Front. Phys. China, 2007, 2(3): 251—272
DOI 10.1007/s11467-007-0050-3

REVIEW ARTICLE

LONG Gui-lu, DENG Fu-guo, WANG Chuan, LI Xi-han, WEN Kai, WANG Wan-ying

Quantum secure direct communication and deterministic secure quantum communication

Abstract In this review article, we review the recent development of quantum secure direct communication (QSDC) and deterministic secure quantum communication (DSQC) which both are used to transmit secret message, including the criteria for QSDC, some interesting QSDC protocols, the DSQC protocols and QSDC network, etc. The difference between these two branches of quantum communication is that DSQC requires the two parties exchange at least one bit of classical information for reading out the message in each qubit, and QSDC does not. They are attractive because they are deterministic, in particular, the QSDC protocol is fully quantum mechanical. With sophisticated quantum technology in the future, the QSDC may become more and more popular. For ensuring the safety of QSDC with single photons and quantum information sharing of single qubit in a noisy channel, a quantum privacy amplification protocol has been proposed. It involves very simple CHC operations and reduces the information leakage to a negligible small level. Moreover, with the one-party quantum error correction, a reation has been established between classical linear codes and quantum one-party codes, hence it is convenient to transfer many good classical error correction codes to the quantum world. The one-party quantum error correction codes are especially designed for quantum dense coding and related QSDC protocols based on dense coding.

Keywords quantum secure direct communication, deterministic secure quantum communication, network, quantum privacy amplification, one-party quantum error correcting codes

PACS numbers 03.67.Hk, 03.65.Ud, 42.50.Dv

1 Introduction

The principles in quantum mechanics provide novel ways for quantum information transmission and processing, such as quantum computation and quantum communication. In a quantum computer, factorization of an integer can be completed in polynomial time using the Shor algorithm [1]. One can find an marked item with very high probability from a unsorted database with a square-root speedup with the Grover algorithm [2], or exactly using the Long algorithm [3]. Quantum computer can simulate a quantum system efficiently [4, 5]. With a quantum computer, many classical cryptography protocols can be attacked. Hence quantum computation is a great threat to modern cryptography. Meanwhile, the rapid development in modern cryptanalysis makes cryptography very vulerable [6].

Quantum key distribution (QKD) is one of the most mature quantum information techniques [7, 8]. Two remote users can exploit QKD to create a private key securely. These keys are then used to crypt the secret message into a ciphertext through a classical cryptographic scheme such as the one-time-pad

LONG Gui-lu, DENG Fu-guo, WANG Chuan, WEN Kai, WANG Wan-ying
Key Laboratory for Atomic and Molecular Nanosciences and Department of Physics, Tsinghua University, Beijing 100084, China

LONG Gui-lu (✉)
Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China
E-mail: gllong@tsinghua.edu.cn

DENG Fu-guo, LI Xi-han
Key Laboratory of Beam Technology and Material Modification of Ministry of Education, and Institute of Low Energy Nuclear Physics, Beijing Normal University, Beijing 100875, China

Received June 30, 2007

[9], and the ciphertexts are then sent from one user to another through a classical channel. Thus there are at least two transmissions in a QKD based communication. The first is to establish a secure key between the two parties, and the second is a classical communication in which the ciphertext is transmitted. There have been many QKD protocols. We can classify these protocols by the type of information carriers, for instance those based on single photons, and those based on the Einstein-Podolsky-Rosen (EPR) pairs. We can also classify them according to the efficiency, for instance some protocols can produce keys deterministically, and some produce them probabilistically.

Recently a novel quantum communication was proposed: the quantum secure direct communication (QSDC). In QSDC, secret messages can be transmitted directly from the sender Alice to the receiver Bob without the classical communication of ciphertext, or in other words, the quantum key distribution and the classical communication of ciphertext are condensed into one single quantum communication. QSDC has a great potential in the future because it is fully quantum mechanical. The QKD may serve as a transition between now to the future quantum communication periods as it relies still heavily on classical communication. With the development of future quantum technology, one needs not worry about the extensive use of quantum resources, just like people does not worry about the heavy use of memory in PC's in designing software in contrast to the common practice at the early days of PC.

Deterministic secure quantum communication (DSQC) is a similar but different type of quantum communication, such as the one proposed in Refs. [10, 11]. As mentioned earlier, to complete a secure communication with the help of QKD, one usually encodes the secret message with an encryption scheme such as the one-time-pad [9], and the ciphered text is transmitted through a classical channel. With a quantum channel, this procedure can be varied. For instance, Alice can encrypt her secret message with a random key and encodes the ciphertext into the states of the information carriers. These ciphertext is then sent from Alice to Bob deterministically. Alice also sends the random key to Bob through a classical channel. With this knowledge, Bob can decode the message from the ciphertext obtained through the quantum communication. Quantum principles ensure that Eve cannot steal the ciphertext. Thus a fundamental difference between QSDC and DSQC is the need of another round of classical communication.

In this review article, we will focus on the QSDC and DSQC, and the privacy amplification and quantum error correction codes specially designed for them. In Section 2, we give a brief history of DSQC and QSDC. In Section 3, we introduce the concept of QSDC and the major related protocols. In Section 4, deterministic secure quantum communication (DSQC) is reviewed. The difference between QSDC and DSQC is that there are no additional classical communications in QSDC whereas there are in DSQC. In Section 5, we briefly review quantum secure direct communication network. In Section 6, the privacy amplification for QSDC with single photons is described. In Section 7, we describe the recently developed one-party quantum error correction codes (QEC). The one-party QEC is a quantum correcting code especially designed for quantum dense coding and QSDC based on quantum dense coding. Finally in Section 8, we give a brief summary.

2 A brief history

In 1999, Shimizu and Imoto proposed a DSQC protocol using entangled photon pairs [10]. In their scheme, the ciphertext is encoded in the state of the entangled pairs, and they are transmitted from Alice to Bob. Bob performs a Bell-basis measurement to read out the partial information. Full information of the ciphertext is read out after Alice notifies him the encoding basis through a classical communication.

In 2002, Beige *et al.* [11] proposed another DSQC scheme based on single photon two-qubit states. In this scheme, the message can be read out only after a transmission of an additional classical information for each qubit, i.e., the cryptographic key of the sender Alice. Moreover, this scheme is, to some extent, insecure as an eavesdropper can steal the message easily with quantum teleportation (this problem was pointed out by the authors themselves in erratum).

In 2002, Boström and Felbinger [12] presented a quasi-secure direct communication scheme with an Einstein-Podolsky-Rosen (EPR) pair, following ideas in quantum dense coding, and the protocol is called the ping-pong scheme. However, ping-pong scheme is not secure as the title suggests, and it can be attacked fully [13] if the transmission efficiencies are lower than 60 % as the two parties of communication only exploit one basis to check eavesdropping. It is also vulnerable under the denial of service attack [14]. It can also be eavesdropped freely in a noisy channel no matter what the information transmitted is [15]. Though it was not secure, it has stimulated wide interests for direct quantum communication.

In 2002, Long and Liu proposed a two-step highly efficient QKD protocol [16]. Though it was designed for QKD, it is also fully a QSDC protocol. In 2003, the formal procedure to use the protocol for quantum secure direct communication (QSDC) was given [17], the two-step QSDC protocol. This is the first secure QSDC protocol. In it we have also introduced the criteria for a true QSDC scheme.

Now, there are many researches in the world studying the subject [17−43], either in QSDC [17−25] or in DSQC [26−43].

3 Quantum secure direct communication

3.1 Deng-Long criteria for QSDC

According to Deng-Long criteria [17, 18], a real secure QSDC scheme should satisfy four requirements [19]: (1) The secret message can be read out by the receiver directly after the quantum states are transmitted through a quantum channel, and there is not additional classical information exchange by the sender and the receiver in principle except for those for checking eavesdropping and estimating the error rate. (2) The eavesdropper, Eve cannot obtain a useful information about the secret message no matter what she does. (3) The two legitimate users can detect Eve before they encode the secret message on the quantum states. (4) The quantum states are transmitted in block by block way.

The two-step scheme [17] is secure as it satisfies all these four requirements. The quantum one-time pad QSDC scheme [18] is secure if the legitimate users can prevent an eavesdropper from stealing the information with Trojan horse attack [31, 44] and can do quantum privacy amplification on unknown single qubits [45]. The QSDC scheme proposed by Wang et al [21] with superdense coding and the multi-step QSDC scheme [22] with multi-particle Greenberger-Horne-Zeilinger (GHZ) states are secure, according to Deng-Long criteria [17−19]. The Ping-Pong scheme proposed by Boström and Felbinger [12] and its revised versions [24, 25] are insecure if there is loss [13] or noises [15] in the quantum channel. These schemes only satisfy the first requirement of the Deng-Long criteria.

3.2 Quantum secure direct communication protocols

3.2.1 *Two-step quantum secure direct communication scheme*

An EPR pair is in one of the four Bell states,

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

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

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

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

The subscripts A and B represent the two photons in an EPR pair, $|0\rangle$ and $|1\rangle$ are the two eigenvectors of the measuring basis (MB) Z.

The two-step QSDC scheme is the first secure model for quantum direct communication. Its principle is shown in Fig.1, and can be described in brief as follows [17].

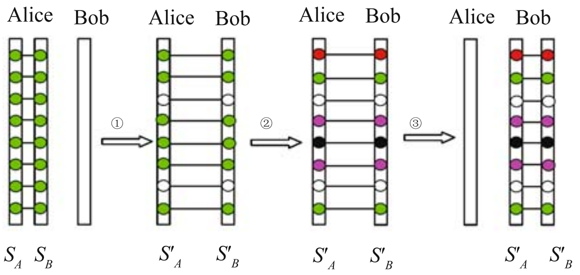

Fig.1 The principle of the two-step QSDC scheme. The two photons connected with a line represent an EPR pair. S_A is the message-coding sequence and S_B is the checking sequence.

Alice prepares an ordered N EPR pairs in the same state $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$. Alice takes one particle from each EPR pair to form an ordered EPR partner particle sequence, say S_A (shown in Fig.1). This sequence is made up of all the photons A in the ordered N EPR pairs. It is called the message-coding (M) sequence S_A. The remaining EPR partner particles compose another particle sequence, called the checking (C) sequence S_B. Alice and Bob agree that the four Bell states $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ are encoded as 00, 01, 10 and 11, respectively. In order to assure the security of the message transmitted, Alice divides the quantum communication into two steps: (1) Alice sends the checking sequence S_B to Bob first and then checks the security of this transmission with Bob. (2) If the two legitimate users confirm that the transmission of the checking sequence S_B is secure, Alice encodes her secret message on the message-coding sequence S_A with four unitary operations U_i ($i = 0, 1, 2, 3$) and then sends S_A to Bob who reads out the secret message directly with Bell-state measurements.

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{5}$$

$$U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{6}$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1| \tag{7}$$

$$U_3 = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \tag{8}$$

In the first step, Alice and Bob check eavesdropping by the following procedure [17]: (a) Bob chooses randomly a large enough subset of the photons received as the samples for checking eavesdropping, and then measures them by choosing randomly one of the two MBs, say Z and $X \equiv \{|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$. (b) Bob tells Alice which photons he has chosen, and his MBs and outcomes of the measurements on the samples. (c) Alice uses the same MBs 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 same, i.e., both Alice and Bob get 0 or 1 when they measure the photons in an EPR pair chosen for checking eavesdropping. This is the first eavesdropping check.

In order to guard for eavesdropping in the transmission of the M sequence in the second step, Alice has to add a small trick in this sequence [17]. She selects randomly some photons in the M sequence and performs on them randomly one of the four operations U_i ($i = 0, 1, 2, 3$). The number of these photons is not big as long as it can provide an analysis of the error rate. Alice keeps the secret of the positions of these sampling photons until the communication is completed. The remaining photons in the M sequence are used to carry the secret message directly.

After Bob performs Bell-state measurements on the EPR pairs received, Alice tells Bob the positions of the sampling pairs and the type of unitary operations on them. By checking the sampling pairs chosen by Alice, Bob will get an estimate of the error rate in the M sequence transmission. We call it the second eavesdropping check. Although this check cannot prevent Eve from eavesdropping, it is useful for determining the fidelity of the message transmitted and helpful for error correction if the error rate of the sampling pairs is reasonably low and the two legitimate users entrust the transmission. In fact, if the transmission of the C sequence S_B is secure, Eve can only disturb the transmission of the M sequence S_A and cannot steal the information encoded on it as none can read out a useful information from a part of maximally entangled quantum system [7].

In a quantum channel with low noises or no loss, Alice and Bob can 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 [46], should be used. If there is a small quantity of loss in the quantum channel, the two legitimate users Alice and Bob should exploit another quantum technique, quantum entanglement swapping [47], to avoid the attack done by Eve with intercepting [17]. Also quantum privacy amplification [48, 49] will reduce the information leakage to a negligible level in the first step. If the loss or noises in the quantum channel is reasonably large, two-step protocol is suitable for creating a private key rather than transmitting the secret message.

3.2.2 *Deng-Long quantum one-time pad QSDC scheme*

The quantum one-time pad QSDC scheme is proposed by Deng and Long [18] in 2003, following some ideas in two-step QSDC scheme [17] and classical one-time pad [8]. In Deng-Long quantum one-time pad QSDC scheme, the two legitimate users, Alice and Bob, first share a sequence of quantum states securely, and then the sender Alice encodes her secret message and returns the states to the receiver Bob.

In detail, Deng-Long quantum one-time pad QSDC scheme contains two phases [18]:

(1) The secure doves sending phase

The receiver Bob prepares a sequence of polarized single photons S and sends these photons to the sender Alice. Each photon is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. After receiving this photon sequence S, Alice and Bob can check the security of the transmission, similar to two-step scheme [17]. That is, Bob chooses randomly some sampling photons from the sequence S, and tells Alice their positions and their states. Alice checks the security of this transmission by measuring the samples with the same MBs as those chosen by Bob when he prepares the photons. We call it the first eavesdropping check. If they confirm that the transmission is safe, Alice and Bob continue their communication to the second phases; otherwise, they abandon their transmission and begin the communication from the beginning.

(2) The message coding and doves returning phase

Alice encodes her secret message on each photon in the sequence S' (composed of the remaining photons in the sequence S after Alice and Bob complete the first eavesdropping check) with the unitary operation $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ or the operation $U_3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ according to the message bit is 0 or 1, respectively. The nice feature of the U_3 operation is that it only flips the two eigenvectors in both MBs Z and X [18], i.e.,

$$U_3|0\rangle = -|1\rangle, \quad U_3|1\rangle = |0\rangle \tag{9}$$

$$U_3|+\rangle = |-\rangle, \quad U_3|-\rangle = -|+\rangle \tag{10}$$

After encoding the photons in the sequence S', Alice returns them to Bob. As the sequence S is prepared by Bob and the two unitary operations U_0 and U_3 do not change the MBs of the photons, Bob can choose the original MB to measure each photon for reading out the secret message. To guarantee the security of the whole communication process, it is necessary for Alice to use randomly some the photons in the sequence S' as checking instances, similar to two-step scheme [17]. For these checking photons, Alice chooses randomly one of the two unitary operations U_0 and U_3 to encode some checking information in the message coding phase. After Bob measures the photons in the sequence S', Alice announces publicly the positions and the coded bit values of these checking photons. Although, these checking photons cannot forbid the eavesdropper Eve to interrupt the transmission of the sequence S', they will give Alice and Bob an estimate whether there is an Eve in the line to intercept their communication or not. Also, Eve's eavesdropping in this phase will give her no chance to get a useful information about the secret message as she does not know the original states of the photons in the sequence S.

Certainly, this QSDC scheme can work efficiently if the sender Alice has the capability of storing quantum states. At present, this technique is not fully developed. However, this technique is a vital ingredient for quantum computation and quantum communication, and there has been great interest in developing techniques for quantum state storage, and it is believed that these techniques will be available in the future [50]. Moreover, this scheme can be implemented with existing techniques. The storage of photons can be done by optical delays in a fibre, shown in Fig.2. In practice, there are also losses in the transmission lines, error correcting techniques are necessary, similar to two-step scheme [17].

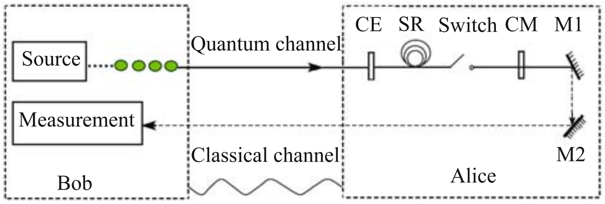

Fig.2 Implementation of the QSDC with optical delays [18]. CE is the eavesdropping check; SR represents an optical delay; Switch is used to control the quantum communication process, if the batch of photons are safe, the switch is on and the message coding is performed; CM encodes the secret message, M1 and M2 are two mirrors for in this simple illustrative set-up.

3.2.3 *QSDC scheme based on superdense coding*

In 2005, Wang *et al.* [21] proposed the QSDC scheme based on superdense coding. With low-loss quantum channels, this superdense-coding-based QSDC scheme improves the two-step QSDC scheme [17] as it does not require the sender to determine whether some of the quantum signals sent by the receiver are lost or not [21].

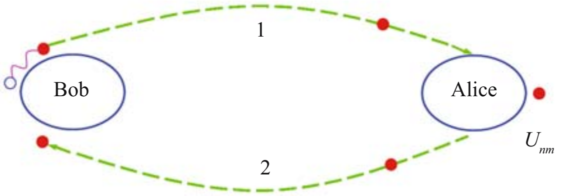

Fig.3 Schematic demonstration of quantum superdense coding [21]. The U_{nm} is the unitary operation for encoding.

For describing the superdense-coding-based QSDC scheme clearly, we first introduce the principle of quantum superdense coding, shown in Fig.3. The d-dimension Bell-basis states in a symmetric channel are [21, 51, 52]

$$|\Psi_{nm}\rangle_{AB} = \sum_j \mathrm{e}^{2\pi \mathrm{i} jn/d}|j\rangle \otimes |j+m \bmod d\rangle/\sqrt{d} \quad (11)$$

where $n, m = 0, 1, \cdots, d-1$. The unitary operations

$$U_{nm} = \sum_j \mathrm{e}^{2\pi \mathrm{i} jn/d}|j+m \bmod d\rangle\langle j| \quad (12)$$

on the particle B can transform the Bell-basis state

$$|\Psi_{00}\rangle_{AB} = \sum_j |j\rangle \otimes |j\rangle/\sqrt{d}$$

into the Bell-basis state $|\Psi_{nm}\rangle_{AB}$, i.e., $(I^A \otimes U^B_{nm})|\Psi_{00}\rangle_{AB} = |\Psi_{nm}\rangle_{AB}$. In quantum superdense coding, one party, say Alice, sends the particle B in the Bell-basis $|\Psi_{00}\rangle_{AB}$ to the other party Bob, and Bob performs the unitary operation U_{nm} on the particle B and then sends it back to Alice. Alice can read out the operation with a Bell-basis measurement on the two particles A and B. In this way, one particle can carry $\log_2 d^2$ bits of information while running forth and back. In a non-symmetric quantum channel, the two particles of the entangled quantum system have the different dimensions [53, 54], for example, the first particle has p dimensions and the second one has q dimensions. Then the capacity is $log_2 pq$.

Just like that in Ref. [21], we use a qutrit system (a quantum system with three levels) to illustrate the principle of superdense-coding-based QSDC scheme proposed by Wang *et al.*

For a qutrit system, there are four unbiased MBs. The MB Z is composed of three eigenvectors, i.e., $|Z_{-1}\rangle = |0\rangle$, $|Z_0\rangle = |1\rangle$ and $|Z_{+1}\rangle = |2\rangle$. The MB X can be chosen as [55]

$$\begin{aligned} |x_{-1}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \\ |x_0\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \mathrm{e}^{2\pi\mathrm{i}/3}|1\rangle + \mathrm{e}^{-2\pi\mathrm{i}/3}|2\rangle) \quad (14) \\ |x_{+1}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \mathrm{e}^{-2\pi\mathrm{i}/3}|1\rangle + \mathrm{e}^{2\pi\mathrm{i}/3}|2\rangle) \end{aligned}$$

The two other bases can be taken as

$$\frac{1}{\sqrt{3}}(\mathrm{e}^{2\pi\mathrm{i}/3}|0\rangle+|1\rangle+|2\rangle) \text{ and cyclic permutation,} \quad (15)$$

and

$$\frac{1}{\sqrt{3}}(\mathrm{e}^{-2\pi\mathrm{i}/3}|0\rangle+|1\rangle+|2\rangle) \text{ and cyclic permutation.} \quad (16)$$

Any basis vectors $|e_j\rangle$ and $|e_u\rangle$ belonging to different measuring bases satisfy the relation $|\langle e_j|e_u\rangle|^2 = \frac{1}{3}$. $|\Psi_{00}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$ in the MB Z, and it is changed to be $|\Psi_{00}\rangle = \frac{1}{\sqrt{3}}(|x_{-1}\rangle|x_{-1}\rangle + |x_0\rangle|x_{+1}\rangle + |x_{+1}\rangle|x_0\rangle)$ in the MB X. It is not difficult to write out the form of $|\Psi_{00}\rangle$ in the other two measuring bases.

The schematic demonstration of this QSDC protocol is shown in Fig.4. The steps can be described in detail as follows [21].

(1) The receiver Bob prepares a sequence of entangled particle pairs which are all in the Bell-basis state $|\Psi_{00}\rangle_{HT}$. Here the subscripts H and T indicate the home particle retained in home and the travelling particle which travels through the quantum channel forth and back from Bob to Alice, respectively.

(2) Bob takes one particle from each entangled particle pair for making up an ordered partner particle sequence, say $[P_1(H), P_2(H), P_3(H), \cdots, P_N(H)]$. It is called the home (H) sequence. The remaining partner particles compose another particle sequence $[P_1(T), P_2(T), P_3(T), \cdots, P_N(T)]$, and it is called the travelling (T) sequence, shown in Fig.4. Here the subscript indicates the pair order in the sequence, i.e., the i represents the i-th entangled particle pair.

(3) Bob sends the T-sequence to the sender of the secret message, Alice, and then they check eavesdropping.

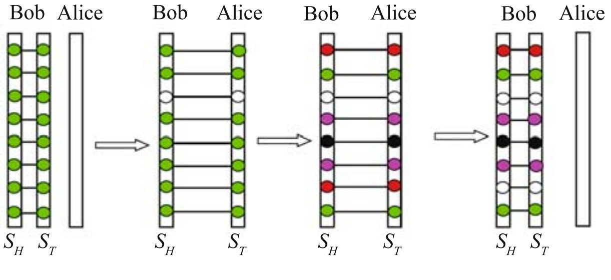

Fig.4 Illustration of the QSDC protocol with a sequence of entangled particle pairs [2]. Two particles linked with a line are in a Bell-basis state. The T sequence is travelling forth and back from Bob to Alice.

The procedure for eavesdropping check can be similar to that in the two-step QSDC [17]: (a) Alice chooses randomly some particles from the T-sequence, say the sample particles, and uses randomly one of several conjugate single-particle measuring bases to measure the particles. (b) Alice tells Bob the positions of the sample particles and the information of the measurements including the results and the measuring bases (MBs). (c) Bob takes a suitable measurement on each sample particle with the same MB as that of Alice's. (d) Bob compares his results with Alice's to determine whether there is Eve monitoring the quantum channel or not. It is the first eavesdropping check. If their results are correlated, they can continue the QSDC to next step, otherwise they abort their quantum communication.

(4) Alice encodes the secret message on the T-sequence with the unitary operations U_{nm} and then transmits it to Bob.

Certainly, Alice has to add a small trick in the procedure of encoding the secret message for the second eavesdropping check. She will select randomly some particles in the T-sequence, called sampling pairs (which are composed of the sampling particle in T-sequence and the particles correlated in H-sequence) and perform on them randomly one of the d^2 unitary operations U_{nm}. It is equal to that Alice adds some redundancy in the coding for checking the security of the transmission of the T-sequence from Alice to Bob. She keeps the secret including the positions of the particles and the operations performed on them until Bob receives the T-sequence.

(5) Bob performs the general joint Bell-basis measuring on the particles combined with H-sequence and T-sequence.

(6) Alice tells Bob the positions of the sampling pairs and the unitary operations on them. Bob completes the second eavesdropping check analysis.

(7) If the error rate of the sampling pairs is reasonably low, Alice and Bob can correct the errors in the secret message using error correction method, such as CASCADE [46] and Calderbank-Shor-Steane (CSS) [7] coding methods. Otherwise, Alice and Bob abandon the results of the transmission and repeat the procedures from the beginning.

Compared with two-step QSDC scheme, this superdense-coding-based QSDC scheme, on the one hand, avoids the use of quantum swapping in the first eavesdropping check after the T-sequence transmitted from Bob to Alice. On the other hand, it appears that high-dimensional QSDC schemes provide better security than that obtainable with two-dimensional Bell-basis states, as has been discussed in detail in Ref. [55]. The disadvantage may be that the T-sequence should be transmitted at least twice of the distance between the sender and the receiver, which will reduce the generating bit rate because of losses in a practical quantum line.

3.2.4 *Multi-step QSDC with Greenberger-Horne-Zeilinger states*

The multi-step QSDC scheme [22] is the generalization of the two-step one to the case with Greenberger-Horne-Zeilinger (GHZ) states. Let us use the three-particle GHZ state to describe the principle of this QSDC scheme. Suppose the maximally entangled three-particle state is

$$|\varphi\rangle_{ABC}=\frac{1}{\sqrt{2}}(|000\rangle_{ABC}+|111\rangle_{ABC}) \tag{17}$$

There are eight independent GHZ states, namely

$$|\varphi\rangle_0=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle) \tag{18}$$

$$|\varphi\rangle_1=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle) \tag{19}$$

$$|\varphi\rangle_2=\frac{1}{\sqrt{2}}(|100\rangle+|011\rangle) \tag{20}$$

$$|\varphi\rangle_3=\frac{1}{\sqrt{2}}(|100\rangle-|011\rangle) \tag{21}$$

$$|\varphi\rangle_4=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle) \tag{22}$$

$$|\varphi\rangle_5=\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle) \tag{23}$$

$$|\varphi\rangle_6=\frac{1}{\sqrt{2}}(|110\rangle+|001\rangle) \tag{24}$$

$$|\varphi\rangle_7=\frac{1}{\sqrt{2}}(|110\rangle-|001\rangle) \tag{25}$$

By performing single-particle unitary operations $\{U_i\}$ $(i=0,1,2,3)$ on any two of the three particles, one can change from one GHZ state to another.

For QSDC, Alice and Bob first make an agreement that each of the states $|\varphi\rangle_k$ $(k=0,1,\cdots,7)$ represents a three bits binary number, namely $|\varphi\rangle_0$, $|\varphi\rangle_1$, $\cdots$, and $|\varphi\rangle_7$ are coded as 000, 001, $\cdots$, and 111, respectively. The sender Alice prepares a sequence of ordered N three-particle GHZ-state quantum systems, labeled as $[P_1(A)P_1(B)P_1(C)$, $P_2(A)P_2(B)P_2(C)$, $\cdots$, $P_N(A)P_N(B)P_N(C)]$. The original states of the quantum systems are $|\varphi\rangle_0=\frac{1}{\sqrt{2}}(|000\rangle_{ABC}+|111\rangle_{ABC})$. Alice divides the sequence into three partner particle sequences, say $S_A=[P_1(A)$, $P_2(A)$, $\cdots,P_N(A)]$, $S_B=[P_1(B)$, $P_2(B)$, $\cdots,P_N(B)]$ and $S_C=[P_1(C)$, $P_2(C)$, $\cdots,P_N(C)]$. Alice and Bob complete their quantum communication with the four steps as follows.

(1) Alice sends the sequence S_C to the receiver Bob. After receiving this sequence, Bob and Alice check the security of the transmission, called the first eavesdropping check. They can accomplish their eavesdropping check with the following steps: (a) Bob randomly chooses some sample particles from his sequence S_C and then measures them by choosing one of the two MBs Z and X randomly; (b) Bob tells Alice the positions and the results of his sample particles; (c) Alice chooses a product MB $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ to measure her corresponding partner particles in the sequences S_A and S_B when Bob chooses the MB Z to measure his sample particles; otherwise, Alice performs a Bell-basis measurement on her particles; (d) Alice analyzes the error rate η_e of the samples, and continues the quantum communication if she finds that η_e is reasonably low; otherwise, Alice and Bob abandon the communication and repeat their quantum communication from the beginning.

(2) Alice encodes her secret message on the GHZ states. She can only operate the particles in the sequence S_B with the two unitary operations U_0 and U_2, and operate the particles in the sequence S_C with the four unitary operations $\{U_0,U_1,U_2,U_3\}$. For the second eavesdropping check, Alice chooses some particles in the sequences S_B and S_A as the samples and operates them randomly with one of the four operations U_i $(i=0,1,2,3)$.

(3) Alice measures half samples chosen from the sequence S_A in the step 2 with the MB Z or X, and then Alice sends the sequence S_B to Bob. After Bob receives the sequence S_B, Alice tells him which sampling particles in the sequence S_A are measured and the MBs chosen. Similar to step 1, Bob measures his partner particles in the sequences S_B and S_C with the product MB $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ if Alice measures her particles with the MB Z; otherwise, Bob chooses the Bell-basis state measurement on his sampling particles. After Alice announces publicly the outcomes of her measurements, Bob can analyze the error rate of those samples. If the error rate is reasonably low, Alice and Bob continue their quantum communication; otherwise, they abandon their outcomes and repeat their quantum communication from the beginning.

(4) Alice sends the sequence S_A to Bob who reads out the secret message with joint three-particle measurements on the particles in the three sequences S_A, S_B and S_C. For checking the security of whole quantum transmission, Alice tells Bob the positions of the sampling particles remained, and then the two parties analyze the error rate of the samples. If the error rate is reasonably low, they can accomplish the transmission of the secret message.

In essence, Alice and Bob transmit one of the three sequences S_C, S_B and S_A each time, and transmit another one only when they confirm that the previous transmission is secure. In this way, the eavesdropper Eve can only capture one sequence if she wants to eavesdrop the quantum communication. Any one cannot read out the whole information from a part of an entangled quantum system. That is, Eve cannot obtain the information about a GHZ-state three-particle quantum system if she only captures one particle. Thus this QSDC scheme can be made secure with other quantum techniques, similar to the two-step QSDC scheme [17].

3.2.5 *Quantum-encryption-based QSDC scheme*

A quantum-encryption-based QSDC scheme is proposed by Li *et al*. [23] in 2006. This scheme uses a controlled-not (CNot) gate to encode and decode the secret message. The two parties first share privately a sequence of two-photon pure entangled states, and then use the states as their private quantum key which is reusable with an eavesdropping check before each round. The receiver can read out directly the message and each photon transmitted between the two parties can carry one bit of message securely in principle. The obvious advantage of this QSDC scheme is that the quantum key is a sequence of pure entangled states, not maximally entangled states, which will make this scheme more convenient than others as an entanglement source usually produces non-maximally entangled signals because of asymmetric features of the quantum source.

The principle of this quantum-encryption-based QSDC scheme is shown in Fig.5. Alice and Bob first share a sequence of two-particle entangled states privately and then use them as their private quantum key. Alice can use her quantum key to encrypt her secret message and then send it to Bob who can read out it with his quantum key.

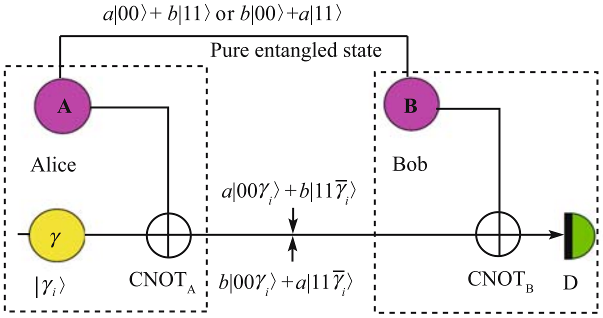
$a|00\rangle + b|11\rangle$ or $b|00\rangle + a|11\rangle$
Pure entangled state
A
B
Alice
Bob
$a|00\gamma_i\rangle + b|11\bar{\gamma}_i\rangle$
γ
$|\gamma_i\rangle$
CNOT$_A$
$b|00\gamma_i\rangle + a|11\bar{\gamma}_i\rangle$
CNOT$_B$
D

Fig.5 Illustration of the quantum-encryption-based QSDC scheme [31]. The pure entangled states are used as quantum key which are repeatedly used. "D" represents the measurement with the MB Z.

In detail, Alice and Bob can share a sequence of pure entangled states with decoy photons [56−59]. In this time, Alice first prepares n two-photon pairs randomly in one of the two pure entangled states $|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B$ and $|\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B$. The latter can be obtained by flipping the bit value of the two photons in the state $|\Psi\rangle_{AB}$; i.e., $|\Phi\rangle_{AB} = (U_2^A \otimes U_2^B)|\Psi\rangle_{AB}$. Alice picks up photon B in each pair to make up the sequence S_B : $[B_1, B_2, \cdots, B_n]$. The other sequence S_A is made up of particles $A_i (i = 1, 2, \cdots, n)$. She sends the sequence S_B to Bob and always keeps the sequence S_A at home. For checking the security of the transmission of the sequence S_B efficiently, Alice inserts some decoy photons S_{de}, which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, into the sequence S_A. Alice can get a decoy photon by measuring one photon in a two-photon pair $|\Psi\rangle_{AB}$ with the basis Z and operating the other photon with σ_x or a Hadamard (H) operation. In a word, it is unnecessary for the users to have an ideal single-photon source in this scheme. After Bob received the sequence S_B, Alice tells him the positions and the states of the decoy photons. Bob measures the decoy photons with the suitable bases and analyzes the error rate of those outcomes with Alice. If the error rate is reasonably low, they can obtain a sequence of quantum key privately and continue to the next step; otherwise, they discard the transmission and repeat quantum communication from the beginning.

For transmitting the secret message, Alice prepares a sequence of travelling particles γ_i which are in one of the two states $\{|0\rangle, |1\rangle\}$ according to the bit value of her secret message is 0 or 1, respectively. We call it the travelling particle sequence S_T. For checking eavesdropping, Alice needs to add a small trick in the sequence S_T before she sends it to the quantum channel, similar to Refs. [17, 18]. That is, he also randomly inserts some decoy photons, say S_D, which are randomly in the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, in the sequence S_T. Alice uses the quantum key, the pure entangled pairs shared $\{|\Psi\rangle_{AB}, |\Phi\rangle_{AB}\}$ to encrypt the travelling particles in the sequence S_T except for the decoy photons, shown in Fig.5. That is, Alice performs a controlled-not (CNOT) operation on the particles A_i and γ_i $(i = 1, 2, \cdots, n)$ by using the particle A_i as the control qubit. Then Alice sends all the travelling particles to Bob. After receiving the sequence S_T, Bob asks Alice to tell him the positions and the states of the decoy photons, and then measures them with the same bases as those Alice chose for preparing them. For the particles B_i and γ_i, Bob takes a CNOT operation on them with the particle B_i as the control qubit, similar to Alice, and then he measures the particles γ_i with the basis Z and records the outcomes of the measurements. If Alice and Bob confirm that the transmission is secure, Bob reads out the message directly and repeat their communication by repeatedly using their quantum key to transmit the secret message again in the next round;

otherwise, they have to abandon their results and repeat their quantum communication form the beginning, i.e., sharing a sequence of pure entangled states.

As the quantum key is randomly in one of the two states $|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B$ and $|\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B$ for the eavesdropper Eve, the state of the composite quantum system composed of the two particles A_iB_i in a quantum key and the travelling particle γ_i is randomly in one of the two states $\{a|00\gamma_i\rangle + b|11\overline{\gamma_i}\rangle, b|00\gamma_i\rangle + a|11\overline{\gamma_i}\rangle\}$. That is, the density matrix of the travelling particle γ_i for Eve is $\rho_i = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The eavesdropping on this travelling particle gives no useful information about the secret message. Moreover, Eve's action will leave a trace in the results of the decoy photons. So this quantum-encryption-based QSDC scheme is secure in principle.

In a practical channel, the users can exploit entanglement purification [48] to keep the entanglement in the quantum key, and do quantum privacy amplification [48, 49] on them as well. However, the two users need not to purify their states to Bell states, just the pure entangled states $|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B$ ($|\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B$) or $|\Psi\rangle'_{AB} = a'|0\rangle_A|0\rangle_B + b'|1\rangle_A|1\rangle_B$ ($|\Phi\rangle'_{AB} = b'|0\rangle_A|0\rangle_B + a'|1\rangle_A|1\rangle_B$) in this scheme. Here $|a'|^2 + |b'|^2 = 1$. As the quantum key is just used to encrypt and decrypt the secret message, it is unnecessary for the users to keep the same states as those they used in last time, just the correlation of each pair, which will increase the efficiency of the entanglement purification process largely. Certainly, on the one hand, the users should do error correction on their results in practical applications, same as the two-step protocol [17]. On the other hand, this QSDC scheme can only used to distribute a private key if the loss of the quantum line is unreasonably large.

3.3 Quasi-secure QSDC protocols

3.3.1 *Ping-pong protocol*

In 2002, Boström and Felbinger [12] proposed the ping-pong protocol for direct communication, following some ideas in quantum dense coding [60]. In their protocol, the receiver Bob first prepares an EPR pair AB in the entangled state $|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$. Bob sends the photon A to the sender Alice who chooses two communication modes, message mode and control mode, with the probabilities $1-c$ and c, to operate the photon A received. When she chooses the message mode, Alice operates the photon A with the unitary operations U_0 and U_1 according to the bit value of her secret message is 0 or 1, respectively, and then Alice returns the photon A back to Bob who performs a Bell-basis measurement on the photons A and B to read out the message. If she chooses the control mode, Alice measures the photon A with the MB Z. When Alice and Bob choose an enough large set of control-mode particles, they analyze the security of their transmission.

Wójcik introduced an interesting eavesdropping attack [13] on the "ping-pong" quantum communication protocol in the case of considerable quantum channel losses. That is, Wójcik showed that the ping-pong protocol is not secure for transmission efficiencies lower than 60 %. Cai showed that the ping-pong protocol can be attacked by the denial of service approach by just measuring the travelling photons in the Z basis without being detected [14]. Though Eve does not steal any useful information, she can destroy the communication completely.

In 2007, Deng *et al.* [15] introduces an attack scheme for eavesdropping freely the ping-pong quantum communication protocol in a noise channel. It means that the ping-pong protocol can be eavesdropped freely if the error rate ε_c introduced by the noise in quantum channel is not zero. We introduce this scheme in detail as follows [15].

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

$$|+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$
$$|-\theta\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle \tag{26}$$

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

$$\sin^2\theta \leqslant \varepsilon_c \tag{27}$$

When the outcome of the measurement is $|0\rangle_A$, Eve prepares the N-photon fake signal in the same state $|+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, shown in Fig.6, 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 Z. In this way, Eve's eavesdropping will introduce the error rate $\varepsilon_E = \sin^2\theta$ 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 origin one to hide her eavesdropping freely.

Let us use an example to demonstrate the principle of this attack. Suppose that $\varepsilon_c = 10$ % and Eve uses an ideal quantum channel to steal the message below. Owing to the symmetric, we assume that there are $N = 2^m$ photons in the fake signal,

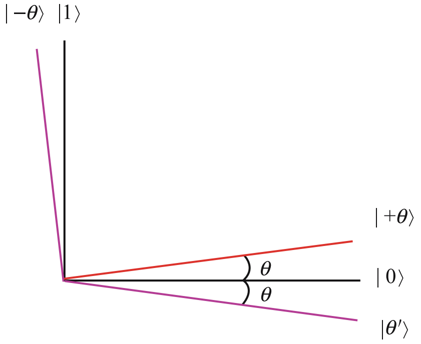

Fig.6 The state of the multi-photon fake signal. $|+\theta\rangle$ and $|-\theta\rangle$ are the two eigenstates of the measuring basis σ_θ.

$$\varepsilon_E = \sin^2\theta = \varepsilon_c = 0.1 \tag{28}$$

After the coding done by Bob with one of the two local unitary operations U_0 and U_1, 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, shown in Fig.7, similar to Ref. [44]. If Alice performs the U_0 operation on the fake signal, the photons in the fake signal are in the state $|A'\rangle = |+\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$; otherwise $|A'\rangle = |\theta'\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$. The attack for obtaining the information about the local unitary operations done by Alice is simplified to distinguish those two states. It is impossible for Eve to get 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. For instance, if there are N photons with which Eve distinguish the two states $|+\theta\rangle$ and $|\theta'\rangle$, the probability that Eve will succeed is $P_s = 1 - (\cos^2 2\theta)^{n-1} = 1 - 0.64^{n-1}$. When $n = 16$, $P_s \approx 0.998\,76$. It means that Eve can obtain the message fully without being detected.

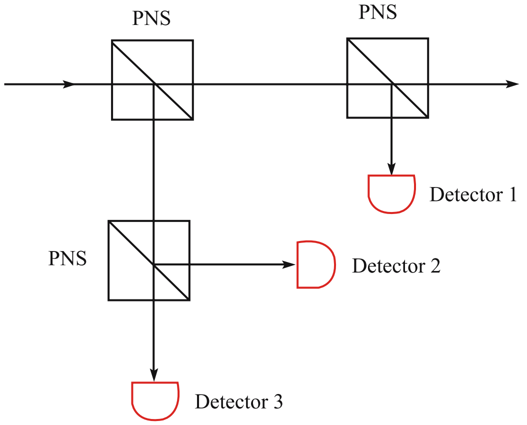

Fig.7 The attack with the photon number splitters (PNS: 50/50) in the case that there are four photons in each fake signal, similar to Ref. [44].

3.3.2 *The modified ping-pong protocol*

In 2004, Cai and Li [24] proposed a way for improving the capacity of the ping-pong quantum communication protocol. We call it the modified ping-pong protocol. In fact, they combine the ideas in quantum dense coding [60] and the two-step QSDC scheme [17] to improve the capacity of the ping-pong protocol. Different from the original ping-pong protocol, the sender Alice, in this time, chooses randomly two MBs Z and X to measure her photon A received when she chooses the control mode, and performs one of the four operations U_i $(i = 0, 1, 2, 3)$ to code her message on the photon A and then sends it back to Bob when Alice chooses the message mode.

The modified ping-pong protocol [24] is secure for distributing a private key, but just quasi-secure for transmitting a secret message directly. In essence, the security issue in ping-pong quantum communication protocol [12] arises from the fact that the two authorized users transmit the qubits one by one and check the eavesdropping only with the same MB Z [15]. The secret message transmitted cannot be discarded, different from the outcomes in QKD [8]. For improving the security of the ping-pong quantum communication protocol, it is necessary for Alice and Bob to transmit the qubits in a quantum data block, similar to [17—19], and measure the sampling instances with two MBs Z and X [15]. 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 do quantum privacy amplification on the quantum date [17—19] before Alice codes her message on the quantum states. Those two interesting characters paly an important role in the security of QSDC protocols.

Although there are some flaws in the modified Ping-Pong protocol [24] for direct communication, it provides a good way for improving the capacity of the original ping-pong protocol. Moreover, this protocol can be used to create a private key efficiently.

3.3.3 *Cai-Li quantum communication protocol*

In 2004, Cai and Li [25] proposed a deterministic secure direct communication protocol using single qubit in a mixed state, following some ideas in the ping-pong protocol [12]. Let us call it Cai-Li quantum communication protocol. For quantum communication, Bob prepares a single photon in one of the two states $\{|0\rangle, |+\rangle\}$, and then sends it to Alice who chooses two modes, message mode and control mode, to deal with the photon received, similar to the ping-pong protocol [12]. When Alice chooses the message mode, she codes the photon with U_0 or U_3 according to the bit value of the secret message is 0 or 1, respectively, and then sends the photon back to Bob who performs a measurement on the photon with the same MB as that he originally chooses for preparing it. When Alice chooses the control mode, she replaces the photon received with a new one which is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then send the new one back to Bob.

Cai-Li quantum communication protocol is insecure with a lossy quantum channel as it can be attacked easily with an opaque attack scheme in principle. In brief, the eavesdropper Eve can intercept the single photon sent from Bob and measure it with two directions, i.e., the directions of the two states $\{|1\rangle, |-\rangle\}$. When Eve finds that the photon clicks the detector correlated to the state $|1\rangle$ (the detector correlated to the state $|-\rangle$), she prepares a fake single photon whose state is $|+\rangle(|0\rangle)$ and sends it to Alice; otherwise, she sends nothing to Alice. After Alice codes her message on the fake photon and returns it to Bob, Eve intercepts the fake photon again and measures it with the same MB as that she chooses for preparing it. Obviously, Eve's action does not introduce errors in the results obtained by Alice and Bob, but just some losses. Eve can hide her eavesdropping with a better quantum channel. That is, Cai-Li quantum communication protocol is insecure for QKD, just like the Bennett 1992 QKD protocol under opaque attack [61]. Therefore some additional procedure is required to improve its security.

4 Deterministic secure quantum communication protocols

There are two kinds of deterministic schemes. One is quantum secure direct communication (QSDC) [17−19] in which the receiver can read the secret message directly, and the two parties of quantum communication exchange classical information only for checking eavesdropping. The other is called deterministic secure quantum communication (DSQC) [26] in which the receiver can read out the secret message by exchanging at least an additional classical bit for each qubit, i.e., classical communication is needed besides eavesdropping check. To some extent, DSQC process is similar to the QKD protocol which is used to creates a random key first and then use it to encrypt the message [17−19]. Although an additional classical bit is needed for each qubit, DSQC process can ensure the security before the message is transmissed and the qubits is transmitted only the distance between the sender and the receiver, which will increase the bit generating rate [26]. In this way, it is also interesting to study deterministic secure quantum communication, especially in the case with a lossy quantum channel.

4.1 DSQC without maximally entangled states

There are two DSQC schemes without maximally entangled states proposed by Li *et al.* [26], following some ideas in the delay-measurement quantum communication protocol [50]. One utilizes the pure entangled states as quantum information carriers, called it pure-entanglement-based DSQC, and the other one makes use of the d-dimensional single photons, called it single-photon-based DSQC. Both of them introduce the decoy photons [56−59] for security checking and only single-photon measurements are required for the two parties, the sender Alice and the receiver Bob.

The pure-entanglement-based DSQC [26] is one of the most convenient protocols as the two parties use pure entangled states as the quantum information carries and this protocol requires that the receiver has the capability of taking single-particle measurements. The information carriers in two-particle pure entangled states can be prepared in experiment easily with present technologies, and a single-photon measurement is simpler than a multi-particle joint measurement at present. We write the pure entangled states as

$$|\Psi'\rangle_{AB} = a|0\rangle_A|1\rangle_B + b|1\rangle_A|0\rangle_B \tag{29}$$

$$|a|^2 + |b|^2 = 1 \tag{30}$$

where the subscript A and B indicate the two correlated photons in each entangled state. As the two photons in this state do not have a good correlation in both Z basis and X basis like EPR pairs, decoy photons [56−59] are introduced for the eavesdropping check. Firstly, the sender Alice prepares ordered N two-photon pairs randomly in one of the two pure entangled states $|\Psi'\rangle_{AB}, |\Psi''\rangle_{AB}$. Here $|\Psi''\rangle_{AB} = a|1\rangle_A|0\rangle_B + b|0\rangle_A|1\rangle_B$. Alice picks up A particles to form an ordered sequence S_A and the other partner photons compose the sequence S_B. For security check, Alice replaces some photons in the sequence S_B with her decoy photons S_{de} which are produced randomly in one of the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The decoy photons can be prepared from the pure entangled quantum system $|\Psi\rangle_{AB}$ by taking a single-photon measurement on the photon A and manipulating the photon B with some unitary operations. Alice encodes her message on photons in S_B by performing I or σ_x, which represent classical bits 0 or 1. Then Alice sends sequence S_B to Bob. After Bob receives S_B, Alice and Bob check the eavesdropping by measuring the decoy photons and comparing the outcomes. If the error rate is low, Alice and Bob measure their remaining photons with basis Z, and they get the results R_A and R_B, respectively. Alice publishes her results R_A. Then Bob reads out the secret message M_A as $M_A = R_A \oplus R_B \oplus 1$. As this scheme requires only single-photon measurements and pure entangled quantum signals, it is far more convenient than others with entanglement swapping and quantum teleportation, and it is more feasible in practice. This protocol also be generalized to the case with d-dimensional quantum system [26]. The intrinsic efficiency approaches 100 % and the total efficiency exceeds $\frac{1}{3}$ in theory which is larger than congeneric schemes using EPR pairs.

The single-photon-based DSQC protocol [26] utilizes the d-dimensional single-photon quantum systems as message carriers. The Z_d basis of a d-dimensional system is

$$|0\rangle\,, \quad |1\rangle\,, \quad |2\rangle\,, \quad \cdots, \quad |d-1\rangle \tag{31}$$

The d eigenvectors of the measuring basis X_d can be described as [26, 57, 62, 63]

$$\begin{aligned}
|0\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + |1\rangle + \cdots + |d-1\rangle\right) \\
|1\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}\,|1\rangle + \cdots + \mathrm{e}^{\frac{(d-1)2\pi \mathrm{i}}{d}}\,|d-1\rangle\right) \\
|2\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + \mathrm{e}^{\frac{4\pi \mathrm{i}}{d}}\,|1\rangle + \cdots + \mathrm{e}^{\frac{(d-1)4\pi \mathrm{i}}{d}}\,|d-1\rangle\right) \\
&\cdots \\
|d-1\rangle_x &= \frac{1}{\sqrt{d}}(|0\rangle + \mathrm{e}^{\frac{2(d-1)\pi \mathrm{i}}{d}}\,|1\rangle + \mathrm{e}^{\frac{2\times 2(d-1)\pi \mathrm{i}}{d}}\,|2\rangle \\
&\qquad + \cdots + \mathrm{e}^{\frac{(d-1)\times 2(d-1)\pi \mathrm{i}}{d}}\,|d-1\rangle)
\end{aligned} \tag{32}$$

Firstly the sender Alice prepares a sequence of d-dimensional single photons sequence S by choosing randomly the basis Z_d or X_d. She chooses some photons as the decoy ones and encrypts her secret message M_A on the other photons with unitary operations U_m, U_m^x, where

$$U_m = \sum_j |j + m \bmod d\rangle\langle j| \tag{33}$$

$$U_m^x = \sum_j \mathrm{e}^{\frac{2\pi \mathrm{i}}{d} jm} |j + m \bmod d\rangle\langle j| \tag{34}$$

That is, Alice encodes her message with U_m if the photon is prepared with the Z_d basis. Otherwise, she will encode the message with U_m^x. Then Alice sends the sequence S to Bob. After the transmission, they check the eavesdropping by measuring the decoy photons and analyzing the error rate. If the transmission is secure, Alice tells Bob the original states of the photons. Then Bob measures them with the suitable bases and reads out the secret message M_A with his outcomes. This protocol is more convenient in practical applications in virtue of that it only requires the parties to prepare and measure single photons.

4.2 DSQC with quantum teleportation

Since the first protocol was proposed in 1993 [51], quantum teleportation has been studied widely, and has been applied in some other quantum communication branches, such as QKD, quantum secret sharing (QSS) and so on. In 2004, Yan *et al.* put forward a secure quantum communication scheme using EPR pairs and quantum teleportation [27]. There is not a transmission of the qubits carrying the secret message between the two parties, which makes this communication more secure and more convenient for privacy amplification.

First, the two parties share a set of entangled pairs randomly in one of the four Bell states securely. Suppose that all the EPR pairs used in the scheme are $|\phi^+\rangle_{AB}$. The sender Bob prepares a sequence of C particles in the X basis $|\psi\rangle_C$ according to his secret message ($|+\rangle$ for "0", $|-\rangle$ for "1"). Bob performs Bell-state measurements on his two particles BC. Each outcome will occur randomly with the equal probability 0.25 and Alice's particles will be related to the initial states of particles C by a fixed unitary transformation U_{ij} lying on Bob's measurement outcomes. After Bob publicly broadcasts his outcomes, Alice can apply the corresponding inverse transformation U_{ij}^{-1} to her particles and measures them with the basis $X \equiv \{|\pm\rangle\}$. Then Alice can obtain Bob's message. As the security is ensured before the secret communication, this protocol is completely secure.

Subsequently, Gao *et al.* proposed two secure direct communication schemes using controlled teleportation [40, 41]. One uses the three-particle GHZ state [40] and the other one utilizes the three-particle entangled state $\frac{1}{2}(|000\rangle + |110\rangle + |011\rangle + |101\rangle)$[41]. Three parties first share a set of the entangled states. The sender performs a Bell-state measurement on a information particle and a particle in the entangle state, and the controller performs a single-particle measurement. According to their measurement outcomes, the receiver Bob can select a suitable unitary operation and then take a single-particle measurement on his particle for reading out the secret message.

4.3 DSQC with entanglement swapping

Entanglement swapping [47] is applied diffusely in quantum communication because of its elegant correlation. In 2005, Man *et al.* [29] exploited entanglement swapping to design a protocol for deterministic secure quantum communication. This protocol also uses the maximally entangled EPR pairs as the quantum carriers. In advance, the two parties assume that each of the four unitary operation represents a two-bit classical information. Bob prepares a series of EPR pairs in $|\Psi^+\rangle_{A_iB_i} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}$ and sends the A sequence, which is composed of all the A particles in the EPR pairs, to Alice. They both store the photons by grouping two photons together, i.e., photons A_1 and A_2 as a group and B_1 and B_2 as one group. In the case that the transmission is secure, Alice performs her two-bit encoding via local unitary operation on one photon of each group. Then Alice and Bob perform the Bell-state measurement on each group of their own particles. Alice publishes her measurement results. Bob can conclude Alice's operation according to his measurement outcomes and those published by Alice, and extract the secret message. The former protocol makes use of two EPR pairs for entanglement swapping. For two bits information, four qubits were prepared and two additional classical bits are transmitted.

In 2004, Gao *et al.* [42] proposed a DSQC scheme using three EPR pairs for entanglement swapping. The preparation is the same as Man's design. Alice and Bob store the photons by using three photons as a group. The sender Alice perform unitary operations on two photons of each group. For one photon, she choose one of the four unitary operations. And for the other, she choose one of I or σ_x to encode one bit information. Then Alice and Bob perform three-particle GHZ measurements on each group. Bob can deduce Alice's message by his own measurement results and Alice's outcomes published. For three bits information, six qubits are utilized and three classical bits are exchanged. We can see the aforesaid two DSQC schemes using entanglement swapping have equivalent efficiency.

Afterward, Gao *et al.* developed the DSQC protocol to three-party situation [43]. There are two senders and one receiver. They use three-particle GHZ state and sort two photons as a group. One sender can selects one of the four unitary operations to encode two bits information and the other one can choose I or σ_x to encrypt one bit message. Each party performs Bell state measurement on his own group. According to two senders' measurement results and his own outcomes, the receiver can read out the two sender's message respectively.

DSQC protocols utilizing quantum teleportation or entanglement swapping have the same advantages that the security of communication is based on the security of the process for sharing the entanglements, so that they can ensure the security before the secret communication. As the qubits do not suffer from the noise and the loss aroused by the channel again, the bit rate and the security will increase in practical conditions.

4.4 DSQC based on the rearrangement of orders of particles

Recently, Zhu *et al.* [30] proposed a new DSQC protocol based on the rearrangement of orders of particles using EPR pairs as quantum information carriers, following some ideas in the controlled-order-rearrangement-encryption QKD protocol [64]. The transmitting order of the particles which ensures the security of communication is secret to any other people except for the sender Bob himself. Let us review the process of this scheme [30] in brief. The two parties agree that the four unitary operations represent two bits of classical information. The receiver Alice prepares a sequence of EPR pairs randomly in one of the four Bell states $\{|\phi^\pm\rangle_{AB}, |\psi^\pm\rangle_{AB}\}$ and divides them into two corresponding sequences, called A sequence and B sequence. The A sequence is composed of all the A particles in the EPR pairs. Alice sends the B sequence to Bob. Bob selects a sufficiently large subset of photons as his checking set and performs one of the four unitary operations on them randomly. For the other photons, Bob chooses a suitable unitary operation on each photon, according to his secret message. Before sending back the encoded photon sequence, Bob rearranges the order of the photons in the sequence. After Alice confirms the receipt of the B sequence, Bob tells Alice the positions of the checking photons. Alice performs the Bell-state measurements on the sample pairs and then checks the eavesdropping with the checking set. In the case that the transmission is secure, Bob exposes the secret order and then Alice can obtain the secret message with Bell-state measurements on the other EPR pairs after recovering their original orders.

Subsequently, Wang *et al.* [33] put forward another DSQC protocol with single photons based on the secret transmitting order of particles. The receiver Alice prepares a sequence of single photons (i.e., ordered N single photons) which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends the sequence to Bob. Bob selects randomly a sufficiently large subset to perform U_0 or U_3 operation randomly for eavesdropping check laterly. He performs one of these two operations on the remaining photons according to his secret message, and sends them back to Alice. If the error rate exceeds the threshold they preset, they abort their quantum communication. Otherwise, Bob publishes the secret order of the photons in the sequence. Alice reads out Bob's message with single-photon measurements using the basis she prepared the photons.

Ostensibly, these two DSQC protocols [30, 33] using transmitting order rearranging method are simpler than the two-step QSDC scheme as they only require one eavesdropping check. However, there is a security loophole because they both are two-way quantum communication protocols. The security of these two quantum communication protocol is based on the secret order of the particles which will be published after the security checking. If Alice and Bob cannot detect the eavesdropper during the checking process, the eavesdropper Eve can get the secret order and the whole message. Recently Li *et al.* point out the security leak and present a possible improvement [31]. They indicate the protocols are insecure with Trojan horse attack strategies. An invisible photon or delay one are introduced to attack these schemes. The invisible photon proposed by Cai is a photon produced with a wavelength different from the wavelength of the authorized parties. As that the single photon detector is only sensitive to the photons with a special wavelength, the invisible photon will not be detected. Generally, the invisible photon may obtain nothing if the legitimate users' operation is done by optical device which is wavelength-dependent. However, in the aforesaid protocols there is no security checking in the line from Alice to Bob. Eve can choose a special wavelength close to the legitimate one to produce the invisible photons without worrying being detected and the probability that Eve can obtain the correct information is close to 1. The delay-photon Trojan horse attack is inserting a spy photon in a legitimate signal with a delay time, shorter than the time windows of the optical device. The attack strategy is described as follows. (1) Eve prepares a set of spy photons (invisible one or delay one both work) and inserts them into the legitimate signal in the line Alice to Bob. (2) After Bob performs the unitary operation, Eve sorts her spy photons out in the line Bob to Alice. As there is no security checking, Eve will not be detected. And when Bob performs his unitary operations on the authorized photons, he also performs them on the spy photons. So does the order rearranging manipulation. (3) After Bob publishes the secret order, Eve can perform measurements on the spy photons and get the secret message freely and fully. In order to defeat this kind of attack, another security checking is inserted before Bob's operations. That is, Bob chooses a large subset of photons randomly as sample photons. He splits the sample signals with photon number splitters (PNS) and measures the two signals with bases Z or X randomly, and analyzes the multiphoton rate and the error rate. If both the error rate and the multiphoton rate are very low, they continue to the next step. Otherwise, they terminate the communication. Furthermore, Bob has to inserts a filter in front of his devices to filter out the photon signal with an illegitimate wavelength. This improvement will help these DSQC protocols defeating the Trojan horse attack. In a word, the insecurity point of these two DSQC protocols is that there is only one security checking for a two-way quantum communication. The most important point is that for each block of transmission, an eavesdropping check is inevitable for secure communication, no matter what is transmitted with a quantum channel [31].

5 Quantum secure direct communication network

To date, there are only a few QSDC network schemes. Maybe it results from the fact that a QSDC network protocol requires high security and almost all the existing point-to-point QSDC schemes cannot be used for QSDC network directly. In a network, there are some servers who prepare and measure the quantum signals, which simplifies the users' devices, same as a classical communication network such as world wide web (WWW). On the other hand, it increases the difficulty for the two legitimate users to prevent the server who has more information about the quantum information carriers from eavesdropping.

In 2006, Li *et al.* [20] proposed the first QSDC network based on the two-step protocol [17] with EPR pairs. Each subsystem of the network has three parties, the server Alice, the sender Bob and the receiver Charlie, shown in Fig.8. Before the communication, the three parties on the network agree on that the four unitary operations $\{U_0, U_1, U_2, U_3\}$ represent two bits of classical information $\{00, 01, 10, 11\}$, respectively. The server Alice prepares ordered N EPR pairs in the same state $|\psi^+\rangle_{CM} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{CM}$, and divides them into two corresponding sequence S_C (checking sequence) and S_M (message sequence), similar to the two-step protocol [17]. Alice sends the two sequences to Bob by means of the two-step QSDC protocol. Bob replaces a subset of photons in the S_C sequence with decoy photons prepared randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then sends this sequence to Charlie. After Charlie confirms the receipt, they check the security using the decoy photons. If the channel is secure, Bob codes his message by performing unitary operations on the S_M sequence. Of course, Bob also picks out a subset of S_M and performs random operations on them for checking eavesdropping. We suppose there are $k + j$ photons were chosen. Then Bob sends the message sequence to Charlie. Charlie and Bob analyze the security of the transmission with k photons. If the error rate is low, Charlie performs one of the four operations randomly on one photon of each EPR pair and sends all the pairs to Alice. Alice performs Bell-state measurements on the EPR pairs and publishes the outcomes. Bob and Charlie use the remaining j photons to estimate the error rate. Charlie can read out Bob's message independently. This is a circular transmission process.

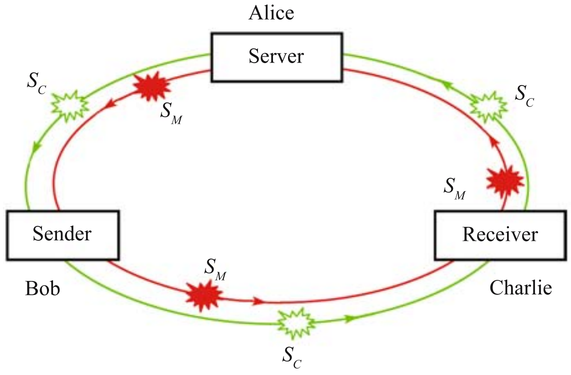

Fig.8 The subsystem of the first QSDC network [20].

In 2006, Deng *et al.* proposed a bidirectional QSDC network [19]. It also uses the EPR pairs as quantum carrier. Its subsystem is shown in Fig.9. The server Alice prepares a set of EPR pairs in the state $|\psi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{BC}$ and divides them into two sequence S_B and S_C. The sequence S_B is composed of all the B particles in the EPR pairs $|\psi^-\rangle_{BC}$. Alice sends the two sequences, S_B and S_C, to Bob and Charlie, respectively. After receiving the two sequences, Bob and Charlie select a sufficiently large subset of these EPR pairs as samples to check eavesdropping. They measure the sample photons with the bases Z and X randomly to check the transmitting security, similar to the Bennett-Brassard-Mermin 1992 (BBM92) QKD protocol [65]. If the error rate is low, Bob encodes his message on the sequence S_B by choosing one of the four unitary operations $\{U_0, U_1, U_2, U_3\}$ and Charlie chooses randomly one of the operations to perform on the photons in S_C sequence. Furthermore, Bob selects a subset of photons as checking samples. They both send the sequences back to Alice. Alice performs Bell-state measurements on the EPR pairs and broadcasts the outcomes. Bob and Charlie use the checking photons to estimate the error rate. If the transmission is secure, Charlie can deduce Bob's message with his random operations chosen. Moreover, Deng *et al.* [19] also put forward a QSDC network with entanglement swapping in which Bob and Charlie have to perform the Bell state measurement. That is, in the above protocol, after Bob and Charlie perform their unitary operations, they perform the Bell-state measurements on the corresponding neighboring photons. Bob publishes his results and Charlie can read out Bob's secret message by combining his outcomes and the information published by Bob. This scheme prevents the server Alice from accessing the photons again, which reduce the probability she eavesdrops the quantum communication, but it requires high technique in the user's port.

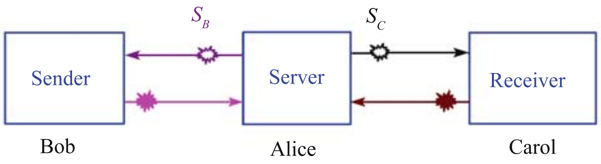

Fig.9 The subsystem of QSDC network [19].

Recently, Deng *et al.* [66] proposed a new QSDC network with single photons, which are initially prepared in the same state $|0\rangle$ by the server Alice. The subsystem of this QSDC network is shown in Fig. 10. Alice sends a single-photon sequence S_0 to the receiver Charlie. Charlie measures a subset of photons selected randomly with the basis Z to check the transmitting security and uses photon beam splitters (PBSs) to analyze the multi-photon rate [31, 44]. If Charlie confirms that there is no eavesdropper monitoring the quantum channel, he operates each photon with I or σ_x randomly and inserts some decoy photons which can be produced by Hadamard operation on the particles Alice prepared into the sequence S, and then sends them to the sender Bob. Bob chooses all the decoy photons and some other single photons for eavesdropping check. He also uses some PBSs to check whether there are more than one photon in each signal. If the error rate is low, Bob encodes his message on the photons by choosing I or σ_x. Before Bob sends the sequence to Alice, he selects a subset of photons as samples for checking the security of transmission between him and Alice. Alice measures the

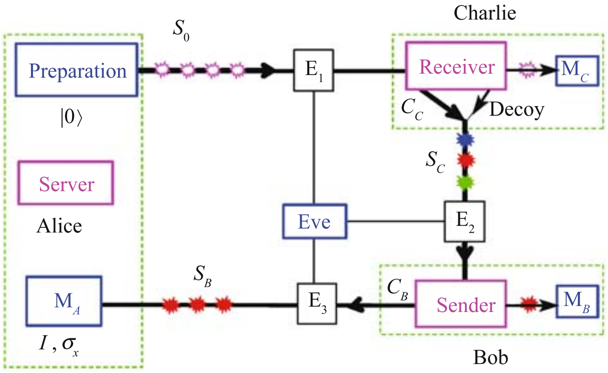

Fig.10 The subsystem of QSDC network based on single photons [66].

photons with Z basis and broadcasts the outcomes. After the last checking process, Charlie can read out Bob's message directly. In this protocol, there are three checking processes for three transmission processes to ensure the security of quantum communication. This QSDC network scheme is easy to be applied in a practical application as the users on the network need only have the ability of performing single-photon measurements and local unitary operations.

In essence, the QSDC network scheme with single photons is a circular one. This topology structure is also used in the QSDC network scheme [62] with superdense coding.

6 Single qubit quantum privacy amplification for QSDC with single photons: the CHC privacy amplification

In a practical quantum channel, noises inevitably exit. These noises are either due to the errors in the channel itself, or the actions of an eavesdropper. Due to the noise, the keys obtained from the QKD process are not complete secure. To get a key sequence with arbitrarily high security, one has to perform privacy amplification. Classical privacy amplification [67, 68] has been used for the BB84 QKD protocol [69]. With entangled photon pairs, the privacy amplification procedure will be different, for instance quantum privacy amplification (QPA) [48, 49] has been used for QKD using entangled quantum systems in the Ekert91 QKD scheme [70]. By far, quantum privacy amplification on a sequence of entangled Einstein-Podolsky-Rosen (EPR) pairs can be performed with entanglement purification [48, 49].

However, in some quantum communication applications, the end results are a batch of single photons in unknown quantum states, for instance in the Deng-Long quantum one-time pad QSDC protocol [18]. This QSDC protocol [18] has two distinct features. First, it uses single photons instead of entangled photon pairs, which has made its experimental realization a lot easier. Secondly, the transmission is operated in a batch by batch manner, and this is a necessary requirement in security [17−19]. This feature is later been used in other QSDC protocols in Refs. [17, 21, 22, 27, 29]. To ensure the safety of the secret message, the quantum channel in public must be assured secure so that no secret message is leaked even though a malicious eavesdropper may intercept the encoded qubits. Over a noiseless quantum channel, the quantum one-time-pad QSDC scheme [18] is completely secure. In a noisy channel, privacy amplification should be used to reduce the information leakage to a required security level. It is also required in controlled teleportation [71].

A quantum privacy amplification for QSDC has recently been designed for privacy amplification of QSDC with single photons, the SQ-QPA [45]. The core operation of the privacy amplification, contains two controlled-not (CNOT) gates and one Hadamard (H) gate, shown in Fig.11. The single qubits are divided into groups of two qubits each. On each group, the CNot-Hadamard-CNot (CHC) operation is performed together with a follow-on single qubit measurement on one qubit (the target qubit) by choosing the basis Z. The measured photon collapses, and the controlled photon is left-over, and it carries the state information of the discarded photon. The state information of the two photons are condensed into a single photon. Hence the privacy of the state of the left-over photon is amplified. If this procedure is repeated, the state information leakage will be reduced to an arbitrarily low level.

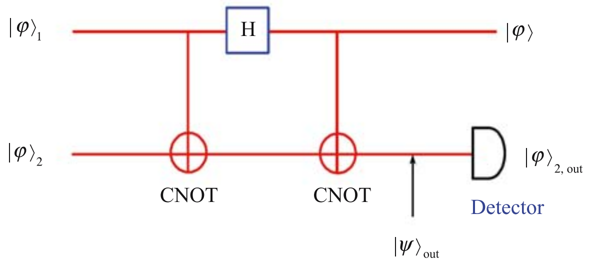

Fig.11 Quantum privacy amplification operation for two qubits [45]. It includes two controlled-not (CNOT) gates and a Hadamard (H) gate. $|\varphi\rangle_1$ and $|\varphi\rangle_2$ are the states of the two qubits (photon 1 and photon 2), respectively. After the operation, the qubit 2 is measured and the information of the original state of photon 2 is incorporated into photon 1.

The basic scientific task for the SQ-QPA scheme is the following. Suppose Bob sends Alice a batch of single photons, each photon is randomly prepared in one of the four quantum states $|+z\rangle \equiv |0\rangle, |-z\rangle \equiv |1\rangle, |+x\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-x\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$. An error bit ratio r is known for the photon batch. The SQ-QPA task is to process a portion of photons from the batch so that Eve's information about the processed photons is below a desired level.

The basic operation of SQ-QPA is shown in Fig.11 for two qubits. Without loss of the generality, we assume the quantum states of single photon 1 and 2 are

$$|\varphi\rangle_1 = a_1 |0\rangle + b_1 |1\rangle \tag{35}$$

$$|\varphi\rangle_2 = a_2 |0\rangle + b_2 |1\rangle \tag{36}$$

where

$$|a_1|^2 + |b_1|^2 = |a_2|^2 + |b_2|^2 = 1 \tag{37}$$

After the CHC operations, the state of the joint system is changed to

$$|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{2}}\{(a_1a_2 + b_1b_2)\,|0\rangle_1 + (a_1b_2 - b_1a_2)\,|1\rangle_1\}\,|0\rangle_2$$

$$+\frac{1}{\sqrt{2}}\{(a_1a_2 - b_1b_2)\,|1\rangle_1 + (a_1b_2 + b_1a_2)\,|0\rangle_1\}\,|1\rangle_2 \qquad (38)$$

After measuring the qubit 2 with the basis Z(name this process $\sigma_{2,z}$), no matter what the result is, the state of the control qubit $|\varphi\rangle_{1,\text{out}}$ will contain the information of the state of the original target qubit (qubit 2). Tables 1 and 2 give the output state of control qubit after the measurement on the target qubit with result 0 and 1, respectively. It depends not only on the result of the measurement on the target qubit, but also on the original states of the two input single photons.

Tables 1 The state of the output qubit when the result of the second qubit measurement is $|0\rangle$. φ_1 and φ_2 are the states of the original control and target qubit, respectively.

φ_2	φ_1			
	$\|+z\rangle$	$\|-z\rangle$	$\|+x\rangle$	$\|-x\rangle$
$\|+z\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-x\rangle$	$\|+x\rangle$
$\|-z\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+x\rangle$	$\|-x\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|0\rangle$	$\|1\rangle$
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|1\rangle$	$\|0\rangle$

Tables 2 The state of the output qubit when the result of the second qubit measurement is $|1\rangle$. φ_1 and φ_2 are the states of the original control and target qubit, respectively.

φ_2	φ_1			
	$\|+z\rangle$	$\|-z\rangle$	$\|+x\rangle$	$\|-x\rangle$
$\|+z\rangle$	$\|1\rangle$	$\|0\rangle$	$\|x\rangle$	$\|-x\rangle$
$\|-z\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-x\rangle$	$\|+x\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|0\rangle$	$\|1\rangle$
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|1\rangle$	$\|0\rangle$

If Eve knows completely the state of the first qubit, but the second photon is unknown to her, then Eve's knowledge about the output state of the control qubit after the quantum privacy amplification operation becomes

$$\rho = \frac{1}{4}\left(|{+z}\rangle\langle{+z}| + |{-z}\rangle\langle{-z}| + |{+x}\rangle\langle{+x}| + |{-x}\rangle\langle{-x}|\right)$$

$$= \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad (39)$$

That is to say, Eve has no knowledge at all about the output state. But for Bob who has prepared the original states of the two qubits, he will know completely the output state when Alice tells him the $\sigma_{2,z}$ measurement result.

If it happens that Eve has complete information about both qubits, she will know the output state exactly just like Bob. However the probability this can happen is only

$$P_2 = r^2 \qquad (40)$$

where r is four times of the error bit rate ε detected by Alice and Bob using random sampling. The factor 4 is because eavesdropper's interception causes only 25 percent of error, i.e., $r = 4\varepsilon$. We can use the output qubit again as a control qubit and choose a third qubit from the batch as the target qubit and perform SQ-QPA operation on them. In this way, as more qubits are used in the SQ-QPA process, Eve's information is reduced exponentially to

$$P_m = r^m \qquad (41)$$

where m is the number of qubits that has been used in the SQ-QPA. In this way, Alice can condense a portion of single photons from a batch of N photons with negligibly small information leakage. This condensed single photon sequence can be used to encode secret message and complete the quantum secure direction communication.

This SP-QPA scheme can be used directly in long-distance quantum information sharing (QIS) of single qubits [72−75] with quantum repeater [76] for improving the security of the quantum information. In QIS, the quantum information is a sequence of unknown single qubits which are unknown for anyone even including the sender Alice. To prevent the eavesdropper Eve from stealing information about the operations if she intercepts it, it is necessary for both parties of quantum communication to do quantum privacy amplification on the single qubits, in particular, in the case of long-distance quantum communication with quantum repeaters. Suppose that the state of the quantum information transmitted is $|\varphi\rangle_1$. The sender can prepare some auxiliary states for implementing the quantum privacy amplification and checking eavesdropping. If the auxiliary state is one of the four polarized states

Tables 3 The state of the output qubit when the result of the second qubit measurement is $|1\rangle$. φ_2 is the states of the target qubit, and $\varphi_{1,\text{out}}$ and $\varphi_{1,\text{out}}$ are the states of the qubit 1 and qubit 2 after the quantum operation with quantum privacy amplification. U_{12} is the unitary operation with which one can reconstruct the original state of the qubit 1, φ_1. $U_H \equiv \mathrm{i}\sigma_y \otimes H$. Here σ_i $(i = x, y, z)$ are the Pauli matrix and H is the Hadamard operation.

φ_2	$\varphi_{2,\text{out}}$			
	0		1	
	$\varphi_{1,\text{out}}$	U_{12}	$\varphi_{1,\text{out}}$	U_{12}
$\|+z\rangle$	$a_1\|0\rangle_1 - b_1\|1\rangle_1$	σ_z	$a_1\|1\rangle_1 - b_1\|0\rangle_1$	σ_x
$\|-z\rangle$	$a_1\|1\rangle_1 - b_1\|0\rangle_1$	σ_x	$a_1\|0\rangle_1 - b_1\|1\rangle_1$	σ_z
$\|+x\rangle$	$a_1\|+x\rangle_1 + b_1\|-x\rangle_1$	H	$a_1\|+x\rangle_1 + b_1\|-x\rangle_1$	H
$\|-x\rangle$	$a_1\|-x\rangle_1 - b_1\|+x\rangle_1$	U_H	$a_1\|-x\rangle_1 - b_1\|+x\rangle_1$	U_H

$\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$, the relation between the outcomes of the qubit 2 operated and the unitary operation U_{12} with which one can obtain the original state of the qubit 1 is shown in Table 3. Different from that in QSDC, the state of the qubit 1 is unknown to anyone.

7 The one-party quantum error correcting codes for QSDC

Quantum error correcting codes(QECC) are a key technique towards protecting quantum system in communication and computation from errors mainly brought by decoherence [77−81]. To correct errors using QECC, we first encode the quantum information into a larger system, then measure its error syndromes and choose appropriate recovering operations. Entanglement purification protocol(EPP) is another quantum error correction method to produce high fidelity entangled pairs with only local operations and classical communications [48, 49]. Both QECC and EPP play an important role in quantum communication through noisy quantum channels. Especially, under assistance of QECC and EPP, we are able to perform unconditional secure QKD protocols [82−92].

Moreover, a recent work on the one-party quantum error correcting codes(one-party-QECC) by Wen and Long [93] can be best employed in QSDC and DSQC. The use of one-party QECC proves that QSDC is able to tolerate higher error rates in certain transmission phases. Similar to the proof of unconditional secure BB84 protocols [87], the success of correcting errors in QSDC may lead a path to prove its unconditional security.

7.1 The theory of one-party-QECC

One-party-QECC focus on correcting errors on entanglement pairs. The logical states in one-party-QECC are built on EPR paris, compared to the logical states built on single qubits in others QECC such as Calderbank-Shor-Steane(CSS) codes [78, 79]. One-party-QECC also employ joint measurements such as Bell measurements to obtain the error syndromes. The aim of one-party-QECC is to make use one part of the entangled pairs to detect and correct the errors on the other part of the pairs. So the condition of using one-party-QECC lies in an error model characterized by unbalanced errors that widely exists in quantum communications.

In a large group of quantum communication protocols based on entanglement pairs, including quantum dense coding, some QSDC and DSQC protocols, there are two kinds of qubits: flying qubits, which are transmitted from one party to the other, and home qubits, which remain in the same party. The unbalanced errors are defined as those whose distribution between the flying and home qubits are unbalanced. Particularly, the home qubits can be stored in some quantum storage with errors low enough to be corrected by CSS codes. On the other hand, the flying qubits are transferred via very noisy quantum channels. The errors on the flying qubits may be too many to be corrected by CSS codes and other existing quantum error correction methods. However, one-party-QECC are designed to correct the errors on the flying qubits, assuming that the home qubits have no error. The underlying quantum correlations between the flying qubits and the home qubits in one-party-QECC not only establish the direct correspondence of one classical linear code to one one-party-QECC, but also make it possible to tolerate much more errors on the flying qubits [93].

To introduce the construction of one-party-QECC, the four kinds of Bell-basis states are relabeled as follows:

$$|00\rangle' = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \tag{42}$$

$$|01\rangle' = |\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \tag{43}$$

$$|10\rangle' = |\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \tag{44}$$

$$|11\rangle' = |\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \tag{45}$$

Thus starting with arbitrary $[n, k, t]$ classical linear code, which encodes k-bit information into n bits and is capable of correcting arbitrary t bit errors, one can create a $[[2n, 2k, t]]$ one-party-QECC.

In stabilizer formalism [7], the one-party-QECC should define the measurement operators of each error syndrome, the logical states and the logical operators. Firstly, suppose that each error syndrome in the $[n, k, t]$ classical linear code is measured by (the superscript of "cl" denotes the classical situation)

$$g_i^{cl} = Z_{i_1}^{cl} Z_{i_2}^{cl} \cdots Z_{i_l}^{cl} \tag{46}$$

Thus two error syndromes in the corresponding one-party-QECC can be created as

$$g_{z,i} = (Z_{2i_1-1}Z_{2i_1})(Z_{2i_2-1}Z_{2i_2}) \cdots (Z_{2i_l-1}Z_{2i_l}) \tag{47}$$

$$g_{x,i} = (X_{2i_1-1}X_{2i_1})(X_{2i_2-1}X_{2i_2}) \cdots (X_{2i_l-1}X_{2i_l}) \tag{48}$$

It is easy to verify that all above error syndromes commute to each other and form a group of stabilizer generators in the one-party QECC.

Secondly, any logical Z-basis state in one-party-QECC is of combination of two codewords in the classical linear code. One picks any two codewords in the $[n,k,t]$ classical linear code, namely,

$$\overline{a_1a_2\cdots a_k}^{cl} = a_1a_2\cdots a_n \tag{49}$$

$$\overline{b_1b_2\cdots b_k}^{cl} = b_1b_2\cdots a_n \tag{50}$$

Then he or she can build a logical Z-basis state in one-party-QECC, based on the relabeled Bell-basis states, as

$$\begin{aligned}&|\overline{a_1b_1;a_2b_2;\cdots;a_kb_k}\rangle\\&\quad = |a_1b_1\rangle_{1,2}\otimes|a_2b_2\rangle_{3,4}\otimes\cdots\otimes|a_nb_n\rangle_{2n-1,2n}\end{aligned} \tag{51}$$

Obviously, there are $2k$ different logical Z-basis states in this one-party-QECC.

Thirdly, the logical Pauli operators are also directly created from the logical bit flip operators in the $[n,k,t]$ classical code. Particularly, the logical i-th bit flip operators in the classical code is defined as

$$\bar{X}_i^{cl} = X_{i_1}^{cl}X_{i_2}^{cl}\cdots X_{i_l}^{cl} \tag{52}$$

As a result, with the correspondence between the classical linear codes and the one-party-QECC, one can define 4 logical Pauli operators on the $(2i-1)$-th and $2i$-th qubits for the one-party-QECC as

$$\bar{X}_{2i-1} = X_{2i_1}X_{2i_2}\cdots X_{2i_l} \tag{53}$$

$$\bar{Z}_{2i-1} = (Z_{2i_1-1}Z_{2i_1})(Z_{2i_2-1}Z_{2i_2})\cdots(Z_{2i_l-1}Z_{2i_l}) \tag{54}$$

$$\bar{X}_{2i} = Z_{2i_1-1}Z_{2i_2-1}\cdots Z_{2i_l-1} \tag{55}$$

$$\bar{Z}_{2i} = (X_{2i_1-1}X_{2i})(X_{2i_2-1}X_{2i_2})\cdots(X_{2i_l-1}X_{2i_l}) \tag{56}$$

To analyze the error correcting capability of one-party-QECC, Wen and Long [93] discover that the measurement operators of $g_{z,i}$ and $g_{x,i}$ are the product of l groups of Bell measurements. Each Bell measurement act on a relabeled physical EPR pair respectively. Note that the logical Z-basis states contains the product of n physical EPR pairs. Therefore, from the error correction process of the classical code, it is easy to prove that $g_{z,i}$ and $g_{x,i}$ are capable of correcting arbitrary t bit-flip errors and t phase-flip errors respectively on the first halves of total n physical EPR pairs. Here we assume that the first halves are the flying qubits that may err and the second halves the home qubits that have no error in our unbalanced error model. In conclusion, from arbitrary $[n,k,t]$ classical linear code, a corresponding $[[2n,2k,t]]$ one-party-QECC is derived to encode $2k$ logical qubits into $2n$ physical qubits of n physical EPR pairs and be capable of correcting arbitrary t bit-flip errors and t phase-flip errors on the first halves of the physical EPR pairs.

The advantage of one-party-QECC is the higher capability of error correction and higher capacity of encoding quantum information. This is best demonstrated by the Gilbert-Varshamov bound of one-party-QECC directly derived from the same bound of classical linear codes, namely,

$$\frac{2k}{2n} = \frac{k}{n} \geqslant 1 - H\Big(\frac{2t}{n}\Big) \tag{57}$$

where the function $H(x)$ is the Shannon entropy, $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$. In our error model, only one halves of the EPR pairs, the flying qubits are transmitted through the channel. Thus, t/n is the exact channel bit error rate. Compared to the Gilbert-Varshamov bound of CSS codes [78], namely,

$$\frac{k}{n} = \frac{k}{n} \geqslant 1 - 2H\Big(\frac{2t}{n}\Big) \tag{58}$$

the one-party-QECC can encode more information given certain channel bit error rate; or they can correct more errors given certain encoding rate of k/n.

In Ref. [93], Wen and Long also give concrete examples of one-party-QECC. Especially, the concatenating $[[6,2,1]]$ one-party-QECC is able to correct the channel bit error rate less than 50 %.

7.2 Applications of one-party-QECC in QSDC

Wen and Long have already shown that one-party-QECC can be used in quantum dense coding [93]. Along with quantum dense coding, a large group of protocols in QSDC and DSQC which employ the idea of quantum dense coding and are based on entanglement pairs can also apply one-party-QECC, so as to increase the capacity of communication and capability of correcting errors.

Most QSDC protocols based on entanglement pairs contain the following schematic phase. In such phase, one communication party are sending one halves of the EPR pairs to the other communication party; while the other party has already hold the other halves of the EPR pairs. For example, in quantum dense coding [60], Alice and Bob first share a number of EPR pairs; after encoding the information, Alice sends her part of the pairs to Bob. In the Two-Step QSDC protocol [17], the second step is that Alice sends the message-coding sequence, also one halves of the EPR pairs, to Bob, while the other halves of the EPR pairs, denoted by the checking sequence, have already been received by Bob in the first step. In the modified ping-pong protocol [24], the second transmission phase is also that Alice sends one part of the EPR pairs back to Bob, while the other halves are held by Bob all through the protocol.

The above schematic phase are well suitable for the application of one-party-QECC. The two halves of the EPR pairs in communication are divided to the flying qubits which are transmitted via the quantum channel and the home qubits which are held by one communication party. Thus, the errors on these two kinds of qubits are unbalanced: the home qubits can be assumed to be of no error if they are stored in some quantum storage; the flying qubits, on the contrary, will be subjected to very high noise. Furthermore, as the measurement operators of error syndromes in one-party-QECC employ the Bell measurements on both halves of the EPR pairs, the application of one-party-QECC also requires that one party should obtain both halves of the pairs in error correction. Obviously, in the end of the schematic phase, one party will hold both halves. Therefore, one-party-QECC can be used in such kind of phase in these QSDC and DSQC protocols. In other phases that are not suitable for one-party-QECC, the traditional error correction methods such as CSS codes or EPP should be used.

As a result, Wen and Long also propose a protocol QSDC protocol that make use of one-party-QECC [93]. The concrete protocol are presented as follows:

Protocol: QSDC protocol with one-party-QECC

(1) Bob first prepares a sequence of $3n$ EPR pairs in the state of $|\Phi^+\rangle$.

(2) Bob chooses a random $3n$ bit binary string b, applies Hadamard transformation H to the second halves of the pairs in which the corresponding bits of b are 1. Then he sends the second halves to Alice.

(3) Alice receives the qubits and publicly acknowledges her receipt. Bob tells Alice the bit values of b. Then Alice applies H to the qubits in her part where the corresponding bits of b are 1.

(4) Alice and Bob randomly chooses an n subset of the EPR pairs as first-round check pairs. They both measure the check qubits in their halves of the check pairs respectively in the Z-basis. Note that because $H \otimes H = I(Identity)$, the results of Alice and Bob in each pair will be the same if there is no error. Therefore, if they find that there are too many inconsistencies, they know that the transmitting qubits are eavesdropped and abort the protocol.

(5) Alice and Bob uses a suitable EPP to purify their rest EPR pairs.

(6) Alice randomly selects m subset of the rest $2m$ first-level logical EPR pairs as second-round check pairs; the rest are served as code pairs. She also randomly chooses a $2m$ bit binary string b', applies first-level logical Hadamard transformation $\bar{H}$ to the second halves of the pairs in which the corresponding bits of b are 1. Then he sends the second halves to Alice.

(7) Alice wants to send a k bit binary sequence of message M. She picks a $[[2m, 2k, t]]$ one-party-QECC that can correct the errors in the second transmission. In the view of one-party-QECC, there are k second-level logical EPR pairs in the code pairs. She encodes M to her halves of the second-level logical qubits in the code pairs by applying

$$\bar{U}_{2i} = \bar{Z}_{2i}\bar{X}_{2i} \tag{59}$$

on the $2i$-th logical qubit where the i-th bit of M is 1. Actually $\bar{U}_{2i}$ only acts on the physical qubits with odd index, so Alice is able to apply this local operation. Then she returns all her qubits to Bob.

(8) Bob receives the qubits from Alice and publicly announces his receipt. Then Alice announces b', and Bob applies the first-level logical $\bar{H}$ to the received first-level qubits where the corresponding bits of b' are 1.

(9) Alice publicly announces the places of second-round check pairs and the one-party-QECC she chooses. The same fact holds that if Bob measures the both qubits in each check pairs in Z-basis respectively, he will get the same results if there is no error. Thus if Bob gets too many errors, the protocol is aborted.

(10) Bob uses the $[[2m, 2k, t]]$ one-party-QECC to correct the errors on the rest m first-level logical EPR pairs and obtains k second-level logical code pairs.

(11) Bob measures both the qubits of the rest k second-level logical code pairs in Z-basis. Therefore, from the comparison of the measurements on corresponding pairs, Bob can retrieve the full information of M.

We analyze the above protocol. In the first phase of transmission, EPP are used to correct the errors, because this phase is similar to an entanglement distribution process. The random Hadamard transformations not only change the bases of the transmitting qubits, but also make the bit-flip and phase-flip errors symmetric, namely, the channel bit error rate is equal to the channel phase error rate. As EPP with two-way classical communications are able to distill corrupted EPR pairs with fidelity greater than 0.5 [48, 49], the maximal correctable channel bit error rate in this phase is $25\ \%$ [93].

The second phase is an example of the schematic phase given in the beginning of this section. Consequently, one-party-QECC are used, and Alice's operations of encoding message become logical operators in the one-party-QECC, shown in Eq. (59). The introduction of one-party-QECC in this phase can greatly increase the communication capacity and error correction capability, given the Gilbert-Varshamov bound of one-party-QECC in Eq. (57). If we just use CSS codes to correct errors on the flying qubits in this phase, their Gilbert-Varshamov bound in Eq. (58) will make them fail to correct very high error rates.

From the discussion above, we have shown another important feature of QSDC protocols: they can employ one-party-QECC to achieve higher communication capacity and error correction capability in noisy quantum channels. This feature will make them feasible to communicate even in the very bad situation. In addition, the analysis of error correction in QSDC protocols will probably enlighten a path towards the unconditional security of these protocols.

8 Summary

In this review article, we have reviewed the recent development of quantum secure direct communication and deterministic secure quantum communication. Both QSDC and DQSC are deterministic quantum communication protocols. They both can transmit secret messages from one user to another user, however, QSDC does not require additional classical information to read out the secret message while DQSC does require additional classical messages in order to read out the secret messages. They are attractive because they are deterministic, in particular, the QSDC protocol is fully quantum mechanical. With sophisticated quantum technology in the future, the QSDC may become more and more popular.

In QSDC, some protocols use single photons in unknown quantum state, and noises are inevitable. To prevent an Eve taking advantage of noise, a quantum privacy amplification protocol has been proposed. It involves very simple CHC operations and reduces the information leakage to a negligible small level.

Many quantum communication protocols are based superdense coding. In this case, at the final stage, both qubits from an EPR pair are in one hand of a single user. In this case, the one-party quantum error correction codes will be very appropriate. Because only one-party of the EPR pair is travelling, the travelling qubit is more vulnerable to the noises. In addition, joint operations can now be performed because both qubits are in one communication party. The one-party codes also have high error tolerance. With the one-party quantum error correction, a relation has been established between classical linear codes and quantum one-party codes, hence it is convenient to transfer many good classical error correction codes to the quantum world.

Acknowledgements This work was supported by the National Fundamental Research Program (Grant No. 2006CB921106), the National Natural Science Foundation of China (Grant Nos. 10325521, 60433050, and 10604008), the SRFDP program of Education Ministry of China (Grant No. 20060003048).

References

1. Shor P. W., Proc. 35th Annual Symposium on Foundations of Computer Science, 1994: 124
2. Grover L., Phys. Rev. Lett, 1997, 78: 325
3. Long G. L., Phys. Rev. A, 2001, 64: 022307
4. Feynman R. P., Int. J. Theor. Phys., 1982, 21: 467
5. Lloyd S., Science, 1996, 273: 1073
6. Wang X. Y. and Yu H. B., Lecture Notes in Computer Science, 2005, 3494: 19
7. Nielsen M. A. and Chuang I. L., Quantum computation and quantum information, Cambridge: Cambridge University Press, 2000
8. Gisin N., Ribordy G., Tittel W., and Zbinden H., Rev. Mod. Phys., 2002, 74: 145
9. Vernam G. S., J. Amer. Inst. Elec. Eng., 1926, 45: 109
10. Shimizu K. and Imoto N., Phys. Rev. A, 1999, 60: 157
11. Beige A., Englert B. G., Kurtsiefer C., and Weinfurter H., Acta Phys. Pol. A, 2002, 101 (3): 357
12. Boström K. and Felbinger T., Phys. Rev. Lett.,2002, 89: 187902
13. Wójcik A., Phys. Rev. Lett., 2003, 90: 157901
14. Cai Q. Y., Phys. Rev. Lett., 2003, 91: 109801
15. Deng F. G., Li X. H., Li C. Y., Zhou P., and Zhou H. Y., Chin. Phys., 2007, 16: 277
16. Long G. L. and Liu X. S., Phys. Rev. A, 2002, 65: 032302
17. Deng F. G., Long G. L., and Liu X. S., Phys. Rev. A, 2003, 68: 042317
18. Deng F. G. and Long G. L., Phys. Rev. A, 2004, 69: 052319
19. Deng F. G., Li X. H., Li C. Y., Zhou P., and Zhou H. Y., Phys. Lett. A, 2006, 359: 359
20. Li X. H., Zhou P., Liang Y. J., Li C. Y., Zhou H. Y., and Deng F. G., Chin. Phys. Lett., 2006, 23: 1080
21. Wang C., Deng F. G., Li Y. S., Liu X. S., and Long G. L., Phys. Rev. A, 2005, 71: 044305
22. Wang C., Deng F. G., and Long G. L., Opt. Commun., 2005, 253: 15
23. Li X. H., Li C. Y., Deng F. G., Zhou P., Liang Y. J., and Zhou H. Y., Chin. Phys., 2007, 16 (8) (in press)
24. Cai Q. Y. and Li B. W., Phys. Rev. A, 2004, 69: 054301
25. Cai Q. Y. and Li B. W., Chin. Phys. Lett., 2004, 21: 601
26. Li X. H., Deng F. G., Li C. Y., Liang Y. J., Zhou P., and Zhou H. Y., J. Korean Phys. Soc., 2006, 49: 1354
27. Yan F. L. and Zhang X., Euro. Phys. J. B, 2004, 41: 75
28. Gao T., Yan F. L., and Wang Z. X., J. Phys. A, 2005, 38: 5761
29. Man Z. X., Zhang Z. J., and Li Y., Chin. Phys. Lett., 2005, 22: 18
30. Zhu A. D., Xia Y., Fan Q. B., and Zhang S., Phys. Rev. A, 2006, 73: 022338
31. Li X. H., Deng F. G., and Zhou H. Y., Phys. Rev. A, 2006, 74:

054302

32. Lee H., Lim J., and Yang H., Phys. Rev. A, 2006, 73: 042305
33. Wang J., Zhang Q., and Tang C. J., Phys. Lett. A, 2006, 358: 256
34. Wang J., Zhang Q., and Tang C. J., Int. J. Quantum information, 2006, 4: 925
35. Wang J., Zhang Q., and Tang C. J., Int. J. Mod. Phys. C, 2006, 17: 685
36. Wang H. F., Zhang S., Yeon K. H., and Um C. I., J. Korean Phys. Soc., 2006, 49: 459
37. Ji X. and Zhang S., Chin. Phys., 2006, 15: 1418
38. Cao H. J. and Song H. S., Chin. Phys. Lett., 2006, 23: 290
39. Cao H. J., Chen J., and Song H. S., Commun. Theor. Phys., 2006, 45: 271
40. Gao. T., Z. Naturforsch, A, 2004, 59: 597
41. Gao. T. and Yan. F. L., Chin. Phys., 2005, 14: 893
42. Gao. T., Yan. F. L., and Wang. Z. X., II Nuovo Cimento B, 2004, 119: 313
43. Gao. T., Yan. F. L., and Wang. Z. X., J. Phys. A: Math. Gen, 2005, 38: 5761
44. Deng F. G., Li X. H., Zhou H. Y., and Zhang Z. J., Phys. Rev. A, 2005, 72: 044302
45. Deng F. G. and Long G. L., Commun. Theor. Phys., 2006, 46: 443
46. Brassard G. and Salrail L., Euro-crypt 193, Lectures Notes in Cumputer Sciences, Vol. 765, New York: Springer-Verlag, 1994: 410
47. Zukowski M., Zeilinger A., Horne M. A., and Ekert A. K., Phys. Rev. Lett., 1993, 71: 4287
48. Bennett C. H., Brassard G., Popescu S., Schumacher B., Smolin J. A., and Wootters W. K., Phys. Rev. Lett., 1996, 76: 722
49. Deutsch D., Ekert A., Jozsa R., Macchiavello C. Popescu S., and Sanpera A., Phys. Rev. Lett., 1996, 77: 2818
50. Deng F. G., Long G. L., Wang Y., and Xiao L., Chin. Phys. Lett., 2004, 21: 2097
51. Bennett C. H., Brassard G., Crépeau C., Jozsa R, Peres A., and Wootters W. K., Phys. Rev. Lett., 1993, 70: 1895
52. Liu X. S., Long G. L., Tong D. M., and Li F., Phys. Rev. A, 2002, 65: 022304
53. Grudka A. and Wójcik A., Phys. Rev. A, 2002, 66: 014301
54. Yan F. L. and Wang M. Y., Chin. Phys. Lett., 2004, 21: 1195
55. Bechmann-Pasquinucci H. and Peres A., Phys. Rev. Lett., 2000, 85: 3313
56. Li C. Y., Zhou H. Y., Wang Y., and Deng F. G., Chin. Phys. Lett., 2005, 22: 1049
57. Li C.Y., Li X. H., Deng F. G., Zhou P., Liang Y. J., and Zhou H. Y., Chin. Phys. Lett., 2006, 23: 2896
58. Deng F. G., Li X. H., Li C. Y., Zhou P., Liang Y. J., and Zhou H. Y., Chin. Phys. Lett., 2006, 23: 1676
59. Li X. H., Li C. Y., Deng F. G., Zhou P., Liang Y. J., and Zhou H. Y., Chin. Phys. Lett., 2007, 24: 23
60. Bennett C. H. and Wiesner S. J., Phys. Rev. Lett., 1992, 69: 2881
61. Bennett C. H., Phys. Rev. Lett, 1992, 68: 3121
62. Deng F. G., Li X. H., Li C. Y., Zhou P., and Zhou H. Y., Phys. Scr., 2007, 76: 25
63. Chen P., Deng F. G., and Long G. L., Chin. Phys., 2006, 15: 2228
64. Deng F. G. and Long G. L., Phys. Rev. A, 2003, 68: 042315
65. Bennett C. H., Brassard G., and Mermin N. D., Phys. Rev. Lett., 1992, 68: 557
66. Deng F. G., Li X. H., Li C.Y., Zhou P., and Zhou H. Y., e-print quant-ph/0606008; Chin. Phys., 2007, 16 (in press)
67. Bennett C. H., Brassard G., and Robert J. M., SIAM J. Comput., 1988, 17: 210
68. Bennett C. H., Brassard G., Crépeau C., and Maurer U M, IEEE Trans. Inf. Theory, 1995, 41: 1915
69. Bennett C. H. and Brassad G., Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York), 1984: 175
70. Ekert A. K., Phys. Rev. Lett., 1991, 67: 661
71. Yang C. P., Chu S. I., and Han S. Y., Phys. Rev. A, 2004, 70: 022329
72. Bandyopadhyay S., Phys. Rev. A, 2000, 62: 012308
73. Karimipour V., Bahraminasab A., and Bagherinezhad S., Phys. Rev. A, 2002, 65: 042320
74. Cleve R., Gottesman D., and Lo H. K., Phys. Rev. Lett., 1999, 83: 648
75. Li Y. M., Zhang K. S., and Peng K. C., Phys. Lett., A, 2004, 324: 420
76. Briegel H. J., Dür W., Cirac J. I., and Zoller P., Phys. Rev. Lett. 1998, 81: 5932
77. Shor P. W., Phys. Rev. A, 1995, 52: R2493
78. Calderbank A. R. and Shor P. W., Phys. Rev. A 1996, 54: 1098
79. Steane A. M., Proc. R. Soc. London A, 1996, 452:2551
80. Feng K. Q., Ling S., and Xing C., IEEE Trans. Inf. Theory, 2006, 52: 986
81. Chen H., Ling S., and Xing C., IEEE Trans. Inf. Theory, 2005, 51: 2915
82. Bennett C. H., DiVincenzo D. P., Smolin J. A., and Wootters W. K., Phys. Rev. A, 1996, 54: 3824
83. Mayers D., Advances in Cryptology-Proceedings of Crypto 96, New York: Springer-Verlag, 1996: 343
84. Biham E., Boyer M., Boykin P. O., et al., Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, New York: ACM Press, 2000: 715
85. Biham E., Boyer M., Boykin P. O., et al., Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, New York: ACM Press, 2000: 715
86. Lo H. K. and Chau H. F., Science, 1999, 283: 2050
87. Shor P. W. and Preskill J., Phys. Rev. Lett., 2000, 85: 441
88. Lo H. K., Quantum Information and Computation, 2001, 1: 81
89. Gottesman D. and Lo H. K., IEEE Trans. Inf. Theory, 2003, 49: 457
90. Chau H. F., Phys. Rev. A, 2002, 66: 060302(R)
91. Hwang W. Y., Wang X. B., Matsumoto K., Kim J., and Lee H. W., Phys. Rev. A, 2003, 67: 012302
92. Wen K. and Long G. L., Phys. Rev. A, 2005, 72: 022336
93. Wen K. and Long G. L., e-print quant-ph/0609207