Vol 16 No 3, March 2007
1009-1963/2007/16(03)/0621-03
Chinese Physics
© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

# Quantum secure direct communication protocol with blind polarization bases and particles' transmitting order*

Song Jie(宋 杰), Zhu Ai-Dong(朱爱东), and Zhang Shou(张 寿)†

*Department of Physics, College of Science, Yanbian University, Yanji* 133002, *China*

(Received 26 April 2006; revised manuscript received 20 June 2006)

This paper presents a modified secure direct communication protocol by using the blind polarization bases and particles' random transmitting order. In our protocol, a sender (Alice) encodes secret messages by rotating a random polarization angle of particle and then the receiver (Bob) sends back these particles as a random sequence. This ensures the security of communication.

**Keywords:** quantum secure direct communication, eavesdropper, blind polarization bases
**PACC:** 0365

Quantum key distribution (QKD) is one of the most remarkable applications of quantum mechanics in quantum information. It can create a common random key between two parties over a public channel. The key can be used to implement a classical private key cryptosystem to ensure secret messages to be communicated safely. In 1984 Bennett and Brassard proposed the standard BB84 QKD protocol.[1] After the pioneering work, there were a lot of different protocols of QKD.[2−11] Different from QKD, quantum secure direct communication (QSDC) is a novel concept of communication which is able to communicate important messages directly and need not create private key to encrypt them. Since Beige *et al*[12] presented a communication protocols based on single-photon two-qubit states in 2002, many QSDC protocols have been proposed.[13−25] In QSDC once eavesdropper (Eve) eavesdrops secret information, this means leakage of the secret. Thus QSDC is more demanding on the security than QKD.

In 2005 Kye *et al*[26] proposed a novel QKD protocol (KKKP) which is based on random polarization and three-way communication between two legitimate users. Zhang *et al*[27] show an eavesdropping protocol against the KKKP, by which eavesdropper can get the full information without being detected by the legitimate users. Kye *et al*[28] modify the KKKP to prevent the impersonation attack. Very recently, Zhu *et al*[29] present a QSDC protocols based on transmitting order of particles in which the Einstein–Podolsky–Rosen (EPR) pairs are used as messages carriers. In this paper, we modify the KKKP as a QSDC protocol basel on Zhu's strategy. Our protocol improves the efficiency and security of communication compared with the modified KKKP protocol.[28]

Now, let us depict our QSDC protocol.

(a.1) Alice prepares $n$ linearly polarized qubit which are in the same states $|\psi\rangle_i^0 = |0\rangle$ $(i = 1, 2, \ldots, n)$ and chooses a random angle $\theta_i$ $(i = 1, 2, \ldots, n)$. $|0\rangle$ and $|1\rangle$ represent two orthogonal polarizations of one qubit.

(a.2) Alice rotates the polarization angles of the $n$ qubits by $\theta_i$ $(i = 1, 2, \ldots, n)$ to bring the states of these qubits to $|\psi\rangle_i^1 = \hat{U}_y(\theta_i)|\psi\rangle_i^0 = \cos\theta_i|0\rangle - \sin\theta_i|1\rangle$, where $\hat{U}_y(\theta)$ $(\hat{U}_y(\theta) = \cos\theta\ \hat{I} - \mathrm{i}\sin\theta\ \hat{\sigma}_y)$ is the unitary operator which rotates the polarization angle along the $y$ axis and $\hat{\sigma}_y$ is the Pauli-$y$ operator. Alice sends these qubits to Bob.

(a.3) After receiving them, Bob rotates the polarization angles of the $n$ qubits by $\varphi_i$ to bring the states of these qubits to $|\psi\rangle_i^2 = \hat{U}_y(\varphi_i)|\psi\rangle_i^1 = \cos(\theta_i + \varphi_i)|0\rangle - \sin(\theta_i + \varphi_i)|1\rangle$ $(i = 1, 2, \ldots, n)$.

(a.4) Bob blocks these qubits and then sends these qubits to Alice with a random order. Alice announces that she had received Bob's qubits, then Bob tells Alice through a classical channel about his order of send-

*Project supported by the National Natural Science Foundation of China (Grant No 60667001).
†E-mail: szhang@ybu.edu.cn

ing qubits.

(a.5) Alice rotates the polarization of the $i$th qubit by corresponding angle $-\theta_i$ according to the information told by Bob and then encodes the messages by further rotating the polarization angles of $\pm\frac{\pi}{4}$; $|\psi\rangle_i^3 = \hat{U}_y(\pm\frac{\pi}{4}) \times \hat{U}_y(-\theta_i)|\psi\rangle_i^2$. She sends these qubits to Bob. (Alice and Bob have agreed on that $\hat{U}(+\frac{\pi}{4})|0\rangle$ represents "0", and $\hat{U}(-\frac{\pi}{4})|0\rangle$ represents "1".)

(a.6) Bob measures the polarization of the $i$th particle after rotating the polarization by $-\varphi_i$; $|\psi\rangle_i^4 = \hat{U}_y(-\varphi_i)|\psi\rangle_i^3 = \hat{U}_y(\pm\frac{\pi}{4})|\psi\rangle_i^0$. $\hat{U}_y(-\frac{\pi}{4})|\psi\rangle$ and $\hat{U}_y(+\frac{\pi}{4})|\psi\rangle$ are orthogonal to each other, which enables Bob to read the secret information by using the measurement basis $\{\hat{U}_y(+\frac{\pi}{4})|0\rangle, \hat{U}_y(-\frac{\pi}{4})|0\rangle\}$.

(a.7) Alice announces a one-way hash function $H$ via a classical channel. Alice and Bob evaluate the hash values , $h_{\rm a} = H(s_{\rm a})$ and $h'_{\rm a} = H(s'_{\rm a})$ respectively, where $s_{\rm a}$ is Alice's information and $s'_{\rm a}$ is Bob's information which is acquired from Alice. If $h_{\rm a} = h'_{\rm a}$, Bob will accept the $k$ bits information. Otherwise, they will abolish the secure information and start the process again from (a.1).

The above protocol can be generalized to a secure bidirectional quantum communication. If Alice wants to receive secret information from Bob at the same time, she will do these steps after (a.4).

(a.5') After Alice encodes her secret messages, she sends these qubits to Bob with another different order. When Bob informs her that he has received these qubits, Alice tells Bob about her transmitting order.

(a.6') Bob rotates the polarization angles of these qubits by $-\varphi_1$, $-\varphi_2$, $\cdots$, $-\varphi_n$ according to Alice's new order and by further $\pm\frac{\pi}{4}$ to encode his messages. He measures the polarization of these qubits by using the measurement basis $\{|0\rangle, |1\rangle\}$.

(a.7') After Bob publicly announces his measurement result for every qubit through a classical channel, Alice and Bob can deduce the secret messages of the other side by $m = s_{\rm a} \oplus s_{\rm b}$. ($m$ is Bob's measurement result, $s_{\rm a}$ is Alice's secret message and $s_{\rm b}$ is Bob's secret message.)

(a.8') Bob and Alice compare $H(s_{\rm a})$ with $H(s'_{\rm a})$ or $H(s_{\rm b})$ with $H(s'_{\rm b})$, where $s_{\rm b}$ is Bob's information and $s'_{\rm b}$ is Alice's information which is acquired from Bob. If $H(s_{\rm a}) = H(s'_{\rm a})$ or $H(s_{\rm b}) = H(s'_{\rm b})$, they will accept the secure information. Otherwise, they will abort these messages and communicate again from (a.1).

Let us discuss the security of the protocol. Our protocol is based on the blind polarization bases and random sequence of transmitting qubits. This ensures the security of communication. Assuming that Eve intends to get the secret information by impersonation attack, after (a.2), Eve intercepts and stores these qubits from Alice. Eve can transmit her qubits to Bob with random angles and she remembers the polarization angles of his qubits. After (a.3), Eve does not know Bob's sending order, so Eve cannot know how to send Alice's qubits back to Alice properly. Because Bob only announces his sending order after verifying that Alice has received these qubits. After (a.5), although Eve can intercept Alice's qubits, she still cannot get any useful messages. Her eavesdropping behaviour will be detected when Alice and Bob compare $H(s_{\rm a})$ and $H(s'_{\rm a})$. In the above discussions, we analyze the security of our protocol for the perfect quantum channel. In a practical quantum channel, there are noise and losses which will threaten the security of quantum communication. We will use error correction and privacy amplification technique on those qubits to improve the security. The quantum error correction technique have been proposed.[25] On the other hand, a perfect single-source is not very economical, we can use not-so weak coherent laser pulses instead of it. So Eve can split out a qubit from each pulse and keep it in the quantum storage in (a.5) by photon-number-splitting attack. But these qubits are not useful for Eve to get Alice's information. Because Eve does not know Bob's rotation angle $\varphi_i$, she cannot rotate corresponding angle $-\varphi_i$ to gain information. Altogether, Eve cannot acquire the secret information by using any eavesdropping method as long as she does not know the sending sequence. Our protocol is secure and feasible either in an ideal or weak noisy channel.

Compared with protocol,[26−28] there are some differences in this paper. We must point out that particles which carry secret messages are sent from Alice to Bob in order, but they go back from Bob to Alice are out of order. So there is no chance for Eve to get any useful information about Alice's secret messages. Our protocol improves the efficiency of communication. Alice can transmit her one bit secret information to Bob with one qubit.

In summary, we have proposed a QSDC protocol with the blind polarization bases and random transmitting order. In our protocol two legitimate users can communicate securely and no messages is leaked to Eve. This protocol is unconditionally secure and efficient either in an ideal or weak noisy channel. Moreover, our protocol can improve the efficiency of communication and be easy realized in experiment.

# References


[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computer, Systems and Signal Processing* 175

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

[3] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 3995 (in Chinese)

[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

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

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

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

[8] He G Q and Zeng G H 2006 *Chin. Phys.* **15** 1284

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

[10] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 961 (in Chinese)

[11] Zhang Q, Tang C J and Zhang S Q 2002 *Acta Phys. Sin.* **51** 1439 (in Chinese)

[12] Beige A, Englert B G, Kurtsiefer C H and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

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

[14] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601

[15] Zhang Z J, Man Z X and Li Y 2004 *Phys. Lett.* A **333** 46

[16] Zhang Z J, Man Z X and Li Y 2005 *Phys. Lett.* A **341** 385

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

[18] Zhang Z J, Man Z X and Li Y 2004 *Int. J. Quant. Inform.* **2** 521

[19] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[20] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[21] Jin X R, Ji X, Zhang Y Q and Zhang S 2006 *Phys. Lett.* A **354** 67

[22] Xia Y, Fu C B, Li F Y, Zhang S, Yeon K H and Um C I 2005 *J. Korean Phys. Soc.* **47** 753

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

[24] Ji X and Zhang S 2006 *Chin. Phys.* **15** 1418

[25] Deng F G and Long G L 2004 quant-ph/0408102

[26] Kye W H, Kim C M, Kim M S and Park Y J 2005 *Phys. Rev. Lett.* **95** 040501

[27] Zhang Q, Wang X B, Chen Y A, Yang T and Pan J W 2005 quant-ph/0508030

[28] Kye W H and Kim M S 2005 quant-ph/0508065

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