Improved Security Detection Strategy in Quantum Secure Direct Communication Protocol Based on Four-Particle Green–Horne–Zeilinger State

Jian Li[a], Jin-Rui Nie[a], Rui-Fan Li[a], and Bo Jing[a,b]

[a] School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, P. R. China

[b] Department of Computer Science, Beijing Institute of Applied Meteorology, Beijing 100029, P. R. China

Reprint requests to J.-R. N.; E-mail: niejinrui200767@bupt.edu.cn

Z. Naturforsch. **67a,** 369 – 376 (2012) / DOI: 10.5560/ZNA.2012-0029
Received October 6, 2011 / revised February 16, 2012

To enhance the efficiency of eavesdropping detection in the quantum secure direct communication protocol, an improved quantum secure direct communication protocol based on a four-particle Green–Horne–Zeilinger (GHZ) state is presented. In the protocol, the four-particle GHZ state is used to detect eavesdroppers, and quantum dense coding is used to encode the message. In the security analysis, the method of entropy theory is introduced, and two detection strategies are compared quantitatively by using the constraint between the information that the eavesdroppers can obtain and the interference that has been introduced. If the eavesdropper wants to obtain all the information, the detection rate of the quantum secure direct communication using an Einstein–Podolsky–Rosen (EPR) pair block will be 50% and the detection rate of the presented protocol will be 87%. At last, the security of the proposed protocol is discussed. The analysis results indicate that the protocol proposed is more secure than the others.

Key words: Quantum Secure Direct Communication Protocol; Dense Coding; Four-Particle GHZ State; Eavesdropping Detection.

1. Introduction

The task of cryptography is to ensure that only the legitimate users like Alice and Bob have access to the secret message in the communication. In 1926, AT&T engineer Vernam presented the one-time-pad (OTP) [1]. Later, Shannon [2] proved that as long as the length of the key equals to the length of the plaintext, and the key is prepared randomly and not reused, the OTP will be perfectly secure. However, there will be the key distribution problem when utilizing the OTP. Thus, the quantum cryptography which is based on basic physical principles was proved to be an effective method in quantum key distribution (QKD) [3 – 6].

The 'ping-pong' protocol [7] was proposed by Boström and Felbinger in 2002. The protocol is proved to be a deterministic QKD scheme. Later, researchers are interested in quantum secure direct communication (QSDC), and many protocols [8 – 18] were proposed, including the protocols without using entanglement [9 – 11], the protocols using entanglement [12 – 18], and the two-way QSDC protocols [19 – 28]. In these protocols, the secret message is transmitted through the transmission channel directly. Compared with the QKD, the security requirement of QSDC is higher because whether the eavesdropper is detected or not, the secret message cannot be leaked out absolutely. For example, there will be some security problems when the 'ping-pong' protocol is used for QSDC [29 – 32]. But the unconditional security can still be achieved by adopting a well-designed QSDC protocol in theory [33 – 35].

In 2002, Long and Liu proposed a theoretical two-step QKD scheme using EPR pairs [8]. They introduced the method of quantum data block transmission for the security based on error rate analysis in QSDC. To guard the secret message, one has to ensure the security of a block of quantum data [8, 10, 12] before encoding the secret message. Moreover, error correction and quantum privacy amplification can be used to maintain its security.

Often there is a detection strategy in quantum cryptography protocols, such as QKD, QSDC, QSS (quantum secret sharing), and so on [37, 38]. Generally speaking, different detection strategies can be chosen in a protocol, and those strategies are often feasible. For example, in order to judge if the Bell states that Alice and Bob shared are secure or not, many methods such as the method of using the conjugate base [39] or single-base [40] to do local measurement for photons, the method of using the entanglement swapping [40] and so on are available. These detection strategies can guarantee the security of the shared Bell states. Obviously, to study more effective detection strategies is a key problem in quantum secure direct communication. A more secure detection strategy can improve the security of the quantum security protocol.

In 2003, modifying the basic idea in [8], Deng et al. proposed a two-step secure QSDC scheme using the EPR pair block [12]. In that scheme, a block of entangled particles is divided into two sequences, the checking sequence and the message-coding sequence. The security is assured by the secure transmission of the checking sequence. However, the detection rate is only 50%.

The efficiency of the different detection strategies can be compared by using the entropy method. To increase the efficiency of eavesdropping detection in the QSDC protocol [12], an improved QSDC protocol based on a four-particle GHZ state is presented. The four-particle GHZ state is used to detect eavesdroppers in this protocol. In order to facilitate the expression, the protocol in [12] is called TSPP and the proposed protocol is called SDPP. During the security analysis, the method of entropy theory is introduced. Two strategies are compared quantitatively by using the constraint between the information that the eavesdroppers can obtain and the interference that has been introduced. If the eavesdroppers get the full information, the detection rate of TSPP will be 50%, while SDPP will be 87%. In the end, the security of the proposed protocol is discussed. The analysis results show that the proposed protocol in this paper is more secure than the other.

2. Related Works

Now let us introduce the TSPP protocol explicitly [12].

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

$$|\psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle), \tag{1}$$

$$|\psi^+\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle), \tag{2}$$

$$|\phi^-\rangle = (1/\sqrt{2})(|00\rangle - |11\rangle), \tag{3}$$

$$|\phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle). \tag{4}$$

Here $|0\rangle$ and $|1\rangle$ are the up and down eigenstate of the σ_z, the photo polarization on operator. If one of the single photons in the Bell state is measured, the Bell state will collapse and the state of the other particle will be completely determined. For example, if the first photon state in the Bell state $|\psi^-\rangle$ is measured and the measurement result is $|0\rangle$, then the second photon state will collapse to $|1\rangle$.

Suppose that the message which will be transmitted is in a sequence $x^N = (x_1, \ldots, x_N)$, where $x_i \in \{0, 1\}, i = 1, 2, \ldots, N$.

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

(i) Alice prepares an ordered N EPR pair in the state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. She extracts all the first particles in the Bell states, and these particles form a series of particles A_1 (*the travel qubits*) in an order which is used to transmit the message. The remaining particles in the Bell states form a series of particles A_2 (*the home qubits*) in order. Then Alice sends the sequence A_1 to Bob.

(ii) Alice and Bob then check eavesdropping through the following procedure: (a) Bob chooses a number of photons from the sequence A_1 randomly and tells Alice which particles he has chosen. (b) Bob chooses one of the two sets measurement basis (MBs) randomly, say δ_z, δ_x to measure the chosen photons. (c) Bob tells Alice which MB he has chosen for each photon and the measurements results. (d) Alice uses the same measurement basis as Bob to measure the corresponding photons in the sequence A_2 and checks the results with Bob. If no eavesdropping exists, their results should be completely opposite, i.e., if Bob gets 0(1), then Alice gets 1(0). After that, if the error rate is low, Alice and Bob can conclude that there are no eavesdroppers in the line. Then Alice and Bob continue to perform step (iii); otherwise, they have to discard their transmission and abort the communication.

(iii) Alice encodes her message on sequence A_1 and transmits it to Bob. To encode the message, Alice uses the dense coding scheme proposed by Bennett and Wiesner [41] where the information is encoded on a single particle with a local operation and transmits the information by EPR pair block. Explicitly, Alice makes one of the four unitary operations U_0, U_1, U_2, and U_3 to each of her particles:

$$U_0 = I_2 \otimes I_2 = \begin{pmatrix} I_2 & 0 \\ 0 & I_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (5)$$

$$U_1 = I_2 \otimes \sigma_z = \begin{pmatrix} \sigma_z & 0 \\ 0 & \sigma_z \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (6)$$

$$U_2 = I_2 \otimes (-\mathrm{i}\sigma_y) = \begin{pmatrix} -\mathrm{i}\sigma_y & 0 \\ 0 & -\mathrm{i}\sigma_y \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (7)$$

$$U_3 = I_2 \otimes \sigma_z = \begin{pmatrix} \sigma_z & 0 \\ 0 & \sigma_z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad (8)$$

where they transform the state $|\phi^+\rangle$ into $|\phi^+\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$, and $|\phi^-\rangle$, respectively. These operations correspond to 00, 01, 10, and 11, respectively. Then Alice broadcasts the sequence A_1 in the public.

(iv) After transmitting the sequence A_1, Alice tells Bob the type of unitary operations on them. Then, Bob performs the Bell-basis measurement on the sequence A_1 and A_2 simultaneously.

(v) The TSPP protocol ends successfully.

3. SDPP Protocol

3.1. The Process of the SDPP Protocol

In the protocol proposed in [8], the transmission is managed in batches of N EPR pairs. An advantage of the block transmission scheme is that the security of the transmission can be checked in the first step by measuring some of the decoy photons [42, 43]. Alice and Bob possess a particle sequence at hand, respectively, which means if an eavesdropper has no access to the first particle sequence, then no information will be leaked to her whatever she has done to the second particle sequence. Following this method using block transmission, the SDPP scheme is proposed.

Suppose that the message to be transmitted is the sequence $x^N = (x_1, \ldots, x_N)$, where $x_i \in \{0,1\}, i = 1,2,\ldots,N$.

Define

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \quad (9)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0000\rangle + |1111\rangle\right). \quad (10)$$

Now let us give the details of the SDPP scheme.

(S1) Bob prepares a large enough number of Bell states and inserts enough four-particle GHZ states as follows.

(i) Bob prepares a large enough number N of Bell states $|\Phi^+\rangle$ in a sequence. He extracts all the first particles in the Bell states, forming a series of particles A (*the travel qubits*) in a given order. The sequence A is used to transmit a secure message. The remaining particles in the Bell states form a series of particles B (*the home qubits*). Thus this step corresponds to the message mode in the original ping-pong protocol (OPP) [35].

(ii) Bob prepares a large number $cN/(1-c)$ of four-qubit GHZ states $|\psi\rangle$, and the particles form a series of particles C to detect eavesdropping. It corresponds to the control mode in OPP. Here, c expresses the probability of switching to the control mode in the OPP. Note that the particles C include $4cN/(1-c)$ qubits.

(iii) Bob inserts the decoy photons C to the particles A randomly. These particles form a new sequence D, but only Bob knows the positions of the decoy photons. Then Bob stores the particles B and sends the particles D to Alice.

(S2) The detection of eavesdropping

After Alice received the particles D, Bob tells her the positions where the decoy photons are. Then Alice extracts the decoy photons from the particles D and performs the four-particle GHZ measurement. If there is no eavesdropper, every result must be in the four-particle GHZ state $|\psi\rangle$. Then they continue to execute the next step (S3), keeping on the SDPP

protocol. Otherwise, the communication is interrupted and the SDPP protocol switches to (S1).

(S3) Alice encodes her secure message based on dense coding and broadcasts her encoded message in public.

Alice extracts all the decoy photons from the particles D and the remaining particles form a series of particles E. According to the secure message she wants to transmit, Alice chooses one of the four unitary operations U_0, U_1, U_2, and U_3 for each of her two particles to perform the unitary transformation on particles E. The series of ciphertext is E′. Here U_0, U_1, U_2, and U_3 are the expressions (5)–(8). Then Alice broadcasts E′ in the public.

(S4) Bob decodes the ciphertext with the Bell measurement.

After receives Alice's particles E′, Bob performs the Bell measurement on both particles E′ and B. Then he can gain Alice's secure message.

(S5) The SDPP protocol ends successfully.

3.2. The Security Analysis of the Protocol

In TSPP, the author has calculated the maximal amount of information $I(d_{\mathrm{TS}})$ that Eve can eavesdrop and the probability d that Eve is detected. And the function $I(d_{\mathrm{TS}})$ is provided. When $p_0 = p_1 = 1/2$,

$$\begin{aligned} I(d_{\mathrm{TS}}) &= 2 - \frac{\left(1+\sqrt{(2d_{\mathrm{TS}}-1)^2}\right)}{2} \\ &\cdot \log_2\left(1+\sqrt{(2d_{\mathrm{TS}}-1)^2}\right) \\ &- \frac{\left(1-\sqrt{(2d_{\mathrm{TS}}-1)^2}\right)}{2} \log_2\left(1-\sqrt{(2d_{\mathrm{TS}}-1)^2}\right). \end{aligned} \tag{11}$$

The above method can be used to compare the efficiency of eavesdropping detection between the two protocols.

Now let us analyze the efficiency of the eavesdropping detection in the SDPP protocol. In order to gain the information that Alice encoded on the travel qubits, Eve performs the unitary attack operation $\hat{E}$ on the composed system at first. Then Alice takes a coding operation on the travel qubits. Eve performs a measurement on the composed system at last. For Eve does not know which particles are used to detect eavesdropping. So what she can do is only to perform the same attack operation on all the particles. As for Eve, the state of the travel qubits is indistinguishable from the complete mixture, so all the travel qubits are considered in either of the states $|0\rangle$ or $|1\rangle$ with equal probability $p = 0.5$.

Generally speaking, suppose that there is a group of decoy photons [42, 43] at the state of four-particle GHZ states $|\psi\rangle$, and after performed the attack operation $\hat{E}$, the states $|0\rangle$ and $|1\rangle$ become

$$|\varphi_0'\rangle = \hat{E}\otimes|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle, \tag{12}$$

$$|\varphi_1'\rangle = \hat{E}\otimes|1x\rangle = m|0y_0\rangle + n|1y_1\rangle, \tag{13}$$

where $|x_i\rangle$ and $|y_i\rangle$ are the pure ancillary states only determined by $\hat{E}$ uniquely, and

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

$$|m|^2 + |n|^2 = 1. \tag{15}$$

First let us suppose that the quantum state of the photon in the hand of Alice is $|0\rangle$. Then the state of the system composed of Alice's photon and Eve's probe can be described by

$$|\varphi_0'\rangle = \hat{E}\otimes|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle, \tag{16}$$

$$\begin{aligned} \rho' = |\psi'\rangle\langle\psi'| &= |\alpha|^2 |0,\chi_0\rangle\langle 0,\chi_0| \\ &+ |\beta|^2 |1,\chi_1\rangle\langle 1,\chi_1| \\ &+ \alpha\beta^* |0,\chi_0\rangle\langle 1,\chi_1| + \alpha^*\beta |1,\chi_1\rangle\langle 0,\chi_0|. \end{aligned} \tag{17}$$

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

$$\begin{aligned} \rho'' = &(p_0+p_3)|\alpha|^2 |0,\chi_0\rangle\langle 0,\chi_0| \\ &+ (p_0+p_3)|\beta|^2 |1,\chi_1\rangle\langle 1,\chi_1| \\ &+ (p_0-p_3)\alpha\beta^* |0,\chi_0\rangle\langle 1,\chi_1| \\ &+ (p_0-p_3)\alpha^*\beta |1,\chi_1\rangle\langle 0,\chi_0| \\ &+ (p_1+p_2)|\alpha|^2 |1,\chi_0\rangle\langle 1,\chi_0| \\ &+ (p_1+p_2)|\beta|^2 |0,\chi_1\rangle\langle 0,\chi_1| \\ &+ (p_1-p_2)\alpha\beta^* |1,\chi_0\rangle\langle 0,\chi_1| \\ &+ (p_1-p_2)\alpha^*\beta |0,\chi_1\rangle\langle 1,\chi_0|. \end{aligned} \tag{18}$$

With the orthogonal basis $\{|0,\chi_0\rangle, |1,\chi_1\rangle, |1,\chi_0\rangle, |0,\chi_1\rangle\}$ the state ρ'' can be rewritten into

$$\rho'' = \begin{pmatrix} (p_0+p_3)|\alpha|^2 & (p_0-p_3)\alpha\beta^* & 0 & 0 \\ (p_0-p_3)\alpha^*\beta & (p_0+p_3)|\beta|^2 & 0 & 0 \\ 0 & 0 & (p_1+p_2)|\alpha|^2 & (p_1-p_2)\alpha\beta^* \\ 0 & 0 & (p_1-p_2)\alpha^*\beta & (p_1+p_2)|\beta|^2 \end{pmatrix}, \tag{19}$$

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

The information I_0 that Eve can get equals to the Von Neumann entropy,

$$I_0 = \sum_{i=0}^{3} -\lambda_i \log \lambda_i , \tag{20}$$

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

$$\lambda_{0,1} = \frac{1}{2}(p_0+p_3) \pm \frac{1}{2}\sqrt{(p_0+p_3)^2 - 16p_0p_3|\alpha|^2|\beta|^2}, \tag{21}$$

$$\lambda_{2,3} = \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2|\alpha|^2|\beta|^2}. \tag{22}$$

After attacked by Eve, the state of composed system becomes

$$\begin{aligned} |\psi\rangle_{\text{Eve}} &= \hat{E}\left[\frac{1}{\sqrt{2}}(|0x0x0x0x\rangle + |1x1x1x1x\rangle)\right] \\ &= \frac{1}{2}(\alpha^4|0x_00x_00x_00x_0\rangle + \alpha^3\beta|0x_00x_00x_01x_1\rangle + \alpha^3\beta|0x_00x_01x_10x_0\rangle + \alpha^2\beta^2|0x_00x_01x_11x_1\rangle \\ &\quad + \alpha^3\beta|0x_01x_10x_00x_0\rangle + \alpha^2\beta^2|0x_01x_10x_01x_1\rangle + \alpha^2\beta^2|0x_01x_11x_10x_0\rangle + \alpha\beta^3|0x_01x_11x_11x_1\rangle \\ &\quad + \alpha^3\beta|1x_10x_00x_00x_0\rangle + \alpha^2\beta^2|1x_10x_00x_01x_1\rangle + \alpha^2\beta^2|1x_10x_01x_10x_0\rangle + \alpha\beta^3|1x_10x_01x_11x_1\rangle \\ &\quad + \alpha^2\beta^2|1x_11x_10x_00x_0\rangle + \alpha\beta^3|1x_11x_10x_01x_1\rangle + \alpha\beta^3|1x_11x_11x_10x_0\rangle + \beta^4|1x_11x_11x_11x_1\rangle \\ &\quad + m^4|0y_00y_00y_00y_0\rangle + m^3n|0y_00y_00y_01y_1\rangle + m^3n|0y_00y_01y_10y_0\rangle + m^2n^2|0y_00y_01y_11y_1\rangle \\ &\quad + m^3n|0y_01y_10y_00y_0\rangle + m^2n^2|0y_01y_10y_01y_1\rangle + m^2n^2|0y_01y_11y_10y_0\rangle + mn^3|0y_01y_11y_11y_1\rangle \\ &\quad + m^3n|1y_10y_00y_00y_0\rangle + m^2n^2|1y_10y_00y_01y_1\rangle + m^2n^2|1y_10y_01y_10y_0\rangle + mn^3|1y_10y_01y_11y_1\rangle \\ &\quad + m^2n^2|1y_11y_10y_00y_0\rangle + mn^3|1y_11y_10y_01y_1\rangle + mn^3|1y_11y_11y_10y_0\rangle + n^4|1y_11y_11y_11y_1\rangle). \end{aligned} \tag{23}$$

Obviously, when Alice performs the measurement on the decoy photons, the probability without eavesdropper is

$$p(|\psi\rangle) = \frac{1}{2}\left(|\alpha^4|^2 + |\beta^4|^2 + |m^4|^2 + |n^4|^2\right). \tag{24}$$

So the lower bound of the detection probability is

$$\begin{aligned} d_{lFG} &= 1 - p(|\psi\rangle) \\ &= 1 - \frac{1}{2}\left(|\alpha^4|^2 + |\beta^4|^2 + |m^4|^2 + |n^4|^2\right). \end{aligned} \tag{25}$$

Now let us analyze how much information Eve can gain maximally when there is no control mode. Suppose $|\alpha|^2 = a, |\beta|^2 = b, |m|^2 = s, |n|^2 = t$, where a, b, s, and t are positive real numbers, and $a+b=s+t=1$. Then

$$\begin{aligned} d_{\text{SD}} &= 1 - p(|\psi\rangle) \\ &= 1 - \frac{1}{2}\left(|\alpha^4|^2 + |\beta^4|^2 + |m^4|^2 + |n^4|^2\right) \\ &= 1 - \frac{1}{2}(a^4+b^4+s^4+t^4) \\ &= -a^4 + 2a^3 - 3a^2 + 2a - t^4 + 2t^3 - 3t^2 + 2t. \end{aligned} \tag{26}$$

In the case $p_0 = p_1 = p_2 = p_3 = 1/4$, the expression (21)–(22) simplifies to

$$\lambda_{0,1} = \lambda_{2,3} = \frac{1}{4} \pm \frac{1}{2}\sqrt{\left(a-\frac{1}{2}\right)^2}. \tag{27}$$

According to expression (20), when Bob sends $|0\rangle$ to Alice, the maximal amount of information equals to the Shannon entropy of a binary channel,

$$I_0 = 2 - \frac{\left(1+\sqrt{(2a-1)^2}\right)}{2}\log_2\left(1+\sqrt{(2a-1)^2}\right) - \frac{\left(1-\sqrt{(2a-1)^2}\right)}{2}\log_2\left(1-\sqrt{(2a-1)^2}\right) = H(a)\,. \quad (28)$$

Then assume that Bob sends $|1\rangle$ rather than $|0\rangle$. The above security analysis can be done in full analogy and results in the same crucial relations. The maximal amount of information equals to the Shannon entropy of a binary channel,

$$I_1 = 2 - \frac{\left(1+\sqrt{(2t-1)^2}\right)}{2}\log_2\left(1+\sqrt{(2t-1)^2}\right) - \frac{\left(1-\sqrt{(2t-1)^2}\right)}{2}\log_2\left(1-\sqrt{(2t-1)^2}\right) = H(t)\,. \quad (29)$$

So the maximal amount of information that Eve can obtain is

$$I = 1/2(I_0+I_1) = 1/2[H(a)+H(t)]\,. \quad (30)$$

After some simple mathematical calculations, when $a=t$, we have the following expression:

$$d_{\mathrm{SD}} = -2a^4+4a^3-6a^2+4a\,. \quad (31)$$

The maximum I is

$$I(d_{\mathrm{SD}}) = H\left(\frac{1+\sqrt{-3+\sqrt{16-8d_{\mathrm{SD}}}}}{2}\right)\,. \quad (32)$$

The above results are obtained under the condition $d \le 0.87$. Actually, the situation $d > 0.87$ can be ignored. Obviously, when $d > 0.5$, the eavesdropped information is too much to meet the requirement of the secure communication. The above analysis shows that the function $I(d_{\mathrm{TS}})$ and $I(d_{\mathrm{SD}})$ have the similar algebraic properties. If Eve gains the full information ($I=2$), the probability of the eavesdropping detection is $d_{\mathrm{TS}}(I=2)=0.5$ in the TSPP protocol, while in the SDPP protocol, $d_{\mathrm{TS}}(I=2)=0.87$.

In order to contrast the two functions, Figure 1 and Table 1 are given. As shown in Figure 1 and Table 1, if

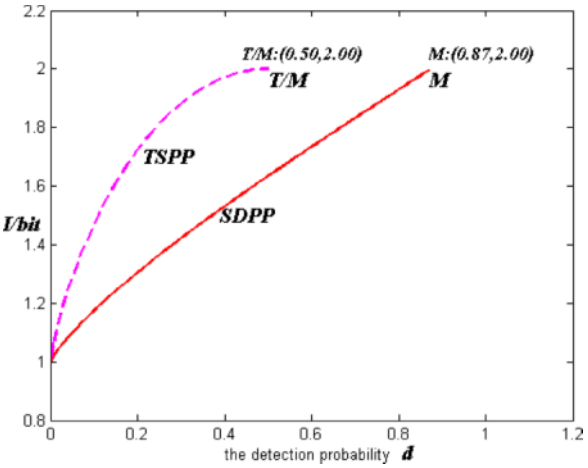

Fig. 1 (colour online). Comparison of the two detection results.

I [bit]	d using TSPP	SDPP
1.2	0.03	0.12
1.4	0.08	0.29
1.6	0.15	0.47
1.8	0.24	0.67
2.0	0.5	0.87

Table 1. Accurate comparison figures: detection probability d for different amounts of information I that Eve can eavesdrop.

Eve gains the same amount of information, she must face a larger detection probability in SDPP than in TSPP. They also indicate that SDPP is more secure than TSPP. Of course, in order to detect eavesdropping, Bob needs to send $4cN/(1-n)$ particles more than in the TSPP protocol. In other words, Bob gains the better security at the cost of sending more particles.

In Figure 1, the dotted line expresses the function $I(d_{\mathrm{TS}})$ in TSPP, the thick line expresses the function $I(d_{\mathrm{SD}})$ in SDPP. Obviously, if Eve wants to get the same amount of information, she must encounter the higher detection efficiency in SDPP. Also, if there is the same detection efficiency, Eve will eavesdrop less information.

Taking the probability c of the control mode into account, the effective transmission rate, i.e. the number of message bits per protocol run, is $1-c$, which equals to the probability for a message transfer. So, if Eve wants to steal one message transfer without being detected, the probability for this event is

$$s(c,d) = (1-c)+c(1-d)(1-c) + c^2(1-d)^2(1-c)+\ldots$$

$$= \frac{1-c}{1-c(1-d)}. \tag{33}$$

Thus the probability to successful eavesdrop $I = nI(d)$ bits reads $s(I,c,d) = s(c,d)^{I/I(d)}$. So

$$s(I,c,d) = \left(\frac{1-c}{1-c(1-d)}\right)^{I/I(d)}, \tag{34}$$

where

$$I(d) = H\left(\frac{1+\sqrt{-3+\sqrt{16-8d_{\mathrm{SD}}}}}{2}\right). \tag{35}$$

In the limit when $I \to \infty$ (a message or key of infinite length), $s \to 0$, so the presented protocol that proposed in this paper is *asymptotically secure*. If the security of the quantum channel is ensured, the protocol is completely secure. For example, a choice of the control mode is $c = 0.5$. In Figure 2, we have plotted the eavesdropping success probability as a function of the information gain I, for $c = 0.5$ and for different detection probabilities d which Eve can choose. Note that for $d < 0.5$, Eve only gets one part of the message right and does not even know which part.

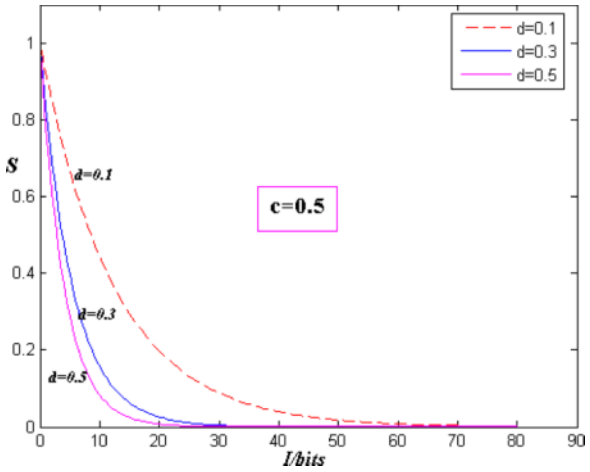

Fig. 2 (colour online). Eavesdropping success probability as a function of the maximal eavesdropped information, plotted for different detection probabilities d.

[1] G. S. Vernam, J. Am. Inst. Electr. Eng. **55**, 109 (1926).
[2] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[3] C. H. Bennett and G. Brassard, in: Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore 1984, p. 175 – 179.

In the step (S3) and (S4) of the SDPP protocol, the secure message is encoded bit by bit with the dense coding operation, and broadcasts the ciphertext in public, which can get OTP's security level. So the SDPP protocol is secure.

4. Conclusion and Further Work

In the SDPP protocol, the security message can be securely transmitted to the receiver, and any useful message will not leak to the potential eavesdropper. Compared with the TSPP protocol, the SDPP protocol has the following differentia:

(i) The eavesdropping detection method using the four-particle GHZ state in the SDPP protocol is similar to the method using measuring EPR in TSPP.

(ii) In the SDPP protocol, the Bell states are prepared by Bob rather than by Alice. This guarantees the home qubits could not leak to Eve and the Bell states that carries the secure message can be reused.

(iii) The SDPP protocol is based on the four-particle GHZ state, which can reduce the times of detection.

In sum, an improved QSDC scheme based on the four-particle GHZ state has been introduced, and two eavesdropping detection strategies are compared quantitatively by using the constraint between the information that the eavesdropper obtains and the interference that has been introduced. In the analysis, if the eavesdropper obtains the same amount of information, she must face a larger detection probability in the SDPP protocol than in the TSPP protocol, which shows that the efficiency of eavesdropping detection in SDPP is higher than the other, so it can ensure the QSDC protocol more secure. While in order to detect eavesdropping, Bob sends $4cN(1-c)$ particles more than in the TSPP protocol. That is, Bob gains the better security at the cost of sending more particles. In the further work, the other QSDC protocol's security and its improvement will be researched.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No. 61100205).

[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[7] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[8] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[9] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).
[10] F. G. Deng, G. L. Long, and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[11] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[12] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
[13] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**, 054301 (2004).
[14] T. Gao, F. L. Yan, and Z. X. Wang, Chin. Phys. Lett. **22**, 2473 (2005).
[15] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).
[16] C. Wang, F. G. Deng, and G. L. Long, Opt. Commun. **253**, 15 (2005).
[17] X. H. Li, F. G. Deng, and H. Y. Zhou, Phys. Rev. A **74**, 054302 (2006).
[18] X. H. Li, C. Y. Li, F. G. Deng, P. Zhou, Y. J. Liang, and H. Y. Zhou, Chin. Phys. Lett. **16**, 2149 (2007).
[19] B. A. Nguyen, Phys. Lett. A **328**, 6 (2004).
[20] Z. X. Man, Z. J. Zhang, and Y. Li, Chin. Phys. Lett. **22**, 22 (2005).
[21] X. Ji and S. Zhang, Chin. Phys. Lett. **15**, 1418 (2006).
[22] Z. X. Man, Y. J. Xia, and B. A. Nguyen, J. Phys. B, At. Mol. Opt. Phys. **39**, 3855 (2006).
[23] Z. X. Man and Y. J. Xia, Chin. Phys. Lett. **23**, 1680 (2006).
[24] Y. Xia, C. B. Fu, S. Zhang, S. K. Hong, K. H. Yeon, and C. I. Um, J. Korean Phys. Soc. **48**, 24 (2006).
[25] X. R. Jin, X. Ji, Y. Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, and C.-I. Um, Phys. Lett. A **354**, 67 (2006).
[26] Z. X. Man and Y. J. Xia, Chin. Phys. Lett. **24**, 15 (2007).
[27] Y. Chen, Z. X. Man, and Y. J. Xia, Chin. Phys. Lett. **24**, 19 (2007).
[28] Y. G. Yang, and Q. Y. Wen, Sci. China Ser. G, Phys. Mech. Astron. **50**, 558 (2007).
[29] A. Wojcik, Phys. Rev. Lett. **90**, 157901 (2003).
[30] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, and H. Y. Zhou, Chin. Phys. Lett. **16**, 277 (2007).
[31] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[32] Z. J. Zhang and Z. X. Man, Int. J. Quantum Inf. **2**, 521 (2004).
[33] H. Hoffmann, K. Boström, and T. Felbinger, Phys. Rev. A **72**, 016301 (2005).
[34] F. G. Deng and G. L. Long, Phys. Rev. A **72**, 016302 (2005).
[35] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, and H. Y. Zhou, Phys. Lett. A **359**, 359 (2006).
[36] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Phys. A **101**, 357 (2002).
[37] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[38] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[39] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[40] F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Phys. Lett. A **349**, 53 (2006).
[41] C. H Bennet and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[42] C. Y. Li, H. Y. Zhou, Y. Wang, and F. G. Deng, Chin. Phys. Lett. **22**, 1049 (2005).
[43] C. Y. Li, X. H. Li, F. G. Deng, P. Zhou, Y. J. Liang, and H. Y. Zhou, Chin. Phys. Lett. **23**, 2896 (2006).