Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block

Fu-Guo Deng,[1,2] Gui Lu Long,[1,2,3,4] and Xiao-Shu Liu[1,2]
[1]*Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*
[2]*Key Laboratory For Quantum Information and Measurements, Beijing 100084, People's Republic of China*
[3]*Center for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China*
[4]*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China*
(Received 18 June 2003; published 20 October 2003)

A protocol for quantum secure direct communication using blocks of Einstein-Podolsky-Rosen (EPR) pairs is proposed. A set of ordered *N* EPR pairs is used as a data block for sending secret message directly. The ordered *N* EPR set is divided into two particle sequences, a checking sequence and a message-coding sequence. After transmitting the checking sequence, the two parties of communication check eavesdropping by measuring a fraction of particles randomly chosen, with random choice of two sets of measuring bases. After insuring the security of the quantum channel, the sender Alice encodes the secret message directly on the message-coding sequence and sends them to Bob. By combining the checking and message-coding sequences together, Bob is able to read out the encoded messages directly. The scheme is secure because an eavesdropper cannot get both sequences simultaneously. We also discuss issues in a noisy channel.

DOI: 10.1103/PhysRevA.68.042317 PACS number(s): 03.67.Hk, 03.65.Ud, 03.67.Dd, 03.65.Ta

I. INTRODUCTION

The goal of cryptography is to ensure that the secret message is intelligible only for the two authorized parties of communication and should not be altered during the transmission. Thus far, it is trusted that the only proven secure cryptosystem is the one-time-pad scheme in which the secret key is as long as the message. The two distant parties who want to transmit their secret message must distribute the secret key first. But it is difficult to distribute securely the secret key through a classical channel. Quantum key distribution (QKD), the approach using quantum mechanics principle for the distribution of secret key, is the only proven protocol for secure key distribution.

A lot of attention has been focused on QKD and it has been developed quickly since Bennett and Brassard [1] proposed the standard QKD protocol in 1984 (BB84). Now there are a lot of theoretical QKD schemes, for instance, in Refs. [1–18]. They can be attributed to one of the two types, the nondeterministic one and the deterministic one. The feature of the nondeterministic schemes is that the sender Alice chooses randomly two sets of measuring bases (MBs) (there are at least two sets of nonorthogonal bases) to produce two kinds of orthogonal states and transmits them to the receiver Bob. Bob then also chooses randomly one of the two sets of bases to measure the states. There are only a certain probability that Alice and Bob choose the same bases. So Alice cannot determine which bit value Bob can receive before they exchange classical information. The typical schemes are the BB84 [1], Ekert 1991 protocol (Ekert91) [2], Bennett-Brassard-Mermin 1992 protocol (BBM92) [3], and six-state protocols [9]. In contrast, in the deterministic schemes, Alice and Bob choose the same orthogonal bases for their measurements, so that they get the same results deterministically if the quantum channel is not disturbed. Typical such protocols are the ones presented in Refs. [5,6,8,10,13].

Different from key distribution whose object is to establish a common random key between two parties, a secure direct communication is to communicate important messages directly without first establishing a random key to encrypt them. Thus secure direct communication is more demanding on the security. As a secure direct communication, it must satisfy two requirements. First, the secret messages should be read out directly by the legitimate user Bob when he receives the quantum states, and no additional classical information is needed after the transmission of qubits. Second, the secret messages which have been encoded already in the quantum states should not leak even though an eavesdropper may get hold of the channel. That is to say, the eavesdropper cannot only be detected but also obtains blind results. As classical message can be copied fully, it is impossible to transmit secret messages directly through classical channels. But when quantum mechanics enters into the communication, the story will change.

Recently, Beige *et al.* proposed a quantum secure direct communication (QSDC) scheme [19]. In this scheme the message can be read only after a transmission of an additional classical information for each qubit. Boström and Felbingeer put forward a ping-pong QSDC scheme [20]. It is secure for key distribution and quasisecure for direct secret communication if perfect quantum channel is used. However, it is insecure if it is operated in a noisy quantum channel, as shown by Wójcik [21]. There is some probability that a part of the message might be leaked to the eavesdropper Eve, especially in a noisy quantum channel, because Eve can use the intercept-resending strategy to steal some secret message even though Alice and Bob will find her out of the end of communication. Moreover, the capacity is restricted, and an entangled state [an Einstein-Podolsky-Rosen (EPR) pair] only carries one bit of classical information.

In this paper, we will introduce a QSDC scheme with EPR pairs generalizing the basic ideas in Ref. [13] in QKD. It will be shown that it is provably secure and has a high capacity. We discuss the problems in a lossy quantum channel.

II. THE TWO-STEP QUANTUM SECURE DIRECT COMMUNICATION SCHEME

An EPR pair can be in one of the four Bell states,

$$|\psi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B-|1\rangle_A|0\rangle_B), \quad (1)$$

$$|\psi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B), \quad (2)$$

$$|\phi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B-|1\rangle_A|1\rangle_B), \quad (3)$$

$$|\phi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B). \quad (4)$$

Here $|0\rangle$ and $|1\rangle$ are the up and down eigenstate of the σ_z, the photon polarization operator. If we measure the state of a single photon, the Bell state will collapse and the state of the other particle will be completely determined if we know the measurement result of the first photon. For example, if we measure the state of photon A in the Bell state $|\psi^-\rangle$ and obtain $|0\rangle$, then the state of photon B will collapse to quantum state $|1\rangle$.

In the QKD protocol in Ref. [13], a set of N ordered EPR pairs, each placed randomly in one of the four Bell states, is prepared and divided into two sequences. Alice transmits the first sequence to Bob, and then they measure a subset of photons in their hands, respectively. After that, they analyze the security of the transmission for the first sequence. If they ensure that the channel is safe, Alice sends the second sequence to Bob. Bob then performs Bell-basis measurement on the ordered N EPR pairs to read out the Bell states. They perform a second eavesdropping check. By analyzing error rate, they can ascertain whether they have safely created a raw key or not. In this protocol, the transmission is done in batches of N EPR pairs. An advantage of block-transmission protocol is that we can check the security of the transmission by measuring some of the photons in the first step where Alice and Bob each hold a particle sequence in the hands. Once the security of the quantum channel is ensured, which means that an eavesdropper has not acquired the first particle sequence, then no information will be leaked to her whatever she may do to the second particle sequence.

Because of this property, this two-step QKD scheme can be modified for secure direct communication, shown in Fig. 1. Here we first give the specific steps of the QSDC protocol; they are the following.

(1) Alice and Bob agree on that each of the four Bell bases can carry two-qubit classical information and encode $|\psi^-\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, and $|\phi^+\rangle$ as 00, 01, 10, and 11, respectively.

(2) Alice prepares an ordered N EPR pair in state $|\psi\rangle_{CM}=|\psi^-\rangle=(1/\sqrt{2})(|0\rangle_C|1\rangle_M-|1\rangle_C|0\rangle_M)$. We denote the N ordered EPR pairs with $[(P_1(C),P_1(M)),\ (P_2(C),P_2(M)),\ (P_3(C),P_3(M)),\ \ldots,(P_N(C),P_N(M))]$. Here the subscript indicates the pair order in the sequence, and C and M represent the two particles, respectively.

(3) Alice takes one particle from each EPR pair to form an ordered EPR partner particle sequence, say, $[P_1(C),P_2(C),P_3(C),\ \ldots,P_N(C)]$. It is called the checking sequence or simply the C sequence. The remaining EPR partner particles compose another particle sequence $[P_1(M),P_2(M),P_3(M),\ \ldots,P_N(M)]$, and it is called the message-coding sequence or the M sequence for short.

(4) Alice sends the C sequence $[P_1(C),P_2(C),P_3(C),\ \ldots,P_N(C)]$ to Bob. Alice and Bob then check eavesdropping by the following procedure: (a) Bob chooses randomly a number of the photons from the C sequence and tells Alice which particles he has chosen. (b) Bob chooses randomly one of the two sets of MBs, say, σ_z and σ_x to measure the chosen photons. (c) Bob tells Alice which MB he has chosen for each photon and the outcomes of his measurements. (d) Alice uses the same measuring basis as Bob to measure the corresponding photons in the M sequence and checks with the results of Bob. If no eavesdropping exists, their results should be completely opposite, i.e., if Alice gets 0 (1), then Bob gets 1 (0). This is the first eavesdropping check. After that, if the error rate is small, Alice and Bob can conclude that there are no eavesdroppers in the line. Alice and Bob continue to perform step 5; otherwise, they have to discard their transmission and abort the communication.

(5) Alice encodes her messages on the M sequence and transmits it to Bob. Before the transmission, Alice must encode the EPR pairs. In order to guard for eavesdropping in this transmission, Alice has to add a small trick in the M sequence. She selects randomly in the M sequence some particles and performs on them randomly one of the four operations. The number of such particles is not big as long as it can provide an analysis of the error rate. Only Alice knows the positions of these sampling particles and she keeps them secret until the communication is completed. The remaining M sequence particles are used to carry the secret message directly. To encode the message, we use the dense coding scheme of Bennett and Wiesner [22], where the information is encoded on an EPR pair with a local operation on a single qubit. Here we generalize the dense coding idea into secure direct communication. Different from dense coding, in this protocol, both the particles in an EPR are sent from Alice to Bob in two steps, and the transmission of EPR pairs is done in block. Explicitly, Alice makes one of the four unitary operations (U_0, U_1, U_2, and U_3) to each of her particles,

$$U_0=I=|0\rangle\langle 0|+|1\rangle\langle 1|, \quad (5)$$

$$U_1=\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|, \quad (6)$$

$$U_2=\sigma_x=|1\rangle\langle 0|+|0\rangle\langle 1|, \quad (7)$$

$$U_3=i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|, \quad (8)$$

and they transform the state $|\psi^-\rangle$ into $|\psi^-\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, and $|\phi^+\rangle$, respectively. These operations correspond to 00, 01, 10, and 11, respectively.

(6) After the transmission of M sequence, Alice tells Bob the positions of the sampling pairs and the type of unitary operations on them. Bob performs Bell-basis measurement on the C and M sequences simultaneously. By checking the sampling pairs that Alice has chosen, he will get an estimate of the error rate in the M sequence transmission. In fact, in the second transmission, Eve can only disturb the transmission and cannot steal the information because she can only get one particle from an EPR pair.

(7) If the error rate of the sampling pairs is reasonably low, Alice and Bob can then entrust the process, and continue to correct the error in the secret message using error correction method. Otherwise, Alice and Bob abandon the transmission and repeat the procedures from the beginning.

(8) Alice and Bob do error correction on their results. This procedure is exactly the same as that in QKD. However, to preserve the integrity of the message, the bits preserving correction code, such as CASCADE [23], should be used.

As discussed above, Alice and Bob can ensure the security of the C sequence and Eve will be found out if she eavesdrops the quantum line. It is of interest that Eve cannot read out the information in the EPR pairs even if she captures one of the two sequences, because no one can read the information from one particle of an EPR pair alone. In this way, no secret message will be leaked to Eve. It is secure. Moreover, the capacity is high in this protocol, because each EPR pair carries two bits of classical information.

III. SECURITY OF THE QSDC SCHEME

Our QSDC protocol is based on EPR pair, so the proof of security is similar to those in Refs. [20,24,25] with entangled photons. The proof for the security of our QSDC protocol is based on the security for the transmission of the C sequence. If Alice and Bob could not detect eavesdropper (Eve) in the transmission of the C sequence, Eve would capture easily the two photons in each EPR pair and take Bell-basis measurement on them to read out the secret message.

The transmission and the security check of the C sequence in our QSDC protocol is similar to the procedures in BBM92 QKD protocol [3], where one particle in an EPR pair is sent to Alice and the other is sent to Bob. Here the M sequence particles are retained securely in Alice's site. Before checking eavesdropping, Eve has no access to the M sequence particles. Therefore the security of transmission for the C sequence simply reduces to the security of the BBM92 QKD protocol. The proof of security for BBM92 in ideal condition is given in Ref. [24] and that with practical conditions was given in detail in Ref. [25]. Hence our QSDC protocol is secure.

Now, let us give the reason why we choose two sets of measuring bases for checking the security of the transmission for the C sequence. According to Stinespring dilation theorem, as Eve is limited only to eavesdropping on the quantum line between Alice and Bob, her eavesdropping can be realized by a unitary operation, say, $\hat{E}$ on a larger Hilbert space, $|b,E\rangle \equiv |b\rangle_B|E\rangle$. Then the state of composite system Alice, Bob, and Eve is

$$|\psi\rangle = \sum_{a,b\in\{0,1\}} |\varepsilon_{a,b}\rangle|a\rangle|b\rangle, \tag{9}$$

where $|\varepsilon_{a,b}\rangle$ describes Eve's probe state, and $|a\rangle$ and $|b\rangle$ are single-photon states of Alice and Bob in each EPR pair, respectively. As in Ref. [24], the condition on the states of Eve's probe is

$$\sum_{a,b\in\{0,1\}} \langle\varepsilon_{a,b}|\varepsilon_{a,b}\rangle = 1. \tag{10}$$

As Eve can only eavesdrop the C sequence before the first checking, we can describe Eve's effect on the system as

$$\hat{E}|0,E\rangle \equiv \hat{E}|0\rangle_B|E\rangle = \alpha|0\rangle_B|\varepsilon_{00}\rangle + \beta|1\rangle_B|\varepsilon_{01}\rangle \equiv \alpha|0,\varepsilon_{00}\rangle + \beta|1,\varepsilon_{01}\rangle, \tag{11}$$

$$\hat{E}|1,E\rangle \equiv \hat{E}|1\rangle_B|E\rangle = \beta'|1\rangle_B|\varepsilon_{10}\rangle + \alpha'|1\rangle_B|\varepsilon_{11}\rangle \equiv \beta'|0,\varepsilon_{10}\rangle + \alpha'|1,\varepsilon_{11}\rangle, \tag{12}$$

i.e, Eve's probe can be modeled by

$$\hat{E} = \begin{pmatrix} \alpha & \beta' \\ \beta & \alpha' \end{pmatrix}. \tag{13}$$

Since $\hat{E}$ has to be unitary, the complex numbers α, β, α', and β' must satisfy

$$|\alpha|^2 + |\beta'|^2 = 1, \tag{14}$$

$$|\alpha'|^2 + |\beta|^2 = 1,$$

$$\alpha\beta^* + \alpha'^*\beta' = 0,$$

we get the following relations:

$$|\beta'|^2 = |\beta|^2, \quad |\alpha'|^2 = |\alpha|^2. \tag{15}$$

For Alice and Bob, the action of Eve's eavesdropping will introduce an error rate

$$\epsilon = |\beta|^2 = |\beta'|^2 = 1 - |\alpha|^2 = 1 - |\alpha'|^2. \tag{16}$$

If Eve can only capture one photon in each EPR pair, she gets no information. The way Eve can steal information is to pretend to Bob to receive the C sequence and send a fake sequence to Bob. If Alice and Bob could not find out her action, Eve would intercept the M sequence and read out the information in the EPR pairs. That is to say, only when Alice and Bob ascertain that there is no eavesdropper monitoring the quantum line, they transmit the M sequence. We can calculate the information Eve can maximally gain. When the C sequence particles reach Bob, its reduced density matrix is

$$\rho_B = \mathrm{Tr}_A(\rho_{AB}) = \mathrm{Tr}_A(|\psi\rangle_{ABAB}\langle\psi|) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{17}$$

that is to say, Bob's photon can be in either state $|0\rangle$ or $|1\rangle$ with equal probability $P = \frac{1}{2}$.

Similar to that in Ref. [20], first let us suppose that the quantum state of the photon in the hand of Alice is $|1\rangle$, i.e., Alice takes measurement on the photon in her hand with single-photon detector and the state is $|1\rangle$. Then the state of the system composed of Bob's photon and Eve's probe can be described by

$$|\psi'\rangle=\hat{E}|0,E\rangle\equiv\hat{E}|0\rangle_B|E\rangle=\alpha|0\rangle_B|\varepsilon_{00}\rangle+\beta|1\rangle_B|\varepsilon_{01}\rangle \equiv\alpha|0,\varepsilon_{00}\rangle+\beta|1,\varepsilon_{01}\rangle, \tag{18}$$

$$\rho'=|\alpha|^2|0,\varepsilon_{00}\rangle\langle 0,\varepsilon_{00}|+|\beta|^2|1,\varepsilon_{01}\rangle\langle 1,\varepsilon_{01} |+\alpha\beta^*|0,\varepsilon_{00}\rangle\langle 1,\varepsilon_{01}|+\alpha^*\beta|1,\varepsilon_{01}\rangle\langle 0,\varepsilon_{00}|. \tag{19}$$

After encoding of the unitary operations U_0, U_1, U_2, and U_3 with the probabilities p_0, p_1, p_2, and p_3, respectively, the state reads

$$\rho''=(p_0+p_3)|\alpha|^2|0,\varepsilon_{00}\rangle\langle 0,\varepsilon_{00}|+(p_0+p_3)|\beta|^2|1,\varepsilon_{01}\rangle \times\langle 1,\varepsilon_{01}|+(p_0-p_3)\alpha\beta^*|0,\varepsilon_{00}\rangle\langle 1,\varepsilon_{01}|+(p_0-p_3) \times\alpha^*\beta|1,\varepsilon_{01}\rangle\langle 0,\varepsilon_{00}|+(p_1+p_2)|\alpha|^2|1,\varepsilon_{00}\rangle\langle 1,\varepsilon_{00}|+(p_1 +p_2)|\beta|^2|0,\varepsilon_{01}\rangle\langle 0,\varepsilon_{01}|+(p_1-p_2)\alpha\beta^*|1,\varepsilon_{00}\rangle\langle 0,\varepsilon_{01}| +(p_1-p_2)\alpha^*\beta|0,\varepsilon_{01}\rangle\langle 1,\varepsilon_{00}|, \tag{20}$$

which can be rewritten in the orthogonal basis $\{|0,\varepsilon_{00}\rangle,|1,\varepsilon_{01}\rangle,|1,\varepsilon_{00}\rangle,|0,\varepsilon_{01}\rangle\}$,

$$\rho''=\begin{pmatrix} (p_0+p_3)|\alpha|^2 & (p_0-p_3)\alpha\beta^* & 0 & 0 \\ (p_0-p_3)\alpha^*\beta & (p_0+p_3)|\beta|^2 & 0 & 0 \\ 0 & 0 & (p_1+p_2)|\alpha|^2 & (p_1-p_2)\alpha\beta^* \\ 0 & 0 & (p_1-p_2)\alpha^*\beta & (p_1+p_2)|\beta|^2 \end{pmatrix}, \tag{21}$$

where $p_0+p_1+p_2+p_3=1$.

The information I_0 that Eve can get is equal to the Von Neumann entropy, i.e,

$$I_0=\sum_{i=0}^{3}-\lambda_i\log_2\lambda_i \tag{22}$$

where λ_i $(i=0,1,2,3)$ are the eigenvalues of ρ'', which are

$$\lambda_{0,1}=\frac{1}{2}(p_0+p_3)\pm\frac{1}{2}\sqrt{(p_0+p_3)^2-16p_0p_3|\alpha|^2|\beta|^2} =\frac{1}{2}(p_0+p_3)\pm\frac{1}{2}\sqrt{(p_0+p_3)^2-16p_0p_3(\epsilon-\epsilon^2)}, \tag{23}$$

$$\lambda_{2,3}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2|\alpha|^2|\beta|^2} =\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2(\epsilon-\epsilon^2)}. \tag{24}$$

If the four operations distribute with equal probability, that is, $p_0=p_1=p_2=p_3=\frac{1}{4}$, Eve can get 1 bit of information from each EPR pair with the error rate $\epsilon=0$. In fact, the simple way for Eve to steal information is that Eve measures each photon with MB σ_z and Alice and Bob cannot find out the action of Eve's. Even though Eve cannot read out the information of phase in EPR pair, she can distinguish between the values of each bit. That is to say, she can distinguish the operations $\{U_0, U_1\}$ from $\{U_2, U_3\}$. This is an intrinsic limitation on the coding in Ref. [20].

Surely, the proof and the above discussion are based on ideal condition and do not take into account noise in transmission. In fact, in low noise channel, the photon loss will be small, and Eve's action will increase either the error rate or loss of signal, so the security of the *C* sequence is assured if Alice and Bob do the first eavesdropping check and analyze the error rate and the efficiency. On the contrary, if quantum channel loss is sufficiently high, two problems arise. The first one is the security of transmission of the *C* sequence, which requires Alice and Bob to share a sequence of entangled states securely. The other is the loss of the *M* sequence. Without measurement Bob cannot make sure whether he receives the particles or not in the *C* sequence and Alice must encode all particles in *M* sequence. In this way, Eve's eavesdropping cannot be detected if she captures some of the particles in *C* sequence and sends the others to Bob with a better quantum channel with which the lossy efficiency of all the photons is not increased. Eve intercepts the *M* sequence and does Bell-basis measurement and then gets some of the secret message. This is the danger of not sharing a sequence of EPR pairs securely. In order to avoid the attack on *C* sequence and share a sequence of EPR pairs securely, Bob can perform quantum entanglement swapping [26] on the particles he receives first and then gets a subset of *C* sequence of particles entangled with Alice's (called the C' sequence): if there are indeed particles there, the swapping will succeed, otherwise the swapping will fail. The swapping operation here serves as a particle existence detection. Then Bob chooses randomly a subset of the C' sequence particles and measures them with either σ_z or σ_x. Alice only encodes on the subset

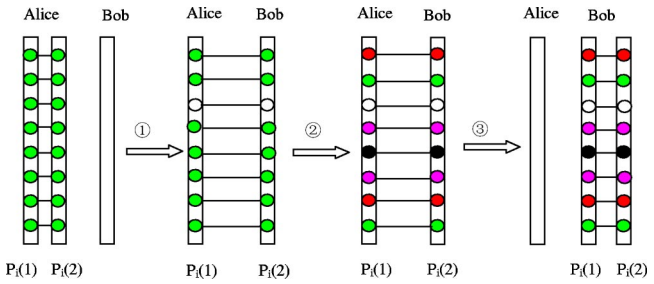

FIG. 1. Illustration of the QSDC protocol. Alice prepares the ordered N EPR pairs in the same quantum states and divides them into two partner-particle sequences. She first sends one sequence to Bob for checking eavesdropping by choosing a fraction of particles to measure with a randomly chosen measuring basis. If the quantum line is secure, Alice encodes the partner EPR pairs, using four unitary operations, the secret messages, and sends the second sequence to Bob.

of M sequence corresponding to the sub-C sequence (called the M' sequence) on which Bob succeeds in quantum entanglement swapping. With these two procedures Alice and Bob can share a subsequence of EPR pairs truly and the action of Eve can be detected even in a highly lossy quantum channel. In practical applications, some coding using redundancy is necessary as has been used extensively in classical communications. For instance, several bits may be used to code a single bit, for instance, using the Calderbank-Shor-Steane coding method [27]. In this way, Alice and Bob must pay a lot of source for the correlated results.

IV. IMPLEMENTATION ISSUES

In our scheme, we need to store the checking sequence of photons for a while, to make eavesdropping check and wait for the M sequence of photons to come. This is the price to pay for the improved security and enhanced efficiency. Here we propose two ways to realize this. One is using light storage device, and the other is to use optical delays.

It has already been demonstrated experimentally that light can be stored together with their quantum states [28,29]. With the electromagnetic induced transparency technique, the C sequence of photons can be stored for a while to complete the eavesdropping check and the traveling of the M sequence. At present, the technique may not be mature enough for a practical implementation of the proposed QSDC scheme. However, as it may be the only light storage device, together with its roles in quantum computation, it is extremely demanding that this technique be developed further (Fig. 1).

Another realization is to use optical delays. This is a well-developed technology and is experimentally feasible. Instead of producing an ordered EPR pairs in space at the same time, we can produce a time-ordered EPR pair sequence. As shown in Fig. 2, a sequence of EPR pairs is produced at Alice's site. One after another photon in the C sequence is sent to Bob's site through the upper line first. The corresponding M sequence is sent to Bob through the lower transmission line. However, the M sequence is delayed by τ at Alice's site before it enters the insecure channel. When the C

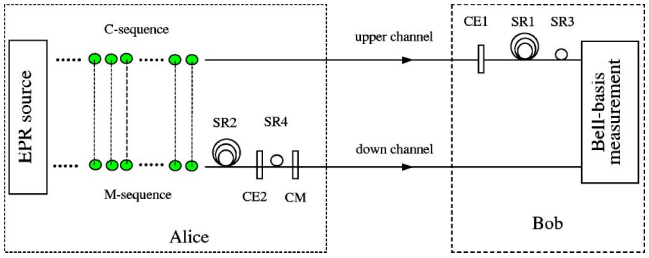

FIG. 2. An example for the QSDC scheme using optical delays. SR1, SR2, SR3, and SR4 represent optical delays; CE1 and CE2 are used to describe the procedure for checking eavesdropping; CM encodes the message sequence according to the secret message.

sequence reaches Bob, Bob selects randomly some photons for eavesdropping check. He measures those chosen photons randomly in the σ_x or σ_z basis and he announces publicly the positions, the measuring basis, and the outcomes of the measurement for these chosen photons. After hearing these results, Alice performs measurement using the same measuring basis as Bob, on the corresponding photons in the M sequence. If the error rate is below a predetermined threshold, she concludes that the quantum channel is secure and preforms coding unitary operation on the M-sequence particles. During the M-sequence transmission, some randomly chosen photons are used to check the transmission error rate. In these chosen sampling photons, an operation randomly chosen from the four operations is applied. Therefore after Bob receives the sampling pairs and combines with his partner photons in the C sequence, he can recover these operations using Bell-basis measurement. These sampling pairs will give an error rate estimate of the second transmission, and this error rate will be used as a parameter later in error correction process.

A very important quantity is the delay τ. It depends on the distance between Alice and Bob, the number N in each block, and the number of photons transmitted per unit time, f. For simplicity, we ignore the times it takes for the eavesdropping check measurement, and the coding operation. Then τ must be long enough for a photon to travel to Bob, and Bob makes measurement and tells Alice the result, and then sends the M-sequence particles to Bob. Thus it must be three times of the period for a photon to travel from Alice to Bob. If this has to be done for a block of N pairs, additional time N/f has to be added. Thus the delay should be

$$\tau \geqslant \frac{3L}{c} + \frac{N}{f}, \tag{25}$$

where L is the distance between Alice and Bob, and c is the velocity of light in quantum channel. Complete Bell-basis measurement is also highly demanding, and has been demonstrated recently [30].

V. DISCUSSION AND SUMMARY

The presented scheme resembles more to a quantum key distribution protocol. In fact, after Bob receives the checking sequence, Alice and Bob can establish a common one-time-

pad key by measuring their particles using a randomly chosen basis from the σ_z or σ_x basis, which is a variant of the Ekert91 [2] QKD and the BBM92 [3] QKD protocol. Then the secret message can be encoded using this one-time-pad key and transmitted through a classical channel. The important distinction between quantum direct communication and the quantum key distribution scheme is that in the quantum direct communication scheme no classical key is ever established, but rather an inherently quantum-mechanical resource (the shared EPR pairs) takes over the role of the key. With the development of efficient EPR source and Bell-state measurement device, quantum direct communication may become easier to realize and be favored in some specific applications.

In summary, a novel QSDC scheme is proposed and secret messages can be coded directly over a quantum channel with security. In this scheme, a block of entangled particles is divided into two sequences, the checking sequence and message-coding sequence. They are sent from Alice to Bob in two steps. The security is assured by the secure transmission of the checking sequence. Moreover, the scheme makes full use of the two-qubit in an EPR pair. We also propose concrete experimental setup for its realization. The scheme is completely secure for an ideal noiseless channel, and conditionally secure with a noisy channel.

ACKNOWLEDGMENTS

This work was supported by the National Fundamental Research Program Grant No. 001CB309308, China National Natural Science Foundation Grant No. 60073009, the Hang-Tian Science Fund, and the Excellent Young University Teachers' Fund of Education Ministry of China.

[1] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference 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, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[7] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[8] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[9] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[10] W.Y. Hwang, I.G. Koh, and Y.D. Han, Phys. Lett. A **244**, 489 (1998).
[11] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[12] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
[13] G.L. Long and X.S. Liu, Phys. Rev. A **65**, 032302 (2002).
[14] B.S. Shi, Y.K. Jiang, and G.C. Guo, Appl. Phys. B: Laser Opt. **B70**, 415 (2000).
[15] P. Xue, C.F. Li, and G.C. Guo, Phys. Rev. A **65**, 022317 (2002).
[16] F.G. Deng *et al.*, Chin. Phys. Lett. **19**, 893 (2002).
[17] S.J.D. Phoenix, S.M. Barnett, P.D. Townsend, and K.J. Blow, J. Mod. Opt. **42**, 1155 (1995).
[18] H.-k. Lo, H.F. Chan, and M. Ardehali, e-print quant-ph/0011056.
[19] A. Beige *et al.*, Acta Phys. Pol. A **101**, 357 (2002).
[20] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[21] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
[22] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[23] G. Brassard and L. Salrail, *Euro-crypt 193*, Lectures Notes in Computer Sciences Vol. 765 (Springer-Verlag, New York, 1994), pp. 410–423.
[24] H. Inamori, L. Rallan, and V. Vedral, J. Phys. A **34**, 6913 (2001).
[25] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[26] C.H. Bennet, G. Brassard, C. Crpeau, K. Jozsa, A. Peres, and W.K. Wotters, Phys. Rev. Lett. **70**, 1895 (1993); M. Zukowski, A. Zeilinger, M.A. Horne, and A. Ekert, *ibid.* **71**, 4287 (1993); S. Rose, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, 822 (1998); J.W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[27] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996); Phys. Rev. Lett. **77**, 793 (1996); P.W. Shor, Phys. Rev. A **52**, R2493 (1995); A.M. Steane *ibid.* **54**, 4741 (1996); A.M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[28] D.F. Phillips *et al.*, Phys. Rev. Lett. **86**, 783 (2001).
[29] C. Liu *et al.*, Nature (London) **409**, 490 (2001).
[30] Y.-H. Kim, S.P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).