PHYSICAL REVIEW A **73**, 022338 (2006)

Secure direct communication based on secret transmitting order of particles

Ai-Dong Zhu,[1,2] Yan Xia,[2] Qiu-Bo Fan,[2] and Shou Zhang[1,2,*]
[1] *Center for the Condensed-Matter Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, People's Republic of China*
[2] *Department of Physics, College of Science, Yanbian University, Yanji, Jilin 133002, People's Republic of China*

(Received 16 November 2005; published 22 February 2006)

We propose the schemes of quantum secure direct communication based on a secret transmitting order of particles. In these protocols, the secret transmitting order of particles ensures the security of communication, and no secret messages are leaked even if the communication is interrupted for security. This strategy of security for communication is also generalized to a quantum dialogue. It not only ensures the unconditional security but also improves the efficiency of communication.

DOI: 10.1103/PhysRevA.73.022338 PACS number(s): 03.67.Hk, 03.65.Ta, 42.79.Sz

I. INTRODUCTION

With the rapid development of information technology, quantum cryptography has been an important and attractive study area. It ensures that the secret message is intelligible only for the two legitimated parties of communication without being altered or stolen. Since Bennett and Brassard proposed BB84 protocol [1] which is a proven secure protocol, many quantum key distribution schemes have been proposed and the experimental feasibility of them is also discussed [2–9]. Although the methods used in these schemes are various, the basic principle is the same, i.e., the two remote legitimated users (Alice and Bob) establish a shared secret key through the transmission of quantum signals; after this they can use this key to encrypt or decrypt the secret messages. This means that the two parties have to share a secret key before the secret message is transmitted. As for communication, this beforehand step undoubtedly reduces the efficiency of communication. Our motive to build a quantum channel is not only to transmit information securely without being eavesdropped on but also to improve the efficiency of communication.

In recent years, a different scheme, quantum secure direct communication (QSDC) has been proposed and pursued [10–15]. In this scheme the transmitted message can be read only after a final transmission of an additional classical information without first establishing a shared secret key. In 2002, Boström and Felbinger [11] proposed a ping-pong QSDC protocol using EPR pairs as quantum message carriers, which is insecure for a noisy quantum channel as shown by Wójcik [16]. Cai and Deng gave a scheme using single photons as a quantum one-time pad to encode the secret messages [12,13]. Meanwhile, Deng *et al.* put forward a two-step QSDC protocol using blocks of EPR pairs [14]. In this two-step scheme the EPR pairs are divided into two sequences, the checking sequence and message sequence, which are sent by two steps, and the receiver needs to check the security of the channel twice (one for checking sequence and another for message sequence). In this paper, two QSDC schemes based on transmitting order of particles are proposed. In these two schemes, we also use EPR pairs as the messages carriers, but the transmitting order of particles is secret to any other people except for the sender himself (herself), so the eavesdropper (Eve) is not able to get any secret messages by performing a valid measurement. And we need checking security only once. Furthermore, we also apply this strategy of secret transmitting order to bidirectional communication, which is the so-called quantum dialogue [17]. Our present schemes not only ensure the unconditional security but also improve the efficiency of communication. The concrete protocols for QSDC are given in Sec. II. In Sec. III the security of the strategy is discussed. In Sec. IV we generalize the application of the strategy based on secret transmitting order to quantum dialogue. Finally, we give a discussion and summary on the present schemes.

II. SCHEMES FOR QSDC

An EPR pair can be in one of the following four states:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_i|1\rangle_{i'} \pm |1\rangle_i|0\rangle_{i'}), \tag{1}$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_i|0\rangle_{i'} \pm |1\rangle_i|1\rangle_{i'}), \tag{2}$$

where $|0\rangle$ and $|1\rangle$ are eigenvectors of the Pauli operator σ_z. The subscripts i and i' stand for the two correlated particles of an EPR pair. First, Alice and Bob agree on that the four local operations $U_0=I=|0\rangle\langle 0|+|1\rangle\langle 1|$, $U_1=\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$, $U_2=\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|$, and $U_3=i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$ represent two bits classical information 00, 11, 01, and 10, respectively. Alice prepares ordered N EPR photon pairs in the same state. Here we assume this state is $|\Psi\rangle=1/\sqrt{2}(|0\rangle_i|1\rangle_{i'} -|1\rangle_i|0\rangle_{i'})$.

On these preconditions, we give the following two schemes for QSDC.

---

[*] Email address: szhang@ybu.edu.cn

A. A round trip scheme based on the secret transmitting order of particles

(1) Alice divides the EPR pairs into two partner-photon sequences $[H_1,H_2,\ldots,H_i,\ldots,H_N]$ and $[T_{1'},T_{2'},\ldots,T_{i'},\ldots,T_{N'}]$, where H_i and $T_{i'}$ are the two photons correlated with each other in the ith (i=1,2,...N) photon pair, and $H(T)$ stands for "home (travel)." Then she sends the T sequence to Bob.

(2) Bob chooses a sufficiently large subset of photons randomly in the T sequence as a checking set (C set) and the rest as a message set (M set). By performing the four unitary operations $U_i,(i=0,1,2,3)$, he encodes his checking message on the C set and secret messages on the M set, respectively.

(3) Bob disturbs the initial order of the T sequence and returns them to Alice, that is, the rearranged order of the T sequence is completely secret to any other person other than Bob himself.

(4) After verifying that Alice has received all T photons, Bob announces the C set and the secret order in it. According to this information and the initial states, Alice can perform Bell measurements and deduce the probable operations performed by Bob. Then she announces her results about Bob's operations.

(5) By comparing his checking messages with Alice's results, Bob can decide whether Eve is online. If Eve is online, Bob terminates the communication. Otherwise, he exposes the secret transmitted order of the M set according to which Alice can read the secret messages by Bell measurements.

In this protocol, one particle (T photon) of each EPR pair undergoes a round trip to transfer information. This makes it impossible for Eve to get two particles of an EPR pair simultaneously. By disturbing the original order of particles, the security of communication is protected from the intercept-and-resend attack. However, the efficiency of a round trip is lower than a one-way trip after all, so we ameliorate this protocol to the one-way protocol based on the strategy of secret transmitting order.

B. A one way scheme based on the secret transmitting order of particles

($1'$) After preparing EPR pairs, Alice chooses a sufficiently large subset randomly as the checking set (C set) and the rest of the pairs as a message set (M set). Different from the above scheme, here the $C(M)$-set is composed of EPR pairs but not single photons. Then Alice encodes her secret messages on the M set and checking messages on the C-set, respectively, by performing the four operations on one particle (e.g., the first one) of each EPR pair. For convenience of describing, we denote the N EPR pairs with $P_1(1,1'),P_2(2,2'),\ldots,P_i(i,i'),\ldots,P_N(N,N')$. Taking C-set for example. Assuming Alice's checking message is (0100101101,...), and she chooses the first 50 EPR pairs as the C set. Then she encodes 01 on $P_1(1,1')$, 00 on $P_2(2,2')$, 10 on $P_3(3,3')$,..., and so on.

($2'$) With an order known only by herself, Alice sends these particles to Bob one by one, namely, the particles are sent as a single form but not as pairs. For instance, Alice sends the particles with an order $S_1(2)$, $S_2(1)$, $S_3(51)$, $S_4(5')$, $S_5(2')$, $S_6(60)$, $S_7(10)$, $S_8(1')$,..., $S_j(x),\ldots,S_k(x'),\ldots,S_{2N}(y)$, where $S_j(i)(j\in 1,2,\ldots,2N,i\in 1,2,\ldots,N)$ denotes that Alice sends particle i with the jth turn.

($3'$) After verifying that Bob has received all the $2N$ particles, Alice declares the initial state and the matching information of two particles in C-set through a public channel. For instance, $S_2\sim S_8,S_1\sim S_5,\ldots,S_j\sim S_k,\ldots$.

($4'$) Alice and Bob check the security of the channel. Bob performs a Bell-basis measurement according to the information from Alice. Comparing with the initial state, he obtains the result messages. Then he tells Alice about his result messages through a classical channel. By comparing Bob's result messages with the checking messages as well as analyzing the error rate, Alice can judge out whether Eve is on line.

($5'$) If the channel is secure, Alice exposes the matching information of two particles in the M set through a classical channel. Otherwise, Alice terminates this communication and starts next one from beginning.

($6'$) By performing a Bell-basis measurement, Bob obtains the secret messages.

In this protocol all the particles undergo only a one-way trip, which greatly reduces the opportunity of the particles being intercepted than the round trip and two-step protocol [14], and thus improves the efficiency of communication.

III. SECURITY OF THE QSDC SCHEMES BASED ON SECRET TRANSMITTING ORDER OF PARTICLES

Firstly, the security of our present schemes are based on the secret order of the particles, while the security of two-step schemes [14] lies in the security of the transmission of the C sequence. In a noisy channel, Eve can hide her eavesdropping in the noise. If Alice and Bob could not detect the eavesdropper in the transmission of the C sequence, Eve would capture easily the two particles in each EPR pair and take Bell-basis measurements on them, i.e., the secret messages would be leaked partly or all. However, this situation can be avoided in our present schemes.

Eve cannot only take intercept-and-resend attacks but also takes entangle-and-measure attacks in the whole communication process. In the round trip scheme, under the condition that Eve uses a intercept-and-resend attack, she also creates N EPR pairs which are in the same state $|\Psi\rangle_{ht}$ with (ht) are Eve's two particles correlated mutually. When Alice sends the T photon sequence to Bob, Eve intercepts these T photons and sends her t photons to Bob. Bob would take t for T and encodes he secret message and checking messages by performing the unitary operations as described above. If Bob returns them to Alice with the initial order, Eve can intercept the "$T(t)$" photons again and takes Bell-basis measurement on her ht pairs to learn Bob's secret messages and checking messages. Eve applies the same unitary operations on the T photons which she intercepted and sends them to Alice. As a result, Eve not only gains the secret messages, but also will not be detected. However, in our scheme in that the initial order of the $T(t)$ sequence is disturbed by Bob in the returning process, so Eve is not able to distinguish the t photon corresponding to her h photon. A blind encoding on T sequence can be detected. In the one-way scheme, all particles are transmitted with a secret order. Even if Eve intercepts all the particles, it is difficult for her to distinguish the partners of each pair and take a valid measurement. So her interception is not useful. Particularly, it should be noticed that in the one way scheme, only one transmission process is used. This not only greatly reduces the opportunity of the particles to be intercepted but also improves the efficiency of communication.

On the basis of the above analysis, our present QSDC schemes using the strategy of secret transmitting order are secure.

IV. GENERALIZATION TO QUANTUM DIALOGUE BASED ON SECRET TRANSMITTING ORDER

The above protocols are monodirectional communication. Using this strategy, we also can generalize the above QSDC schemes to a bidirectional communication, the so-called quantum dialogue [17].

Suppose that Alice and Bob have respective secret messages consisting of $2N$ bits to transmit to the other side. They can do according to the following steps.

(1) To securely carry out a secret dialogue, Alice firstly prepares a large enough number (M) of ordered EPR pairs, all in the same state (e.g., $|\psi_{0,0}\rangle_{ht}$). Then she encodes her secret messages M_m^A on N particles $t\,(t=t_1,t_2,t_3\cdots t_N)$ (M-set) and the checking messages M_c^A on the rest $(M-N)t$ particles (C set) by means of the four unitary operations above.

(2) Alice sends the particles string t to Bob in order. In accordance with the order of the travel particles t, Alice stores the remaining particles h with him.

(3) Confirming that Bob has received the sequence t, Alice will tell Bob about the M and C sets. Then Bob also encodes his secret messages M_m^B and checking messages M_c^B on M-set and C-set, respectively. Then Bob disturbs the order of a t sequence and returns them to Alice.

(4) After confirming the receiving of Alice, Bob announces the secret order of the particles t of the C set. Alice performs Bell-basis measurement on particles t and corresponding partners in the C set and announces the results on R_c. Then both Alice and Bob can deduce the probable checking messages m_c^B and m_c^A of the other sides by $m_c^B=R_c-M_c^A$ and $m_c^A=R_c-M_c^B$, respectively.

(5) Alice and Bob publicly announce their respective true checking messages M_c^A and M_c^B. If the error rates of m_c^A versus M_c^A, m_c^B versus M_c^B are relatively high, the communication should be terminated. Otherwise, Bob announces the secret order of the M set. Then Alice measures on the corresponding EPR pairs and publicly announces the results R_m.

(6) Alice and Bob decode the secret messages of the other side in terms of $M_m^B=R_m-M_m^A$ and $M_m^A=R_m-M_m^B$, respectively.

Similarly, because the transmitting order of particles is secret before the security checking, Eve cannot perform a valid measurement, so the unconditional security is ensured.

V. DISCUSSION AND SUMMARY

The present schemes for monodirectional and bidirectional communication are secure in an ideal lossless channel as the analysis above. In a practical quantum channel, there are noise and loss which will threaten the security of quantum communication. We need to illustrate that our scheme is still secure in a weak noisy channel. The security-checking is based on the statistical analysis for the error rate. Under a condition of weak noise, a higher error rate may indicate the eavesdropping. Hence our scheme is still valid.

In the meantime, we also notice that in most protocols on direct communication, once Eve is detected, as the communication is terminated, the secret messages are discarded. It is noticeable that direct communication is different from QKD. QKD allows the secret key between the two legitimate users to be produced over again for security. But the motive of QSDC is communicating messages directly, discarding messages means leakage of secret. As for our present schemes, the secret messages are hidden in the disordered transmitting order of particles. Eve cannot get any useful message without a correct order even if she captures the particles. Hence, no message is leaked except the communication is terminated, and the secret messages can be used repeatedly between the two legitimate users.

In summary, basing on the strategy of the secret transmitting order, two QSDC schemes and a quantum dialogue scheme have been proposed. This strategy ensures the security of communication not only in an ideal lossless channel but also in a weak noisy channel. Moreover, because the secret message is impossibly leaked even if when communication is terminated for security, the secret messages can be transmitted repeatedly between the sender and the receiver.

---

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

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

[3] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).

[4] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).

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

[6] A. Cabello, Phys. Rev. A **61**, 052312 (2000).

[7] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[8] P. Xue, C. F. Li, and G. C. Guo, Phys. Rev. A **65**, 022317 (2002).
[9] D. Song, Phys. Rev. A **69**, 034301 (2004).
[10] A. Beige, B.-G. Englert, Ch. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).
[11] K. Boströem and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[12] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**, 054301 (2004).
[13] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[14] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[15] F. L. Yan and X. Q. Zhang, Eur. Phys. J. B **41**, 75 (2004).
[16] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[17] B. A. Nguyen, Phys. Lett. A **328**, 6 (2004).