Quantum broadcast communication with authentication*

Yang Yu-Guang(杨宇光)[a)c)d)†], Wang Ye-Hong(王叶红)[a)], and Wen Qiao-Yan(温巧燕)[b)]

[a)] *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124, *China*
[b)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[c)] *State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences), Beijing* 100049, *China*
[d)] *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an* 710071, *China*

(Received 24 March 2009; revised manuscript received 21 April 2009)

Two simple quantum broadcast communication schemes are proposed. A central party can broadcast his secret message to all the legitimate receivers simultaneously. Compared with the three schemes proposed recently (Wang *et al.* 2007 *Chin. Phys.* **16** 1868), the proposed schemes have the advantages of consuming fewer quantum and classical resources, lessening the difficulty and intensity of necessary operations, and having higher efficiency.

Keywords: quantum broadcast communication, authentication, quantum secure direct communication

PACC: 0367

1. Introduction

Entanglement is one of the most intriguing properties of quantum physics and a kind of very useful resource which plays a very important role in quantum information processing. By using entanglement, many cryptographic tasks can be securely completed, such as quantum key distribution (QKD),[1,2] quantum secret sharing (QSS),[3,4] quantum secure direct communication (QSDC).[5−16] The QKD protocols are used to share a key between two distant parties while the QSDC protocols are used to transmit a secret message directly without creating a key to encrypt it beforehand. The QSS is the generalization of classical secret sharing to quantum scenario and can share both classical and quantum messages among sharers.

The existing models of QSDC protocols are mainly divided into several types: point-to-point one-way QSDC,[5−9] point-to-point two-way QSDC,[10] multi-point-to-point one-way QSDC,[11,12] point-to-multi-point one-way QSDC,[13,14] and multi-point-to-multi-point two-way QSDC.[15,16] For example, Bostroem and Felbinger[5] put forward a ping-pong QSDC scheme by using Einstein–Podolsky–Rosen (EPR) pairs and Deng *et al.*[6] proposed a QSDC scheme based on EPR pairs. In essence, the protocols in Refs. [5] and [6] belong to the point-to-point one-way communication. Based on the idea of the ping-pong QSDC scheme, Nguyen[10] proposed a quantum dialogue scheme (belonging to point-to point two-way communication) by using EPR pairs. More recently, Gao *et al.*[11] presented a simultaneous QSDC scheme between the central party and many other parties based on entanglement swapping. The scheme shows how the many parties transmit their secret messages to one party. Deng *et al.*[12] presented a multiparty quantum secret report scheme based on quantum encryption. The broadcast encryption allows the sender to securely distribute his/her secret to a dynamically changing group of receivers over a broadcast channel. Wang *et al.*[13] proposed three quantum broadcast communication(QBC) schemes based on entanglement swapping, dense coding and quantum encryption, separately. Man and Xia[14] proposed a novel multiparty QSDC protocol where a sender could simultaneously transmit different messages to N receivers in a secure manner, which is different from the scheme suggested in Ref. [13]. In 2006, Jin *et al.*[15] in-

*Project supported by the National Basic Research Program of China (Grant No. 2007CB311100), the National Natural Science Foundation of China (Grant Nos. 60873191 and 60821001), the National High-Tech Research, Development Plan of China (Grant Nos. 2006AA01Z440, 2009AA012441 and 2009AA012437), the Scientific Research Common Program of Beijing Municipal Commission of Education, China (Grant No. KM200810005004), Beijing Natural Science Foundation (Grant Nos. 1093015 and 1102004), the State Key Laboratory of Integrated Services Network (ISN) open Foundation, China (Grant No. ISN-9-10), and the Specialized Research Fund for the Doctoral Program of Higher Education, China (Grant No. 20091103120014).
†Corresponding author. E-mail: yangyang7357@bjut.edu.cn
© 2010 Chinese Physical Society and IOP Publishing Ltd

troduced a three-party simultaneous QSDC scheme by using Greenberger–Horne–Zeilinger (GHZ) states and further generalized it to the N-party case by using N-particle GHZ states, in which any legitimate party can obtain the secret messages of the other parties. Li *et al.*[16] presented two schemes for multiparty quantum remote secret conference in which each legitimate conferee can read out securely the secret message announced by another.

In the present paper, we present two simple QBC protocols with authentication based on GHZ states. The first QBC protocol combines the idea in Ref. [17] with that in Ref. [18]. And the second one in fact combines the idea in Ref. [17] with that in Ref. [14]. We suppose a central party, Trent, wishes to broadcast his secret message $\{s_m\}$ to all the r legitimate receivers. So he need authenticate the r legal receivers, Alice_1, Alice_2, ..., Alice_r before he sends the secret message. In a way similar to that in Refs. [13] and [17], 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 receiver. Here the hash function is defined as

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

where l, m and n denote the length of the identity number, the length of a counter and the length of the authentication key, respectively. Thus the receiver's authentication key can be expressed as $\text{AK} = h(\text{ID}, C)$, where with C being the counter of calls on the receiver's hash function. When the length of the authentication key is not enough to satisfy the requirement for a 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 as $\text{AK}_{A_1} = h_{A_1}(\text{ID}_{A_1}, C_{A_1})$, $\text{AK}_{A_2} = h_{A_2}(\text{ID}_{A_2}, C_{A_2})$, ..., $\text{AK}_{A_r} = h_{A_r}(\text{ID}_{A_r}, C_{A_r})$, respectively.

2. Description of QBC schemes

The first QBC protocol combines the idea in Ref. [17] with that in Ref. [18]. Now we describe this QBC scheme. We consider only the ideal condition, that is, there is neither noise nor loss in the quantum channel. Each receiver shares an authentication key with Trent, as we have described above.

(S1) Trent generates a sequence of ordered identical N $(r+1)$-partite GHZ-state quantum systems in the form

$$|\Phi_m\rangle = \frac{1}{\sqrt{2}}(|000\ldots0\rangle + |111\ldots1\rangle)_{T_m A_{1m} \ldots A_{rm}}, \tag{2}$$

where m represents the state order in the sequence and the subscripts $T_m, A_{1m}, \ldots, A_{rm}$ represent the $r+1$ particles of the mth GHZ state. Trent takes particles $T_m, A_{1m}, \ldots, A_{rm}$ from each state to form an ordered particle sequence, called $T(A_1, \ldots, A_r)$ sequence. For each GHZ state, Trent performs I or H operation on particles $T_m, A_{1m}, \ldots, A_{rm}$ according to Alices' authentication keys. Here

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

If the ith value of AK_{A_1} is 0(1), then Trent performs $I(H)$ operation on the ith particle of sequence. The similar conclusions for other sequences can be obtained. Then he keeps T sequence and sends $A_1, \ldots, A_r$ sequences to Alice_1, Alice_2, ..., Alice_r, respectively.

(S2) After receiving $A_1, \ldots, A_r$ sequences, Alice_1, Alice_2, ..., Alice_r perform corresponding I or H operation on the received sequences according to their respective authentication keys. For example, if the ith value of AK_{A_1} is 0(1), then Alice_1 performs $I(H)$ operation on the ith particle of A_1 sequence. The similar conclusions for other Alices can be obtained. Trent then authenticates the receivers and checks eavesdropping during the transmission of A_1, ..., A_r sequences.

(S3) The procedure of authentication and eavesdropping check is as follows. (a) Trent selects at random a subset $\{|\Phi_l\rangle\}$ out of the shared $\{|\Phi_m\rangle\}$-states, measures his particle randomly in Z-basis or in the X-basis

$$\{(|+\rangle, |-\rangle || \pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\}$$

and then publishes the positions and the measuring bases (MBs) of the sampling particles. (b) Alices measure their qubits in the same basis as Trent. $\forall 1 \le i \le r$, Alice_i's outcome in Z-basis is $j^z_{A_{il}} = \{0, 1\}$ corresponding to finding $\{|0\rangle, |1\rangle\}$ and that in X-basis is $j^x_{A_{il}} = \{+1, -1\}$ corresponding to finding $\{|+\rangle, |-\rangle\}$. (c) Trent requires each Alice to publish the outcomes of his measurement and makes an analysis. For those measurements in Z-basis he compares $j^z_{T_l}$ with $j^z_{A_{il}}$: if $j^z_{T_l} = j^z_{A_{il}}$ for $1 \le i \le r$, it is all-right, otherwise he judges a possible attack of an outside eavesdropper in the quantum channel. As for measurements in X-basis he compares $j^x_{T_l}$ with $J^x_l = \prod_{i=1}^{r} j^x_{A_{il}}$: if $j^x_{T_l} = J^x_l$ for $1 \le i \le r$, it is all-right, otherwise there is an outside eavesdropper in the quantum channel. If the error rate is lower than a predetermined small value, they continue on the next broadcast communication.

(S4) For a given m, Trent measures her qubit T_m in Z-basis with the result $j^z_{T_m} = \{0, 1\}$ and then asks Alices to do so with their qubits A_{im} with the same outcome $j^z_{A_{im}} = \{0, 1\}$.

(S5) Trent publicly broadcasts the value $x_m = s_m \oplus j^z_{T_m}$, where $\oplus$ denotes an addition modulo 2.

(S6) Each Alice decodes Trent's secret message as $s_m = x_m \oplus j^z_{A_{im}}$ because $j^z_{A_{im}}$ is dynamically equal to $j^z_{T_m}$.

The second QBC protocol combines the idea in Ref. [17] with that in Ref. [14]. We consider also only the ideal condition, that is, there is neither noise nor loss in the quantum channel. Each receiver shares an authentication key with Trent, as we have described above.

(S'1) Trent generates a sequence of ordered N $(r+1)$-partite GHZ-state quantum systems, each of which is in the form

$$|\Phi_m\rangle = \frac{1}{\sqrt{2}}(|0 s_m s_m \ldots s_m\rangle + |1\overline{s_m}\,\overline{s_m}\ldots\overline{s_m}\rangle)_{T_m A_{1m}\ldots A_{rm}}, \quad (3)$$

where s_m =0 or 1, $\overline{s_m} = s_m \oplus 1$, with $\oplus$ denoting the addition modulo 2. Trent takes particles $T_m, A_{1m}, \ldots, A_{rm}$ from each state to form an ordered particle sequence, called $T(A_1, \ldots, A_r)$ sequence. For each GHZ state, Trent performs I or H operation on particles $A_1, \ldots, A_r$ according to Alices' authentication keys. Afterwards, before Trent sends the sequences to Alice, she inserts a certain number of single qubits into each sequence at random positions. All these single qubits are randomly in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, which can be used to check eavesdropping. Then he keeps T sequence and sends $A_1, \ldots, A_r$ sequences to $\mathrm{Alice}_1, \ldots, \mathrm{Alice}_r$, respectively.

(S'2) The procedure of authentication and eavesdropping check is as follows. (a) After hearing from the Alices, Trent first publishes the positions and the MBs of the sampling particles. (b) The Alices measure the sampling particles in the received sequence in the same MBs and then publish their measurement results. (c) Trent can then check eavesdropping by comparing the Alices's measurement results with the initial states of the sampling particles. If the error rate is lower than a predetermined small value, Trent confirms that no eavesdropper exists and announces this fact. If the Alices confirm that there is no eavesdropping, they continue to execute the next step. Otherwise, they abort the communication.

(S'3) $\mathrm{Alice}_1, \ldots, \mathrm{Alice}_r$ perform corresponding I or H operation on the received sequences according to their respective authentication keys respectively.

(S'4) For a given m, Trent measures her qubit T_m in Z-basis with the result $j^z_{T_m} = \{0, 1\}$ and then asks the Alices to do so with their qubits A_{im}. If $j^z_{T_m} = 0$, then the Alices' measurement outcomes $j^z_{A_{im}}$ are equal to s_m. Otherwise $s_m = j^z_{A_{im}} \oplus 1$.

3. Security analysis

Now we come to discuss the security for the two QBC protocols. To gain useful information (i.e. the broadcast secret) in the protocol, an eavesdropper Eve must attack the quantum channel during the transmission of quantum signals. The security of our scheme completely depends on whether the procedures of both the authentication and the eavesdropping check are secure. If it is secure, Trent and the r legitimate parties can securely share the quantum channel and the r legitimate parties can obtain the broadcast secret. In fact, without the authentication key, the attack from the eavesdropper will be found. The security analysis is similar to that in Ref. [13]. We demonstrate the procedures of authentication and eavesdropping check in the first QBC protocol with two receivers first.

At step (S1), Trent performs I or H operation on particles A_1 and A_2 according to the Alices authentication keys. The three-particle GHZ state becomes one of the following states:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|\varphi^+\rangle + |-\rangle|\varphi^-\rangle)$$
$$= \frac{1}{2}(|+\rangle|+\rangle|+\rangle + |+\rangle|-\rangle|-\rangle + |-\rangle|+\rangle|-\rangle + |-\rangle|-\rangle|+\rangle), \quad (4)$$
$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|0++\rangle + |1--\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|\varphi^+\rangle + |-\rangle|\psi^+\rangle)$$
$$= \frac{1}{2}(|+\rangle|+\rangle|+\rangle + |+\rangle|-\rangle|-\rangle + |-\rangle|+\rangle|+\rangle - |-\rangle|-\rangle|-\rangle), \quad (5)$$

$$|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|00+\rangle + |11-\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|\varphi^-\rangle + |+\rangle|\psi^+\rangle + |-\rangle|\psi^-\rangle + |-\rangle|\varphi^+\rangle)$$
$$= \frac{1}{2}\begin{pmatrix} |+\rangle|+\rangle|+\rangle + |+\rangle|-\rangle|+\rangle + |-\rangle|+\rangle|+\rangle + |-\rangle|-\rangle|+\rangle \\ +|+\rangle|+\rangle|-\rangle - |+\rangle|-\rangle|-\rangle - |-\rangle|+\rangle|-\rangle + |-\rangle|-\rangle|-\rangle \end{pmatrix}, \quad (6)$$

$$|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|0+0\rangle + |1-1\rangle) = \frac{1}{\sqrt{2}}\left(|+\rangle|\varphi^-\rangle + |+\rangle|\psi^+\rangle - |-\rangle|\psi^-\rangle + |-\rangle|\varphi^+\rangle\right)$$
$$= \frac{1}{2}\begin{pmatrix} |+\rangle|+\rangle|+\rangle + |+\rangle|+\rangle|-\rangle + |-\rangle|+\rangle|+\rangle + |-\rangle|+\rangle|-\rangle \\ +|+\rangle|-\rangle|+\rangle - |+\rangle|-\rangle|-\rangle - |-\rangle|-\rangle|+\rangle + |-\rangle|-\rangle|-\rangle \end{pmatrix}, \quad (7)$$

where

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$|\varphi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (8)$$

According to expressions (4)–(7), Eve cannot obtain the information about the receiver's authentication key because he cannot distinguish the four states by using Bell basis measurement. In the processes of authentication and eavesdropping check, Trent measures his sampling particles in Z-basis or X-basis randomly and allows the receivers to measure their corresponding particles in the same MBs. 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 $|\Psi_1\rangle$, Eve will not introduce any error in the processes of authentication and eavesdropping check. However, if the state is $|\Psi_2\rangle$ or $|\Psi_3\rangle$ or $|\Psi_4\rangle$, it is possible for her to publish a wrong result after measurements. Similarly, when Eve utilizes X-basis or Bell basis measurement, she will publish a wrong result with some probability and her action will be detected by Trent in the processes of authentication and eavesdropping check.

In addition, because our protocol is based on Ref. [18], it can also resist several common types of attacks such as measure-resend, disturbance, entangle-measure and intercept-resend attacks which were discussed in Ref. [18]. According to the above analysis, all in all, the first QBC scheme is secure against any outsider's eavesdropping.

Now we discuss the security of the second QBC protocol. Gao *et al.*[19] pointed out that Ref. [14] was vulnerable to the double-CNOT-operation attack which is a special attack on the transmission of GHZ states. However, this attack is invalid in the second QBC scheme because 1) I or H operation has been performed on every qubit A_{im} according to every Alice's authentication key before they are sent to the Alices via the quantum channel; 2) the secret sent to the Alices is the same, no different. When Eve does the double-CNOT operation to eavesdrop, the states of these additional checking qubits will be disturbed by her intervention. For example, if such an operation is performed on two checking qubits $|+\rangle_1$ and $|+\rangle_2$, the composite system of the checking qubits and the ancilla is initially in the state

$$|\Delta^1\rangle_{12e} = |+\rangle|+\rangle|0\rangle$$
$$= \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle). \quad (9)$$

When the first CNOT operation C_{1e} is performed, this state changes into

$$|\Delta^2\rangle_{12e} = \frac{1}{2}(|000\rangle + |010\rangle + |101\rangle + |111\rangle). \quad (10)$$

Then the second CNOT operation C_{2e} is done and the state becomes

$$|\Delta^3\rangle_{12e} = \frac{1}{2}\left[(|00\rangle + |11\rangle)|0\rangle + (|01\rangle + |10\rangle)|1\rangle\right]. \quad (11)$$

When Eve measures the ancilla in Z-basis, the checking qubits will be projected onto $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ randomly, which obviously introduces disturbance to qubits 1 and 2. Therefore, this attack strategy would be detected by Trent and it follows that our second QBC protocol is secure against the special attack.

According to the above analysis, all in all, the present schemes are secure against any outsider's eavesdropping.

4. Comparison with Ref. [13]

Now, we make some simple comparisons between our schemes (named Y1 and Y2 schemes respectively) and the three schemes (named W1, W2, W3 schemes respectively) in Ref. [13] and see the advantages of our protocols from the following four aspects: the cost of quantum resource, the difficulty or intensity of necessary operations, the cost of classical resource and the total efficiency. From these four aspects we summarize the five schemes in Table 1. The total efficiency is defined as

$$\eta = \frac{b_{\rm s}}{q_{\rm u} + b_{\rm t}}, \tag{12}$$

where $b_{\rm s}$ is the number of classical bits that consist of the classical information to be broadcast, $q_{\rm u}$ is the number of the qubits which is used as the quantum channel (except for those chosen for eavesdropping check) and $b_{\rm t}$ is the classical bits exchanged.

Table 1. Comparisons between our two schemes and W1,W2 and W3 schemes in Ref. [13]. QR: quantum resource. NO: necessary operation. CR: classical resource. SQ: single qubit. SQM: single-qubit measurement. SQUO: single-qubit unitary operation. TQUO: two-qubit unitary operation. BSM: Bell state measurement. GHZM: GHZ state measurement. For simplicity and clarity, we list the values of QR, NO, CR and η given that a classical secret bit has been received by Alices. See the text for further details.

Scheme	QR	NO	CR	η
W1 scheme	2 GHZ states	6 SQUOs, 3BSMs	8cbits	1/7
W2 scheme	1 GHZ state	3 SQUOs, 1GHZM	6cbits	2/9
W3 scheme	1 GHZ state, 2SQs	4TQUOs	0cbit	1/5
Y1 scheme	1 GHZ state	3 SQMs	1 cbit	1/4
Y2 scheme	1 GHZ state	3 SQMs	1 cbit	1/4

From Table 1, obviously, one can very easily find that our schemes have the remarkable advantages of consuming fewer quantum and classical resources, lessening the difficulty and intensity of necessary operations, and possessing higher efficiency. Therefore, our scheme is optimal for implementing multi-receiver broadcast communication simultaneously.

5. Conclusion

We propose two efficient and economical QBC protocols based on GHZ states, where the classical and the quantum resource consumptions, the operation complexity and the scheme efficiency are optimized. We analyse the scheme security and consequently confirmed it. A comparison shows that our schemes are obviously better than those in Ref. [13]. Hence, our schemes are optimal.

References

[1] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[2] Bennet C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[3] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[4] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[5] Bostroem K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[6] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[7] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359
[8] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[9] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[10] Nguyen B A 2004 *Phys. Lett.* A **328** 6
[11] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473
[12] Deng F G, Li X H, Li C Y, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1676
[13] Wang J, Zhang Q and Tang C J 2007 *Chin. Phys.* **16** 1868
[14] Man Z X and Xia Y J 2006 *Chin. Phys. Lett.* **23** 1973
[15] Jin X R, Zhang Y Q, Zhang S, Hong S K and Yeon K H 2006 *Phys. Lett.* A **354** 67
[16] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 23
[17] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305
[18] Nguyen B A 2006 *Phys. Lett.* A **350** 174
[19] Gao F, Lin S, Wen Q Y and Zhu F C 2008 *Chin. Phys. Lett.* **25** 1561