Vol 16 No 5, May 2007
1009-1963/2007/16(05)/1197-04

Chinese Physics

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

Quantum secure direct communication via partially entangled states*

Man Zhong-Xiao(满忠晓)† and Xia Yun-Jie(夏云杰)

College of Physics and Engineering, Qufu Normal University, Qufu 273165, *China*

(Received 2 July 2006; revised manuscript received 27 November 2006)

We present in this paper a quantum secure direct communication (QSDC) protocol by using partially entangled states. In the scheme a third party (Trent) is introduced to authenticate the participants. After authentication, Alice can directly, deterministically and successfully send a secret message to Bob. The security of the scheme is also discussed and confirmed.

Keywords: quantum secure direct communication, partially entangled state
PACC: 0365

Quantum secure communication along a physical channel[1−6] is doubtless one of the most attractive perspectives related to the recent developments of quantum physics. Based on physical laws instead of mathematical complexities, communication with perfect secrecy could be guaranteed over an insecure channel in Vernam's sense of one-time pad, which is known as quantum cryptography. The pioneering work of Bennett–Brassard (BB84)[1] shows how to exploit quantum resources for cryptographic purposes. Conventionally, the problem is referred to as quantum key distribution (QKD) which allows for a secret generation of a random key through which legitimate users can accomplish a thoroughly private communication (for a review see Refs.[2,7–9]). Recently, a new concept in quantum cryptography, quantum secure direct communication (QSDC) has been proposed,[10−23] which permits messages to be communicated directly without establishing a random key to encrypt them first. In Ref.[11], Boström and Felbinger proposed a Ping–Pong QSDC protocol, but it failed completely for QSDC and even for quantum key distribution.[24,25] Subsequently, Deng *et al* put forward a two-step QSDC protocol[12] with Einstein–Podolsky–Rosen (EPR) pairs transmitted in quantum data block by generalizing the two-step QKD protocol.[26]

Very recently, two QSDC protocols with authentication have been proposed by Lee *et al*[27] using the Greenberg–Horne–Zeilinger (GHZ) states, which are composed of two parts: one is for an authentication process and the other is for a direct communication. In Lee–Lim–Yang's schemes, the transmission of the qubits in the quantum channel is of two-way. The qubits are first distributed to the legitimate users in the quantum channel, and after encoding, these qubits are transmitted again to a participant for decoding. Thus an eavesdropper has two chances to attack the quantum channel and also these qubits would be confronted with more threats from environmental disturbances. In addition, it is generally admitted that, to the present-day technique, the preparation of bipartite entangled states is much easier than that of GHZ states. Hence, it is desirable to design a communication scheme with bipartite entangled states. To our best knowledge, most QSDC protocols to date have been based on maximally bipartite or multipartite entangled states. However, in a realistic situation, decoherence and noise degrade the channel, and we do not have a maximally entangled state anymore. One possible way is to employ quantum distillation protocols,[28] through which one can obtain a maximally entangled state from a large ensemble of nonmaximally entangled states. But quantum distillation would be useless if we do not have the sufficient number of partially entangled states and it only achieves a maximally entangled state asymptotically. With these considerations and enlightened by Lee–Lim–Yang's QSDC schemes, we present a new QSDC scheme by using partially entangled bipartite stats and the one-way transmission of the qubits in the quantum channel.

*Project supported by National Natural Science Foundation of China (Grant No 10534030).
†E-mail: manzhongxiao@163.com

The same as Lee–Lim–Yang's QSDC schemes[27], our QSDC protocol is also composed of two parts: one is for an authentication process and the other is for a direct communication. A third party, Trent, is introduced to authenticate the users Alice and Bob. He is assumed to be cooperative and honest. Here, we use the authentication method proposed in Ref.[29]. Alice's and Bob's secret identity sequences and one-way hash functions are known to Trent in advance, which must be kept secret. We assume Alice's (Bob's) identity sequence is $\mathrm{ID_A}$ ($\mathrm{ID_B}$) and the one-way function is h_A (h_B). If Alice wants to send N secret messages to Bob, she notifies them to Bob and Trent as well. On receiving this request, Trent produces $2(N+\delta)$ bipartite entangled states $|\psi_i\rangle$ $(i=1,2,\cdots,2(N+\delta))$ in the following form:

$$|\psi_i\rangle = \alpha|00\rangle_{\mathrm{HT}} + \beta|11\rangle_{\mathrm{HT}}, \tag{1}$$

where α and β are complex coefficients satisfying $|\alpha|^2+|\beta|^2=1$ and H (T) denotes the home (travel) qubit. Trent divides equally the $2(N+\delta)$ states into two groups, say, A group and B group. In the A (B) group, the qubits T correspond to Alice (Bob) and the qubits H will be always in Trent's hands. The user's authentication key shared with Trent can be calculated as $h_{\mathrm{user}}(\mathrm{ID_{user}}, c_{\mathrm{user}})$, where c_{user} is the counter of calls on the user's hash function. Before distributing the qubits T in A and B groups to Alice and Bob, Trent encodes them with Alice's and Bob's authentication keys $h_\mathrm{A}(\mathrm{ID_A}, c_\mathrm{A})$ and $h_\mathrm{B}(\mathrm{ID_B}, c_\mathrm{B})$, respectively. The encoding method can be described as follows. If the ith value of the authentication key is '0', then Trent makes an identity operation I on the ith state. If it is '1', a Hadamard operation H is applied. After making all the operations, Trent distributes the encoded qubits T of A and B groups to Alice and Bob respectively, and keeps qubits H for himself.

After receiving the qubits, Alice and Bob notify their confirmation to Trent and decode the qubits with the same unitary transformations as Trent's. According to the unitary properties of the operators H and I, after Alice's and Bob's operations the encoded states by Trent would be transformed into their initial states, i.e. $|\psi_i\rangle = \alpha|00\rangle_{\mathrm{HT}}+\beta|11\rangle_{\mathrm{HT}}$. Next, determine whether the current receivers are the legitimate ones or not. Trent may select a subset δ out of the decoded qubits and make von Neumann measurements on them. Then he requires Alice and Bob to make the same measurements on their corresponding qubits and compare the results through a public channel. If the error rate is higher than the expected, then Trent aborts the protocol. Otherwise Trent can confirm that the present receivers are legitimate ones and the channel is secure.

After the authentication process, Alice can communicate with Bob directly with the help of Trent as follows. Firstly, for the remaining $2N$ qubits in A and B groups after authentication, Trent makes Bell-basis measurements in sequence on every two H qubits: one qubit is taken from A group and the other from B group. Then he publishes the Bell-basis measurements publicly. As an example, we consider two states $|\psi\rangle_{\mathrm{H_A T_B}} \otimes |\psi\rangle_{\mathrm{H_B T_B}}$, where the subscripts A and B refer to the qubits belonging to A and B groups, respectively. After Trent's Bell-basis measurement on qubits $\mathrm{H_A}$ and $\mathrm{H_B}$, Alice's and Bob's corresponding qubits $\mathrm{T_A}$ and $\mathrm{T_B}$ without interacting previously will be entangled in the sense of quantum entanglement swapping. The possible states into which Trent's Bell-basis measurements are projected can be expressed as follows:

$$\langle \Phi^{\pm}|_{\mathrm{H_A H_B}}|\psi\rangle_{\mathrm{H_A T_A}} \otimes |\psi\rangle_{\mathrm{H_B T_B}} = \frac{1}{\sqrt{2}}(\alpha^2|00\rangle_{\mathrm{T_A T_B}} \pm \beta^2|11\rangle_{\mathrm{T_A T_B}}) \tag{2}$$

$$\langle \Psi^{\pm}|_{\mathrm{H_A H_B}}|\psi\rangle_{\mathrm{H_A T_A}} \otimes |\psi\rangle_{\mathrm{H_B T_B}} = \alpha\beta\left[\frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{T_A T_B}} \pm |10\rangle_{\mathrm{T_A T_B}})\right], \tag{3}$$

where $|\Phi^{\pm}\rangle_{\mathrm{H_A H_B}} = \frac{1}{\sqrt{2}}(|00\rangle_{\mathrm{H_A H_B}} \pm |11\rangle_{\mathrm{H_A H_B}})$ and $|\Psi^{\pm}\rangle_{\mathrm{H_A H_B}} = \frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{H_A H_B}} \pm |10\rangle_{\mathrm{H_A H_B}})$. The probability of obtaining the less entangled states $\frac{1}{\sqrt{2}}(\alpha^2|00\rangle_{\mathrm{T_A T_B}} \pm \beta^2|11\rangle_{\mathrm{T_A T_B}})$ is $\frac{\alpha^4+\beta^4}{2}$, and the probability of achieving the maximally entangled states $\alpha\beta\left[\frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{T_A T_B}} \pm |10\rangle_{\mathrm{T_A T_B}})\right]$ is $\alpha^2\beta^2$. With Trent's Bell-basis measurements published, one can

conclude the projected state of Alice's and Bob's shared qubits.

Next, Alice can encode the secret messages by using a classical error correction code (ECC) such as the Hamming code, the Reed–Solomon code, or the Bose–Chaudhuri–Hochquenghem (BCH) code, so that Bob will be able to correct errors in the decoded message.[27] Then Alice can encode her secret messages as follows. If the message is "0", Alice makes an identity operation I on her qubit. Otherwise if it is "1", Alice performs a bit-flip operation $U = |1\rangle\langle 0| + |0\rangle\langle 1|$ on her qubit. After making all operations, Alice performs a measurement in the basis $\beta_z = \{|0\rangle, |1\rangle\}$ on each of her encoded qubits and notifies the measurement outcomes to Bob. Having received Alice's measurements, Bob also implements a measurement in the β_z basis on his corresponding qubits. Bob can then recover Alice's messages using Table 1. In the following we make an explicit analysis for the communication process described above. For example, if Trent reveals $|\Phi^+\rangle_{\mathrm{H_A H_B}}$ and Alice's publication is $|1\rangle_{\mathrm{T_A}}$ while Bob measures $|0\rangle_{\mathrm{T_B}}$, then Bob can infer that Alice has performed a bit-flip operation U and the secret message she sent is "1".

Table 1. Corresponding relations among Trent's announcement, Alice's announcement, Bob's measurement, and Alice's operation.

Trent's publication	Alice's publication	Bob's measurement	Alice's operation
$\|\Phi^{\pm}\rangle_{\mathrm{H_A H_B}}$	$\|0\rangle_{\mathrm{T_A}}(\|1\rangle_{\mathrm{T_A}})$	$\|0\rangle_{\mathrm{T_B}}(\|1\rangle_{\mathrm{T_B}})$	$I(0)$
	$\|0\rangle_{\mathrm{T_A}}(\|1\rangle_{\mathrm{T_A}})$	$\|1\rangle_{\mathrm{T_B}}(\|0\rangle_{\mathrm{T_B}})$	$U(1)$
$\|\Psi^{\pm}\rangle_{\mathrm{H_A H_B}}$	$\|0\rangle_{\mathrm{T_A}}(\|1\rangle_{\mathrm{T_A}})$	$\|1\rangle_{\mathrm{T_B}}(\|0\rangle_{\mathrm{T_B}})$	$I(0)$
	$\|0\rangle_{\mathrm{T_A}}(\|1\rangle_{\mathrm{T_A}})$	$\|0\rangle_{\mathrm{T_B}}(\|1\rangle_{\mathrm{T_B}})$	$U(1)$

Now we analyse the security of the communication process described above. In the scheme we adopt the properties of entanglement swapping, i.e. Alice's and Bob's qubits without interacting previously can be entangled after the Bell-basis measurements of Trent. Hence, after user authentication process, the encoded qubits by Alice need not to be transmitted to Bob in the quantum channel, which leads to a distinct advantage that Eve has not a chance to attack the message qubits any more. Actually, there exists only one chance for Eve to attack the quantum channel when Trent distributes the qubits to the receivers. Therefore the security of the communication process between the legitimate users reduces to the security of the user authentication process, which has been discussed and confirmed in Ref.[27]. As one can see that Eve has no access to Trent's home qubits, all of her operations are limited to the travel qubits. In addition, Trent performs a Hadamard operation on a subset of the travel qubits conditioned on his secret authentication keys, thus the state of the qubit is (to Eve) indistinguishable from the four states of two conjugate bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ (with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$), which is much like BB84 protocol.[1] In the following, we will compare the authentication process of our scheme with that of BB84 protocol. In the BB84 protocol, the preparation of the states is completely random. However, in our scheme, the sender first produces a bipartite entangled state and then transforms the travel qubit into a determined base $\{|+\rangle, |-\rangle\}$ or $\{|0\rangle, |1\rangle\}$ with an identity or a Hadamard operation based on his secret authentication keys. Therefore, different from the random preparation of the state in the BB84 protocol, the preparation base of the qubit is determined in our scheme. In the BB84 protocol, on receiving the sending qubits the receiver measures the qubits in a randomly chosen base while they will disregard the cases in which they have used incompatible bases in a later error correction scheme. In the present scheme, the previously shared secret authentication keys actually determine the preparation base of Trent and the measurement base of the receivers. Hence, Alice and Bob know the preparation base of the travel qubits and will measure the qubits always in the compatible base. In fact, if a qubit is prepared in the base $\{|+\rangle, |-\rangle\}$, i.e. Trent has performed a Hadamard operation on it, the receiver will transform it into the base $\{|0\rangle, |1\rangle\}$ also with a Hadamard operation. As a consequence, the authentication process of our scheme is essentially a determined BB84 protocol in the sense that the preparation base and measurement base have been determined in advance. To discuss the security of our scheme we can follow the discussion on security of the BB84 protocol.

Subsequently, we will introduce a class of attacks that Eve commonly adopts. Firstly, we consider that Eve intercepts the qubits passed to Alice or Bob and impersonates the sender Trent. Then, Eve can either measure each qubit in one of the two bases and resend to the receivers another qubit in the state corresponding to her measurements, or prepare directly another qubit and send it to the receivers. For the former case, Eve can be detected with a probability of $\frac{1}{4}$ per check qubit as indicated in the BB84 protocol. In this

case, Eve cannot acquire any useful information but makes the scheme be denial-of-service. For the latter case, Eve can intercept all the travel qubits and substitute them with her own prepared qubits. Eve can be detected with a probability of $\frac{1}{2}$ for this case. On the other hand, Eve may steal some information by entangling her ancilla (prepared, say, in the state $|\chi\rangle_{\rm E}$) with a travel qubit T (assumed to be in the state $|i\rangle$ with $i \in \{0, 1\}$) before this qubit reaches the receiver: $|\chi\rangle_{\rm E}\otimes|i\rangle \rightarrow \gamma|\chi_i\rangle_{\rm E}|i\rangle+\delta|\chi_{i\oplus1}\rangle_E|i\oplus1\rangle$, where $|\gamma|^2 + |\delta|^2 = 1$ and $\langle\chi_i|\chi_{i\oplus1}\rangle = 0$. Then she resends this qubit to the receiver. However, she is detected with a probability of $|\delta|^2$ if the security is checked by Trent and the receiver is performed on this state.

In this paper, by using partially entangled bipartite states as the quantum channels, we propose a controlled direct communication scheme. To prevent man-in-the-middle attacks, an additional user authentication process has been introduced.[27,29] Comparing with the previously presented QDC schemes, the present version has some advantages. Firstly, we adopt partially entangled states instead of maximally entangled states from the beginning of our scheme, thus it is more useful in a realistic situation where the channel would be degraded by decoherence and noise. Secondly, by using the properties of quantum entanglement swapping, the transmission of the message qubits in the quantum channel is of one-way. Hence Eve has only one chance to attack the quantum channel when Trent distributes the travel qubits to Alice and Bob. It has been shown above (and also in the Ref.[27]) that the authentication process can detect any attack from Eve. Therefore, if no eavesdropping is found in the detecting procedure it is deterministically successful to transmit the secret messages in the message transmission procedure in our protocol, but it cannot do so in the two-way transmission protocol. Lastly, in the scheme we use bipartite entangled states instead of GHZ state, which can reduce the difficulties in experiment.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) (New York: IEEE) p175

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

[3] Yuan H C and Qi K G 2005 *Chin. Phys.* **14** 1716

[4] Lin X and Li H C 2005 *Chin. Phys.* **14** 1724

[5] Zheng Y Z, Gu Y J and Guo G C 2003 *Chin. Phys.* **12** 1070

[6] Sun L L, Fan Q B and Zhang S 2005 *Chin. Phys.* **14** 1313

[7] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese)

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

[9] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 5549 (in Chinese)

[10] Beige A, Englert B G, Kurtsiefer C 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] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41**(1) 75

[16] Gao T, Yan F L and Wang Z X 2004 *Il Nuovo Cimento Della Societa Italiana di Fisica* B **119**(3) 313

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

[18] Gao T, Yan F L and Wang Z X 2004 *Zeitschrift für Naturforschung* A **59**(9) 597

[19] Wang J, Zhang Q and Tang C J 2006 quant-ph/0602166
Wang J, Zhang Q and Tang C J 2005 quant-ph/0511092

[20] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305

[21] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338

[22] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 *Phys. Lett.* A **354** 67

[23] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[24] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[25] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[26] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

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

[28] Shi B S, Jiang Y K and Guo G C 2000 *Phys. Rev.* A **62** 054301

[29] Lee H, Lee S, Lee D, Lim J and Yang H 2005 quant-ph/0510144