Vol 16 No 8, August 2007
1009-1963/2007/16(08)/2149-05

Chinese Physics

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

Quantum secure direct communication with quantum encryption based on pure entangled states*

Li Xi-Han(李熙涵)[a)b)c)], Li Chun-Yan(李春燕)[a)b)c)], Deng Fu-Guo(邓富国)[a)b)c)†], Zhou Ping(周 萍)[a)b)c)], Liang Yu-Jie(梁玉洁)[a)b)c)], and Zhou Hong-Yu(周宏余)[a)b)c)]

[a)] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing* 100875, *China*
[b)] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing* 100875, *China*
[c)] *Beijing Radiation Center, Beijing* 100875, *China*

(Received 7 November 2006; revised manuscript received 21 November 2006)

This paper presents a scheme for quantum secure direct communication with quantum encryption. The two authorized users use repeatedly a sequence of the pure entangled pairs (quantum key) shared for encrypting and decrypting the secret message carried by the travelling photons directly. For checking eavesdropping, the two parties perform the single-photon measurements on some decoy particles before each round. This scheme has the advantage that the pure entangled quantum signal source is feasible at present and any eavesdropper cannot steal the message.

Keywords: quantum secure direct communication, quantum encryption, quantum key, pure entangled states

PACC: 0155, 0367

Quantum mechanics provides some novel ways for processing and transmission of quantum information. Quantum key distribution (QKD) is considered to be the safest system for creating a private key between two remote authorized users, say Alice and Bob, and may be the most advanced application of quantum information. The noncloning theorem forbids an eavesdropper, Eve, to eavesdrop the quantum communication freely. In 1984, Bennett and Brassard (BB84)[1] proposed an original QKD protocol with nonorthogonal polarized single photons. As an unknown quantum states cannot be eavesdropped without leaving a trace in the outcomes obtained by the two parties, the BB84 protocol is unconditionally secure.[2] In 1991, Ekert[3] introduced another QKD scheme based on the correlation of an Einstein–Podolsky–Rosen (EPR) pair, the maximally entangled two-particle state, by using Bell inequality for error rate analysis. Subsequently, Bennett, Brassard and Mermin (BBM92)[4] simplified the process for eavesdropping check in this scheme with two nonorthogonal measuring bases. Lo *et al*[5] presented a QKD model with two nonsymmetric bases. Huang *et al*[6] and Deng *et al*[7] designed two QKD models by using repeatedly a sequence of private classical bits shared initially for improving their efficiency for qubits or reducing the delay time in QKD with some orthogonal states. To date, much attention has been focused on QKD.[5−11]

Recently, quantum secure direct communication (QSDC), a novel concept, was proposed and pursued by some groups.[12−27] Different from QKD whose goal is to generate a private key between the two remote parties of communication, QSDC is used to communicate the secret message directly without generating a key in advance and then encrypting the message for its transmission in a classical channel. According to the Deng–Long–Liu criterion, on the one hand, the sender Alice should confirm whether the quantum channel is secure before she encodes the message on the quantum states transmitted as the messages cannot be discarded in QSDC.[14,28,29] Moreover, the message should be read out by the receiver Bob directly.[14] On the other hand, the security of quantum communication is based on the error rate analysis with the theories in statistics.[14,28,29] In this way, the quantum states in QSDC should be transmitted in a quantum data block, the same as those in Refs.[14–18, 28, 29]. This is not a necessary condition in QKD as the error

*Project supported by the National Natural Science Foundation of China (Grant Nos 10604008 and 10435020) and the Beijing Education Committee (Grant No XK100270454).
†E-mail: fgdeng@bnu.edu.cn

rate analysis is just a postprocessing step, and the results transmitted do not include the information about the secret message and can be abandoned.[14,28,29]

In 2002 Beige *et al*[19] proposed a QSDC scheme with single-photon two-qubit states. In their scheme, one qubit is used to check the security of the quantum channel after some results are transmitted, and the other is used to carry the message. The message can be read out after a transmission of an additional classical bit for each qubit.[20] Subsequently Boström and Felbinger proposed a quasi-secure QSDC protocol, called the Ping-Pong QSDC protocol,[20] with an EPR pair. In this scheme the eavesdropping done by Eve can be hidden with the loss of a practical quantum channel[21] and the error aroused by the noise of the quantum channel.[22] Moreover, the two parties can accomplish the error rate analysis only after they transmit an enough large set of messages, and some messages may leak to Eve in a noisy channel. The two-step QSDC scheme[28] and the scheme with single photons proposed by Deng and Long [29] can be made secure even in a noisy channel with quantum privacy amplification[30,31] as the states are transmitted in a quantum date block and the confirmation of the security of the quantum channel has been achieved before the sender encodes her message on the states. These ideas are borrowed by Wang *et al*[15] to design the QSDC models as well.

In this paper, we will present a scheme for QSDC with quantum encryption. This protocol uses a controlled-not (CNot) gate to encode and decode the secret message. The two parties first share privately a sequence of two-photon pure entangled states which are feasible with the present technologies, and then use the states as their private quantum key which is reused with a eavesdropping check before each round. The receiver can read out directly the message and each photon transmitted between the parties can carry one bit of message securely in principle.

Generally speaking, many QKD and QSDC schemes choose EPR pairs as quantum information carriers to transmit a private key or a secret message. The reason is that the two photons in the four Bell states have good correlations in both the measuring bases $Z = \{|0\rangle, |1\rangle\}$ and $X = \left\{|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\right\}$.

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}(|+x\rangle_A|+x\rangle_B + |-x\rangle_A|-x\rangle_B), \tag{1}$$

$$|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}(|+x\rangle_A|-x\rangle_B + |-x\rangle_A|+x\rangle_B), \tag{2}$$

$$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}(|+x\rangle_A|+x\rangle_B - |-x\rangle_A|-x\rangle_B), \tag{3}$$

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}(|+x\rangle_A|-x\rangle_B - |-x\rangle_A|+x\rangle_B). \tag{4}$$

This feature is very useful in the eavesdropping check process. However, it is difficult to produce the maximally two-particle entangled states with the present technologies. Contrarily, in experiments the two photons prepared are usually in the pure entangled state, such as $|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B$ ($|a|^2 + |b|^2 = 1$). The two photons are always correlated in the basis Z, but not in the basis X, as

$$\begin{aligned}|\Psi\rangle_{AB} &= a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B \\ &= \frac{1}{2}[(a+b)(|+x\rangle_A|+x\rangle_B + |-x\rangle_A|-x\rangle_B) \\ &\quad +(a-b)(|+x\rangle_A|-x\rangle_B + |-x\rangle_A|+x\rangle_B)].\end{aligned} \tag{5}$$

This means that the security of the quantum communication with pure entangled states is lower than that with Bell states if we use the two bases X and Z to check the security. On the other hand, those pure entangled quantum sources are more convenient in practical applications. In this QSDC scheme, we use some decoy photons to check the eavesdropping[12] for overcoming the flaw of pure entangled states.

Now, let us describe our QSDC scheme in detail as follows. It includes four steps.

(S1) The two authorized users (Alice and Bob) share a sequence of two-particle pure entangled states securely as their private quantum key.

For this task, Bob first prepares n two-photon pairs randomly in one of the two pure entangled states $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$. Here $|\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B$ which can be obtained by flipping the bit value of the two photons in the state $|\Psi\rangle_{AB}$, i.e., $|\Phi\rangle_{AB} = \sigma_x^A \otimes \sigma_x^B |\Psi\rangle_{AB}$ (here σ_x is a Pauli operator). Bob picks up photon B in each pair for forming the sequence $S_B : [B_1, B_2, \cdots, B_n]$. The other sequence S_A is made up of particles $A_i (i = 1, 2, \cdots, n)$. He keeps the sequence S_B at home and sends the sequence S_A to Alice. For checking eavesdropping, Bob inserts some decoy photons S_{de}, which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$, into the sequence S_A. He can get a decoy photon by measuring one photon in a two-photon pair $|\Psi\rangle_{AB}$ with the basis Z and operating on the other photon with σ_x or a Hadamard (H) operation.[12] In a word, it is unnecessary for the users to have an ideal single-photon source in this scheme.

After Alice announces the receipt of the sequence S_A, Bob tells her the positions and the states of the decoy photons. Alice measures the decoy photons with the suitable bases and analyses the error rate of those outcomes with Bob. If the error rate is very low, they can obtain a sequence of quantum key privately and continue to the next step; otherwise, they discard the transmission and repeat quantum communication from the beginning.

(S2) Alice and Bob use their private quantum key to encrypt and decrypt the secret message directly.

For QSDC, Alice prepares a sequence of travelling particles γ_i which are in one of the two states $\{|0\rangle, |1\rangle\}$ according to the bit value 0 or 1 of her secret message, respectively. We call it the travelling particle sequence S_T. For checking eavesdropping, similar to Refs.[28,29], Alice needs to add a small trick in the sequence S_T before she sends it to the quantum channel. That is, he inserts some decoy photons,[12] say S_D which are randomly in the four states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$ and distributed randomly in the sequence S_T. Alice uses the quantum key, the pure entangled pairs shared $\{|\Psi\rangle_{AB}, |\Phi\rangle_{AB}\}$ to encrypt the travelling particles in the sequence S_T except for the decoy photons. That is, Alice performs a CNot operation on the particles A_i and γ_i $(i = 1, 2, \ldots, n)$ by using the particle A_i as the control qubit. Then Alice sends all the travelling particles to Bob.

After receiving the sequence S_T, Bob asks Alice to tell him the positions and the states of the decoy photons in the sequence S_T, and then measures them with the same bases as those chosen by Alice for preparing them. For the particles B_i and γ_i, Bob takes a CNot operation on them with the particle B_i as the control qubit, similar to Alice, and then he measures the particles γ_i with the basis Z and records the outcomes of the measurements.

(S3) Alice and Bob check the security of their transmission. They analyse the error rate of the decoy photons. If the error rate is very low, Bob can trust this transmission, and read out the message directly. Otherwise they have to abandon the results and repeat the procedures from the beginning.

(S4) If the quantum communication succeeds, Alice and Bob repeat their communication from step 2. That is, they use repeatedly the pure entangled pairs as their quantum key and transmit the secret message again in the next round.

In an ideal condition, this QSDC scheme is secure for any intercepting–resending attack strategies if the quantum key is private because it is equivalent to a quantum one-time-pad crypto-system.[8,29] The encryption on a travelling particle γ_i with a CNot operation makes it entangle with a quantum system in the quantum key. For an eavesdropper, any quantum system in the quantum key is randomly in one of the two states $\{|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B, |\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B\}$. After the CNot operation done by Alice, the three particles A_i, B_i, and γ_i are in the GHZ-class state $|\Psi\rangle_{s1} = a|00\gamma_i\rangle + b|11\bar{\gamma}_i\rangle)_{A_iB_i\gamma_i}$ or $|\Phi\rangle_{s1} = b|00\gamma_i\rangle + a|11\bar{\gamma}_i\rangle)_{A_iB_i\gamma_i}$ randomly. The reduced density matrix of the traveling particle γ_i is $\rho_{\gamma_i} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. That is, the travelling particle is in one of the two eigenvectors of any measuring operator with the same probability 50% for any eavesdropper, and none can get a useful information about the state of the travelling particle γ_i when the effect of his eavesdropping on the travelling particle is the same as that by guessing its outcome randomly.

If Eve wants to steal the message carried by the travelling particles, she should eavesdrop the quantum key by capturing the travelling particles first, and then steal the information of the travelling particles transmitted in the next round. However, her action will leave a track in the eavesdropping check. The reason

is that the procedure of checking eavesdropping done by the two authorized users in this scheme, in essence, is the same as that in the BB84 QKD protocol[1] for any eavesdropper. That is, the decoy photons are produced by choosing randomly one of the two bases Z and X, and are inserted into the travelling sequence S_T randomly. Also, Bob measures them with the same bases as those chosen by Alice after he receives the travelling sequence and obtains the information about their bases of the decoy photons. For any eavesdropper, the bases chosen by Bob are random even though they are announced in public finally as no eavesdropper has the access to the travelling particles after Bob receives them. Any eavesdropping will inevitably disturb the states of the decoy photons and be detected by the two authorized users if an eavesdropper monitors the quantum line, same as that in the BB84 protocol.[1]

In a practical channel, noises will affect the entanglement of the quantum key. In this time, the users should exploit entanglement purification[32] to keep the entanglement in the quantum key, and do quantum privacy amplification[30] on them as well. However, the two users need not to purify their states to Bell states, just as the pure entangled states $|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B$ ($|\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B$) or $|\Psi'\rangle_{AB} = a'|0\rangle_A|0\rangle_B + b'|1\rangle_A|1\rangle_B$ ($|\Phi'\rangle_{AB} = b'|0\rangle_A|0\rangle_B + a'|1\rangle_A|1\rangle_B$) in this scheme. Here $|a'|^2 + |b'|^2 = 1$. As the quantum key is just used to encrypt and decrypt the secret message, it is unnecessary for the users to keep the same states as those used by them in last time, just as the correlation of each pair, which will increase the efficiency of the entanglement purification process largely. Certainly, on the one hand, the users should do error correction on their results in practical applications, same as the two-step protocol.[12] On the other hand, this QSDC scheme can only used to distribute a private key if the loss of the quantum line is unreasonably large.

In summary, QSDC can be done with quantum encryption by means of the fact that the two authorized users first share privately a sequence of pure entangled pairs and use them repeatedly as the quantum key for encrypting the travelling particles which are in the eigenvectors of the basis Z. The receiver can read out the message directly and each particle can carry one bit of the message securely. For checking eavesdropping, the sender adds a small trick in the travelling particles which can forbid Eve to eavesdrop the quantum channel freely. The most important advantage of this protocol is that the pure entangled quantum signal source is feasible at present. As the photons used for security checking is not the quantum key shared, the quantum key can be reused without abatement in principle.

References

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

[2] Lo H K and Chau H F 1999 *Science* **283** 2050

[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] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133

[6] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489

[7] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

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

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

[10] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311

[11] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097

[12] 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
Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896

[13] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[14] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359

[15] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305
Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

[16] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y and Deng F G 2006 *Chin. Phys. Lett.* **23** 1080
Deng F G, Li X H, Li C Y, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1676

[17] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41** 75
Gao T, Yan F L and Wang Z X 2004 *Il Nuovo Cimento* B **119** 313

[18] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[19] Beige A, Engler B G , Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357
[20] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[21] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[22] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Chin. Phys.* **16** 277
[23] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301
[24] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[25] Xia Y, Fu C B, Zhang S, Hong S K, Yeon K H and Um C I 2006 *J. Korean Phys. Soc.* **48** 24
Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302
[26] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290
[27] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[28] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[29] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[30] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[31] Deng F G and Long G L 2006 *Commun. Theor. Phys.* **46** 443
[32] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722