Vol 17 No 7, July 2008
1674-1056/2008/17(07)/2352-04

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Efficient quantum secure communication with a publicly known key*

Li Chun-Yan(李春燕)[a)b)c)], Li Xi-Han(李熙涵)[a)b)c)],
Deng Fu-Guo(邓富国)[a)d)†], 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*

[d)] *Department of Physics, Applied Optics Beijing Area Major Laboratory, Beijing Normal University, Beijing* 100875, *China*

(Received 23 November 2007; revised manuscript received 24 December 2007)

This paper presents a simple way for an eavesdropper to eavesdrop freely the secret message in the experimental realization of quantum communication protocol proposed by Beige *et al* (2002 *Acta Phys. Pol.* A **101** 357). Moreover, it introduces an efficient quantum secure communication protocol based on a publicly known key with decoy photons and two biased bases by modifying the original protocol. The total efficiency of this new protocol is double that of the original one. With a low noise quantum channel, this protocol can be used for transmitting a secret message. At present, this protocol is good for generating a private key efficiently.

Keywords: quantum communication, quantum cryptography
PACC: 0367

Quantum communication supplies some interesting ways for secure transmission of message. For example, quantum key distribution (QKD),[1] the most mature branch of quantum communication, provides a secure way for two remote users, say Alice and Bob, to create a private key. The non-cloning theorem forbids a vicious eavesdropper, say Eve, to steal the information freely. Eve's action will inevitably leave a trace in the outcome obtained by the two legitimate users with two conjugate measuring bases (MBs). Quantum secure direct communication (QSDC), a novel branch of quantum communication, was proposed and actively pursued by some groups.[2−23] With QSDC the two legitimate users can communicate their secret message directly without creating a private key in advance. In 2003, Deng, Long and Liu[2] proposed the first secure quantum direct communication (QDC) protocol with Einstein–Podolsky–Rosen (EPR) pair block. In 2004, Deng and Long[3] introduced another secure scheme for QDC with single photons. Moreover, the criteria for a really secure QDC are introduced in these two works[2,3] and are described in detail in Ref.[4]. In 2005, Wang *et al* put forward a secure QDC scheme[5] with high-dimensional quantum systems and quantum superdense coding, and they also presented a QSDC scheme[6] with Greenberger–Horne–Zeilinger (GHZ) states. In 2006, Li *et al*[7] proposed a QSDC scheme with quantum encryption based on pure entangled states. Now, QSDC has also been studied in the case of a network[4,8,9] and in the case between a centre and some parties.[10]

In essence, the schemes in Refs.[11–22] are all used for deterministic secure quantum communication (DSQC).[11] The difference between QSDC and DSQC is that the secret message can be read out only when the two parties transmit at least one bit of classical information for each qubit in the latter.[2,3,11] DSQC is similar to a class of QKD protocols[24] which can be used to obtain deterministic information,[11] not a random binary string. This may be the crucial difference between DSQC and the traditional QKD protocols[1] in which the users cannot predict whether an instance is useful or not. DSQC has some advantages in the case with a low noise channel.[11] Reference [23] is

*Project supported by the National Natural Science Foundation of China (Grant No 10604008), Foundation for the Author of National Excellent Doctoral Dissertation of China (Grant No 200723), and Beijing Education Committee of China (Grant No XK100270454).

†E-mail: fgdeng@bnu.edu.cn

a review article about QSDC and DSQC. First, it may be more secure than the two-way quantum communication as the legitimate users do not transmit the qubits that carry the secret message through the noisy channel again. Secondly, DSQC schemes are more convenient for quantum error correction than others. Moreover, the attenuation of quantum signals in DSQC is less than that in two-way quantum communication protocols. In 2002, an original DSQC protocol was proposed by Beige *et al* [12] with a two-qubit state, two degrees of a quantum system, i.e., the spatial degree of freedom and the polarization degree of freedom. In 2005, Yan *et al* [13] and Man *et al* [14] proposed several DSQC schemes with quantum teleportation and entanglement swapping. In 2006, a DSQC scheme with pure entangled states and another scheme with d-dimensional single photons were proposed.[11] These two DSQC schemes are optimal and more convenient than others[12−22] at the aspect of quantum signal preparation and measurement.

In this paper, we first analyse the security of the DSQC protocol proposed by Beige *et al* (let us call it Beige protocol).[12] Then it will show that the proposal for an experimental realization of Beige protocol is insecure and an eavesdropper Eve can obtain all the secret message with quantum teleportation freely. Moreover, we will introduce an efficient secure quantum communication protocol based on a publicly known key with the decoy-photon technique.[25,26] This protocol can be used to transmit secret message efficiently if the noise in the quantum channel is very low. With present technology, this protocol can be used to distribute a private key with a high efficiency and a high capacity.

Now, let us start with the brief description of the Beige protocol[12] below.

In the Beige protocol, the sender Alice prepares the quantum carriers (single photons) in the states $|n_{\pm}\rangle$, where n label different types of states. If Alice wants to transmit a '+' bit (for instance the binary number '0'), she prepares the photons in the states $|n_{+}\rangle$. In order to transmit a '−' bit (for instance the binary number '1') Alice prepares the state $|n_{-}\rangle$.

$$\sum_n |n_+\rangle\langle n_+| = \sum_n |n_-\rangle\langle n_-|. \tag{1}$$

When photons arrive at the receiver Bob's end, he chooses at least two different MBs to measure the single photon, say $|B_n\rangle$ and $|C_n\rangle$. In the concrete scheme in Ref.[12]

$$|n_+\rangle \equiv |B_n\rangle, \qquad |n_-\rangle \equiv |C_n\rangle. \tag{2}$$

To assure that Bob always knows how to interpret his measurement result there should be no overlap between basis states with the same index n,[12] i.e.

$$\langle B_n|C_n\rangle = 0, \tag{3}$$

and

$$(|C_1\rangle, |C_2\rangle, |C_3\rangle, |C_4\rangle) = (|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle)\ \boldsymbol{A}, \tag{4}$$

where

$$\boldsymbol{A} = \mathrm{i}\begin{pmatrix} 0 & a_1 & a_2 & a_3 \\ -a_1 & 0 & a_3 & -a_2 \\ -a_2 & -a_3 & 0 & a_1 \\ -a_3 & a_2 & -a_1 & 0 \end{pmatrix}, \tag{5}$$

$$a_1^2 + a_2^2 + a_3^2 = 1, \tag{6}$$

and

$$a_1 a_2 a_3 \neq 0. \tag{7}$$

We use the experimental realization of Beige protocol to demonstrate its principle below, shown in

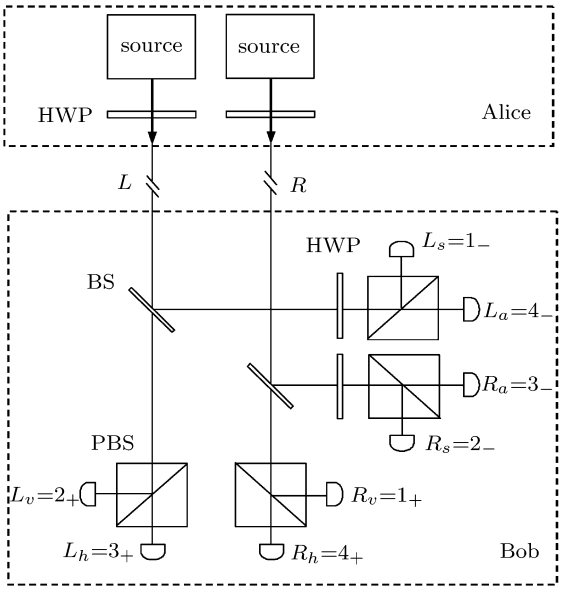


Fig.1. The proposal for an experimental realization of Beige protocol shown in Ref.[12]. BS: beam splitter; PBS: polarization beam splitter; HWP: half-wave plate.

Fig.1. Alice uses two MBs $(|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle) = (|R_v\rangle, |L_v\rangle, |L_h\rangle, |R_h\rangle)$ and $(|C_1\rangle, |C_2\rangle, |C_3\rangle, |C_4\rangle) = \mathrm{i}(-|L_s\rangle, |R_s\rangle, |R_a\rangle, -|L_a\rangle)$ to prepare her quantum signals. Here $|R\rangle$ and $|L\rangle$ represent the right path and the left path through which a quantum signal is transmitted, respectively. $|h\rangle$ and $|v\rangle$ are the horizontal and vertical polarization states of the photons, respectively. $|s\rangle$ and $|a\rangle$ are the two superposition states of $|h\rangle$ and $|v\rangle$, i.e., $|s\rangle = \frac{1}{\sqrt{2}}(|v\rangle + |h\rangle)$ and $|a\rangle = \frac{1}{\sqrt{2}}(|v\rangle - |h\rangle)$. If Alice wants to send the bit '+'

('–') to Bob, she prepares her photon randomly in one of the four states with the basis B (C) and then sends it to Bob. Bob chooses randomly one of the two bases $\{B, C\}$ to measure the photon received. After Alice publishes the number n, Bob can deduce that Alice's basis is B or C, according to his measurement outcome. For example, if Alice prepares a photon in the state $|R_v\rangle$ which represents the bit +, Bob will get the outcomes 1_+, 2_- and 3_- with the probabilities 50%, 25% and 25%, respectively. After Alice tells Bob the number of the state of the photon is 1, Bob can read out the message + sent by Alice in a deterministic way.

The authors in Ref.[12] did not consider the simple case: an eavesdropper can determine which path a photon passes through, without destroying the photon polarization state in their experimental protocol. In fact, the photon sent by Alice is in the eigenvector of its spatial degree of freedom, which means that the information of the path of the photon can be read out with quantum non-demolition measurement. A simple way to eavesdrop the message freely is using the quantum teleportation.[27] In detail, the eavesdropper Eve can first prepare an EPR pair $|\phi\rangle_{\rm BC} = \frac{1}{\sqrt{2}}(|h\rangle_{\rm B}|h\rangle_{\rm C} + |v\rangle_{\rm B}|v\rangle_{\rm C})$ and then intercept the photon A sent by Alice. Eve performs a Bell-state measurement on the photons A and B. If she obtains an useful outcome of Bell-state measurement, Eve can determine that there is a photon in the path (R or L). Then she can perform unitary operation on the photon C, same as the process in teleportation,[27] and send it to Bob. Eve can in principle easily determine the spatial degree of freedom of the photon sent by Alice. After Alice publishes the information of the number of the state n, Eve can determine which state the photon is in. That is, Eve can obtain the secret message fully and freely.

The generic communication scheme in Ref.[12] is secure in principle, but it has the disadvantage that its total efficiency $\eta_{\rm t} = \frac{q_{\rm u}}{q_{\rm t} + b_{\rm t}}$ is low, less than 25%. Here $q_{\rm u}$, $q_{\rm t}$ and $b_{\rm t}$ are the numbers of the useful qubits, the total qubits used, and the total classical bits exchanged for reading out the message, respectively. In Beige protocol, $q_{\rm u} = 1$, $q_{\rm t} = 2$ and $b_{\rm t} = 2$, so its total efficiency $\eta_{\rm t} = 25\%$ in theory.

Now, let us present a way to improve the total efficiency of the Beige protocol. As discussed in Refs.[11, 25, 26, 28], the two legitimate users need only use a fraction of their outcomes chosen randomly to analyse the security of their quantum communication, not all the outcomes. As the samples chosen for checking eavesdropping are random for Eve, her action will inevitably leave a trace in the samples. In order to improve the efficiency for qubits $\eta_q \equiv \frac{q_{\rm u}}{q_{\rm t}}$ in the Beige protocol, we can use some decoy photons[25,26] to prevent Eve from eavesdropping freely. In detail, the modified version of the Beige protocol can be described as follows.

(1) Alice prepares a sequence of single photons S which are randomly in one of the four states $\{|R_v\rangle, |L_v\rangle, |L_h\rangle, |R_h\rangle\}$. Alice encodes her message on the photons with the unitary operations $U_1 = I^1 \otimes I^2$, $U_2 = I^1 \otimes \sigma_x^2$, $U_3 = \sigma_x^1 \otimes I^2$, and $U_4 = \sigma_x^1 \otimes \sigma_x^2$ which represent the bits 00, 01, 10, and 11, respectively. Here I means doing nothing, σ_x^1 means flipping the eigenvectors of the spatial freedom, and σ_x^2 means flipping the eigenvectors of the polarization freedom.

(2) Alice prepares some decoy photons $S_{\rm d}$ with the two bases $B = \{|B_1\rangle = |R_v\rangle, |B_2\rangle = |L_v\rangle, |B_3\rangle = |L_h\rangle, |B_4\rangle = |R_h\rangle\}$ and $C' = B\boldsymbol{A'}$. Here

$$A' = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 1 & -1 & 0 \end{pmatrix}. \tag{8}$$

Alice can choose the basis C' with a large probability $1 - p$ to prepare her decoy photons and the basis B with a small probability p. Alice inserts her decoy photons $S_{\rm d}$ into the message sequence S randomly, and then sends all the photons to Bob.

(3) Bob measures the photons received with the basis B by using the large probability $1 - p$ and the basis C' by using the small probability p.

(4) Alice tells Bob which photons are the decoy ones and their states. Bob analyses the error rate of the samples. Different from Refs.[25, 26], the decoy photons all are obviously useful for checking eavesdropping no matter what bases are chosen for preparing the photons.

(5) If Alice and Bob confirm that their quantum communication is secure, Bob tells Alice which photons he has chosen the basis B and keeps these outcomes; otherwise, they discard their outcomes and repeat their quantum communication from the beginning.

(6) Alice tells Bob the original states of the photons kept.

(7) Bob reads out the information about Alice's operations, i.e. the secret message.

In essence, this new quantum secure communication protocol is the revised version of the Beige protocol with decoy photons and biased bases. Just these revisions make the total efficiency be doubled. As the probability p is small, Bob can obtain an useful outcome with a large probability $1-p$ when he measures the message photons. Moreover, each photon can carry two bits of secret message, i.e. $q_{\rm u}=q_{\rm t}=2$. For reading out the message, Alice and Bob should at least exchange two bits of classical information, i.e. $b_{\rm t}=2$ and $\eta_{\rm t}=\dfrac{q_{\rm u}}{q_{\rm t}+b_{\rm t}}=\dfrac{2}{2+2}=50\%$.

In the case with a low noise quantum channel, this scheme can be used for transmitting secret message efficiently. As the eavesdropping done by Eve will inevitably disturb the quantum states of the samples and Alice publishes the original states of the photons kept for transmitting secret message only after Alice and Bob confirm the fact that their quantum channel is secure, this scheme is secure in principle with single-qubit quantum privacy amplification.[29] With present technology,[30] we should take the influence of the noise on the quantum states into account, which means that this scheme is good for generating a private key, not for transmitting secret message directly.

In summary, we have discussed the security of the proposal for an experimental realization of Beige protocol. It can be eavesdropped freely in principle by an eavesdropper with quantum teleportation. Also, we have proposed an efficient quantum secure communication protocol based on a publicly known key with decoy photons and two biased bases by modifying the Beige protocol. The total efficiency of this new protocol is double of that of the original one. This protocol can be used to transmit secret message directly if the noise in the quantum channel is very low. With present technology, this protocol is good for generating a private key.

References

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

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

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

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

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

[6] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

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

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

[9] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Phys. Scr.* **76** 25
Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Chin. Phys.* **16** 3553

[10] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473

[11] 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

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

[13] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41** 75
Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761

[14] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
Man Z X and Xia Y J 2007 *Chin. Phys.* **16** 1197

[15] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290

[16] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
Song J, Zhu A D and Zhang S 2007 *Chin. Phys.* **16** 621

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

[18] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[19] Xia Y and Song H S 2007 *Phys. Lett.* A **364** 117
Xia Y, Fu C B, Zhang S, Hong S K, Yeon K H and Um C I 2006 *J. Korean Phys. Soc.* **48** 24

[20] Wang J, Zhang Q and Tang C J 2007 *Commun. Theor. Phys.* **48** 637
Wang J, Chen H Q, Zhang Q and Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese)

[21] Wang G Y, Fang X M and Tan X H 2006 *Chin. Phys. Lett.* **23** 2658

[22] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 1838

[23] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. China* **2** 251

[24] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097
Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311
Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[25] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

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

[27] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wooters W K 1993 *Phys. Rev. Lett.* **70** 1895

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

[29] Deng F G and Long G L 2006 *Commun. Theor. Phys.* **46** 443

[30] Li X H, Deng F G and Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101