22

Quantum Direct Communication

Gui Lu Long[1,2], Chuan Wang[1,3], Fu-Guo Deng[4], and Wan-Ying Wang[1]
[1]*Key Laboratory of Atomic and Molecular Nanosciences and Department of Physics, Tsinghua University, Beijing 100084,*
[2]*Tsinghua National Laboratory for Information Science and Technology, Beijing 100084,*
[3]*School of Science and Key Laboratory of Optical Communication and Lightwave Technologies, Beijing University of Posts and Telecommunications, Beijing, 100876,*
[4]*Department of Physics, Beijing Normal University, Beijing 100875,*
People's Republic of China

1. Introduction

Quantum key distribution (QKD) is considered as an ideal method to make secret message unreadable to eaves-dropper but intelligible to the two authorized parties of the communication [1-6]. In the research of experimental quantum key distribution, single photons and entangled photon pairs are used as the carriers. In quantum key distribution, secret keys are generated first between the communication parties. The security of quantum key distribution is guaranteed by the laws of quantum mechanics. After the quantum key distribution is completed, the communication parties should share secret keys, then the sender encrypts the secret message using the secret keys to form the ciphertext and transmits the ciphertext through a classical channel. The receiver receives the ciphertext and then decrypt the ciphertext to get the secret message. Altogether there are four steps in a secret communication process with QKD: key generation, encryption, transmission and decryption.

Here in this review, we review some new development in quantum communication, quantum direct communication (QDC). Quantum direct communication is a form of quantum communication where secret messages can be transmitted through a quantum channel with or without additional classical communications. There are two forms of quantum direct communication, quantum secure direct communication (QSDC) [7{9] and deterministic secure quantum communication (DSQC) [10, 11]. In QSDC, secret messages are transmitted directly between the communication parties, from sender Alice to receiver Bob, without additional classical communication except those for the necessary eavesdropping check. In other words, the quantum key distribution process and the classical communication of ciphertext are condensed into one single quantum communication procedure in QSDC. Deterministic secure quantum communication is another type of quantum direct communication, such as those proposed in Ref. [10, 11], where classical communication is required in order to read out the secret message. As mentioned earlier, to complete a secure communication with the help of QKD, one usually encodes the secret message with an encryption scheme, and the ciphered text is transmitted through a classical channel. With a quantum channel, this procedure can be varied. For

Source: Advances in Lasers and Electro Optics, Book edited by: Nelson Costa and Adolfo Cartaxo,
ISBN 978-953-307-088-9, pp. 838, April 2010, INTECH, Croatia, downloaded from SCIYO.COM

instance, Alice can encrypt her secret message with a random key and encodes the ciphertext into the quantum states of the information carriers. The 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 principle ensures that Eve cannot steal the ciphertext. Because the ciphertext needs be transmitted through a quantum channel deterministically, not all quantum key distribution can be adapted to construct DSQC. Only deterministic QKD schemes can be adapted for DSQC purposes. The fundamental difference between QSDC and DSQC is the need of another round of classical communication. Hence it is always possible to use a QSDC scheme as a DSQC scheme.

The first QSDC protocol is the two-step QSDC protocol where qubits in an EPR pair are sent from one user to another user in two steps [8, 9]. The two-step QSDC protocol was first proposed by Long and Liu in 2001 [8], and standardized and analyzed by Deng, Long and Liu in 2003 [9]. Another QSDC protocol is the ping-pong QSDC protocol where one qubit of an EPR pair is sent from one user to another and then back to the sender again like the ping-pong. While the two-step QSDC protocol uses all four dense coding operations, the ping-pong protocol uses only two of the four dense coding operations. In another development, Shimizu and Imoto proposed the first DSQC protocol using entangled photon pairs [10]. In their scheme, the ciphertext is encoded in the state of entangled pairs, and the photons are transmitted from Alice to Bob. The receiver 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. The message can be read out only after a transmission of an additional classical information for each qubit. In recent years, quantum direct communication has attracted extensive interests and many interesting and important works have been carried out in QSDC for instance in Refs. [12-30], and in DSQC for instance in Refs. [31-39]. In the following sections, we will focus on the development of these two forms of quantum direct communication. We will also discuss their applications, such as in quantum secret sharing and quantum network.

2. Deterministic secure quantum communication protocols

As mentioned above, there are two kinds of deterministic schemes. One is quantum secure direct communication (QSDC) in which the receiver can read out the secret message directly, and classical information is exchanged between the two parties of quantum communication only for security checking. The other is called deterministic secure quantum communication (DSQC) [31] in which the receiver can read out the secret message by exchanging at least an additional 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 create a random key first and then use it to encrypt the message. In the following, we will describe some DSQC protocols.

A. DSQC with nonmaximally entangled states

We describe here two DSQC protocols without using maximally entangled states which was proposed by Li et al. [31], following some ideas in the delay-measurement quantum communication protocol [40]. It utilizes the pure entangled states as quantum information

carriers, called the pure-entanglement-based DSQC, and the other one makes use of the d-dimensional single photons, called the single-photon-based DSQC. Both of them introduce the decoy photons [41, 42] for security checking and only single-photon measurements are required for the two communication parties.

The two parties use pure entangled states as the quantum information carries in the pure-entanglement-based DSQC protocol [31]. Also this protocol assumes that the receiver has the capability of making single-particle measurements. The pure entangled states can be described as

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

where the subscript A and B indicate the two correlated photons in each entangled state. $|0\rangle$ and $|1\rangle$ are the two eigenvectors of the two-level operator σ_z, say the basis Z. a and b satisfy the relation $|a|^2 + |b|^2 = 1$.

Firstly, the sender, say Alice prepares a sequence of ordered N two-photon pairs, and each pair is randomly in one of the two pure entangled states $|\Psi'\rangle_{AB}$, $|\Psi''\rangle_{AB}$, and

$$|\Psi''\rangle_{AB} = a|1\rangle_A|0\rangle_B + b|0\rangle_A|1\rangle_B. \tag{2}$$

Alice picks up A particles to form an ordered sequence S_A and picks up the other partner photons to form the sequence S_B. For security checking, Alice replaces some photons in the sequence S_B with her decoy photons S_{de} which are produced randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Here $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are the two eigenvector of the two-level operator σ_x, say the basis X. The decoy photons is easily 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. Secret message is encoded on the photons in S_B sequence by performing $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$ at Alice's side and the two unitary operations represent classical bits 0 or 1, respectively. Then Alice sends sequence S_B to Bob. After Bob receives S_B sequence, Alice and Bob check the security of communication by measuring the decoy photons and comparing the outcomes. If the error rate is lower than the security bound, Alice and Bob measure their remaining photons with basis Z, and they get the final results R_A and R_B, respectively. Alice announces 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 the schemes with entanglement swapping and quantum teleportation, and it is more feasible in practice. In this protocol, the information carriers in two-particle pure entangled states can be prepared in experiment easily with present technology, and a single-photon measurement is simpler than a multi-particle joint measurement at present. This protocol is also generalized to the case with d-dimensional quantum systems [31]. The intrinsic efficiency approaches 100% and the total efficiency exceeds $\frac{1}{3}$ in theory which is larger than congeneric schemes using Einstein-Podolsky-Rosen (EPR) pairs.

B. DSQC with single photons

In the single-photon-based DSQC protocol [31], d- dimensional single-photon quantum systems are utilized as the information carriers. The Z_d basis of a d- dimensional system is

$$|0\rangle\,,\quad |1\rangle\,,\quad |2\rangle\,,\quad \cdots,\quad |d-1\rangle\,. \tag{3}$$

The d-dimensional eigenvectors of the measuring basis X_d are

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

At first, sender Alice prepares a sequence of d-dimensional single-photons randomly in the eigen-basis states of Z_d or X_d operators, the sequence is labeled as S. She chooses some photons in the S-sequence as the decoy photons and encrypts her secret message M_A on the other photons with unitary operations U_m, U_m^x, where

$$U_m = \sum_j |j+m \bmod d\rangle\langle j|, \tag{5}$$

$$U_m^x = \sum_j e^{\frac{2\pi i}{d}jm}|j+m \bmod d\rangle\langle j|. \tag{6}$$

In other words, 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 S sequence 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 information 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.

C. DSQC with quantum teleportation and entanglement swapping

Quantum teleportation [43] has been studied widely since it was first proposed in 1993, 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 DSQC scheme using EPR pairs and quantum teleportation [32]. In their scheme, the qubits do not carry the secret message when they are transmitted between the two parties, and this makes this communication more secure and convenient for post-processing such as privacy amplification.

At first, the two parties share a set of entangled pairs randomly in one of the four Bell states. Suppose that all the EPR pairs used in the scheme are $|\phi^+\rangle_{AB}$. The sender Alice prepares a

sequence of C particles in the X basis $|\psi\rangle_C$ according to her secret message ($|+\rangle$ for "0", $|-\rangle$ for "1"). Then Alice performs Bell-state measurements on her two particles BC. Each outcome will appear with equal probability 0.25 and Bob's particles will be related to the initial states of particles C by a unitary transformation U_{ij} relying on Alice's measurement outcomes. After Alice publicly announces her out-comes, Bob applies the corresponding inverse transformation U_{ij}^{-1} to his particles and measures them with the basis $X \equiv \{|+\rangle, \{|-\rangle\}$. Then Bob can obtain Alice's message. The security of this scheme is ensured because the security of quantum channel is ensured before the trans- mission of secret message, hence it is completely secure.

Subsequently, Gao et al. proposed another direct secure quantum communication scheme using controlled teleportation [20]. Three-particle entangled states are used in this scheme. When the communication starts, the three parties first share a set of entangled states. The sender Alice performs a Bell-state measurement on a information particle and a particle in the entangle state, and the controller Charlie performs a single-particle measurement. According to their measurement outcomes, the receiver Bob chooses a suitable unitary operation and then takes a single-particle measurement on his particle for reading out the secret message.

Entanglement swapping is also exploited to design a deterministic secure quantum communication protocol [35]. The protocol also uses the maximally entangled EPR pairs as the information carriers. The two parties assume that each of the four unitary operation represents a two-bit classical information beforehand. Bob prepares a series of EPR pairs in the state $|\Psi^+\rangle_{A_iB_i} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}$ and sends the A sequence to Alice which consists of all the A particles in the EPR pairs. They both store the photons into two groups, i.e. photons A_1 and A_2 as a group and B_1 and B_2 as another 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 they perform the Bell-state measurement on each group of their own particles. Alice announces her measurement results to Bob. Bob then concludes Alice's operation according to his measurement outcomes and those published by Alice, and extracts the secret message. This protocol makes use of two EPR pairs for entanglement swapping. For two bits of information, four qubits were prepared and two additional bits are transmitted.

Quantum teleportation or entanglement swapping can be utilized in DSQC schemes because they 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 message communication. Once entanglement is established, the qubits do not suffer from the noise and the loss aroused by the channel again, the bit rate and the security will very high.

D. DSQC based on the rearrangement of orders of particles

In this part, we describe DSQC protocols based on the rearrangement of orders of particles which uses EPR pairs as the information carriers, following some ideas in the controlled-order-rearrangement-encryption QKD protocol [6].

One DSQC protocol uses EPR pairs [21]. The transmitting order of the particles which ensures the security of communication is secret to anyone except for the sender Bob himself. The two parties agree that the four unitary operations in the dense coding represent two bits of classical information. The receiver Alice prepares a sequence of EPR pairs randomly in one of the four Bell states $\{|\phi^{\pm}\rangle_{AB}, |\psi^{\pm}\rangle_{AB}\}$. Here

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

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

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

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

Alice divides them into two corresponding sequences, called A sequence and B sequence. 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, a DSQC protocol was proposed with single photons based on the secret transmitting order of particles [22], following some ideas in Refs[6, 12]. 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⟩, |1⟩, |+⟩, |–⟩} and sends the sequence to Bob. Bob selects randomly a sufficiently large subset to perform $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|$ operation randomly for eavesdropping check later. 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.

These two DSQC protocols [21, 22] using transmitting order rearranging method are simple 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 [44]. They indicate that the protocols are insecure with Trojan horse attack strategies. An invisible photon or delayed 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 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 about 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 from Alice to Bob. (2) After Bob performs the unitary operation, Eve sorts her spy photons out in the line from Bob to Alice. As there is no security check at this stag, Eve will not be detected. 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 multi-photon rate and the error rate. If both the error rate and the multi-photon rate are very low, they continue to the next step. Otherwise, they terminate the communication. Furthermore, Bob has to insert 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 [44].

3. Quantum secure direct communication protocols

QSDC transmits secret messages directly through a quantum channel. QSDC has higher security requirement than both QKD and DSQC. In secret communication with QKD, one can protect secret message by first ensuring the security of the keys in the QKD process. In DSQC one can protect the secret message by checking the security of the DSQC process while holding the classical information. However in QSDC, the secret message is encoded in the information carriers directly, hence it is more stringent to ensure the security. According to Deng-Long criteria [9, 12], a real secure QSDC scheme should satisfy four requirements:

1. The secret message can be read out by the receiver directly and there is no additional classical information exchange between the sender and the receiver in principle except in the process for security checking and error rate estimating.
2. The eavesdropper cannot obtain any useful information about the secret message no matter what kind of attack she will perform.
3. Eve can be detected by the legitimate users before Alice and Bob encode the secret message on the quantum states.
4. The quantum states are transmitted in block by block way.

The last one of the four criteria is a necessary tool in QSDC hence one can use it easily to see if a quantum communication is a QSDC or not. It is a necessary condition hence even though some protocols are not QSDC even though they use block data transmission.

The two-step QSDC scheme [8, 9] is secure as it satisfies all these four requirements. In the following, we will discuss some QSDC protocols in details.

A. Two-step Quantum Secure Direct Communication

The two-step QSDC protocol is the first QSDC protocol using EPR states [8, 9]. The communication utilizes EPR pairs as information carriers in which each is in one of the four Bell states $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$.

The two-step QSDC scheme is the first secure model for quantum direct communication. This QSDC principle is shown in Fig.1, and the protocol is described in detail as follows [9].

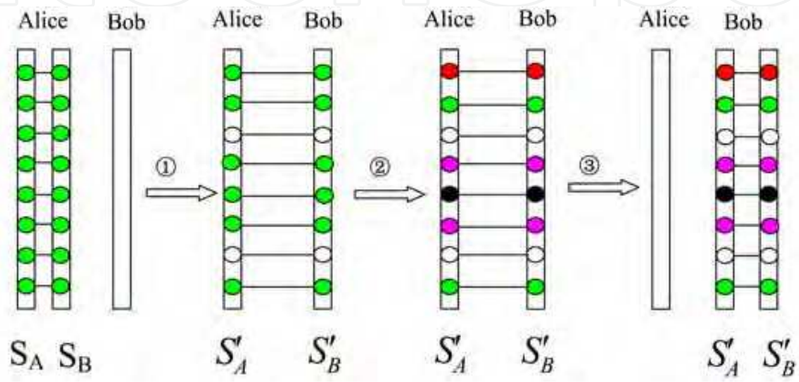


Fig. 1. The principle of the two-step QSDC scheme. Each line connect two photons represents an EPR pair. S_A is the message-coding sequence and S_B is the checking sequence.

In the QSDC process, Alice prepares an ordered N EPR pairs which are in the same state $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$. Alice separates the two particles into two parts. Each part is an ordered EPR partner particle sequence. One of the sequence is made up of all the photons marked with A in the ordered N EPR pairs which is called the message-coding (M) sequence S_A. The remaining EPR particles forms another particle sequence which is called the checking (C) sequence S_B. Alice and Bob agree that the four Bell states $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ correspond to the classical bits 00, 01, 10 and 11, respectively.

The security of two-step QSDC protocol is also considered. The security checking process during QSDC consists of two steps: first, Alice sends the checking sequence S_B to Bob and checks the security of transmission with Bob. Then if the two legitimate users confirm that the transmission of the checking sequence S_B is secure, Alice encodes her secret message on the S_A sequence 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 by Bell-state measurements. Here the four unitary operations used for coding are described below:

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{11}$$

$$U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{12}$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \tag{13}$$

$$U_3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \tag{14}$$

In the first step, Alice and Bob perform the security checking procedures. Bob chooses randomly a subset of the photons that he received as the samples for security checking, then he measures them by choosing randomly one of the two basis, $Z \equiv \{|0\rangle, |1\rangle\}$ and $X \equiv \{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Then Bob tells Alice the positions of the sample photons he has chosen, also the measuring bases and the outcomes. Alice chooses the same bases to mea- sure the corresponding photons in the M sequence. They compare their results publicly. If there is no eavesdrop- ping attack, their results should be in correspondence with each other, otherwise the eavesdropping behavior will be discovered.

In the second step, Alice selects some photons in the M sequence randomly and performs on them one of the four operations U_i (i = 0, 1, 2, 3). The remaining photons in the M sequence are used for information transmission. After Bob's Bell-state measurements on the EPR pairs, they perform the second step of security checking. Alice first tells Bob the positions of the checking qubits and the type of unitary operations. Bob's measurement will get an estimate of the error rate in the M sequence transmission. 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 get any information encoded on it as none can read out a useful information from part of maximally entangled quantum system.

If the quantum channel shows low noises or no loss, error correction procedures can be used in the communication. The bits preserving correction code should be used to preserve the integrity of the message.

In 2005, Wang et al. [14] generalized the two-step QSDC scheme based on superdense coding. Using high level particles, each particle could carry more than one bit information than two-step QSDC.

In d-dimension QSDC, the Bell-basis states are described as:

$$|\Psi_{nm}\rangle_{AB} = \sum_j e^{2\pi ijn/d}|j\rangle \otimes |j + m \bmod d\rangle/\sqrt{d} \tag{15}$$

where n,m = 0, 1, …, d –1. The unitary operations in d-dimensional Hilbert space are

$$U_{nm} = \sum_j e^{2\pi ijn/d}|j + m \bmod d\rangle\langle j|. \tag{16}$$

The unitary operations on the particle B can make the following transformations on the d-dimension Bell-basis state

$$|\Psi_{00}\rangle_{AB} = \sum_j |j\rangle \otimes |j\rangle/\sqrt{d} \tag{17}$$

into the Bell-basis state $|\Psi_{nm}\rangle_{AB}$.

When the QSDC starts, Alice and Bob transmit their information directly in two rounds which is shown in Fig.2. The procedures of communication is described in detail as follows:

1. The receiver Bob prepares a sequence of entangled photon pairs which are in the Bell state $|\Psi_{00}\rangle$.

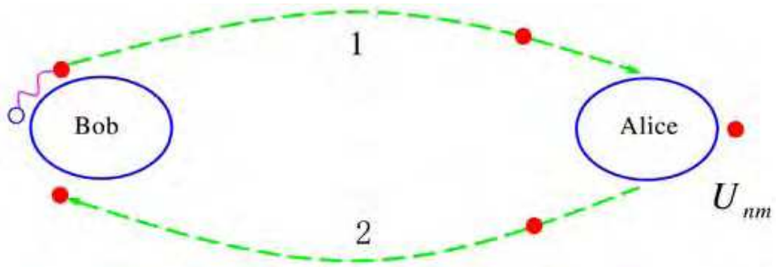


Fig. 2. Schematic description of quantum superdense coding [14].

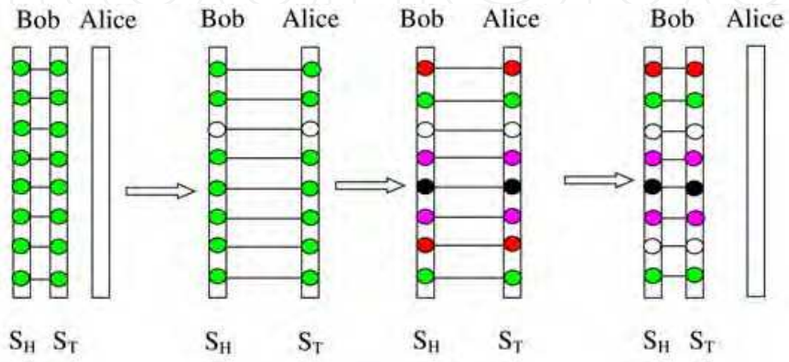


Fig. 3. Illustration of the QSDC protocol with a sequence of d-dimensional EPR pairs [14]. The T sequence is traveling forth and back from Bob to Alice.

2. Bob takes one particle from each entangled particle pair for making up of an ordered partner particle sequence, say [$P_1(H)$, $P_2(H)$, $P_3(H)$, ... , $P_N(H)$]. It is called the home (H) sequence. The remaining partner particles compose another particle sequence [$P_1(T)$, $P_2(T)$, $P_3(T)$, ... , $P_N(T)$], and it is called the traveling (T) sequence, shown in Fig.3. Here the subscript indicates the pair order in the sequence.
3. Bob sends the photon sequence to the sender of the secret message and then they check eavesdropping.

B. Deng-Long quantum one-time pad QSDC scheme

Single photons are easy to be produced than entangled photons for quantum communication. So Deng and Long proposed the QSDC scheme using one-time pad QKD method, called Deng-Long quantum one-time pad quantum secure direct communication. In quantum one-time pad QSDC scheme, Alice and Bob first share a sequence of single-photon quantum states securely, then the sender Alice encodes her secret message and transmits the states to the receiver Bob. The implementation of quantum one-time pad QSDC scheme is described in Fig.4.

Deng-Long quantum one-time pad QSDC scheme are described in details as follows:

(1) The secure doves sending phase.

In this step, Alice and Bob first share a series of single photons. The receiver Bob prepares a sequence of polarized single photons S and sends these photons to Alice.The states of the photons are chosen randomly in one of the four states {$|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$}. Alice and Bob can check the security of the transmission after receiving the photons. Bob chooses randomly the

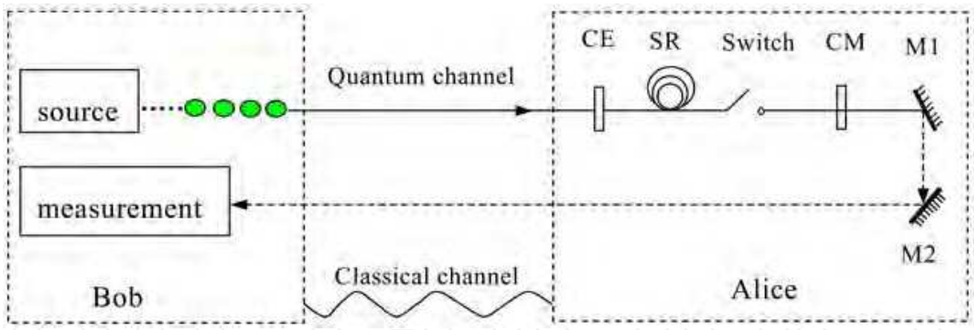


Fig. 4. Implementation of the quantum one-time pad QSDC scheme with optical delays [12]. CE is the eavesdropping check; SR represents an optical delay; Switch is used to control the quantum communication process, if the batch of photons are safe, the switch is on and the message coding is performed; CM encodes the secret message, M1 and M2 are two mirrors for in this simple illustrative set-up.

security checking qubits from the sequence S. Alice checks the security of this transmission by measuring the samples with the randomly chosen MBs and compares the states information with Bob. If they confirm that the transmission is secure, 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' 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 S' sequence are the remaining photons in the sequence S after the first eavesdropping check. The U_3 operation only flips the two eigenvectors in both MBs Z and X, i.e.,

$$U_3|0\rangle = -|1\rangle, \quad U_3|1\rangle = |0\rangle, \tag{18}$$

$$U_3|+\rangle = |-\rangle, \quad U_3|-\rangle = -|+\rangle. \tag{19}$$

the two unitary operations U_0 and U_3 do not change the MBs of the photons. Alice sends the encoded photon sequence S' back to Bob. Since Bob knows the initial state information completely, he can choose the original MBs to measure each photon for reading out the secret message. Alice picks some photons in the S' sequence to check the security of transmission. She chooses randomly the U_0 and U_3 operations to encode some checking information in the message coding phase. After Bob measures the photons in the sequence S', Alice tells Bob the positions and the coded bit values of these checking photons. These checking photons gives Alice and Bob opportunity to estimate whether there is an Eve in the line to intercept their communication. Eve's eavesdropping in this phase will not get any useful information about the secret message as she does not know the original states of the photons in the sequence S.

Single photons and quantum memories are needed in this practical QSDC scheme. The sender Alice must have the capability of storing quantum states. By now, 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 [40]. In this book, we would like to introduce the method of the photon storage realized by optical delays in a fibre, as shown in Fig.4. In practice, there are also losses in the transmission lines, error correcting techniques are necessary.

C. multi-step QSDC with Greenberger-Horne-Zeilinger states

The two-step QSDC can be generalized to multi-step QSDC scheme with multi-particle entangled state, such as Greenberger-Horne-Zeilinger (GHZ) states [15]. The three-particle GHZ state can be described as:

$$|\varphi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}). \tag{20}$$

There are eight independent GHZ states, namely

$$|\varphi\rangle_0 = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{21}$$

$$|\varphi\rangle_1 = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \tag{22}$$

$$|\varphi\rangle_2 = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \tag{23}$$

$$|\varphi\rangle_3 = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle), \tag{24}$$

$$|\varphi\rangle_4 = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \tag{25}$$

$$|\varphi\rangle_5 = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle), \tag{26}$$

$$|\varphi\rangle_6 = \frac{1}{\sqrt{2}}(|110\rangle + |110\rangle), \tag{27}$$

$$|\varphi\rangle_7 = \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle). \tag{28}$$

By performing single-particle unitary operations $\{U_i\}$ (i = 0, 1, 2, 3) on two of the three particles, the initial GHZ state can be changed to any of the state in the set.

In the beginning, Alice and Bob make an agreement that each of the states $|\varphi\rangle_k$ (k = 0, 1,…, 7) represents a three bits binary number, namely $|\varphi\rangle_0$, $|\varphi\rangle_1$, …, and $|\varphi\rangle_7$ corresponds to the classical coded as 000, 001, …, and 111, respectively.

The sender Alice prepares a sequence of ordered N three-particle GHZ-state quantum systems, labeled as [$P_1(A)P_1(B)P_1(C)$, $P_2(A)P_2(B)P_2(C)$, …, $P_N(A)P_N(B)P_N(C)$] which are in

the state: $|\varphi\rangle_0 = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC})$. Then Alice divides the sequence into three partner particle sequences, $S_A = [P_1(A), P_2(A), \ldots, P_N(A)]$, $S_B = [P_1(B), P_2(B), \ldots, P_N(B)]$ and $S_C = [P_1(C), P_2(C), \ldots, P_N(C)]$.

Then Alice and Bob complete the multi-step QSDC as follows:

(1) First step entanglement sharing process.

Alice sends the sequence labeled with C to the receiver Bob. After that she checks the security of the transmission with Bob to discover the eavesdropping attack. Bob randomly chooses some particles from S_C sequence as the sample qubits and measures them by choosing one of the two MBs Z and X randomly. Then Bob notice Alice the positions and the MBs of the sample particles. After that Alice chooses a MB in the state {|00⟩, |01⟩, |10⟩, |11⟩} 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. Alice checks the correspondence of the qubits with Bob and analyzes the error rate η_e of the samples. If they find that η_e is reasonably low then they continues the quantum communication; otherwise, Alice and Bob abandon the communication and repeat their quantum communication from the beginning.

(2) Information coding process.

Alice encodes the secret message on the GHZ states using the U_0 and U_2 operations which can be used on the S_B sequence and the four unitary operations $\{U_0, U_1, U_2, U_3\}$ which are performed on the S_C particles. Alice also chooses some sample particles in the sequences S_B and S_A for the second step of security check which are operated by one of the four operations U_i (i = 0, 1, 2, 3) randomly.

(3) Second step entanglement sharing process.

Alice measures the samples chosen from the remaining particles in sequence S_A using the MB Z or X with 50% probabilities. Then she sends the sequence S_B to Bob. When Bob receives the S_B sequence, Alice tells Bob the positions of the samples. Bob measures the corresponding particles in the sequence S_B and S_C based on Alice's MBs' information. If Alice measures her particles with the basis Z, then Bob chooses to measure with the measuring basis {|00⟩, |01⟩, |10⟩, |11⟩}; otherwise, he chooses the Bell-basis state measurement on his sampling particles. After that they compare the outcomes of the measurement to analyze the error rate of these particles. If the error rate is lower than the security bound, Alice and Bob continue their quantum communication; otherwise they abort the communication and repeat it again.

(4) Information decoding process.

Alice sends the S_A sequence to Bob in the last step. Bob reads out the secret message with joint three-particle measurements on the particles in the three sequences S_A, S_B and S_C. Then they turn to the third step security checking, Alice tells Bob the positions of the sampling particles and they analyze the error rate of the samples. If the error rate is lower than the security bound, they can accomplish the transmission of the secret message.

During the communication process, Alice and Bob transmit one of the three sequences S_C, S_B and S_A each time. So the eavesdropper Eve can only capture one sequence during eavesdropping. She cannot obtain any information about a GHZ-state quantum system if she only captures one particle. Thus this QSDC scheme is secure as that of the two-step QSDC scheme [8, 9].

Besides Bell states and GHZ states, various entangled sources are used in QSDC and DSQC protocols. In 2008, Lin et al. constructs a QSDC scheme [45] using χ-type entangled states which is in the form

$$|\chi^{00}\rangle_{1234} = \frac{1}{2\sqrt{2}}(|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)_{1234}. \quad (29)$$

An efficient QSDC process based on the χ-type entangled states is discussed both in ideal and noisy communication channels. Later Dong et al. proposed a QSDC protocol using three-particle W states [46]. Also another DSQC protocol using four-particle entangled states is proposed by Xiu et al. in the same group [47].

D. quantum-encryption-based QSDC scheme

The principle of the quantum-encryption-based QSDC scheme [16] is shown in Fig.5. In this protocol, a controlled-not (CNot) gate is used to encode and decode the secret message. The two parties share privately a sequence of two-photon pure entangled states before-hand, and then use the states as their private quantum key which is reusable with a eavesdropping check before each round. The message can be readout directly by the receivers and each photon transmitted between the two parties can carry one bit of message securely in principle.

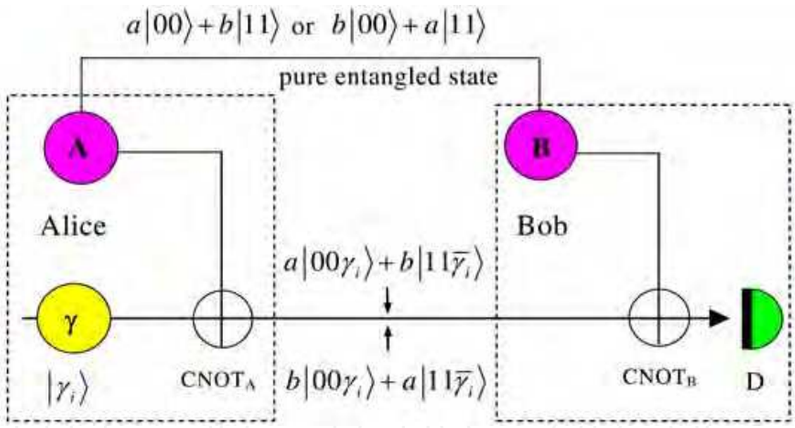


Fig. 5. Illustration of the quantum-encryption-based QSDC scheme [44]. The pure entangled states are used as quantum key which are repeatedly used. D represents the measurement with the MB Z.

In the quantum-encryption-based QSDC protocol, Alice and Bob first share a sequence of two-particle entangled states privately and then use them as their private quantum key which are used to encrypt secret message.

In detail, 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 $|\Phi\rangle_{AB} = b|0\rangle_A|0\rangle_B+a|1\rangle_A|1\rangle_B$. For the purpose of secure communication, decoy photons are used in secure sharing the pure entangled states [41, 42]. Alice picks up the photon marked with B in each pair to make up the sequence S_B : [B_1, B_2, … ,B_n]. The other sequence S_A is made up of particles A_i (i = 1, 2…n). The sequence S_B is

sent to Bob and the sequence S_A is kept by Alice. Alice inserts some decoy photons S_{de} into the sequence S_B for checking the security of the transmission. The decoy photons are randomly in one of the four states {|0⟩, |1⟩, |+⟩ = $\frac{1}{\sqrt{2}}$ (|0⟩ + |1⟩), |–⟩ = $\frac{1}{\sqrt{2}}$ (|0⟩ – |1⟩)}. 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. Bob measures the decoy photons with the suitable bases that Alice told him 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; otherwise, they discard the qubits and repeat quantum communication from the beginning.

Alice prepares a sequence of traveling particles γ_i in one of the two states {|0⟩, |1⟩} according to the bit value of her secret message is 0 or 1 (called the traveling particle sequence S_T). As discussed in Refs. [8, 9, 12], Alice randomly inserts some decoy photons in the sequence S_T for security checking. The sequence, say S_D, are randomly in the four states {|0⟩, |1⟩, |+⟩, |–⟩}. The quantum key, the pure entangled pairs shared {$|\Psi\rangle_{AB}$, $|\Phi\rangle_{AB}$} are used by Alice to encrypt the traveling particles in the sequence S_T except for the decoy photons, shown in Fig.5. Alice performs a controlled-not (CNOT) operation on the particles A_i and γ_i (i = 1, 2, …, n) by using the particle A_i as the control qubit. Then all the traveling particles are sent to Bob. Alice announces to Bob the positions and the states of the decoy photons and then Bob measures them with the same bases. Bob then takes a CNOT operation on the particles B_i and γ_i with the particle B_i as the control qubit and then he measures the particles γ_i with the basis Z. The outcomes of the measurements are recorded. If the transmission channel is secure, Bob reads out the message directly. The quantum keys are used to transmit the secret message in the next round by repeating the communications. Otherwise, they have to abandon their results and repeat their quantum communication form the beginning.

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 traveling particle γ_i is randomly in one of the two states {$a|00\gamma_i\rangle+b|11\overline{\gamma_i}\rangle$, $b|00\gamma_i\rangle+a|11\overline{\gamma_i}\rangle$}. So the density matrix of the traveling particle γ_i for Eve is $\rho_i = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The eavesdropping behavior on the traveling particle reveals no useful information about the secret message. Moreover, Eve's action will leave a trace in the results of the decoy photons and be discovered by the communication parties. So this quantum-encryption-based QSDC scheme is secure in principle.

Noises are inevitably exist in the practical quantum channel, so the users must exploit entanglement purification [49] to keep the entanglement in the quantum key, and quantum privacy amplification [50] on them as well. However, Bell states are not needed in this protocol, 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 $|\Psi\rangle'_{AB} = a'|0\rangle_A|0\rangle_B+ b'|1\rangle_A|1\rangle_B$ ($|\Phi\rangle'_{AB} = b'|0\rangle_A|0\rangle_B + a'|1\rangle_A|1\rangle_B$) are used 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. On the one hand, the users should do error correction on their results in practical applications. 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. The obvious advantage of the quantum-encryption-based 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 pure entangled signals because of asymmetric features of the quantum source.

E. QSDC using one party quantum error correction code

Quantum error correcting codes(QECC) is a key technique towards protecting quantum system in quantum communication and quantum computation from errors mainly brought by decoherence. Here we introduce the QSDC protocol using the one-party quantum error correcting codes(one-party-QECC) [51]. The use of one- party QECC proves that QSDC is able to tolerate higher error rates in transmission process. As described in the proof of unconditional secure BB84 protocols, the success of error correction in QSDC may lead a path to prove its unconditional security.

Protocol: one-party-QECC QSDC protocol

1. Bob owns the entanglement source and prepares a sequence contains $3n$ EPR pairs in the initial states $|©^{+}\rangle$.
2. Bob chooses $3n$ bit binary string b, then he chooses to apply the Hadamard transformation H to the second halves of the pairs in which the corresponding bits of string b are 1. After that he sends the second halves to Alice.
3. Alice announces receiving the qubits to Bob publicly. Bob tells Alice which qubits are operated by the Hadamard operations. Then Alice applies Hadamard transformation H on the corresponding qubits in her part.
4. Alice and Bob choose an n subset of the EPR pairs randomly for security checking. They measure the checking qubits respectively in the Z-basis and compare the results publicly. The results on both Alice's and Bob's sides in each pair will be the same if there are no errors. However, if there are too many inconsistencies, they notice that the transmitting qubits are been eavesdropped and the protocol is aborted.
5. Alice randomly selects m subset of the rest $2m$ logical EPR pairs as the second-round check pairs and the rest are used for coding. A $2m$ bit binary string b' is also chosen randomly. Bob applies the Hadamard transformation $\bar{H}$ to the second halves of the pairs when the corresponding bits of b are 1. Then the second halves are sent to Bob. During the communication process, if Alice wants to send a k bit binary sequence of message M. She first picks a [[$2m$, $2k$, t]] one-party-QECC that are used to correct the errors in the second transmission. There are k logical EPR pairs in the code pairs and she encodes M to her halves of the second-level logical qubits in the code pairs by applying

$$\bar{U}_{2i} = \bar{Z}_{2i}\bar{X}_{2i} \tag{30}$$

on the $2i$-th logical qubit where the i-th bit of M is 1. Actually Alice is able to apply this local operation. Then she returns all her qubits to Bob.

6. Bob receives the qubits and announces his receipt publicly. Then Alice tells Bob the binary string b', and Bob applies the first-level logical $\bar{H}$ to the received qubits where the corresponding bits of b' are 1.
7. Alice announces to Bob the places of second-round check pairs and the one-party-QECC that she chooses. If Bob measures both the qubits in each checking pairs in Z-basis respectively, he will get the same results with Alice without error. Thus if Bob's error rate is high than the security bound, the protocol is aborted.
8. Bob then uses the [[$2m$, $2k$, t]] one-party-QECC to correct the bit errors on the rest m first round transmission logical EPR pairs and obtains k second round transmission logical code pairs.
9. Bob measures both the qubits of the rest k second round transmission logical code pairs in Z-basis. By comparing the measurements on corresponding pairs, Bob can retrieve the full information of M.

F. Quantum secret sharing based on quantum secure direct communication

Classical secret sharing aims to distribute secret keys between the boss and his agents. When 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. Quantum secret sharing(QSS) is a special utilization of quantum mechanics in classical secret sharing. The basic model of QSS permits the boss and two(or more) remote parties to share the secret keys and any eavesdropping behavior will be discovered by the communication parties. QSS was first proposed by M. Hillery, V. Buμzek and A. Berthiaume. In the protocol, three-particle maximally entangled state (Green-Horne-Zeilinger state) is used to realize the secret sharing process.

In 2005, Zhang et al. proposed a (n, n)-threshold multiparty quantum secret sharing protocol [48] of secure direct communication based on the two-step QSDC protocol. In the QSS process, the sender's secure message can be extracted only if all the agents collaboration. Different from the protocol of multi-particle GHZ states QSS, if the agents number is larger than 3, the use and identification of Bell states are enough in their two protocols disregarding completely the sharer number. Later, Li et al. generalized Zhang's protocol and propose a (t, n)- threshold QSS protocol using secure direct communications [27]. In Li's QSS protocol, the boss distributes the classical secret shares to his agents and each agent owns a secret share in advance. His secure direct communication message can be extracted by the collaboration of at least t or more agents can obtain the secret message with the mutual assistances. Any t-1 or fewer agents cannot reveal any information. Compared with the previous multiparty quantum secret sharing protocols in which the sender's secret message can be recovered only if all the agents collaborate and the protocol is more practical and more flexible. Wang et al. generalized Zhang's QSS protocol to the high-dimensional case via quantum superdense coding [28]. The channel capacity and security are improved by the high-dimensional quantum coding, so the protocol shows a better efficiency and security.

4. Quantum secure direct communication network

Quantum communication network is also an important branch of quantum information and there are many related works. But 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 quantum network, servers who prepare and measure the quantum signals are needed, which simplifies the users' devices. On the other hand, it increases the di±culty for the two legitimate users to prevent the server from eaves-dropping. Here in this section, we will introduce three different QDC network protocols.

A. Quantum secure direct communication based on entangled pairs

As we have discussed in Ref.[9], maximally entangled photon states are used as the information carriers in two- step QSDC process. Recently, Li et al. [17] proposed the first QSDC network based on the two-step QSDC protocol with the EPR states. The communication network consists of three parties, the server Alice, the sender Bob and the receiver Carol. Each member in the network is required to exchange message with others securely. Here the three parties are going to finish the network communication by a circular transmission process.

When the communication starts, the sever Alice prepares the initial states which are described as: $|\psi^{+}\rangle_{CM} = \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{CM}$. Then she divides them into two corresponding sequence S_C (checking sequence) and S_M (message sequence). The two sequence are sent to Bob by two steps transmission process. After receiving the S_C sequence, Bob begins his QSDC with Carol by replacing some of the checking qubits with his decoy photons. The decoy photons are prepared randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ which are used for security checking. Then he sends this sequence to Carol. After Carol confirms the receipt, they check the security of the channel by comparing the states of the decoy photons after measuring the photons in randomly chosen basis.

If the error rate of the publicly comparing results, they confirm that the channel is secure. Bob then performs the unitary operations on his coding qubits in the S_M sequence. These operations are represented by Pauli operators which corresponds to the classical two bits information. Bob also picks out a subset of S_M and performs random operations on them for security checking. Then Bob sends the coding sequence to Carol. After that, they perform the second step of security checking. If the error rate is lower than the security bound, Carol 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 announces the outcomes. Bob and Carol use the remaining photons to estimate the error rate and Carol can read out Bob's message independently.

Another protocol of QSDC network based on entangled photon is proposed by Deng et al. using bidirectional QSDC scheme [13]. The structure of this network protocol is shown in Fig.6.

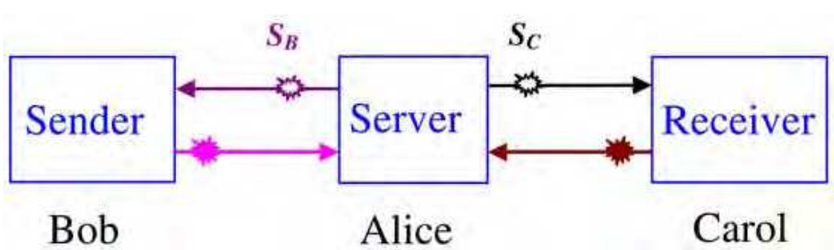


Fig. 6. The subsystem of QSDC network [13].

The sever Alice prepares a set of EPR pairs in the state $|\psi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{BC}$. The two photons in each state are divided into two sequence S_B and S_C. The S_B and S_C sequences are composed of all the particles marked with B and C in the EPR pairs $|\psi^-\rangle_{BC}$ respectively.
The S_B sequence is sent to Bob and the S_C sequence is sent to Carol. After receiving the two sequences, Bob and Carol perform the security checking. They select a sufficiently large subset of these EPR pairs as samples to check eavesdropping. They choose to measure the sample photons randomly with σ_x and σ_z operators to check the security of transmission. If the transmission process is secure, Bob encodes his message on the S_B sequence by choosing one of the four Pauli operations and Carol performs on the photons in S_C sequence either. Also Bob selects a subset of photons as checking samples in this process, then Bob and Carol both send the sequence back to Alice. After receiving the sequences, Alice performs Bell-state measurements on the EPR pairs and announces the outcomes. Carol can deduce Bob's message with his random operations that he has chosen after the security checking process. Then the network communication is finished.

B. Quantum secure direct communication network based on single photons

Single photons are easy to realized by attenuated laser pulses which exhibit ideal properties for quantum communication. Deng et al. proposed a more practical QSDC network based on single photons. The initial states are prepared in the same state $|0\rangle$ by the sever Alice. Then Alice sends the single-photon sequence S_0 which is formed by the single photons to the receiver Carol. Carol measures photons selected randomly from the S_0 sequence with the basis Z to check the transmitting security and uses beam splitters to check the multi- photon rate.
If she confirms that there is no eavesdroppers, she encodes the information by performing the I or σ_x operations on the single photons randomly. She also inserts some decoy photons which are produced by Hadamard operation on the particles in S, and then she sends them to the sender Bob. Bob checks the states with Carol of all the decoy photons to confirm the security of the communication. If the error rate is lower than the security bound, Bob encodes his message on the photons by choosing the Pauli operators I or σ_x. Bob selects a subset of photons as samples for checking the security and then he sends the photons to Alice. Alice measures the photons with Z basis and announces the outcomes to all the parties. So Carol can read out Bob's message directly. In this protocol, three checking processes are needed for three transmission processes to ensure the security of quantum communication. This QSDC network scheme is easy to be realized as only the single-photon measurement and local unitary operation are needed.

5. Singe qubit quantum privacy amplification for QSDC with single photons

In a practical quantum communications, noises inevitably exit, so the keys obtained from the QKD process are not complete secure. Quantum privacy amplification is often used to generate a key sequence with arbitrarily high security. Privacy amplification with single photons have been used in the BB84 QKD protocol. With entangled photon pairs, the privacy amplification procedure will be different, for instance quantum privacy amplification (QPA) [49, 50] has been used for QKD using entangled quantum systems in the Ekert91 QKD scheme [2].

A quantum privacy amplification for QSDC has recently been designed by Deng et al. for privacy amplification of QSDC with single photons [52]. The circuit of the privacy amplification is shown in Fig.7 which includes two controlled-not (CNOT) gates and one Hadamard (H) gate. Thee neighboring two qubits are sent to the circuit each time, then 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 target photon collapses to the eigen-state of the Z basis. The controlled photon is preserved and it carries the state information of both the two initial photons. After the CHC operation, the state information of the two photons is condensed into a single photon. Hence the privacy of the state of the left-over photon is amplified. After repeating the process many times, the leakage of the state information will be reduced to an arbitrarily low level.

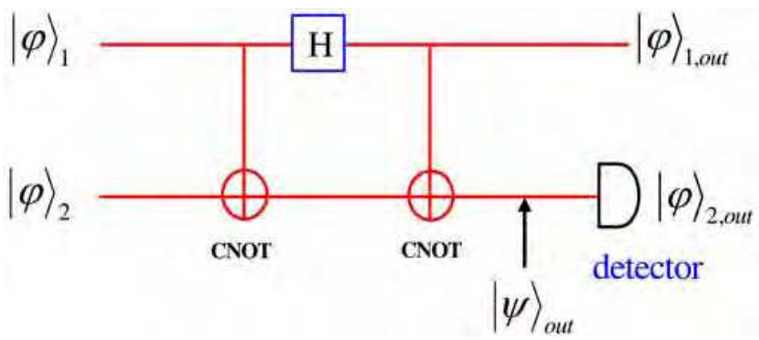


Fig. 7. Quantum privacy amplification operation for two qubits [52]. It consists of two controlled-not (CNOT) gates and a Hadamard (H) gate. $|\varphi\rangle_1$ and $|\varphi\rangle_2$ are the states of the two qubits, respectively. After the three unitary operations, the qubit 2 is measured and the information of the original state of photon 2 is incorporated into photon 1.

In the following, we will discuss the SQ-QPA process in detail. Suppose that Bob prepares a series of single photons which are randomly prepared in one of the four quantum states $|0\rangle$, $|1\rangle$, $(|0\rangle+|1\rangle)/2$ and $(|0\rangle-|1\rangle)/2$ and sends to Alice. An error bit ratio r is known for the photon batch. The SQ-QPA task is to process a portion of photons from the photon batch so that Eve's information about the processed photons is below a desired level.
The basic CHC operations of SQ-QPA is shown in Fig.7 for two qubits. We assume that the quantum states of single photon 1 and 2 are in the general forms:

$$|\varphi\rangle_1 = a_1|0\rangle + b_1|1\rangle, \tag{31}$$

$$|\varphi\rangle_2 = a_2|0\rangle + b_2|1\rangle, \tag{32}$$

where

$$|a_1|^2 + |b_1|^2 = |a_2|^2 + |b_2|^2 = 1. \tag{33}$$

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

$$
\begin{aligned}
|\psi\rangle_{out} &= \frac{1}{\sqrt{2}}\{(a_1a_2+b_1b_2)\,|0\rangle_1+(a_1b_2-b_1a_2)\,|1\rangle_1\}\,|0\rangle_2 \\
&+ \frac{1}{\sqrt{2}}\{(a_1a_2-b_1b_2)\,|1\rangle_1+(a_1b_2+b_1a_2)\,|0\rangle_1\}\,|1\rangle_2 .
\end{aligned} \tag{34}
$$

After measuring the second qubit with the Z basis, the state of the control qubit $|\varphi\rangle_{1out}$ will contain the information of the state of the original target qubit. Tables I and II 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.

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

Table I. 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_1			
φ_2	$\|+z\rangle$	$\|-z\rangle$	$\|+x\rangle$	$\|-x\rangle$
$\|+z\rangle$	$\|1\rangle$	$\|0\rangle$	$\|x\rangle$	$\|-x\rangle$
$\|-z\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-x\rangle$	$\|+x\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|0\rangle$	$\|1\rangle$
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|1\rangle$	$\|0\rangle$

Table II. 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 qubit and target qubit, respectively.

QPA reduces the information leakage to the eavesdropper in quantum communications. For example, if the eavesdropper (say Eve) knows completely the state information 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

$$
\rho = \frac{1}{4}\left(|+z\rangle\langle+z|+|-z\rangle\langle-z|+|+x\rangle\langle+x|+|-x\rangle\langle-x|\right) = \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}. \tag{35}
$$

So Eve has no knowledge at the density matrix, all the out put state will appear with the same probabilities. 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. However, if it happens that Eve has complete information about both qubits, the probability is

$$P_2 = r^2, \tag{36}$$

where r is four times of the error bit rate ε detected by Alice and Bob using random sampling. For advanced privacy amplification, 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 again. Since more qubits are used in the SQ-QPA process, Eve's information is reduced exponentially to

$$P_m = r^m, \tag{37}$$

where m is the number of qubits that have 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 SQ-QPA scheme is a practical method for quantum communication. Single qubit unitary and a two-qubit unitary operations are used for the QPA process. The measurement process consists of only single qubit measurement which is easy to realized using current technology.

6. Conclusion

In this study, we present several deterministic secure quantum communication and quantum secure direct communication protocols. The QSDC protocol permits exchange secret information directly through quantum channel. In QSDC, when the secure channel is established, all the eavesdropping behaviors will be discovered before the information transmission. Besides these protocols, high capacity QSDC protocols, QSDC with quantum error correction codes and QSDC networks are also discussed. DSQC is another form quantum direct communication. In DSQC secret messages can be transmitted between the legitimate users securely with the help of some classical communication.

In these protocols, both single photons and entangled photon states are used as the information processing carriers for secure direct communication. Signals are transmitted both in optical fibers and in free space. Single photon detectors are usually required, and in some protocol, Bell-basis measurements are also required.

At present, technical efforts are concentrated in quantum key distribution. We can see that in the future quantum technology will become more popular and demanding, the need and feasibility of other forms of quantum information processing such as QSDC and DSQC will increase. As we may see from this review, the technical requirements for QSDC and DSQC are almost the same as those for QKD. We expect that in the future intensive research on QSDC and DSQC, especially experimental studies of these subject, will remain and become an active and fruitful area of research.

7. Acknowledgments

Supported by the National Fundamental Research Program Grant Nos. 2006CB921106, 2009CB929402. China National Natural Science Foundation Grant Nos. 10874098, 10775076.

8. References

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

[2] Ekert A. K., Quantum cryptography based on Bells theorem. Phys. Rev. Lett., 1991, 67: 661-663.

[3] Bennett C. H., Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett, 1992, 68: 3121-3124.

[4] Bennett C. H., Brassard G., and Mermin N. D., Quantum cryptography without Bell's theorem, Phys. Rev. Lett., 1992, 68: 557-559.

[5] Bennett C.H. and Wiesner S.J., Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett., 1992, 69: 2881.

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

[7] Boström K. and Felbinger T., Deterministic secure direct communication using enganglement, Phys. Rev. Lett., 2002, 89: 187902

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

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

[10] Shimizu K. and Imoto N., Communication channels secured from eavesdropping via transmission of photonic Bell states, Phys. Rev. A, 1999, 60: 157-166

[11] Beige A., Englert B. G., Kurtsiefer C. and Weinfurter H., Secure communication with a publicly known key, Acta Phys. Pol. A, 2002, 101 (3): 357.

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

[13] Deng F. G., Li X. H., Li C. Y., Zhou P. and Zhou H. Y., Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs, Phys. Lett. A, 2006, 359: 359.

[14] Wang C., Deng F. G., Li Y. S., Liu X. S. and Long G. L., Quantum secure direct communication with high-dimension quantum superdense coding, Phys. Rev. A, 2005, 71: 044305.

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

[16] Li X. H., Li C. Y., Deng F. G., Zhou P., Liang Y. J. and Zhou H. Y., Quantum secure direct communication with quantum encryption based on pure entangled states, Chin. Phys., 2007, 16 (8): 2149-2153.

[17] Li X. H., Zhou P., Liang Y. J., Li C. Y., Zhou H. Y. and Deng F. G., Quantum secure direct communication network with two-step protocol, Chin. Phys. Lett., 2006, 23: 1080.

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

[19] Cai Q. Y. and Li B. W., Deterministic secure communication without using entanglement Chin. Phys. Lett., 2004, 21: 601-603.

[20] Gao T., Controlled and secure direct communication using GHZ state and teleportation, Z. Naturforsch, A, 2004, 59: 597

[21] Zhu A. D., Xia Y., Fan Q. B., and Zhang S., Secure direct communication based on secret transmitting order of particles Phys. Rev. A, 2006, 73: 022338.

[22] Wang J., Zhang Q., and Tang C. J., Quantum secure direct communication based on order rearrangement of single photons, Phys. Lett. A, 2006, 358: 256-258.

[23] Cao H. J. and Song H. S., Quantum secure direct communication with W state, Chin. Phys. Lett., 2006, 23: 290-292.

[24] Long G.L, Deng F.G., Wang C., Li X.H., Wen K. and Wang W.Y., Quantum Secure Direct Communication and Deterministic Secure Quantum Communication, Frontiers of Physics in China, 2007, 2(3) 251.

[25] Wang T. Y., Qin S. J. , Wen Q. Y., Zhun F. C., Analysis and improvement of multiparty controlled quantum secure direct communication protocol, ACTA PHYSICA SINICA, 2008, 57: 7452-7456.

[26] Qin S. J., Wen Q. Y., Meng L. M., Zhu F. C., High Efficiency of Two Efficient QSDC with Authentication Is at the Cost of Their Security, Chin. Phys. Lett., 2009, 26: 020312.

[27] Li B. K., Yang Y. G., Wen Q. Y., Threshold Quantum Secret Sharing of Secure Direct Communication, Chin. Phys. Lett., 2009, 26: 010302.

[28] Wang X., Liu Y. M., Han L. F., Zhang Z. J., Multiparty quantum secret sharing of secure direct communication with high-dimensional quantum superdense coding, Int. J. Quant. Info., 2008, 6: 1155-1163.

[29] Chamoli A., Bhandari C. M., Secure direct communication based on ping-pong protocol, Quant. Info. Proc., 2009, 8: 347-356.

[30] Qin S. J., Wen Q. Y., Meng L. M., Zhu F. C., Quantum secure direct communication over the collective amplitude damping channel Sci. China Ser. G, 2009, 52: 1208- 1212

[31] Li X. H., Deng F. G., Li C. Y., Liang Y. J., Zhou P., and Zhou H. Y., Deterministic secure quantum communication without maximaly entangled states, J. Korean Phys. Soc., 2006, 49: 1354-1359

[32] Yan F. L. and Zhang X., A scheme for secure direct communication using EPR pairs and teleportation Euro. Phys. J. B, 2004, 41: 75-78.

[33] Gao. T., Yan. F. L., and Wang. Z. X., Deterministic secure direct communication using GHZ states and swapping quantum entanglement, J. Phys. A: Math. Gen, 2005, 38: 5761C5770.

[34] Gao T., Yan F. L. and Wang Z. X., Deterministic secure direct communication using GHZ states and swapping quantum entanglement J. Phys. A, 2005, 38: 5761-5770.

[35] Man Z. X., Zhang Z. J., Li Y., Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations, Chin. Phys. Lett. 2005, 22: 18-21.

[36] Wang J., Zhang Q., and Tang C. J., Quantum secure direct communication without a pre-established secure quantum channel, Int. J. Quantum information, 2006, 4: 925-934

[37] Wang H. F., Zhang S., Yeon K. H., and Um C. I., Quantum secure direct communication by using a GHZ state, J. Korean Phys. Soc., 2006, 49: 459-463

[38] Dong L., Xiu X. M., Gao Y. J. and Chi F., Multiparty controlled deterministic secure quantum communication through entanglement swapping, Int. J. Mod. Phys. C, 2008, 19:1673-1681

[39] Han L. F., Chen Y. M., Yuan H., Deterministic Quantum Secure Direct Communication with Dense Coding and Continuous Variable Operations, Comm. Theo. Phys., 2009, 51: 648-652

[40] Deng F. G., Long G. L., Wang Y., and Xiao L., Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement, Chin. Phys. Lett., 2004, 21: 2097-2100

[41] Li C.Y., Zhou H.Y., Wang Y., and Deng F.G., Secure quantum key distribution network with Bell states and local unitary operaitons, Chin. Phys. Lett., 2005, 22: 1049-1052

[42] Deng F. G., Li X. H., Li C. Y., Zhou P., Liang Y. J., and Zhou H. Y., Multiparty quantum secret report, Chin. Phys. Lett., 2006, 23: 1676-1679

[43] Bennett C. H., Brassard G., Crépeau C., Jozsa R, Peres A., and Wootters W, K,, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett., 1993, 70: 1895-1899

[44] Li X. H., Deng F. G. and Zhou H. Y., Improving the security of secure direct communication based on the secret transmitting order of particles, Phys. Rev. A, 2006, 74: 054302

[45] Lin S., Wen Q. Y., Gao F. and Zhu F. C., Quantum secure direct communication with χ-type entangled states, Phys. Rev. A, 2008, 78: 064304

[46] Dong L., Xiu X. M., Gao Y. J. and Chi F., Quantum Secure Direct Communication Using W State, Comm. Theo. Phys. 2008, 49: 1495-1498

[47] Xiu X. M., Dong H. K., Dong L. Gao Y. J. and Chi F., Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping, Opt. Comm. 2009, 282: 2457-2459

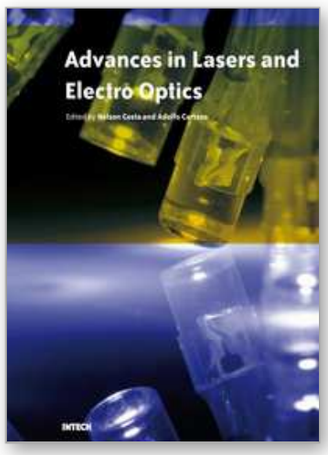
[48] Zhang Z. J., Multiparty quantum secret sharing of secure direct communication, Phys. Lett. A 2005, 342: 60-66

[49] Bennett C. H., Brassard G., Popescu S., Schumacher B., Smolin J. A., and Wootters W. K., Purification of noisy entanglement and faithful teleportation via noisy channels, Phys. Rev. Lett., 1996, 76: 722-725

[50] Deutsch D., Ekert A., Jozsa R., Macchiavello C. Popescu S., and Sanpera A., quantum privacy amplification and the security of quantum cryptography over noisy channels, Phys. Rev. Lett., 1996, 77: 2818-2821

[51] Wen K. and Long G. L., One-party Quantum Error Correcting Codes for Unbalanced Errors: Principles and Application to Quantum Dense Coding and Quantum Secure Direct Communications, e-print quant-ph/0609207

[52] Deng F. G. and Long G. L., Quantum privacy amplification for a sequence of single qubits, Commun. Theor. Phys., 2006, 46: 443-446



Advances in Lasers and Electro Optics

Edited by Nelson Costa and Adolfo Cartaxo

ISBN 978-953-307-088-9
Hard cover, 838 pages
Publisher InTech
Published online 01, April, 2010
Published in print edition April, 2010

Lasers and electro-optics is a field of research leading to constant breakthroughs. Indeed, tremendous advances have occurred in optical components and systems since the invention of laser in the late 50s, with applications in almost every imaginable field of science including control, astronomy, medicine, communications, measurements, etc. If we focus on lasers, for example, we find applications in quite different areas. We find lasers, for instance, in industry, emitting power level of several tens of kilowatts for welding and cutting; in medical applications, emitting power levels from few milliwatt to tens of Watt for various types of surgeries; and in optical fibre telecommunication systems, emitting power levels of the order of one milliwatt. This book is divided in four sections. The book presents several physical effects and properties of materials used in lasers and electro-optics in the first chapter and, in the three remaining chapters, applications of lasers and electro-optics in three different areas are presented.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen