Improving the security of secure direct communication based on secret transmitting order of particles

Xi-Han Li,[1,2] Fu-Guo Deng,[1,2,3*] and Hong-Yu Zhou[1,2,3]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, People's Republic of China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, People's Republic of China*
[3] *Beijing Radiation Center, Beijing 100875, People's Republic of China*

(Dated: December 5, 2006)

We analyzed the security of the secure direct communication protocol based on secret transmitting order of particles recently proposed by Zhu, Xia, Fan, and Zhang [Phys. Rev. A **73**, 022338 (2006)], and found that this scheme is insecure if an eavesdropper, say Eve, wants to steal the secret message with Trojan horse attack strategies. The vital loophole in this scheme is that the two authorized users check the security of their quantum channel only once. Eve can insert another spy photon, an invisible photon or a delay one in each photon which the sender Alice sends to the receiver Bob, and capture the spy photon when it returns from Bob to Alice. After the authorized users check the security, Eve can obtain the secret message according to the information about the transmitting order published by Bob. Finally, we present a possible improvement of this protocol.

PACS numbers: 03.67.Hk, 03.65.Ud

I. INTRODUCTION

Since an original quantum key distribution (QKD) scheme was proposed by Bennett and Brassard [1] in 1984 (BB84), quantum communication has progressed quickly. There are several remarkable branches of quantum communication, such as QKD [2, 3, 4, 5, 6, 7, 8], quantum secret sharing [9, 10, 11], quantum secure direct communication (QSDC), and so on. QKD whose task is to create a private key between two remote authorized users is one of the most important applications of quantum mechanics in the field of information. By far, there has been a lot of attention focused on QKD [2, 3, 4, 5, 6, 7, 8].

QSDC is a new branch of quantum communication and is used to transmit a secret message directly without creating a private key in advance [12, 13, 14, 15, 16]. In 2002, Boström and Felbinger proposed a quasi-secure quantum direct communication protocol, called "ping-pong" protocol [15]. They used Einstein-Podolsky-Rosen (EPR) pairs as quantum information carriers (QIC), following some ideas in quantum dense coding [17]. However, it has been proved insecure in a noise channel [18]. In 2003, Deng *et al.* put forward a two-step QSDC protocol using a block of EPR pairs [12] and another one with a sequence of single photons [13]. Wang *et al.* [14] introduced a high-dimension QSDC scheme.

Another class of quantum communication has been called deterministic secure quantum communication (DSQC) [19] in which the receiver can read out the secret message only after the transmission of an additional classical bit for each qubit, different from QSDC in which the secret message can be read out directly without exchanging classical information anymore. Compared with QKD, DSQC can be used to obtain a deterministic information, other than a random binary string. Recently, Gao *et al.* [20, 21] and Man *et al.* [22] proposed several DSQC protocols based on quantum teleportation [23] and entanglement swapping [24]. Although the users have to exchange a lot of classical information to obtain the secret message, they can check the eavesdropping before they transmit the secret message, and the qubits which carry the secret message need not be transmitted again after the users check eavesdropping. Therefore these schemes may be more secure in a noise channel and more convenient for quantum error correction [19].

Recently, Zhu *et al.* [25] proposed a new secure direct communication protocol using EPR pairs as QIC (We called it ZXFZ protocol for short below), similar to the two-step QSDC protocol [12]. The transmitting order of particles is secret to any other people except for the sender, and the most important advantage emphasized is that this protocol only needs one security checking process. However, we found this scheme is insecure just due to lack of sufficient security-checking processes. We can use the Trojan horse attack strategy [5] to get the secret message completely without leaving a trace. In this paper, we first review the protocol they proposed and then introduce the way to eavesdrop it freely. Finally, we present a possible improvement of this secure direct communication scheme.

II. EAVESDROPPING ON THE SECURE DIRECT COMMUNICATION PROTOCOL

It is well known that a crucial issue of secret communication is its security. The security of quantum communication is guaranteed by the principles in quantum me-

---

*Email address: fgdeng@bnu.edu.cn

chanics against an eavesdropper with unlimited powers, whose technology is confined only by the laws of quantum mechanics. For QSDC or DSQC protocols, their security is more important than that in QKD protocols because they are used to transmit a secret message, other than a private key.

Now, let us start with the brief description of the ZXFZ protocol [25]. First, Alice and Bob agree that the four unitary operations $U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|$, $U_2 = |0\rangle\langle 1| + |1\rangle\langle 0|$, and $U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|$ represent two bits of classical information 00, 11, 10, and 10, respectively. Alice prepares a sequence of EPR pairs in one of the four Bell states, say $|\Psi\rangle_i = \frac{1}{\sqrt{2}}(|0\rangle_{H_i}|1\rangle_{T_i} - |1\rangle_{H_i}|0\rangle_{T_i})$, and then divides them into two parter-photon sequences. She keeps one sequence (home sequence) in her laboratory and sends the other sequence (travel sequence) to Bob through a quantum channel. After receiving the travel sequence, Bob chooses a sufficiently large subset of photons as a checking set (C set) and the rest as a message set (M set). Bob encodes his checking message and secret message by performing the four unitary operations U_i $(i = 0, 1, 2, 3)$ on the C set and the M set respectively. Then Bob rearranges the order of the T sequence and returns them to Alice. After Alice claims her receipt of all the T sequence, Bob announces the position of the C set and the secret order in it. Alice performs the Bell-state measurements on the checking photons and publishes the results. Bob can distinguish whether there is an eavesdropper monitoring their quantum line by comparing his checking message with Alice's outcomes. If there exists an eavesdropper, Bob terminates the communication. Otherwise, he exposes the secret order of the M set, and then Alice can obtain the secret message with Bell-state measurements.

The security of the ZXFZ scheme [25] is based on the secret order of the particles. However, the secret order will be published by Bob after the security checking. One can see that the two authorized users only check the security once in the line from Bob to Alice. The secret message is encoded with the unitary operations done by Bob. If Alice and Bob cannot detect the eavesdropper during the checking process, Eve can get the secret order and the whole secret message. The eavesdropper can utilize the loophole that the users do not check the security of the quantum channel from Alice to Bob to insert some additive photons in each legitimate one to get Bob's operation information freely. There are two kinds of Trojan horse attack strategies. One is the invisible photon eavesdropping (IPE) scheme proposed by Cai [26] and the other is the delay-photon Trojan horse attack [5, 27].

Firstly, the invisible photon eavesdropping scheme utilizes the fact that the single photon detector is only sensitive to the photons with a special wavelength [26]. Therefore, Eve can select a wavelength far away from that the authorized users use, which is invisible to Bob's detector. But there exist some problems if Eve uses the IPE to attack the quantum communication protocols in which the wavelength-dependent optical devices are used to code the useful information. That is, Eve maybe obtain nothing about the information of the operations done by the legitimate users with optical devices (such as $\lambda/2$ and $\lambda/4$ plates) if the wavelength of the invisible photon is far away from that used by the users. However, it is worthy to point out that no security checking is performed in the line from Alice to Bob, which is a serious security loophole of the ZXFZ protocol [25]. Eve can choose a special wavelength which is close to the legitimate wavelength to produce the invisible photons. As we assumed [5, 18], Eve has absolutely no technological limits for her eavesdropping; i.e., she can do everything that quantum mechanics does not explicitly forbid. Since the number of photons and the polarization of a photon are commutative, Eve can insert a spy photon in each signal pulse and sort it out without disturbing the state of the travel photon of Alice's in principle. Now we analyze the attack scheme in detail. First, the eavesdropper Eve prepares a sequence of EPR pairs with the wavelength λ' (The legitimate wavelength is λ, $\lambda' \approx \lambda$. Eve can distinguish them in principle even though there may be no those devices existing at present.) also in the state $|\Psi'\rangle_{i'} = \frac{1}{\sqrt{2}}(|0\rangle_{H_{i'}}|1\rangle_{T_{i'}} - |1\rangle_{H_{i'}}|0\rangle_{T_{i'}})$. When Alice sends the T sequence to Bob, Eve adds her T' sequence to the T sequence and forwards them to Bob. In detail, Eve inserts each photon T' into the photon T's pulse. When Bob performs his unitary operation on the T sequence, he also performs his operation on the T' sequence Eve sent. After Bob rearranges the order of the T sequence, Eve captures her spy photons when they run back from Bob to Alice, and stores them. It is important to point out that all of the operations Eve does have no effect on the secret order and the secret states of the Alice's T sequence. Since the optical devices used to accomplish the unitary operations are often wavelength-dependent in practical, the information carried by Eve's additional sequence T' is not as exactly same as the photon sequence T in the line from Bob to Alice. However, since λ' is close to λ, the probability that Eve obtain the correct outcome with her Bell-state measurements is close to 1. In other words, almost all the information about the secret message will be leaked to Eve without being detected. After Alice and Bob accomplish the security checking, Eve can rearrange the sequence order according to the information published by Bob, and do the same measurements as Alice to obtain Bob's secret message with a large probability in principle.

Secondly, the delay-photon Trojan horse attack [27] is inserting a spy photon in a legitimate signal with a delay time, shorter than the time windows. As we know, in experiment there is a "door" (a time window) of the optical device which is open only during a short time, i.e., only when the qubits arrive. In order to limit the Trojan horse attack, the door should be open only during a time as short as possible [28]. However, in practice, timing has a finite accuracy, the eavesdropper Eve with a infinite power can add her probes before or after the legitimate pulses. Different from the IPE attack, the delay spy photon has the same wavelength as the legitimate photon. Therefore the spy photon sequence T'' will carry the same information as the legitimate T sequence. Eve can prepare the EPR pair sequence in the same state $|\Psi''\rangle_{i''} = \frac{1}{\sqrt{2}}(|0\rangle_{H_{i''}}|1\rangle_{T_{i''}} - |1\rangle_{H_{i''}}|0\rangle_{T_{i''}})$, and insert her T'' sequence into the T sequence when Alice sends it to Bob. In detail, Eve inserts each T'' photon after each T pulse with a delay time which is shorter than the time windows of Bob's optical devices. Since the T'' photons have the same wavelength as the T photons, Bob will perform the exact same operation on the T'' sequence when he performs his unitary operations on the T sequence. Eve sorts out her T'' photons when Bob returns them back to Alice, and rearranges the order according to the information published by Bob after Alice and Bob complete their eavesdropping checking. Thus Eve can perform the Bell-state measurement on her spy photons and get the secret message fully and freely.

Certainly, these attack schemes also work for the other QSDC protocols, such as those in Refs. [13, 14, 15]. However, the user can exploit a complex eavesdropping-checking process to avoid it [27]. As there is not eavesdropping checking when the photons are transmitted from the sender Alice to the receiver Bob in the ZXFZ protocol [25], this attack cannot be detected in principle.

III. IMPROVEMENT TO DEFEAT THE TROJAN HORSE ATTACK

In order to defeat Eve's IPE attack, a filter with which only the wavelengths close to the operating one can be let in should be added before all of the Bob's devices. In this way, Eve's invisible photons will be filtered out. Moreover, a photon number splitter (PNS: 50/50), which is used to divide each signal into two pieces, should be introduced to defeat the delay-photon Trojan horse attack. Thus, with the PNS and two single-photon measurements the users can distinguish whether there exists a multiphoton signal (including the delay-photon signal and the invisible photon whose wavelength is so close to the legitimate one that it cannot be filtered out with the filter). Although a PNS is not feasible with current technology, the users can use a photon beam splitter (PBS: 50/50) to prevent Eve from stealing the secret message with a little modification [27].

In order to improve the security of the ZXFZ protocol [25], we have to take these two kinds of attacks into account. For integrity, we describe the improved ZXFZ protocol in steps as follows.

(1) Alice prepares a sequence of EPR pairs in the state $|\Psi\rangle_i = \frac{1}{\sqrt{2}}(|0\rangle_{H_i}|1\rangle_{T_i} - |1\rangle_{H_i}|0\rangle_{T_i})$ and divides them into two sequences, the home (H) sequence and the travel (T) sequence, same as Refs. [14, 25]. She sends the T sequence to Bob.

(2) Bob inserts a filter in front of his devices to filter out the photon signal with an illegitimate wavelength, and then chooses a sufficiently large subset of photons randomly. He splits each sampling signal with a PNS and measures the two signals after the PNS with the two measure bases σ_z and σ_x chosen randomly. If the multiphoton rate is unreasonable high, Bob terminates the transmission and repeats the communication from the beginning. Otherwise, he continues to the next step.

(3) Bob chooses a large subset of photons from the photons remained as checking set (C set) and the others as the message set (M set). He encodes his message (checking message and secret message) by performing one of the four unitary operations U_i $(i = 0, 1, 2, 3)$. Then he disturbs the initial order of the photons in the T sequence and returns them to Alice.

(4) After Alice announces the receipt of all the T photons, Bob tells her the position and the order of the C set. Alice performs the Bell-state measurement on the photons in the C set and publishes the results with which Bob can estimates the security of the transmission. If there is an eavesdropper, Bob stops the communication. Otherwise, Bob publishes the order of the M set, and Alice can obtain the secret message with Bell-state measurements.

The improved ZXFZ protocol introduces a filter and another eavesdropping-checking process to defeat the IPE and the delay-photon Trojan horse attacks. In principle, the eavesdropper Eve with a infinite power can always find loopholes in quantum communication protocols with a non-ideal quantum channel. Our improvement can only counter the attacks we have already known. If some sophisticate Trojan horse attacks would be put forward in the future, we should choose a more complex eavesdropping-check way. The sticking point we want to emphasis is that two times of security checking is inevitable to ensure this bidirectional secure communication, same as those in the two-step protocol [12]. In this way, the origin ZXFZ protocol [25] cannot improve the efficiency of secure communication and has no superiority, compared with the two-step QSDC scheme [12], not the case announced by the authors [25]. It is worthy to point out that if the authorized users perform the security checking twice, the step to disturb the order of the photons in the T sequence can be reduced, and Alice can read out the secret message directly without the information of the order Bob published if Bob also has the capability of storing the quantum states. In this way, the protocol is equivalent to the QSDC scheme proposed by Wang *et al.* [14]. On the other hand, the improved ZXFZ protocol is useful if one of the two users, i.e., the sender of the secret message (Bob), does not have the device for storing quantum states. In this time, Bob can sample some photons from the T sequence synchronously for checking eavesdropping in the line from Alice to Bob, and then disturbs the orders of the others after encoding the message. The process for eavesdropping checking of the line from Alice to Bob needs not the storage of the other photons, which will reduce the requirements on Bob's devices largely in a practical application.

IV. DISCUSSION AND SUMMARY

In Ref. [25], the authors also proposed a one-way secure direct communication scheme based on the secret transmitting order of particles with EPR pairs. We found this scheme is secure in an ideal quantum channel. Also, the authors announced that their one-way scheme greatly reduces the opportunity of the particles being intercepted than the two-step protocol [25]. Unfortunately, we found that the opportunity of the particles being intercepted in these two schemes is the same one. In both schemes $2N$ (N is the number of EPR pairs used) particles were transmitted from Alice to Bob. The only difference between those two protocols is that the $2N$ particles is transmitted in one step in the one-way scheme [25] and through two steps in the two-step protocol [27]. In the two-step protocol the receiver can read out the secret message directly. But in this one-way scheme, for each qubit information to be understood at least one additional classical bit of information is exchanged. Both these two protocols need the quantum memory. Suppose the times for the transmission of the photons and the classical information transmitted from one user to the other both are t (Let us neglect the time for measurement and comparison). We found that the receiver needs to store the $2N$ particles at least for $4t$ time in the one-way scheme [25] and he stores N particles at least for $2t$ time in the two-step scheme [12]. In detail, in the one-way scheme [25] the receiver (Bob) should first tells the sender (Alice) the information that he has received all the photons, and then Alice publishes the positions of the photons in the checking set (i.e., C set) and their orders. After Bob transmits the outcomes of the C set to Alice, she tells him the orders of the other photons. That is, Bob at least stores the $2N$ photons for four times of the time t. In the two-step protocol [12], after receiving the checking sequence Bob first picks out some samples and measures them, and then he exchanges some classical information with the sender Alice. If the transmission of the checking sequence is secure, Alice sends the other sequence to Bob. In this time, Bob need in principle store the checking sequence for two times of the time t. From these analyses above, we can see that the two-step protocol is more convenient than the one-way scheme proposed by Zhu *et al.* [25].

In summary, we analyzed the security of the secure direct communication proposed by Zhu *et al.* [25] and found that this protocol is insecure because the two parties only execute one security-checking process. We proved that the eavesdropper can get Bob's secret message with a large probability without being detected by using the invisible photon eavesdropping scheme [26] or get all the secret message with the delay-photon Trojan horse attack [27]. We also present a possible improvement of this protocol by introducing a filter and another complex security-checking process to defeat these two kinds of attacks. The most important point is that for each block of transmission, an eavesdropping checking is inevitable for secure communication no matter what is transmitted with a quantum channel.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China under Grant No. 10604008, 10435020, 10254002 and A0325401, and Beijing Education Committee under Grant No. XK100270454.

[1] C. H. Bennett and G. Brassad, *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore*, India (IEEE, New York, 1984), PP.175-179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett *et al.*, Phys. Rev. Lett. **68**, 557 (1992).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] N. Gisin et al., Rev. Mod. Phys. **74**, 145 (2002).
[6] G. L. Long *et al.*, Phys. Rev. A **65**, 032302 (2002).
[7] F. G. Deng *et al.*, Phys. Rev. A **68**, 042315 (2003).
[8] F. G. Deng *et al.*, Phys. Rev. A **70**, 012311 (2004).
[9] M. Hillery *et al.*, Phys. Rev. A **59**, 1829 (1999); A. Karlsson *et al.*, Phys. Rev. A **59**, 162 (1999).
[10] L. Xiao *et al.*, Phys. Rev. A **69**, 052307 (2004); F. G. Deng *et al.*, Phys. Lett. A **337**, 329 (2005); Phys. Lett. A **340**, 43 (2005); F. G. Deng *et al.*, Chin. Phys. Lett. **21**, 2097 (2004).
[11] R. Cleve *et al.*, Phys. Rev. Lett. **83**, 648 (1999); F. G. Deng *et al.*, Phys. Rev. A **72**, 044301 (2005); Phys. Rev. A **72**, 022338 (2005); X. H. Li *et al.*, J. Phys. B **39**, 1975 (2006); F. G. Deng *et al.*, Euro. Phys. D **39**, 459 (2006).
[12] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[13] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[14] C. Wang *et al.*, Phys. Rev. A **71**, 044305 (2005).
[15] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[16] C. Wang et al., Opt. Commun. **253**, 15 (2005).
[17] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **68**, 3121 (1992).
[18] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[19] X. H. Li *et al.*, J. Korean Phys. Soc. **49**, 1354 (2006).
[20] T. Gao, Z. Naturforsch. A **59**, 597 (2004); T. Gao et al., Nuovo Cimento B **119**, 313 (2004).
[21] F. L. Yan and X. Zhang, Euro. Phys. J. B **41**, 75 (2004).
[22] Z. X. Man et al., Chin. Phys. Lett. **22**, 18 (2005).
[23] C. H. Bennett *et al.*, Phys. Rev. Lett **29**, 1895 (1993).
[24] M. Zukowski et al., Phys. Rev. Lett. **71**, 4287 (1993); J. W. Pan *et al.*, Phys. Rev. Lett. **80**, 3891 (1998).
[25] A. D. Zhu *et al.*, Phys. Rev. A **73**, 022338 (2006).
[26] Q. Y. Cai, Phys. Lett. A, **351**, 23 (2006)
[27] F. G. Deng *et al.*, quant-ph/0508168
[28] N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006)