Vol 18 No 8, August 2009
1674-1056/2009/18(08)/3233-05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Economical multiparty simultaneous quantum identity authentication based on Greenberger–Horne–Zeilinger states*

Yang Yu-Guang(杨宇光)[a)c)d)] 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)] *National Mobile Communications Research Laboratory, Southeast University, Nanjing* 210096, *China*
[d)] *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an* 710071, *China*

(Received 4 September 2008; revised manuscript received 18 December 2008)

A multiparty simultaneous quantum identity authentication protocol based on Greenberger–Horne–Zeilinger (GHZ) states is proposed. The multi-user can be authenticated by a trusted third party (TTP) simultaneously. Compared with the scheme proposed recently (Wang *et al* 2006 *Chin. Phys. Lett.* **23**(9) 2360), the proposed scheme has the advantages of consuming fewer quantum and classical resources and lessening the difficulty and intensity of necessary operations.

Keywords: quantum identity authentication, multiparty simultaneous quantum identity authentication, Greenberger–Horne–Zeilinger state

PACC: 0367

1. Introduction

One of the most mature branches of quantum information science is quantum cryptography[1], which provides an unconditional method of secure communication. Warranted by the fundamentals of quantum mechanics, quantum cryptography has received a lot of attention. A good many quantum communication schemes have been proposed, such as quantum key distribution (QKD),[2−4] quantum secret sharing (QSS),[5−7] quantum secure direct communication (QSDC)[8−13] and quantum identity authentication (QIA).[14−18] QKD's goal is to provide a secure way of exchanging a private key. QSS is the generalization of classical secret sharing to the quantum scenario and can share both classical and quantum messages among sharers. Unlike QKD, whose goal is to generate a common key between parties, QSDC's goal is to transmit the secret messages directly without first establishing a random key to encrypt them. The object of QIA is to authenticate the parties of communication in a quantum way.

Most QIA schemes involve only point-to-point authentication, i.e., authentication between two parties. DuŠek *et al*[14] proposed a hybrid QIA system by combining QKD with classical authentication. Using one qubit as the authentication key, Curty and Santos[15] proposed a QIA protocol for binary classical messages in a secure manner. There have been a lot of papers devoted to this topic (see, e.g., Ref.[16] and the references therein).

In 2006, Wang *et al*[17] proposed a multiparty simultaneous QIA protocol based on entanglement swapping. In their scheme, all the users can be authenticated by a trusted third party (TTP) simultaneously with entanglement swapping. We call this model the multiparty simultaneous quantum identity authentication (MSQIA). We proposed an MSQIA protocol with single photons which utilizes the secret shares as their authentication keys obtained by the

*Project supported by the National High-Tech Research, Development Plan of China (Grant Nos 2006AA01Z440, 2009AA012441 and 2009AA012437) and National Basic Research Program of China (973 Program) (Grant No 2007CB311100), the National Natural Science Foundation of China (Grant Nos 60873191 and 60821001), the Scientific Research Common Program of Beijing Municipal Commission of Education (Grant No KM200810005004), Beijing Natural Science Foundation (Grant No 1093015), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, the ISN Open Foundation, and Science and Technology Program of Beijing (Grant No Z07000100720706).

users by performing secret sharing protocols.[18]

In this paper, we will present an MSQIA protocol based on GHZ states, which combines the idea in Ref.[19] with that in Ref.[20]. Similar to Refs.[17] and [19], we suppose that a TTP, Trent, authenticates r legal users, Alice_1, Alice_2, ..., Alice_r simultaneously. 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. 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 user's authentication key can be expressed as $AK = h(\text{ID}, C)$, where C is the counter of calls on the user's hash function. When the length of the authentication key is not enough to satisfy the requirement of 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 $AK_{A_1} = h_{A_1}(\text{ID}_{A_1}, C_{A_1}), AK_{A_2} = h_{A_2}(\text{ID}_{A_2}, C_{A_2}), \ldots, AK_{A_r} = h_{A_r}(\text{ID}_{A_r}, C_{A_r})$ respectively. Zhang *et al*[21] pointed out that the two protocols in Ref.[19] are insecure because they cannot prevent the authenticator from knowing the secret message. Similar to Ref.[17], we only utilize the definition of the authentication key in Ref.[19], and the messages exchanged between Trent and the users are their shared authentication information. Such problems do not exist in our protocol.

2. Our scheme

Let us describe this MSQIA scheme. We consider only the ideal condition: there are no noise and losses in the quantum channel. Each user shares an authentication key with Trent, as we have described above.

All the $(r+1)$-particle GHZ states can be described by[22]

$$|G_{\underbrace{j\ldots k}_{r}+}\rangle = \frac{1}{\sqrt{2}}\left(|0\underbrace{j\ldots k}_{r}\rangle + |1\underbrace{(j\oplus 1)\ldots(k\oplus 1)}_{r}\rangle\right)_{TA_1A_2\ldots A_r},$$
$$|G_{\underbrace{j\ldots k}_{r}-}\rangle = \frac{1}{\sqrt{2}}\left(|0\underbrace{j\ldots k}_{r}\rangle - |1\underbrace{(j\oplus 1)\ldots(k\oplus 1)}_{r}\rangle\right)_{TA_1A_2\ldots A_r}, \tag{2}$$

where $j, k \in \{0,1\}$, $\oplus$ denotes addition modulo 2, $|0\rangle$ and $|1\rangle$ are the two eigenstates of the Z-basis.

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

$$|\Phi_m\rangle = \frac{1}{\sqrt{2}}\left(|0\underbrace{s_{A_{1m}}s_{A_{2m}}\ldots s_{A_{rm}}}_{r}\rangle + |1\underbrace{(s_{A_{1m}}\oplus 1)(s_{A_{2m}}\oplus 1)\ldots(s_{A_{rm}}\oplus 1)}_{r}\rangle\right)_{T_mA_{1m}A_{2m}\ldots A_{rm}}, \tag{3}$$

where m represents the state order in the sequence and the subscripts $T_m, A_{1m}, A_{2m}, \ldots, A_{rm}$ represent the $r+1$ particles of the m-th GHZ state. Trent takes particle $T(A_1, A_2, \ldots, A_r)$ for each state to form an ordered particle sequence, called $T(A_1, A_2, \ldots, A_r)$ sequence. And for each i and m, the value of $s_{A_{im}}$ chosen at random between 0 and 1 is known only to Trent but by no means to any other person including the Alices. Before Trent sends the sequences to the Alices, he inserts a certain number of decoy photons into each sequence at random positions. All these single photons are randomly in one of the states $\{|+\rangle, |-\rangle\}$ $(|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$, which can be used to check eavesdropping. Afterwards, he keeps the T sequence and sends $A_1, A_2, \ldots, A_r$ sequences to Alice_1, Alice_2, ..., Alice_r, respectively.

(Step 2) To ensure the security of the quantum channel, the parties check eavesdropping as follows: (a) After hearing from the Alices, Trent publishes the positions of the decoy photons. (b) the Alices measure the decoy photons in the received sequence in the X-basis $\{|+\rangle, |-\rangle\}$ and then publish their measurement results. (c) Trent can then check eavesdropping by comparing the Alices' measurement results and the

initial states of the decoy photons. If the channel is safe, their results must be completely consistent. (d) If Trent confirms that no eavesdropper exists, he announces this fact. If the Alices confirm that there is no eavesdropping, they continue to execute the next step. Otherwise, they abort the communication.

(Step 3) For a given m, Trent measures her qubit T_m in Z-basis with the result $j^Z_{T_m} = \{0, 1\}$ then asks the Alices to do so with their qubits A_{im} with the outcome $j^Z_{A_{im}} = \{0, 1\}$.

(Step 4) Each Alice$_i$ publicly broadcasts the value $y_{A_{im}} = a_{A_{im}} \oplus j^Z_{A_{im}}$, where $a_{A_{im}}$ is the m-th value of AK_{A_i}.

(Step 5) Trent decodes the authentication information of Alice$_i$ as $a_{A_{im}} = y_{A_{im}} \oplus [\delta_{0,s_{A_{im}}} j^Z_{T_m} + \delta_{1,s_{A_{im}}}(j^Z_{T_m} \oplus 1)]$. If the decoded authentication information of Alice$_i$ is equal to AK_{A_i} for $1 \le i \le r$, Trent can authenticate the Alices.

3. Security analysis

Now let us discuss the security for the present protocol. To gain useful information (i.e. the authentication information of the Alices) in the protocol, an eavesdropper (an outside eavesdropper or a dishonest user) must attack the quantum channel during the transmission of quantum signals. As pointed out in Refs.[23]–[25], a participant generally has more opportunity to make an attack than an outside eavesdropper in the QSS protocols. If a QSS protocol is secure for a dishonest participant, it is secure for any eavesdropper. So the participant attack has received more attention in the security analysis of a QSS protocol. In fact, the same is also the case in the present MSQIA protocol. In our protocol, to check eavesdropping, the TTP does not use the correlation property between the measurement results on the GHZ states, but adopts the decoy photon technique.[26] The reasons are as follows. If only the correlation property of GHZ states is used in the security check, the protocol cannot resist the double-CNOT (controlled-NOT)-operation attack which was described in Ref.[27]. The process of the double-CNOT attack is as follows:

Suppose the dishonest user is Alice$_i$. Alice$_i$ prepares an ancilla $|0\rangle_e$. The GHZ state and the ancilla compose a composite system

$$\begin{aligned} &\left|\Pi^1\right\rangle_{T_m A_{1m} A_{2m} \ldots A_{rm} e} \\ &= |\Phi_m\rangle_{T_m A_{1m} A_{2m} \ldots A_{rm}} |0\rangle_e \\ &= \frac{1}{\sqrt{2}} \left(|0 s_{A_{1m}} s_{A_{2m}} \ldots s_{A_{rm}}\rangle + |1(s_{A_{1m}} \oplus 1)(s_{A_{2m}} \oplus 1) \ldots (s_{A_{rm}} \oplus 1)\rangle\right)_{T_m A_{1m} A_{2m} \ldots A_{rm}} |0\rangle_e , \end{aligned} \tag{4}$$

where the subscript e represents the ancilla. Second, if Alice$_i$ wants to eavesdrop the information about Alice$_j$'s authentication key, she executes a CNOT operation $C_{A_j e}$ (the first subscript A_j denotes the control qubit and the second one e denotes the target qubit) on the qubit Aj sent to Alice$_j$ by the TTP and the ancilla, the state of the system changes into

$$\begin{aligned} &\left|\Pi^2\right\rangle_{T_m A_{1m} A_{2m} \ldots A_{rm} e} \\ &= \frac{1}{\sqrt{2}} \left(|0 s_{A_{1m}} s_{A_{2m}} \ldots s_{A_{rm}}\rangle \left|s_{A_{jm}}\right\rangle_e + |1(s_{A_{1m}} \oplus 1)(s_{A_{2m}} \oplus 1) \ldots (s_{A_{rm}} \oplus 1)\rangle \left|s_{A_{jm}} \oplus 1\right\rangle_e\right) , \end{aligned} \tag{5}$$

Third, Alice$_i$ performs another CNOT operation $C_{A_i e}$ on the qubit A_i sent to her and the ancilla; she will obtain

$$\begin{aligned} &\left|\Pi^3\right\rangle_{T_m A_{1m} A_{2m} \ldots A_{rm} e} \\ &= \frac{1}{\sqrt{2}} \left(|0 s_{A_{1m}} s_{A_{2m}} \ldots s_{A_{rm}}\rangle + |1(s_{A_{1m}} \oplus 1)(s_{A_{2m}} \oplus 1) \ldots (s_{A_{rm}} \oplus 1)\rangle\right) \left|s_{A_{jm}} \oplus s_{A_{im}}\right\rangle_e , \end{aligned} \tag{6}$$

It can be seen that the ancilla is disentangled from the multipartite entangled state, and more importantly, the original state $|\Phi_m\rangle_{T_m A_{1m} A_{2m} \ldots A_{rm}}$ is left alone. Lastly, Alice$_i$ measures the ancilla in the Z-basis and she will obtain $s_{A_{jm}} \oplus s_{A_{im}}$ definitely.

When all Alices publicly broadcast the value y_{A_m} in step 4, Alice$_i$ can deduce the authentication key $a_{A_{jm}}$ according to her authentication key $a_{A_{im}}$ and the value of $s_{A_{jm}} \oplus s_{A_{im}}$. That is, from the equations

$$y_{A_{im}} = a_{A_{im}} \oplus j^Z_{A_{im}} = a_{A_{im}} \oplus [\delta_{0,s_{A_{im}}} j^Z_{T_m} + \delta_{1,s_{A_{im}}}(j^Z_{T_m} \oplus 1)], \tag{7}$$

and

$$y_{A_{jm}} = a_{A_{jm}} \oplus j^Z_{A_{jm}} = a_{A_{jm}} \oplus [\delta_{0,s_{A_{jm}}} j^Z_{T_m} + \delta_{1,s_{A_{jm}}} (j^Z_{T_m} \oplus 1)], \tag{8}$$

Alice$_i$ can obtain

$$y_{A_{im}} \oplus y_{A_{jm}} = a_{A_{im}} \oplus a_{A_{jm}} \oplus \left[\delta_{0,s_{A_{im}}} j^Z_{T_m} + \delta_{1,s_{A_{im}}} (j^Z_{T_m} \oplus 1)\right] \oplus \left[\delta_{0,s_{A_{jm}}} j^Z_{T_m} + \delta_{1,s_{A_{jm}}} (j^Z_{T_m} \oplus 1)\right]. \tag{9}$$

Case 1: $s_{A_{jm}} \oplus s_{A_{im}} = 0$, that is, $s_{A_{jm}} = 0$ and $s_{A_{im}} = 0$ or $s_{A_{jm}} = 1$ and $s_{A_{im}} = 1$. Alice$_i$ can obtain

$$y_{A_{im}} \oplus y_{A_{jm}} = a_{A_{im}} \oplus a_{A_{jm}}, \tag{10}$$

and

$$a_{A_{jm}} = y_{A_{im}} \oplus y_{A_{jm}} \oplus a_{A_{im}}. \tag{11}$$

Case 2: $s_{A_{jm}} \oplus s_{A_{im}} = 1$, that is, $s_{A_{jm}} = 0$ and $s_{A_{im}} = 1$ or $s_{A_{jm}} = 1$ and $s_{A_{im}} = 0$. Alice$_i$ can obtain

$$y_{A_{im}} \oplus y_{A_{jm}} = a_{A_{im}} \oplus a_{A_{jm}} \oplus 1, \tag{12}$$

and

$$a_{A_{jm}} = y_{A_{im}} \oplus y_{A_{jm}} \oplus a_{A_{im}} \oplus 1. \tag{13}$$

So Alice$_i$ can obtain Alice$_j$'s authentication key $a_{A_{jm}}$ without introducing any error.

To resist this attack, the present protocol uses the decoy photon technique to detect eavesdropping by inserting single qubits randomly in states $\{|+\rangle, |-\rangle\}$ into each sequence sent to the Alices so that the eavesdropper's double-CNOT-operation attack will introduce errors in the results. If no such attack is detected, Trent and the Alices can obtain a secure quantum channel. The detailed process of detecting eavesdropping was discussed in Ref.[28]. And the process of checking for eavesdropping with decoy photons between TTP and each user does not require the other users to participate. It will also prevent a dishonest user from eavesdropping the quantum channel from TTP to the other users with an opaque attack strategy,[29] especially when the transmission efficiency is lower than 50%. In addition, our protocol can resist several common types of attack such as measure–resend, disturbance, entangle–measure and intercept–resend attack. In a word, our scheme is secure.

4. Comparison with Ref.[17]

Now, let us make a comparison with the protocol in Ref.[17] and see the advantages of our protocol. First, let us compare the quantum resource consumption. Let us denote the quantum resource by QR, Trent's (Alices') necessary operation by NO$_T$(NO$_A$), single-qubit measurement by SQM, single-qubit unitary operation by SQUO and Bell state measurement by BSM. Then, in our protocol, QR = 1 $(r+1)$-qubit GHZ state (negligible for the decoy photons for the eavesdropping check), NO$_T$ = 1 SQM and NO$_A$ = r SQMs. As for Ref.[17] QR = 2 $(r+1)$-qubit GHZ states, NO$_T$ = 1 SQUO and NO$_A$ = r SQUOs+ r BSMs. Obviously, one can very easily find that our scheme has the remarkable advantages of consuming fewer quantum and classical resources and lessening the difficulty and complexity of the necessary operations. Therefore, our scheme is optimal for implementing multi-user authentication simultaneously.

5. Conclusion

In summary, we have proposed an efficient and economical MSQIA protocol based on GHZ states, where the classical and quantum resource consumption, the measurement and unitary operation complexity and the scheme efficiency are optimized. We have analysed the scheme security and consequently confirmed it. By comparison, we have revealed the distinct advantages of our scheme in contrast to Ref.[17].

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C H and Brassard G 1984 in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York), p175

[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

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

[6] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[7] Yang Y G and Wen Q Y 2008 *Chin. Phys.* B **17** 0419

[8] Yan F L and Zhang X 2004 *Eur. Phys. J.* B **41** 75

[9] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18

[10] Xia Y and Song H S 2007 *Phys. Lett.* A **364** 117

[11] Xia Y, Song J and Song H S 2008 *Commun. Theor. Phys.* **49** 919

[12] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149

[13] Song J, Zhu A D and Zhang S 2007 *Chin. Phys.* **16** 621

[14] Dušek M, Haderka O, Hendrych M and Myška R 1999 *Phys. Rev.* A **60** 149

[15] Curty M and Santos D J 2001 *Phys. Rev.* A **64** 062309

[16] Zhang Z S, Zeng G H, Zhou N R and Xiong J 2006 *Phys. Lett.* A **356** 199

[17] Wang J, Zhang Q and Tang C J 2006 *Chin. Phys. Lett.* **23** 2360

[18] Yang Y G, Wen Q Y and Zhang X 2008 *Sci. Chin.* G*: Phys. Mech. Astron.* **51** 321

[19] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305

[20] Nguyen B A 2006 *Phys. Lett.* A **350** 174

[21] Zhang Z J, Liu J, Wang D and Shi S H 2007 *Phys. Rev.* A **75** 026301

[22] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301

[23] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101

[24] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[25] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329

[26] Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2897

[27] Gao F, Wen Q Y and Zhu F C 2007 *Phys. Lett.* A **360** 748

[28] Gao F, Lin S, Wen Q Y and Zhu F C 2008 *Chin. Phys. Lett.* **25** 1561

[29] Deng F G, Li X H and Zhou H Y 2007 arXiv:0705.0279