Quantum broadcast communication and authentication protocol with a quantum one-time pad*

Chang Yan(昌 燕)[a)b)†], Xu Chun-Xiang(许春香)[a)], Zhang Shi-Bin(张仕斌)[a)b)], and Yan Li-Li(闫丽丽)[b)]

[a)] School of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China
[b)] Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, China

(Received 19 June 2013; revised manuscript received 25 July 2013; published 3 December 2013)

A quantum broadcast communication and authentication protocol with a quantum one-time pad based on the Greenberger–Horne–Zeilinger state is proposed. A binary string is used to express the identity of the receiver, which is encoded as a single sequence of photons. The encoded photon sequence acts as a detection sequence and implements authentication. An XOR operation serves as a one-time pad and is used to ensure the security of the protocol. The binary string is reused even in a noisy channel and proves to be unconditionally secure. In contrast with the protocols proposed by Wang *et al.* [*Chin. Phys.* **16** 1868 (2007)] and Yang *et al.* [*Chin. Phys. B* **19** 070304 (2010)], the protocol in this study implements the identity authentication with a reusable binary string; no hash function or local unitary operation is used. The protocol in this study is also easier to implement and highly efficient without losing security.

Keywords: quantum broadcast communication, quantum secure direct communication, Greenberger–Horne–Zeilinger (GHZ) state, authentication

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a, 03.65.Ud **DOI:** 10.1088/1674-1056/23/1/010305

1. Introduction

Cryptography is playing an increasingly important part in our information-oriented society. With the rapid development of quantum technology, especially the realization of quantum computing, the current classical cryptography schemes are potentially in danger. Quantum cryptography utilizes the principle of quantum mechanics to provide unconditionally secure information exchange. The quantum key distribution (QKD),[1–5] intended to create a private key between two remote authorized users, is one of the most remarkable applications of quantum mechanics. Since Bennett and Brassard[1] put forward the pioneering QKD protocol (BB84 protocol) in 1984, a lot of quantum information schemes have been proposed, such as quantum teleportation[6–10] and quantum secret sharing.[11–16]

Recently, a novel concept, quantum secure direct communication (QSDC), has been proposed and pursued.[17–44] Unlike QKD, QSDC aims to transmit the secret message directly without first establishing a key to encrypt it. The research on QSDC can be divided into the research with single photons and that based on entangled states. Long and Liu first put forward a QSDC scheme based on Einstein–Podolsky–Rosen (EPR) pairs in 2000, in which the concept of quantum data block was proposed to detect eavesdropping efficiently.[17] In 2003, Deng *et al.* presented a two-step QSDC scheme by using entanglement pairs.[18] After that, Deng and Long developed a QSDC scheme based on single photons, which acted as a quantum one-time pad cryptosystem.[19] In 2005, Wang *et al.* presented a QSDC scheme with high-dimension quantum superdense coding[20] and a multi-step QSDC scheme by using a multi-particle Greenberger–Horne–Zeilinger (GHZ) state.[21] The order rearrangement of the particles is another important method to improve the transmission security, which was first proposed by Deng and Long in 2003.[4] In 2006, Zhu *et al.* put forward a QSDC scheme based on a secret transmitting order of particles.[22] Li *et al.* questioned the security of the protocol in Ref. [22] and pointed out that Trojan horse attack strategies can be successfully implemented.[23] Wang *et al.* proposed a QSDC scheme based on an order rearrangement of single photons.[24] After that, Wang *et al.* generalized it to a multiparty controlled QSDC scheme, which could be applied to some special cryptographic tasks.[26] Li *et al.* then put forward a deterministic quantum secure direct communication (DQSDC) scheme by using single photons[25] and a QSDC scheme based on pure entangled states[27] in 2006 and 2007, respectively. Eavesdropping detection is an important part of quantum communication, guaranteeing its security. In 2009, Gao *et al.* presented a new detection strategy by using two photons in each Bell state and mixing into the sending sequence randomly, thereby improving the security and efficiency of the ping–pong protocol.[28] After that, Li *et al.* put forward other efficient detection strategies by using three-particle GHZ states,[29] extended three-particle GHZ states,[31] four-particle cluster states[32] and five-particle cluster states,[30] which brought higher eavesdropping

*Project supported by the National Natural Science Foundation of China (Grant No. 61370203), the Science and Technology Support Project of Sichuan Province, China (Grant No. 13ZC2138), and the Fund for Young Persons Project of Sichuan Province, China (Grant No. 12ZB017).

†Corresponding author. E-mail: cyttkl@cuit.edu.cn

© 2014 Chinese Physical Society and IOP Publishing Ltd

detection probabilities. Yang *et al.* proposed the concept of a generalized Bell state and unitary operations on the basis of logical qubits, based on which a QSDC scheme was developed that was immune to collective noise.[33] In 2011, Wang *et al.* proposed a quantum hyperdense coding protocol with hyperentanglement and developed a QSDC scheme based on this quantum hyperdense coding protocol.[34] In the same year, Gao *et al.* analyzed the security of QSDC and authentication protocol based on Bell states and presented a man-in-the-middle attack.[35] Gu *et al.* proposed a two-step QSDC scheme with hyperentanglement[37] and a robust QSDC scheme with a quantum one-time pad over a collective-noise channel.[38] In 2012, Huang *et al.* put forward a QSDC scheme against collective noise with decoy states based on channel encryption.[41] Liu *et al.* proposed a high-capacity QSDC scheme with single photons in both polarization and spatial-mode degrees of freedom.[43] Ren *et al.* presented a robust QSDC scheme by using quantum dot-cavity systems.[44]

Quantum broadcast communication (QBC)[45–51] is a special QSDC which involves a sender and multiple receivers.[45] The sender transmits a secret message 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 2007, Li *et al.* put forward a multiparty quantum remote secret conference based on the same key being shared by all the parties with GHZ states; the quantum secret conference is essentially a QBC protocol, in which each conferee sends his secret message to the others with a one-time pad crypto-system.[46] In the same year, Wang *et al.* presented three QBC protocols in which the identity authentication is implemented by using a previously shared secret identity number and a hash function with each user.[47] In 2010,Yang *et al.* proposed two more QBC protocols also based on shared secret identity number and hash function with GHZ states, which improves the efficiency compared with that of Wang *et al.*[48]

In this paper, a quantum broadcast communication and authentication protocol is proposed with a quantum one-time pad based on the GHZ state. It is similar to the protocol in Ref. [46] in previously sharing a key and sending secret messages with one-time pad crypto-systems. The main difference in this study is the addition of identity authentication. The authentication of the receiver's identity is implemented by using an unconditionally secure reusable identity string without a hash function. The identity string of the receiver is encoded as a single sequence of photons in Z basis or X basis. The encoded photon sequence, which acts as a detection sequence, not only guarantees the security of the quantum channel but also validates the legitimacy of the receiver. Positions and bases of the identity photons' sequence in the information sequence are not publicly announced in the classical channel, which ensures the unconditional security of a reusable identity string even in a noisy channel. The idea of reusing the previously shared base string with unconditional security in quantum cases was first proposed by Wen *et al.*[52] The classical XOR operation, serving as a one-time pad, is used to ensure the security of the protocol. Compared with protocols proposed by Wang *et al.*[47] and Yang *et al.*[48], 1) the protocol in this study implements the identity authentication with a reusable identity string; 2) the hash function and local unitary operations are not used; 3) the protocol in this study is easier to implement and has a high efficiency without losing the security.

2. The protocol

Now let us briefly describe the three-party quantum broadcast communication protocol. We suppose that the sender, Alice, wants to transmit her secret message to two legitimate receivers, say Bob and Charlie. Bob has a secret N-bit string $\mathrm{ID_B}$ representing his identity. Charlie has $\mathrm{ID_C}$. Alice shares $\mathrm{ID_B}$ and $\mathrm{ID_C}$. Suppose that Alice's secret message M is a series of classical numbers 0 and 1 in order.

Step 1 Alice prepares N ordered three-particle GHZ states, each of which is in the state

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

We denote the ordered N GHZ states by $\{[P_1(1), P_1(2), P_1(3)], [P_2(1), P_2(2), P_2(3)], \ldots, [P_N(1), P_N(2), P_N(3)]\}$, where the subscript indicates the order of each state in the sequence and 1, 2, 3 represent the three particles in each state. Alice takes one particle from each state to form an ordered particle sequence, $[P_1(1), P_2(1), \ldots, P_N(1)]$, called S_1 sequence. The remaining particles compose $\mathrm{S_2}$ sequence $[P_1(2), P_2(2), \ldots, P_N(2)]$ and S_3 sequence $[P_1(3), P_2(3), \ldots, P_N(3)]$. This is similar to the original protocol.[17]

Step 2 Alice prepares two N-qubits called S_{IDB} and S_{IDC} respectively. That is, if the i-th bit of $\mathrm{ID_B}$ or $\mathrm{ID_C}$ is 0, she randomly prepares the i-th qubit of S_{IDB} or S_{IDC} in $|0\rangle$ or $|1\rangle$ state; otherwise she randomly prepares the qubit in $|+\rangle$ or $|-\rangle$ state. The S_{IDB} and S_{IDC} are used as decoy photons, as in Refs. [49] and [50].

Step 3 Alice mixes S_{IDB} and S_{IDC} into S_2 and S_3 according to $\mathrm{ID_B}$ and $\mathrm{ID_C}$ respectively, forming S_2' and S_3'. For example, if the i-th bit of $\mathrm{ID_B}$ is 0, Alice inserts the i-th photon of S_{IDB} behind the i-th photon in S_2; if the i-th bit of $\mathrm{ID_B}$ is 1, Alice inserts the i-th photon of S_{IDB} before the i-th photon in S_2. The same thing goes for S_{IDC} and S_3. Then Alice sends S_2' and S_3' to Bob and Charlie respectively.

Step 4 After Bob and Charlie receive S_2' and S_3' respectively, Bob and Charlie extract S_{IDB} and S_{IDC} according to $\mathrm{ID_B}$

and ID_C and measure these photons in the right bases respectively. That is, they use the basis $B_Z = \{|0\rangle, |1\rangle\}$ when the one-to-one bit in ID_B or ID_C is 0 and $B_X = \{|+\rangle, |-\rangle\}$ when it is 1.

Step 5 Bob and Charlie announce the states of photons in S_{IDB} and S_{IDC} they received; the basis information is not included in this declaration, as in Ref. [35]. For example, Bob and Charlie use bit 0 to denote states $|0\rangle$ and $|+\rangle$, and 1 for $|1\rangle$ and $|-\rangle$. 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. In this condition, the communication goes on. Otherwise Alice interrupts it.

Step 6 Bob and Charlie measure each of the photons in the S_2 and S_3 sequences with the Z basis in order. They can form a series of classical numbers C_{S2} and C_{S3} in order. Bob and Charlie respectively tell Alice which photons in S_2 and S_3 they have received. For photons lost in Step 2 or Step 3, Alice discards the one-to-one matching photons in Step 1. For example, if the 5th photon in S_2 is not received by Bob and the 6th in S_3 is not received by Charlie, then Alice discards the 5th and the 6th in S_1; Bob and Charlie do the same thing with S_2 and S_3 respectively.

Step 7 Alice measures each remaining photon in S_1 in order with the Z basis (similar to the delayed measurement technique in Ref. [51]) and forms a series of classical numbers C_{S1} in order. Suppose that the length of C_{S1} is N_1. Alice takes the first N_1 bit from secret message M (called M_1) and encrypts it with C_{S1} bit by bit using the XOR operation (M_1 XOR $C_{S1} \to C$). Then Alice publishes C.

Step 8 Bob and Charlie decrypt C with C_{S2} and C_{S3} bit by bit respectively by using the XOR operation and obtain M_1 (C XOR $C_{S2} \to M_1, C$ XOR $C_{S3} \to M_1$).

Step 9 Bob and Charlie store secret message M_1.

Step 10 Alice, Bob and Charlie make a second transmission.

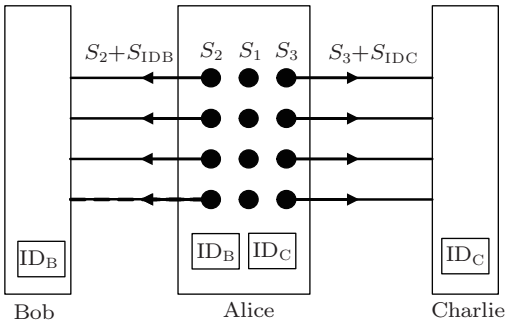


Fig. 1. Transmission of S_2 and S_3 and authentication between sender and receivers. The black dots are photons; the solid lines with arrowheads represent the transmission of photons in the quantum channel; $S_2 + S_{IDB}$ represents mixing the photons in S_{IDB} into S_2 according to ID_B bit by bit.

The three-party protocol can be easily generalized to a multi-party one. Suppose that Alice is the sender, Bob is receiver one, Charlie is receiver two, ..., and Dick is receiver m. Bob, Charlie, ..., and Dick have their secret N-bit strings ID_B, ID_C, ..., and ID_D representing their identities respectively. Alice shares ID_B, ID_C, ..., and ID_D. Alice prepares N ordered m-particle GHZ states, each of which is in the state

$$|\phi_m\rangle = \frac{1}{\sqrt{2}}(|000\ldots0\rangle + |111\ldots1\rangle)_{123\ldots m}. \quad (2)$$

Alice takes one particle from each state to form an ordered sequence, called S_1 sequence. The rest of the particles compose S_2 sequence, S_3 sequence, ..., and S_m sequence, respectively. Alice prepares $m-1$ N-qubits called S_{IDB}, S_{IDC}, ..., and S_{IDD} according to ID_B, ID_C, ..., and ID_D respectively. Alice mixes S_{IDB}, S_{IDC}, ..., and S_{IDD} into S_2, S_3, ..., and S_m according to ID_B, ID_C, ..., and ID_D respectively, forming S'_2, S'_3, ..., and S'_m. Alice sends S'_2, S'_3, ..., and S'_m to Bob, Charlie, ..., and Dick respectively. The details of the multi-party protocol are very similar to those of the three-party one. The security of the multi-party protocol is the same as that of the three-party one.

3. Security analysis

Photons in sequence S_1 are measured with the Z basis in order, and form a classical number sequence C_{S1}. In accord with the uncertainty principle of quantum theory, C_{S1} is a real random number used as a one-time pad to encrypt the secret message using the XOR operation. The number C_{S1} is not known by anybody except Alice, which ensures the security of the protocol.

When Alice transmits S_2 and S_3 to Bob and Charlie respectively, she mixes S_{IDB} and S_{IDC} into S_2 and S_3 according to ID_B and ID_C respectively. The positions and bases of S_{IDB} and S_{IDC} are secret and will not be publicly announced in a classical channel, which prevents Eve from performing targeted attacks and makes use of ID_B and ID_C in subsequent communication unconditionally secure.[52] Suppose that Eve intercepts some photons called S_E. Because she does not know which photons are detecting photons and which photons are from S_2 or S_3, to decrease the detection probability she can only perform the same attack on all photons in S_E. Assuming that Eve measures each photon in S_E with the X basis, she has a 50% chance of measuring each photon with the correct basis. However, because of not knowing which photons are detecting photons, Eve cannot obtain any information about ID_B and ID_C. Furthermore, because the positions of S_{IDB} and S_{IDC} are secret, Eve cannot succeed in a correlation-elicitable (CE) attack.

In Step 5, Bob and Charlie announce the states of the photons they received in S_{IDB} and S_{IDC}, but the basis information is not included. In this step, Alice not only verifies the legitimacy of Bob and Charlie but also detects eavesdropping

without revealing any information about ID_B and ID_C, which makes ID_B and ID_C reusable in subsequent communication.

Obviously, in ideal cases, the protocol in this study is secure. We can also verify that the protocol is secure in a noisy channel. First, we can perform quantum privacy amplification on the photons to make a perfect quantum state and perform error correction on the measurement results. Second, in this protocol, in each communication, there is a one-to-one relationship between photons in Alice's S_1 , Bob's S_2 and Charlie's S_3; therefore, a secret message will not be encoded on photons lost by eavesdropping or by noise in the channel, which ensures the accuracy of information and provides security. Third, positions and bases of identity strings are secret and will not be publicly announced, which makes their reuse unconditionally secure[52] even in a noisy channel.

4. Conclusion

In the QBC protocol presented in this paper, the secret information can be securely transmitted to the receiver without any useful information being leaked to an eavesdropper. Compared with the protocols presented by Wang *et al.*[47] and by Yang *et al.*,[48] the QBC protocol in this paper has the following differences: the measurement result of S_1 is used as a one-time pad to encrypt the secret message by using the classical XOR operation; the identity strings of the sender and the receiver can be reused with unconditional security even in a noisy channel; there is only one measurement of photons in the protocol; S_{IDB} and S_{IDC} act as detection sequences and are mixed into S_2 and S_3 according to ID_B and ID_C respectively; the positions and bases of S_{IDB} and S_{IDC} will not be publicly announced, which guarantees the security of ID_B and ID_C and precludes CE attacks; local unitary operations are not used; and no hash function is used in identity authentication.

In summary, a proposed QBC protocol based on a one-time pad is introduced in full detail. The security of the protocol is analyzed. The protocol is easier to implement and highly efficient without sacrificing security.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Processing* (New York: IEEE) p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Deng F G and Long G L 2003 *Phys. Rev. A* **68** 042315
[5] Li X H, Deng F U and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[6] Bennett C H 1993 *Phys. Rev. Lett.* **70** 1895
[7] Yan F L and Wang D 2003 *Phys. Lett. A* **316** 297
[8] Zhan Y B 2004 *Chin. Phys.* **13** 1801
[9] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev. A* **72** 022338
[10] Li Y L and Feng J 2007 *Acta Phys. Sin.* **56** 1888 (in Chinese)
[11] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[12] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[13] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[14] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228
[15] Han L F, Liu Y M, Yuan H and Zhang Z J 2007 *Chin. Phys. Lett.* **24** 3312
[16] Zhou P, Li X H, Deng F G and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 2181
[17] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[18] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[19] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[20] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[21] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[22] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev. A* **73** 022338
[23] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev. A* **74** 054302
[24] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett. A* **358** 256
[25] 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
[26] Wang J, Chen H Q, Zhang Q and Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese)
[27] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149
[28] Gao F, Guo F Z, Wen Q Y and Zhu F C 2009 *Sci. China Ser. G Phys. Mech. Astron.* **51** 1853
[29] Li J, Jin H F and Jing B 2011 *Sci. Chin. Phys. Mech. Astron.* **54** 1612
[30] Li J, Song D J, Guo X J and Jing B 2012 *Chin. Phys. C* **36** 31
[31] Li J, Guo X J, Song D J, Xie F and Peng Y 2012 *China Communications* **9** 111
[32] Li J, Jin H F and Jing B 2012 *Chinese Science Bulletin* **57** 4434
[33] Yang J, Wang C and Zhang R 2010 *Chin. Phys. B* **19** 110311
[34] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[35] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *Chin. Phys. Lett.* **28** 020303
[36] Gu B, Huang Y G, Fang X and Chen Y L 2011 *Commun. Theor. Phys.* **56** 659
[37] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[38] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. China.Phys. Mech. Astron.* **54** 942
[39] Shi J, Gong Y X, Xu P, Zhu S N and Zhan Y B 2011 *Commun. Theor. Phys.* **56** 831
[40] Gao G, Fang M, Wang L P and Cui X Y 2011 *Int. J. Theor. Phys.* **50** 1726
[41] Huang W, Wen Q Y, Jia H Y, Qin S J and Gao F 2012 *Chin. Phys. B* **21** 100308
[42] Sun Z W, Du R G and Long D Y 2012 *Int. J. Theor. Phys.* **51** 1946
[43] Liu D, Chen J L and Jiang W 2012 *Int. J. Theor. Phys.* **51** 2923
[44] Ren B C, Wei H R, Hua M, Li T and Deng F G 2013 *Eur. Phys. J. D* **67** 30
[45] Fiat A and Naor M 1994 *Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Science* **773** 480
[46] Li X H, Li C Y and Deng F G 2007 *Chin. Phys. Lett.* **24** 23
[47] Wang J, Zhang Q and Tang C J 2007 *Chin. Phys.* **16** 1868
[48] Yang Y G, Wang Y H and Wen Q Y 2010 *Chin. Phys. B* **19** 070304
[49] Li C Y, Zhou H Y and Wang Y 2005 *Chin. Phys. Lett.* **22** 1049
[50] Li C Y, Li X H and Deng F G 2006 *Chin. Phys. Lett.* **23** 2897
[51] Deng F G, Long G L and Wang Y 2004 *Chin. Phys. Lett.* **21** 2097
[52] Wen K, Deng F G and Long G L arXiv: 0706.3791v1 [quant-ph]