Review

Chinese Science Bulletin

Quantum Information

December 2012 Vol. 57 No. 36: 4694–4700
doi: 10.1007/s11434-012-5600-6

Recent development in quantum communication

SONG SiYu[1,2] & WANG Chuan[3*]

[1] *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China;*
[2] *Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China;*
[3] *School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Received September 26, 2012; accepted November 1, 2012

In this review article, we will review the recent process of quantum communications. In the past decades, there are many developments in quantum communication, for instance, quantum key distribution, quantum teleportation, quantum secure direct communication, deterministic secure quantum communication, quantum secret sharing and so on. And we focus our attention on the recent developments in quantum communication protocols.

quantum information, quantum key distribution, quantum teleportation, quantum secure direct communication (QSDC), quantum secret sharing

Citation: Song S Y, Wang C. Recent development in quantum communication. Chin Sci Bull, 2012, 57: 4694–4700, doi: 10.1007/s11434-012-5600-6

The principles in quantum mechanics provide novel ways for quantum information transmission and processing, such as quantum computation and quantum communication. In the past decades, quantum information processing has emerged as a promising technology with strategic importance. Because of the peculiar properties of quantum systems, quantum computers possess enormous power that is superior to classical computer. Using quantum computer, factorization of an integer can be accomplished in polynomial time with the Shor algorithm [1]. And we can find a marked item with high probability from an unsorted database with a square-root speedup with the Grover algorithm [2]. In the past decades, the field of quantum information processing and quantum computation have attracted much attention [3–6]. With these quantum algorithms and a quantum computer, many classical cryptography protocols can be attacked. Thus it is vital to find new cryptographic systems for defending against these attacks.

In the following years, there are many branches of quantum communications that are generated which provides us secure ways of communications, such as quantum key distribution (QKD), quantum teleportation, quantum secure direct communication, quantum secret sharing and so on. QKD provides a secure way to distribute secret keys between distant users which solves the problem for secure distributing of keys in the classical one-time-pad protocol [7]. However, quantum communication offers more power than QKD. Quantum secret sharing (QSS) distributes secret keys to two or more shared users [8], which can be viewed as the quantum key distribution between multi-users. Quantum teleportation is a basic ingredient in quantum information architectures [9, 10]. The principle of quantum teleportation is to transfer an unknown state to the legal user at a distant distance. Quantum secure direct communication (QSDC) offers direct communication of secret messages between distant users, which saves completely the need for another classical communication as in the QKD case. In recent years, there have been considerable developments from researchers in the design of quantum communication protocols. In this article, we will focus on these developments in quantum communications.

1 A brief history and key techniques of quantum communication

QKD provides an unconditional secure way of information exchange between two distant users. The first QKD protocol is proposed by Bennett and Brassard [7], called the BB84 protocol. In 1992, Bennett proposed a simplified version of

*Corresponding author (email: wangchuan@bupt.edu.cn) the BB84, called the B92 protocol [11]. Since then there have been many important theoretical improvements and experimental demonstrations of BB84 and other QKD protocols.

Quantum teleportation is pertinent to quantum communication only, and there is no classical counterpart [12]. Quantum teleportation transmits an unknown state to a remote place without actually transporting the actual particle. It has become a basic ingredient in quantum information architectures [9, 10]. Teleportation includes two legal users and two communication channels, which are the sender and the receiver, and the quantum channel and the classical channel. The first quantum teleportation protocol is proposed by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [12]. Up to now, there have been many researches on quantum teleportation, some of the recent developments can be found in [13–16]. Also quantum teleportation has been experimentally implemented with photonic qubits [17–23].

A quantum secret sharing (QSS) protocol is to distribute secret keys among two or more legal users. The shared secret can only be recovered by the legal users when they cooperate together. In 1999, Hillery et al. proposed the first QSS protocol [8] for sharing a secret with three-particle and four-particle entangled Greenberger-Horne-Zeilinger (GHZ) states. Up to now, QSS has been extensively studied in both theory and experiments, for instance, in [24–27] for theory, and in [28–30] for experiments. In parallel, the sharing of a quantum state, which is called quantum state sharing (QSTS), has also been developed [29]. QSTS protocols of an arbitrary single-particle state [31, 32], two-particle state [33, 34] and multi-particle state [35, 36] have been studied.

Quantum secure direct communication (QSDC) as a new way to implement information transmission has attracted much attention. In 2000, the first QSDC scheme was proposed [37]. In QSDC, secret information is transmitted directly from the sender to the receiver which is different from the QKD schemes with an advanced encryption process. QSDC has a good application prospect because it is complete quantum but the communication process should be more secure than the security for QKD. QSDC protocols have been proposed with different implementation ways [38–48].

Here we will discuss some key problems of quantum communication.

1.1 Information leakage before eavesdropper detection

The security of classical cryptography relies on mathematical complexities. However, the security quantum cryptography relies on the principles of quantum mechanics. Information leakage before eavesdropper detection (ILBED) is essential for the security of quantum communication, which has been extensively used in practice, but is recently pointed explicitly in [49]. In quantum communication, eavesdroppers are detected by sampling measurement, usually in alternative conjugate basis. For example in QKD, if some eavesdroppers are detected, the transmission is halted and the transmitted data are discarded. Therefore, ILBED is eliminated by dropping the transmitted data in QKD. In QSS, similar to QKD, the transmitted data is also dropped if the eavesdropper has been discovered. Avoiding ILBED is also important in QSDC. This is achieved in QSDC by the essential technique of block transmission. Quantum information carriers are transported in batches. The information carriers consist of a sequence of single photons, or particles formed by taking one particle from each Einstein-Podolsky-Rosen (EPR) pairs. The security of these information carriers is checked by sampling measurement. In QKD, secret message is then transmitted by classical transmission of the ciphertext encoded with the keys generated by QKD. If eavesdropper is found in the quantum channel, then we withhold the key and ILBED is avoided.

1.2 Methods of quantum communication

In this section, we will briefly review several key methods for constructing quantum communication protocols.

(i) Multi-step transmission. If we have an entangled quantum system, we can transmit the system from one user to another in multiple steps. Because it is entangled, measurement on part of an entangled quantum system does not provide the whole information of the quantum system, this provides us with a novel way for constructing quantum communication protocols. Multi-step transmission was first proposed in [37]. It has been extensively used in various protocol designs of quantum communications.

(ii) Block transmission. Block transmission is essential for QSDC. In block transmission, the information carriers are transmitted in a block. For instance in [37], the two ordered particle sequences are transmitted in a block of N particles. Security is guaranteed by checking on the block of N particles which are chosen randomly and measured to give an estimated error rate.

(iii) Order Rearrangement. Similar to conjugate-basis method where an eavesdropper does not know which of the conjugate-basis the legal users are used, one can reorder the orders of the particles within a block. The order number of a particle is completely unknown to the eavesdropper. The eavesdropper can only guess the order number of the particle. The order rearrangement method was first proposed in [50], called the CORE protocol. The method has been used extensively.

1.3 Information carriers and measurement

In the early stage, quantum communication protocols with discrete variables are based on single photons [7, 11] and entangled photon states [51] as the information carriers. Now multi-photons entangled states are proposed for quantum communication realization, such as the GHZ state, cluster states [44], highly entangled six-qubit genuine state [16], χ-state [13], and so on. Recently, entangled photons with multi-photon have been implemented in experiment, for example the two photons entanglement [52], the four photons entanglement [53], the six photons entanglement [54]. The realization of entangled photon sources is becoming a crucial element for quantum communication.

To implement quantum communication, the measurement of single photons or entangled photons is another important ingredient. Many related works have been done for investigating the measurements of single photon and entangled photons. The avalanche photodiodes are used as the detector for single photons detection. The single photon detectors should fulfill the following requirements: firstly, the detector should be response to a wide range wavelength light with high detection efficiency; secondly, the noise of the detector should be lower; thirdly, the time between detection of a photon and generation of an electrical signal should be constant; fourthly, the dead time should be short enough to allow the detectors work at high frequency situation. For these four points, the response ability and working requirements of the single photon detectors are investigated [55] to improve the detection efficiency.

2 Quantum key distribution

QKD, as an important branch of quantum information, provides a secure way for creating secret keys between communication parties, Alice and Bob. In this section, we will review the recent QKD protocols. Since Bennett and Brassard presented the BB84 QKD protocol [7], quantum key distribution has progressed quickly [11, 51, 56–61].

"Plug and play" system is proposed in [62], which uses the Faraday mirrors to make a compensation for the polarization of the photons automatically. A plug and play QKD in 50 km optic fibers is implemented by Zeng et al. [63]. In the experiment, B92 protocol is implemented. In the experiment, Alice prepares and sends the photons with one of two non-orthogonal phases randomly to Bob. Bob makes measurement randomly selected in two non-orthogonal bases. Secret keys are created between Alice and Bob when Bob's base matched Alice's state, while those mismatched results are discarded. In order to reduce the noises in fiber, a variable attenuator which controls the photon number is connected with the laser on Alice's site. The experimental results show that quantum key distribution system can be hopefully used in practical secret communication, and to work at a high speed with a lower error rate.

Recently, a new QKD protocol is proposed by Gao et al. [64], and the quantum public-key cryptography (QPKC) is investigated. In the proposed protocol, Bell state is divided into two parts, one is used for the public key, and the other one is used to generate the private key. Symmetric keys are reasonable to be used. The security of the scheme is discussed, and it reveals a good character. The unconditional security must be assured for QKD, and then QPKC can replace it to complete the task. This scheme is an important work for QPKC.

3 Quantum teleportation

The original idea of quantum teleportation was first proposed by Bennett et al. [12] and was experimentally realized by Bouwmeester et al. [65]. The task of quantum teleportation is to transmit and reconstruct over arbitrary distances of the state of a quantum system. Many related works have been proposed in the past decades. Recently, the protocol to teleport an unknown two-qubit state is given in [66]. Different from the original protocol [12], teleporting one-qubit state with two qubits quantum channel, four qubits state is used as the quantum channel in [66]. An arbitrary unknown two qubits state can be presented as

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{1}$$

where a, b, c, and d are complex numbers and $\{|ij\rangle\}$ is an orthonormal basis set. The channel state $|\phi_c\rangle$ can be written by Schmidt decomposition as

$$\begin{aligned}|\psi_c\rangle &= \frac{1}{2}\sum_{i,j=0}^{1}|\psi_{i,j}\rangle_A \otimes |\varphi_{i,j}\rangle_B \\ &= (1_A \otimes \widehat{V}\widehat{U}^T)|EPR\rangle_{A_1B_1} \otimes |EPR\rangle_{A_2B_2},\end{aligned} \tag{2}$$

where the state $|EPR\rangle = \sum_i |i,i\rangle/\sqrt{2}$. Alice performs a joint measurement on the four qubits A_1, A_2, U_1, and U_2. After Alice got the measurement results, Bob's two qubits become to be a state similar with the state that Alice transmits. Then when receiving the classical information of Alice's result, he makes a special unitary operation on his particles, to get the transmitting unknown state information.

While in the protocol of quantum teleportation of [66] or even in latter improved paper [67], the four-qubit entangled channel can be reduced to a tensor product of two Bell states. To avoid this problem and to ensure the success of faithfully teleporting any arbitrary two-qubit state, Ye et al. proposed a protocol to implement teleporting process using a four-qubit entangled channel. At first, Alice and Bob share a priori two pairs of particles, A_3, A_4, and B_1, B_2 in the state

$$|\overline{\chi}^{00}\rangle_{A_3A_4B_1B_2} = \frac{1}{2}\sum_{J=0}^{3}|J\rangle_{A_3A_4} \otimes |J'\rangle_{B_1B_2}. \tag{3}$$

The $|J\rangle$s constitute a set of orthonormal bases

$$\begin{aligned}|0\rangle &= \cos\theta_1|00\rangle + \sin\theta_1|11\rangle,\\ |1\rangle &= \cos\phi_1|01\rangle + \sin\phi_1|10\rangle,\\ |2\rangle &= -\sin\phi_1|01\rangle + \cos\phi_1|10\rangle,\\ |3\rangle &= -\sin\theta_1|00\rangle + \cos\theta_1|11\rangle,\end{aligned} \tag{4}$$

then using the new channels for teleportation, it can be perfect completed.

Perfect teleportation of an arbitrary three-qubit state are discussed in many works [16, 68, 69]. In [16], quantum teleportation using highly entangled six-qubit state as the quantum channel was investigated. In the beginning, the two involved parties share the state in the form

$$\begin{aligned}
&|G\rangle_{a_1a_2a_3b_1b_2b_3} \\
&= \frac{1}{\sqrt{32}}[|000000\rangle + |111111\rangle + |000011\rangle \\
&\quad + |111100\rangle + |000101\rangle + |111010\rangle + |000110\rangle \\
&\quad + |111001\rangle + |001001\rangle + |110110\rangle + |001111\rangle \\
&\quad + |110000\rangle + |010001\rangle + |101110\rangle + |010010\rangle \\
&\quad + |101101\rangle + |011000\rangle + |100111\rangle + |011101\rangle \\
&\quad + |100010\rangle - |001010\rangle - |110101\rangle - |001100\rangle \\
&\quad - |110011\rangle - |010100\rangle - |101011\rangle - |010111\rangle \\
&\quad - |101000\rangle - |011011\rangle - |100100\rangle - |011110\rangle \\
&\quad - |100001\rangle], \qquad (5)
\end{aligned}$$

where particles a_1, a_2, and a_3 belong to Alice and particles b_1, b_2, and b_3 belong to Bob. Alice wants to transmit the information state

$$|u\rangle_{x_1x_2x_3} = \sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1}\xi_{ijk}|ijk\rangle_{x_1x_2x_3}. \qquad (6)$$

Then Alice chooses a proper measurement base to measure her six particles a_1, a_2, a_3, x_1, x_2, and x_3. Bob only needs to perform an appropriate unitary operation on his three particles to recover the initial state. The teleportation of three qubits state can be completed through this way.

Similarly, quantum teleportation of arbitrary n-qubit state with 2n-qubit pure state [70] and probabilistic teleportation [71] are investigated.

4 Quantum secure direct communication

Quantum secure direct communication (QSDC) is to transmit the secret information directly. For securely and effectively complete the QSDC, three requirements are needed: firstly, the secret informaiton can be transmit and readout directly, the additional classical information is not needed. Secondly, Eve cannot gain any useful information about the secret message. Thirdly, the secret information should not be revealed before the encoding process.

Two-step QSDC scheme is the first secure communication model for quantum direct communication proposed in [37, 38]. The proposed QSDC exploits an EPR pair which is in one of the four Bell states,

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B), \qquad (7)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B), \qquad (8)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B), \qquad (9)$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \qquad (10)$$

The subscripts A and B represent the two photons in an EPR pair, and $|0\rangle$ and $|1\rangle$ are the two eigenvectors of the measuring basis (MB) Z (for instance, the polarizations of a photon along the z-direction).

In the communication process, Alice first prepares an ordered N EPR pairs in the same state $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$, then she takes one particle from each EPR pair to form an ordered particle sequence. This sequence is made up of all the photons A in the ordered N EPR pairs. After that, Alice sends the checking sequence to Bob and they check the security of this transmission. If they confirm that the transmission of the checking sequence is secure, Alice encodes her secret message on the message-coding sequence with four unitary operations U_i ($i = 0, 1, 2, 3$) and then sends the sequence to Bob. The coding operations can be described as follows:

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad (11)$$

$$U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \qquad (12)$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \qquad (13)$$

$$U_3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \qquad (14)$$

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. Bob can read out the secret message directly with Bell-state measurements. The security checking process are also discussed in the proposed protocol. Later, there are many researches in the world studying the subject of QSDC [39–42, 46–48].

Recently, fault tolerant QSDC protocol against collective noises is investigated [43]. In the proposed paper, two QSDC schemes are proposed, one is proposed for defending against the collective-dephasing noises and the other one is for defending against the collective-rotation noises. The DF states are used in these two protocols, which can resist collective dephasing noises and collective-rotation noises, they contain two logical qubits. Then the sender-Alice can prepare her information carriers on these DF states. The transmitting process is similar with the implementation process in [38], for defending the Eves, decoy state photons are inserted into the information photons sequence. At last, the receiver simply performs two Bell state measurements to obtain the secret message. In these two protocols, twice times qubit efficiency are obtained, they are robust against general attacks. Moreover, they can defend against Trojan horse attacks.

In [72], robust QSDC with a quantum one-time pad over a collective-noise channel is proposed. The original one time pad QSDC scheme is proposed by Long et al. [39], it realizes the information direct communication using single photons. In [72], two robust QSDC schemes are presented, one is implemented with a quantum one-time pad over a collective-dephasing noise channel, the other one is to build a quantum one-time pad over a collective-rotation. The information is encoded using two unitary operations on each logical qubit, each logical qubit is implemented with two photons-two physical bits, entangled photon pairs can be used for one logical qubit. The information is transmitted from Alice to Bob, the transmitting process is similar with [39]. After Bob received the photons, he makes single-photon measurements for each photons and construct the information from each logical qubit-two single photons.

Recently, Cao et al. proposed a QSDC with cluster states [44], which uses two steps to implement the transmitting of information.

5 Quantum secret sharing and quantum state sharing

Quantum secret sharing (QSS) is an important branch of quantum communication, which has attracted much attention. The purpose of QSS is to distribute secret message between the boss and two or more agents. The boss expects to generate secret keys with the two agents separately and the two agents cannot reveal the boss's information until they combine their results together. QSS is a special utilization of quantum mechanics in classical secret sharing. QSS was first proposed by Hillery et al. [8] (here we called HBB QSS protocol). The idea of QSS have attracted a vast amount of effort ever since the work [8] in the following years. There have been many theoretical development in this subject [73–76].

Another generalization of secret sharing is the quantum state sharing (QSTS) which replace a quantum state by the secret information. Cleve et al. [24] introduced a way for a (k, n) threshold QSTS scheme to split a secret quantum state. Later, Li et al. [31] proposed a scheme for sharing an unknown single qubit with EPR pairs and multi-particle joint measurement. In 2010, Wang et al. generalized a QSTS protocol of an arbitrary two-particle state using non-maximally GHZ states and generalized Bell state measurement in [77].

In QSTS protocol, Alice wants to transmit an arbitrary two-particle state to Bob or Charlie. Alice holds the initial known state of the particles marked with x and y which is described as $|\tau\rangle_{xy} = \alpha|00\rangle_{xy} + \beta|01\rangle_{xy} + \gamma|10\rangle_{xy} + \delta|11\rangle_{xy}$. The composite quantum system which consists of the eight particles are

$$|\Lambda\rangle_s = |\tau\rangle_{xy}|\mathrm{GHZ}_m\rangle_{a_1,b_1,c_1}|\mathrm{GHZ}_m\rangle_{a_2,b_2,c_2}, \tag{15}$$

where a_1, b_1, c_1 and a_2, b_2, c_2 are the GHZ particles shared by Alice, Bob and Charlie respectively. The generalized GHZ state in the form:

$$\begin{aligned}
|\mathrm{GHZ}^+_{n_1}\rangle &= N(|000\rangle + n|111\rangle),\\
|\mathrm{GHZ}^-_{n_1}\rangle &= N(n^*|000\rangle - |111\rangle),\\
|\mathrm{GHZ}^+_{n_2}\rangle &= N(|001\rangle + n|110\rangle),\\
|\mathrm{GHZ}^-_{n_2}\rangle &= N(n^*|001\rangle + |110\rangle),\\
|\mathrm{GHZ}^+_{n_3}\rangle &= N(|010\rangle + n|101\rangle),\\
|\mathrm{GHZ}^-_{n_3}\rangle &= N(n^*|010\rangle - |101\rangle),\\
|\mathrm{GHZ}^+_{n_4}\rangle &= N(|100\rangle + n|011\rangle),\\
|\mathrm{GHZ}^-_{n_4}\rangle &= N(n^*|100\rangle - |011\rangle),
\end{aligned} \tag{16}$$

where the coefficient $N = 1/\sqrt{1 + |n|^2}$.

Now Alice wants to build the communication channel, she keeps the particles a_1, a_2 at her hand and distributes the generalized GHZ state $|\mathrm{GHZ}^+_{n_1}\rangle$ particles to Bob and Charlie respectively. Not lose generality, the initial state prepared by Alice is chosen as $|\tau\rangle_{xy} = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$. The state of composite system can be described as

$$\begin{aligned}
|\Lambda\rangle_s = N^2(&\alpha|00000000\rangle + \alpha n|00111000\rangle\\
&+ \beta|01000000\rangle + \beta n|01111000\rangle\\
&+ \gamma|10000000\rangle + \gamma n|10111000\rangle\\
&+ \delta|11000000\rangle + \delta n|11111000\rangle\\
&+ \alpha n|00000111\rangle + \alpha n^2|00111111\rangle\\
&+ \beta n|01000111\rangle + \beta n^2|01111111\rangle\\
&+ \gamma n|10000111\rangle + \gamma n^2|10111111\rangle\\
&+ \delta n|11000111\rangle + \delta n^2|11111111\rangle).
\end{aligned} \tag{17}$$

Firstly Alice performs joint generalized Bell state measurements on her four particles x, a_1 and y, a_2, and then she announces her results publicly. The particles marked with x, y, a_1, a_2 are in the product state: $R_{xa_1} \otimes R_{ya_2}$, here $R_{x(y)a_1(a_2)} \in \{|\phi^{\pm}_m\rangle, |\psi^{\pm}_m\rangle\}$. Assuming that her measurement results are $|\phi^+_m\rangle_{x,a_1}|\phi^+_m\rangle_{y,a_2}$, the composite system of particles $b_1b_2c_1c_2$ becomes to

$$\begin{aligned}
|\Lambda\rangle_{\mathrm{sub}} = \frac{N^2}{M^2}(&\alpha|0000\rangle + \frac{n\beta}{m}|0101\rangle\\
&+ \frac{n\gamma}{m}|1010\rangle + \frac{n^2\delta}{m^2}|1111\rangle)_{b_1b_2c_1c_2}.
\end{aligned} \tag{18}$$

Secondly, Bob applies a joint X basis measurement $\hat{X}_{b_1} \otimes \hat{X}_{b_2}$ on his two particles b_1 and b_2 which is the Von Neumann measurement on the basis: $|\pm X\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. And it is the same for Charlie's two particles. Then Alice's results are correlated with Bob's outcomes and Charlie's states. For example, in the case of Alice's generalized Bell state measurement results $|\phi^+_{m1}\rangle|\phi^+_{m2}\rangle$, the correspondence between Bob's results and Charlie's state is listed in Table 1.

Lastly, Charlie makes some unitary operations on his two particles:

$$\begin{aligned}
U_0 &= |0\rangle\langle 0| + |1\rangle\langle 1|, U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|,\\
U_2 &= |0\rangle\langle 1| + |1\rangle\langle 0|, U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|.
\end{aligned} \tag{19}$$

After Alice and Bob announce the results publicly, Charlie

Table 1 The correspondence between Bob's results and Charlie's state with the results of Alice's result is $|\phi^+_{m1}\rangle|\phi^+_{m2}\rangle$

Bob's results (b_1,b_2)	Charlie's results
$\lvert +X\rangle\lvert +X\rangle$	$\alpha\lvert 00\rangle + \gamma n/m\lvert 10\rangle + \beta n/m\lvert 01\rangle + \delta n^2/m^2\lvert 11\rangle$
$\lvert +X\rangle\lvert -X\rangle$	$\alpha\lvert 00\rangle + \gamma n/m\lvert 10\rangle - \beta n/m\lvert 01\rangle - \delta n^2/m^2\lvert 11\rangle$
$\lvert -X\rangle\lvert +X\rangle$	$\alpha\lvert 00\rangle - \gamma n/m\lvert 10\rangle + \beta n/m\lvert 01\rangle - \delta n^2/m^2\lvert 11\rangle$
$\lvert -X\rangle\lvert -X\rangle$	$\alpha\lvert 00\rangle - \gamma n/m\lvert 10\rangle - \beta n/m\lvert 01\rangle + \delta n^2/m^2\lvert 11\rangle$

Table 2 The correspondence between parity and operations

V	$V\bigoplus P_b$	Operation
ϕ_m	0	U_0
ϕ_m	1	U_1
ψ_m	0	U_2
ψ_m	1	U_3

performs the joint unitary operations $U_{0,1,2,3}$ operators on his two particles. The correspondence of the results between Alice, Bob and Charlie is shown in Table 2.

In details, when Bob measures in the basis $|++\rangle$, Charlie does not need to perform any unitary operation on the two-particle state after Bob's announcement. If Bob's measuring basis is $|+-\rangle$, Charlie performs U_0U_1 operations on her particles. Similarly, $|-+\rangle$ corresponds to the U_1U_0 operation and $|--\rangle$ corresponds to the U_1U_1 operation. After that, the particles on Charlie's side is in the state which Alice needs to share with her. Charlie recovers the original unknown state on Alice's side with a certain fidelity. The fidelities is $F = N^2||\alpha|^2 + |\gamma|^2n/m + |\beta|^2n/m + |\delta|^2n^2/m^2|/M^2$.

The QSTS protocol can also be realized by using generalized Bell state channels instead of generalized GHZ state channels. So the non-maximally entangled state can be used in quantum state sharing as well. And it is secure to implement the communication.

6 Summary

In this review article, we have reviewed the recent development of quantum communication theory in which secret messages can be transmitted from one user to another user. They are attractive because they are unconditionally secure. With current and near future technology, the quantum communication protocols may become more and more popular. In most quantum communication protocols, single photons and entangled photon pairs are used as the information carriers. To prevent an Eve taking advantage of noise, a quantum privacy amplification protocol has been proposed. It involves very simple operations and reduces the information leakage to a negligible small level.

This work was supported by the National Basic Research Program of China (2010CB923202), Specialized Research Fund for the Doctoral Program of Education Ministry of China (20090005120008), Fundamental Research Funds for the Central Universities and National Natural Science Foundation of China (61205117).

1 Shor P W. Algorithms for quantum computation: Discrete logarithm and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994. 124–134

2 Grover L. Quantum Mechanics helps in searching for a needle in a haystack. Phys Rev Lett, 1997, 78: 325–328

3 Dong H, Liu X F, Sun C P, et al. Thermodynamic witness of quantum probing. Chin Sci Bull, 2010, 55: 3256–3260

4 Guo Y, Qi X F, Hou J C. Sufficient and necessary conditions of separability for bipartite pure states in infinite-dimensional systems. Chin Sci Bull, 2011, 56: 840–846

5 Cao H X, Li L, Chen Z L, et al. Restricted allowable generalized quantum gates. Chin Sci Bull, 2010, 55: 2122–2125

6 Wang C, Li Y S, Hao L. Optical implementation of quantum random walks using weak cross-Kerr media. Chin Sci Bull, 2011, 56: 2088–2091

7 Bennett C H, Brassad G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984. 175

8 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829

9 Gottesman D, Chuang I L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature, 1999, 402: 390

10 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge, UK: Cambridge University Press, 2000

11 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124

12 Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895

13 Zhang W, Liu Y M, Zuo X Q, et al. Preparation of genuine Yeo-Chua entangled state and teleportation of two-atom state via cavity QED. Sci China Phys Mech Astron, 2010, 53: 2232–2237

14 Cirac J I, Zoller P, Kimble H J, et al. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. Phys Rev Lett, 1997, 78: 3221

15 Long L R, Li H W, Zhou P, et al. Multiparty-controlled teleportation of an arbitrary GHZ-class state by using a d-dimensional $(N+2)$-particle nonmaximally entangled state as the quantum channel. Sci China Phys Mech Astron, 2011, 54: 484–490

16 Yin X F, Liu Y M, Zhang Z Y, et al. Perfect teleportation of an arbitrary three-qubit state with the highly entangled six-qubit genuine state. Sci China Phys Mech Astron, 2010, 53: 2059–2063

17 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390: 575

18 Boschi D, Branca S, De Martini F, et al. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1998, 80: 1121

19 Furusawa A, Sorensen J L, Braunstein S L, et al. Unconditional quantum teleportation. Science, 1998, 282: 706

20 Kim Y H, Kulik S P, Shih Y. Quantum teleportation of a polarization state with a complete Bell state measurement. Phys Rev Lett, 2001, 86: 1370

21 Marcikic I, de Riedmatten H, Tittel W, et al. Long-distance teleportation of qubits at telecommunication wavelengths. Nature, 2003, 421: 509

22 Pan J W, Gasparoni S, Aspelmeyer M, et al. Experimental realization of freely propagating teleported qubits. Nature, 2003, 421: 721

23 Ursin R, Jennewein T, Aspelmeyer M, et al. Communications: Quantum teleportation across the Danube. Nature, 2004, 430: 849

24 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648

25 Sudhir K S, Srikanth R. Generalized quantum secret sharing. Phys Rev A, 2005, 71: 012328

26 Hao L, Li J L, Long G L. Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. Sci China Phys Mech Astron, 2010, 53: 491–495

27 Shi R H, Huang L S, Yang W, et al. Quantum secret sharing between multiparty and multiparty with Bell states and Bell measurements. Sci China Phys Mech Astron, 2010, 53: 2238–2244

28 Tittel W, Zbinden H, Gisin N. Long-range effects in granular avalanching. Phys Rev A, 2001, 63: 042301

29 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. Phys Rev Lett, 2004, 92: 177903

30 Xia Y, Song J, Song H S. Quantum state sharing using linear optical elements. Opt Commun, 2008, 281: 4946

31 Li Y M, Zhang K, Peng K C. Multiparty secret sharing of quantum information based on entanglement swapping. Phys Lett A, 2004, 324: 420

32 Liu J, Liu Y M, Zhang Z J. Generalized multiparty quantum single-qutrit-state sharing. Int J Theor Phys, 2008, 47: 2353

33 Deng F G, Li C Y, Li Y S. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 022338

34 Yuan H, Liu Y M, Han L F, et al. Tripartite arbitrary two-qutrit quantum state sharing. Commun Theor Phys, 2008, 49: 1191

35 Li X H, Zhou P, Li C Y, et al. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J Phys B: At Mol Opt Phys, 2006, 39: 1975

36 Sheng Y B, Deng F G, Zhou H Y. Efficient and economic five-party quantum state sharing of an arbitrary m-qubit state. Eur Phys J D, 2008, 48: 279

37 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302

38 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317

39 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319

40 Deng F G, Li X H, Li C Y, et al. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs. Phys Lett A, 2006, 359: 359

41 Wang C, Deng F G, Li Y S, et al. Quantum secure direct commuication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305

42 Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using mult-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253: 15

43 Yang C W, Tsai C W, Hwang T. Fault tolerant two-step quantum secure direct communication protocol against collective noises. Sci China Phys Mech Astron, 2011, 54: 496–501

44 Cao W F, Yang Y G, Wen Q Y. Quantum secure direct communication with cluster states. Sci China Phys Mech Astron, 2010, 53: 1271–1275

45 Gu B, Zhang C Y, Cheng G S, et al. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. Sci China Phys Mech Astron, 2011, 54: 942–947

46 Li X H, Zhou P, Liang Y J, et al. Quantum secure direct communication network with two-step protocol. Chin Phys Lett, 2006, 23: 1080

47 Cai Q Y, Li B W. Improving the capacity of the Bostrom-Felbinger protocol. Phys Rev A, 2004, 69: 054301

48 Cai Q Y, Li B W. Deterministic secure communication without using entanglement. Chin Phys Lett, 2004, 21: 601–603

49 Long G L, Wang C, Li Y S, et al. Quantum secure direct communication (in Chinese). Sci Sin Phys Mech Astron, 2011, 41: 332–342

50 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315

51 Ekert A K. Quantum cryptography based on Bells theorem. Phys Rev Lett, 1991, 67: 661

52 Kwiat P G, Mattle K, Weinfurter H, et al. New high-intensity source of polarization-entangled photon pairs. Phys Rev Lett, 1995, 75: 4337

53 Weinfurter H, Zukowski M. Four-photon entanglement from down-conversion. Phys Rev A, 2001, 64: 010102

54 Lu C Y, Zhou X Q, Gühne O, et al. Experimental entanglement of six photons in graph states. Nat Phys, 2007, 3: 91–95

55 You L X, Shen X F, Yang X Y. Single photon response of superconducting nanowire single photon detector. Chin Sci Bull, 2010, 55: 441–445

56 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145

57 Zhang Y S, Li C F, Guo G C. Quantum key distribution via quantum encryption. Phys Rev A, 2001, 64: 024302

58 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050

59 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503

60 Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901

61 Yan T, Yan F L. Quantum key distribution using four-level particles. Chin Sci Bull, 2011, 56: 24–28

62 Muller A, Herzog T, Huttner B, et al. Plug and play systems for quantum cryptography. Appl Phys Lett, 1997, 70: 793–795

63 Zhou C Y, Wu G, Chen X L, et al. Quantum key distribution in 50 km optic fibers. Sci China Phys Mech Astron, 2004, 47: 182–188

64 Gao F, Wen Q Y, Qin S J, et al. Quantum asymmetric cryptography with symmetric keys. Sci China Ser G-Phys Mech Astron, 2009, 52: 1925–1931

65 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390: 575–579

66 Lee J, Min H, Oh S D. Multipartite entanglement for entanglement teleportation. Phys Rev A, 2002, 66: 052318

67 Rigolin G. Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement. Phys Rev A, 2005, 71: 032303

68 Borras A, Plastino A R, Batle J, et al. Multiqubit systems: Highly entangled states and entanglement distribution. J Phys A, 2007, 40: 13407–13421

69 Choudhury S, Muralidharan S, Panigrahi P K. Quantum teleportation and state sharing using a genuinely entangled six-qubit state. J Phys A, 2009, 42: 115303

70 Zuo X Q, Liu Y M, Zhang Z Y, et al. Simpler criterion and flexibility of operation complexity for perfectly teleporting arbitrary n-qubit state with $2n$-qubit pure state. Sci China Phys Mech Astron, 2010, 53: 2069–2073

71 Yan F L, Yan T. Probabilistic teleportation via a non-maximamlly entangled GHZ state. Chin Sci Bull, 2010, 55: 902–906

72 Gu B, Zhang C Y, Cheng G S, et al. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. Sci China Phys Mech Astron, 2011, 54: 942–947

73 Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2005, 72: 012304

74 Wang J, Zhang Q, Tang C J. Multiparty quantum secret sharing of secure direct communication using teleportation. Comm Theor Phys, 2007, 47: 454

75 Man Z X, Xia Y J, An N B. Multiparty secret sharing of quantum information using and identifying Bell states. Eur Phys J D, 2007, 42: 333

76 Zhang Z J, Li Y, Man Z X. Multiparty quantum secret sharing. Phys Rev A, 2005, 71: 044301

77 Wang C, Zhang Y, Jin G S. Generalized quantum state sharing of the arbitrary two particles state. Sci China Phys Mech Astron, 2010, 53: 2064–2068