z-basis or X-basis measurement. If the users are legal and the channel is safe, they will continue to the next step. Otherwise, Trent will stop the communication.

(S3) Trent utilizes controlled-NOT (CNOT) operation to encrypt his secret message. For example, Trent wants to transmit his secret $P=\{p_1,p_2,\ldots,p_m\}$, where $p_i\in\{0,1\}$ $(i=1,2,\ldots,m)$ represents classical bit 0 or 1, to two users {Alice$_j$, Alice$_k$} $(1\le j,k\le r)$. He prepares his secret in the state $|p_ip_i\rangle_{S_jS_k}$, where S_j, S_k denote the two particles of the state. Trent performs CNOT operation on particles T, S_j and S_k (particle T is the controller and S_j and S_k are the targets). Then the GHZ state of the whole quantum system becomes

$$\begin{aligned}|\Upsilon\rangle=\frac{1}{\sqrt{2}}(&|00\ldots0,p_i,p_i\rangle\\&+|11\ldots1,1\oplus p_i,1\oplus p_i\rangle)_{T,A_1,\ldots,A_r,S_j,S_k}.\end{aligned} \tag{19}$$

According to Alice$_j$ and Alice$_k$'s authentication keys, Trent performs I or H operation on particles S_j and S_k. For example, if the ith value of Alice$_j$'s authentication key is 0 (1), he performs I (H) operation on particle S_j. Here we denote the operation performed on S_j (S_k) as $H_{\mathrm{AK}^i_{A_j}}$ $(H_{\mathrm{AK}^i_{A_k}})$, where $\mathrm{AK}^i_{A_j}$ $(\mathrm{AK}^i_{A_k})$ represents the ith value of Alice$_j$'s (Alice$_k$'s) authentication key and H_0 (H_1) represents I (H) operation. Thus $|\Upsilon\rangle$ is transformed into

$$\begin{aligned}|\Upsilon'\rangle=\frac{1}{\sqrt{2}}[&|00\ldots0,H_{\mathrm{AK}^i_{A_j}}(p_i),H_{\mathrm{AK}^i_{A_k}}(p_i)\rangle\\&+|11\ldots1,H_{\mathrm{AK}^i_{A_j}}(1\oplus p_i),\\&H_{\mathrm{AK}^i_{A_k}}(1\oplus p_i)\rangle]_{T,A_1,\ldots,A_r,S_j,S_k}.\end{aligned} \tag{20}$$

Trent then sends S_j and S_k sequences to Alice$_j$ and Alice$_k$, respectively. To ensure the security of the transmission of S_j and S_k sequences, Trent should insert randomly some sampling particles into S_j and S_k sequences before sending them to the users. Inserting the sampling particles aims to make the parties detect Eve's disturbance attack although Eve cannot obtain any information of Trent's secret message.

(S4) After receiving S_j (S_k) sequence, Alice$_j$ (Alice$_k$) first performs I or H operation on the transmitting particles according to AK_{A_j} (AK_{A_k}) and then executes CNOT operation on particles A_j (A_k) and S_j (S_k). For example, if the ith value of Alice$_j$'s authentication key is 1, she performs H operation on the corresponding particle in S_j sequence and does CNOT operation on particles A_j and S_j (A_j is the controller and S_j is the target). According to Eqs.(19) and (20), Alice$_j$ and Alice$_k$ can obtain Trent's secret message.

In the above scheme, we just give an example of sending secret to any two of the r users. Obviously, Trent can send his secret to any subset of the legal users in the scheme. Strictly speaking, the present scheme is not a genuine QBC scheme because Trent have to transmit a particle sequence to each user. In view of Trent's transmitting his secret to multi-users directly in this scheme, we still regard it as QBC. The security for authentication and eavesdropping check in the scheme is the same as that in QBC-DC scheme. After confirming the users are legal and ensuring the security of the quantum channel, Trent can regard the GHZ states as quantum key and then encrypts his secret message by using quantum key they share. If Trent wants to transmit his secret to a subset of the

users, he then performs I or H operation on the encoding particles according to each designated user's authentication key, which ensures that only the users in this subset can obtain Trent's secret. After ensuring the security for the transmitting particles, the designated users decrypt the secret by using quantum key. The procedure of encryption and decryption in our scheme is the same as quantum one-time pad, but the quantum key is the GHZ state shared by the parties. In this scheme, the quantum key can be used repeatedly for the next round of cryptographic task.

5. Discussion

In summary, we have presented three schemes for quantum broadcast communication. In our schemes, Trent broadcasts his secret message to multi-users directly and only the legal users can obtain Trent's secret. In scheme 1, based on the idea in Ref.[27], we utilize entanglement swapping to realize a QBC scheme, in which Trent sends his secret to a group of users who share a GK with Trent. In scheme 2, based on the idea in Ref.[28], we present a QBC scheme that Trent broadcasts his secret to multi-users, each of whom shares an authentication key with Trent, by using dense coding. Scheme 3 is based on quantum encryption,[30] in which Trent can broadcast his secret to any subset of the legal users.

We then analyse the advantages and disadvantages of the three schemes from the aspects of security and feasibility. All the schemes utilize random I or H operation and random Z-basis or X-basis measurement to ensure the security of authentication and eavesdropping check. In scheme 1, as long as the procedure of authentication and eavesdropping check is secure, the scheme is completely secure. However, in schemes 2 and 3, besides the procedure of eavesdropping check and authentication which is similar to scheme 1, it is necessary for the communication parties to perform the second eavesdropping check in order to prevent Eve from disturbing the transmitting particles. For example, in scheme 2, Trent should check the security of the returned particle sequences at step (S5). In scheme 3, Trent should insert some sampling particles into the transmitting particle sequences to detect Eve's disturbance attack. Thus the procedure of eavesdropping check in scheme 1 is the simplest among the three schemes. All the schemes need prepare multi-particle entangled states. In scheme 1, it is necessary for the communication parties to perform Bell basis measurement. In scheme 2, it needs GHZ basis measurement and the measurement will be more difficult along with the increase of the number of users. In scheme 3, the communication parties do not need to perform measurement and they only need to execute CNOT operation. Quantum logic operation can be realized by using linear optical elements. From the angle of feasibility, scheme 3 is more realizable than scheme 2. Due to our schemes utilizing block transmission, quantum memory is necessary. The storing of particle sequence can be resolved by using optical delays, as described in Ref.[12]. Bell basis measurement can be realized by using entanglement in additional degree of freedom[34] or atomic coherence.[35] However, the preparation of multi-particle GHZ state is apparently complicated. At present, only six-photon GHZ state can be realized in experiment.[36]

Moreover, compared with classical broadcast encryption which allows the sender to securely distribute the secret to a dynamically changing group of users, the present schemes are not genuine quantum broadcast encryption schemes. That is why we call them quantum broadcast communication schemes. We hope that our work will attract more attention and give impetus to further research on quantum broadcast communication.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore, India) (New York: IEEE) pp175–179

[2] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese)

[3] Ma H Q, Li Y L, Zhao H and Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese)

[4] Hillery M, Buzěk V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[5] Zhang Y Q, Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252

[6] Zhang Z J 2005 *Phys. Rev.* A **342** 60

[7] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[8] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301

[9] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307

[10] Beige A, Englert B G, Kurtsiefer Ch and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

[11] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[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] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[15] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301
[16] Wang J, Zhang Q and Tang C J 2006 *Int. J. Mod. Phys.* C **17** 685
[17] Wang J, Zhang Q and Tang C J 2006 *Opt. Commun.* **266** 732
[18] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256
[19] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305
[20] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[21] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 898
[22] Man Z X and Zhang Z J 2005 *Chin. Phys. Lett.* **22** 18
[23] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305
[24] Wang J, Zhang Q and Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese)
[25] Nguyen B A 2006 *Phys. Lett.* A **350** 174
[26] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761
[27] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473
[28] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 quant-ph/0601125
[29] Fiat A and Naor M 1994 *Advances in Cryptology-CRYPTO'93*, Lecture Notes in Computer Science **773** 480
[30] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **64** 024302
[31] Zukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287
[32] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[33] Wang J, Zhang Q and Tang C J 2006 *Chin. Phys. Lett.* **23** 2360
[34] Kwiat P G and Weinfurter H 1998 *Phys. Rev.* A **58** R2623
[35] Scully M O, Englert B G and Bednar C J 1999 *Phys. Rev. Lett.* **83** 4433
[36] Zhang Q, Goebel A, Wagenknecht C, Chen Y A, Zhao B, Yang T, Mair A, Schmiedmayer J and Pan J W 2006 *Nature Phys.* **2** 678