Vol 16 No 2, February 2007
1009-1963/2007/16(02)/0277-05

Chinese Physics

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

Eavesdropping on the 'ping-pong' quantum communication protocol freely in a noise channel*

Deng Fu-Guo(邓富国)[a)b)c)†], Li Xi-Han(李熙涵)[a)b)],
Li Chun-Yan(李春燕)[a)b)], Zhou Ping(周 萍)[a)b)], 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 15 May 2006; revised manuscript received 14 June 2006)

We introduce an attack scheme for eavesdropping freely the ping-pong quantum communication protocol proposed by Boström and Felbinger [*Phys. Rev. Lett.* **89**, 187902 (2002)] in a noise channel. The vicious eavesdropper, Eve, intercepts and measures the travel photon transmitted between the sender and the receiver. Then she replaces the quantum signal with a multi-photon signal in the same state, and measures the returned photons with the measuring basis, with which Eve prepares the fake signal except for one photon. This attack increases neither the quantum channel losses nor the error rate in the sampling instances for eavesdropping check. It works for eavesdropping the secret message transmitted with the ping-pong protocol. Finally, we propose a way for improving the security of the ping-pong protocol.

Keywords: quantum communication, ping-pong protocol, eavesdropping
PACC: 0155, 0365B

Quantum mechanics offers some unique capabilities for the processing of information, such as quantum computation and quantum communication.[1] Quantum cryptography, one of the most mature quantum techniques, provides a novel way of transmitting the message securely. Since Bennett and Brassard proposed the original quantum key distribution (QKD) protocol in 1984, many works have been focused on this topic, such as Refs.[2–12]. In QKD, the two parties, say the sender, Alice and the receiver, Bob, can create a random binary string with quantum channel unconditionally secure.[1] The no-cloning theorem[13] forbids any eavesdropper to eavesdrop an unknown quantum state without disturbing it. In fact, QKD is secure as the authorized users can find out the eavesdropping done by Eve if she wants to steal the quantum information, and then they discard the string which does not reveal the secret message.

Recently, a novel concept, quantum secure direct communication (QSDC), has been proposed and actively pursued.[14−28] Also, it is extended to the controlled teleportation.[29] With QSDC, the secret message is transmitted directly without first creating a random key to encrypt it, which is different from QKD whose object is just to establish a common random key between two remote parties. As the secret message cannot be altered by the two authorized users when it has been transmitted in the quantum channel, the security of QSDC depends on the fact that Eve can only have a random outcome if she monitors the line.[15−17] Moreover, Alice and Bob can detect the eavesdropping if Eve monitors the quantum line before they code the message in the quantum states. So far, almost all the existing QSDC protocols can be attributed to one of the two types. The first one includes the QSDC protocols in which the secret message can be read out directly without exchanging an additional classical information for each qubit except for the sampling qubits for eavesdropping check, such as those in Refs.[14–20]. The other one includes those protocols in which each qubit can be read out by the legitimate user after at least a bit of classical information is exchanged.[21−25] An interesting feature of the QSDC protocols in Refs.[15–17] is that the quan-

*Project supported by the National Natural Science Foundation of China (Grant No 10604008) and the Beijing Education Committee (Grant No XK100270454).

†E-mail: fgdeng@bnu.edu.cn

tum states are transmitted in a quantum data block and the two legitimate users can maintain its security with error correction and quantum privacy in a noise channel.

The well-known ping-pong QSDC protocol proposed by Boström and Felbinger[14] has been claimed to be secure for establishing a random key and quasisecure for transmitting a plain text message (a secret message) as Eve is able to gain a small amount of message information before being detected. Recently, the ping-pong protocol has proven insecure if the quantum channel losses are high enough,[30−32] even for distributing a common random key. Also it can be attacked without eavesdropping.[33,34] In this paper, we will show that the ping-pong protocol can be eavesdropped freely if the error rate introduced by the quantum channel noise is not zero, without requiring that the loss of the quantum channel is high. Moreover, we introduce a way of improving its security in a noise channel.

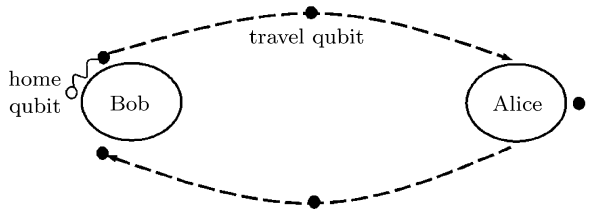


Fig.1. Schematic diagram of the ping-pong QSDC protocol, similar to Fig.1 in Ref.[17]. Alice is the sender of the message, and Bob is the receiver.

In the ping-pong QSDC protocol[14] as shown in Fig.1, the message receiver Bob prepares the quantum source, an Einstein–Podolsky–Rosen (EPR) pair. An EPR pair is in one of the four Bell states shown as follows:[1]

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle),$$
$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle), \quad (1)$$

where $|0\rangle$ and $|1\rangle$ are the horizontally and vertically polarized states of a single photon, respectively. The two photons in each EPR pair prepared by Bob are in the maximal entangled state $|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\rm H}|1\rangle_{\rm T} + |1\rangle_{\rm H}|0\rangle_{\rm T})$. Here H and T represent the home qubit and the travel qubit,[14] respectively. Using the quantum dense coding,[35] Bob keeps the qubit H and sends the qubit T to Alice. Alice chooses two modes, the control mode and the message mode, in dealing with the T qubit at a probability c for picking up the control mode for the photon and $1-c$ for coding the message. When she chooses the control mode, Alice performs a single-photon measurement on the T qubit with the horizontal–vertical measuring basis (MB), say σ_z, otherwise she codes the photon with $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ when the messages are 0 and 1, respectively,

$$(Z \otimes I)|\psi^{+}\rangle = |\psi^{-}\rangle. \quad (2)$$

Cai[18] introduced an attack way without eavesdropping. In Cai's eavesdropping scheme, Eve measures the T photon with the MB σ_z. This attack cannot be detected if Alice and Bob only take the MB σ_z in their sampling photons. In an ideal channel without noise and loss, this attack cannot obtain the information about the secret message. However, we have to confess that there are noises in a practical quantum channel, which will introduce an error rate ε_c in the outcomes.[1,2] With the improvement of technology, ε_c can be small, but not zero. Moreover, a single-photon detector has a special recovery time (i.e. the dead time)[2] in which the N photons attained are recorded as just one. Eve can exploit the error rate ε_c and the recovery time to hide her eavesdropping on the ping-pong protocol and gain almost all the information about the secret message with a multi-photon fake signal even though the quantum channel loss is low. We introduce it in detail as follows, similar to the Trojan horse attack in Refs.[2,36].

For the eavesdropping, Eve first intercepts and measures the T photon with MB σ_z, and then she prepares an N-photon fake signal with the MB σ_θ whose two eigenstates can be written as

$$|+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,$$
$$|-\theta\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle, \quad (3)$$

where $\theta \in \left[0, \frac{\pi}{2}\right)$ and

$$\sin^2\theta \leq \varepsilon_c. \quad (4)$$

When the outcome of the measurement is $|0\rangle_{\rm T}$, Eve prepares the N-photon fake signal in the same state $|+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ shown in Fig.2, and resends it to Alice in a time slot, shorter than the recovery time of the single-photon detector. In its dead time, Alice's detector only records a single photon when Alice measures the signal by choosing the control mode with the MB σ_z. In this way, Eve's eavesdropping will introduce the error rate $\varepsilon_{\rm E} = \sin^2\theta$ in the sampling instances between Alice and Bob. Eve can use a better

quantum channel with which the error rate is by far lower than the original one to hide her eavesdropping freely.

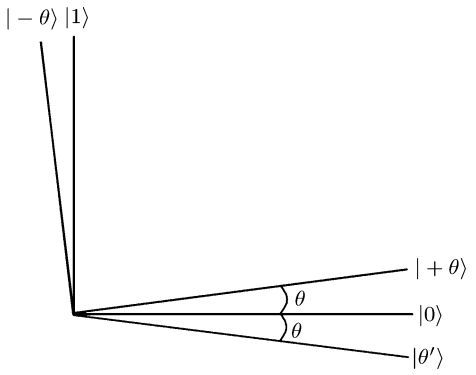


Fig.2. The state of the multi-photon fake signal. $|+\theta\rangle$ and $|-\theta\rangle$ are the two eigenstates of the measuring basis σ_θ.

As an example for demonstrating the principle of this attack, we assume that $\varepsilon_c = 10\%$ and Eve uses an ideal quantum channel to steal the message. Owing to the symmetry, we assume that there are $N = 2^m$ photons in the fake signal.

$$\varepsilon_{\rm E} = \sin^2\theta = \varepsilon_c = 0.1. \tag{5}$$

After the coding done by Bob with one of the two local unitary operations I and Z, Eve intercepts the fake signal again. She splits the multi-photon signal with some photon number splitters (PNS: 50/50), and sends one photon to Bob and measures the other photons (see in Fig.3).

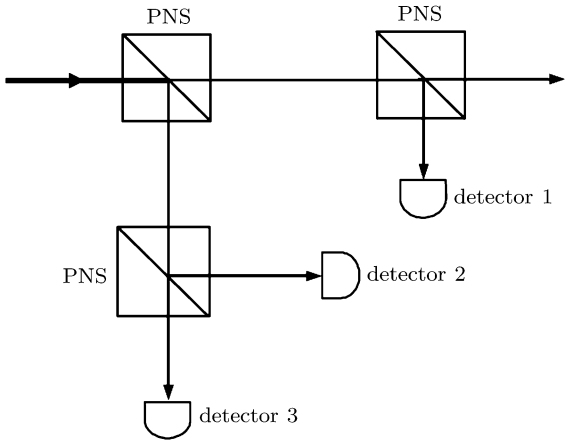


Fig.3. The attack with the photon number splitters (PNS: 50/50) in the case that there are four photons in each fake signal.

If Alice performs the I operation on the fake signal, the photons in the fake signal are in the state $|T'\rangle = |+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$; otherwise $|T'\rangle = |\theta'\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$. The attack for obtaining the information about the local unitary operations done by Alice is simplified into distinguishing those two states. It is impossible for Eve to gain almost all the information about Alice's operation if she has only one photon coded by Alice as $|\langle\theta'|+\theta\rangle|^2 = \cos^2 2\theta = 0.64$. But the story is changed if there are many photons in each fake signal. Eve can distinguish those two states with a large probability and then steal almost all of the message freely.

Figure 3 gives an example for Eve to eavesdrop the message with four photons in each fake signal. Eve splits the fake signal with three PNS when the signal returns from Alice to Bob. She sends one of the four photons to Bob and measures the other three photons with the MB σ_θ (see Fig.2). If the three photons are all in state $|+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, i.e. Alice performs the identity operation I on the fake signal, Eve has the outcome $|+\theta\rangle$ with the probability 100%; otherwise Eve has the probability $(\cos^2 2\theta)^{n-1} = (0.64)^3 = 0.262144$ to obtain the state $|+\theta\rangle$ for her measurements on all the three photons. That is, Eve has the probability $P_{\rm F} = 0.262144$ at which she will fail to distinguish the two operations done by Alice on the fake signal. If there are N photons with which Eve distinguishes the two states $|+\theta\rangle$ and $|\theta'\rangle$, the probability at which Eve will fail is reduced to $P_{\rm F} = (\cos^2 2\theta)^{n-1} = (0.64)^{n-1}$. When $n = 64$, $P_{\rm F} \cong 6.16 \times 10^{-13}$. It means that Eve can obtain the message fully if there are a large number of photons in each fake signal because this attack increases neither the signal losses nor the error rate in the sampling instances.

In essence, the security issue in ping-pong QSDC protocol[14] arises from the fact that the two authorized users transmit the qubits one by one and check the eavesdropping only with the same MB σ_z. The secret message transmitted cannot be discarded, different from the outcomes in QKD.[2] For improving its security, it is necessary for Alice and Bob to transmit the qubits in a quantum data block, similar to what is done in Refs.[15–17], and measure the sampling instances with two MBs σ_z and σ_x. Here $\sigma_x = \left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$. As the eavesdropping check depends on the public statistical analysis of the sampling instances, the transmission of the

quantum data block ensures that the message is coded after the verification process is accomplished. Moreover, the two parties can perform quantum privacy amplification on the quantum data[15−17] before Alice codes her message in the quantum states. These two interesting characters play an important role in the security of QSDC protocols.

With the two MBs for the sampling instances, the action done by the eavesdropper, Eve, will leave a trace in the results and will be detected. Moreover, this modification can improve the capacity in the ping-pong QSDC protocol as discussed in Ref.[37]. For most of the existing QSDC protocols, there is a probability at which Eve can obtain a part of the message if she eavesdrops the quantum channel with a Trojan horse attack strategy[2] and replaces the original quantum channel with an ideal one. In the QSDC protocols,[15−17] the parties can reduce the information leaked to Eve to a negligible value with quantum privacy amplification.[2,15,16] Also, Alice and Bob can prevent Eve from eavesdropping with this attack if they use some PNS to monitor the sampling instances. That is, they split the signal with some PNS and measure them individually by choosing the MB σ_z and σ_x randomly, similar to what is done in Ref.[36]. This strategy for eavesdropping check can also be used to improve the security in the QKD protocol[5] and the secure deterministic communication protocol[38] proposed by Lucamarini and Mancini following the ideas in Refs.[5,16]. In a practical application, the users can also use some photon beam splitters to replace the PNSs.

In conclusion we have presented an attack strategy on the ping-pong QSDC protocol freely in a noise quantum channel. This attack works for obtaining the secret message transmitted with the ping-pong protocol.[14] The eavesdropper, Eve can intercept the signal transmitted between Alice and Bob and measures it first, and then she replaces it with a multi-photon fake signal. Eve's eavesdropping can be hidden by the error rate introduced by the noise in the practical quantum channel and the dead time of a detector. She can obtain almost all the information about the message with some photon number splitters and measurements along some direction. We have also suggested the way of improving the security of the ping-pong protocol and introduce a way to prevent the eavesdropper from stealing the information with the Trojan horse attack strategy.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum computation and quantum information* (Cambridge: Cambridge University Press)

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

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

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

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

[6] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

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

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

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

[10] Wu G, Zhou C Y, Chen X L, Han X H and Zeng H P 2005 *Acta Phys. Sin.* **54** 3622

[11] Ma H Q, Li Y L, Zhao H and Wu L A 2005 *Acta Phys. Sin.* **54** 5014

[12] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 5544

[13] Wootters W K and Zurek W H 1982 *Nature* (London) **299** 802

[14] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

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

[16] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
Deng F G and Long G L 2006 *Commun. Theor. Phys.* **46** 443

[17] 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

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

[19] Nguyen B A 2004 *Phys. Lett.* A **328** 6

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

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

[22] Yan F L and Zhang X 2004 *Euro. Phys. J.* B **41** 75

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

[24] Gao T 2004 *Z. Naturforsch.* A **59** 597 (2004)
Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento* B **119** 313
Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761

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

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

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

[28] 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

[29] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338
Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys.* B **39** 1975
Deng F, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Euro. Phys. J.* D **39** 459
Yang J 2005 *Chin. Phys.* **14** 2149

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

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

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

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

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

[35] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[36] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[37] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[38] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501