Article

Chinese Science Bulletin

Quantum Information

December 2012 Vol.57 No.34: 4434–4441
doi: 10.1007/s11434-012-5516-1

Improved eavesdropping detection strategy based on four-particle cluster state in quantum direct communication protocol

LI Jian[1], JIN HaiFei[1*] & JING Bo[1,2]

[1] *School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China;*
[2] *Department of Computer Science, Beijing Institute of Applied Meteorology, Beijing 100029, China*

Received April 14, 2012; accepted July 9, 2012

In order to improve the eavesdropping detection efficiency in a two-step quantum direct communication protocol, an improved eavesdropping detection strategy using the four-particle cluster state is proposed, in which the four-particle cluster state is used to detect eavesdroppers. During the security analysis, the method of the entropy theory is introduced, and two detection strategies are compared quantitatively using the constraint between the information that the eavesdropper can obtain and the interference that has been introduced. If the eavesdroppers intend to obtain all information, the eavesdropping detection rate of the original two-step quantum direct communication protocol using EPR pair block as detection particles will be 50%; while the proposed strategy's detection rate will be 75%. In the end, the security of the proposed protocol is discussed. The analysis results show that the eavesdropping detection strategy presented is more secure.

quantum direct communication, four-qubit cluster state, eavesdropping detection, protocol security, dense coding scheme

Citation: Li J, Jin H F, Jing B. Improved eavesdropping detection strategy based on four-particle cluster state in quantum direct communication protocol. Chin Sci Bull, 2012, 57: 4434–4441, doi: 10.1007/s11434-012-5516-1

The goal of researching cryptography is to ensure that the secret message is only available to the two authorized parties of the communication and that the transmission will be altered. So far, it is trusted that the only proven secure cryptosystem is the one-time-pad scheme in which the secret key is as long as the message. The two parties staying far apart who want to transmit their secret message must distribute the secret key first. However it is difficult to distribute the secret key securely through a classical channel. The quantum key distribution (QKD), whose task is to create a secret key between two remote authorized users, is one of the most remarkable applications of quantum mechanics and the only proven protocol for secure key distribution. Since Bennett and Brassard presented the pioneer QKD protocol (BB84 protocol) [1] in 1984, a lot of quantum information security processing methods have been advanced, such as quantum teleportation [2–7], quantum dense coding [8–10], quantum secret sharing [11,12] and so on.

In recent years, a novel concept, quantum secure direct communication (QSDC) [13,14] was put forward and studied by some groups. Different from the key distribution whose object is to establish a common random key between two parties, the secure direct communication is to transmit important message directly without establishing a random key to encrypt them first. Thus, the secure direct communication is more demanding on the security. As a secure direct communication, it must satisfy two requirements. First, the secure message should be read out directly by the legitimate user Bob when he receives the quantum states and no additional classical information is needed after the transmission of particles. Second, the secret message which has been encoded already in the quantum states should not leak even though an eavesdropper may get hold of the channel. That is to say, the eavesdropper cannot only be detected but also obtains blind results. As classical message can be copied fully, it is impossible to transmit secret message directly through classical channels. But when quantum mechanics enters into the communication, the story will change.

*Corresponding author (email: jinhaifei@bupt.edu.cn)

Another class of quantum communication protocols [15–17] used to transmit secret message is called deterministic secure quantum communication (DSQC). Certainly, the receiver can read out the secret message only after he exchanges at least one bit of classical information for each particle with the sender in a DSQC protocol, which is different from QSDC. DSQC is similar to QKD, but it can be used to obtain deterministic information, not a random binary string, which is different from the QKD protocols in which the user cannot predict whether an instance is useful or not.

Many people are interested in researching QSDC, and many protocols like QSDC have already been proposed, including the protocols without using entanglement [18], the protocols using entanglement [19,20] and the two-way QSDC protocols [21–27]. The QSDC protocol can also be used in some special environments such as the environment proposed by Boström et al. [28] and Deng et al. [21]. In [28], Boström and Felbinger presented a famous QSDC protocol which is called "ping-pong" protocol. But researchers have found much vulnerability in the "ping-pong" protocol. For example, the "ping-pong" protocol cannot resist the "man-in-middle attack" and the transmission capacity is low.

In order to improve the eavesdropping detection efficiency in two-step quantum direct communication protocol, an improved eavesdropping detection strategy using the four-particle cluster state is proposed, in which the four-particle cluster state is used to detect eavesdroppers. During the security analysis, the method of the entropy theory is introduced, and two detection strategies are compared quantitatively using the constraint between the information that the eavesdropper can obtain and the interference that has been introduced. If the eavesdroppers intend to obtain all information, the eavesdropping detection rate of the original two-step quantum direct communication protocol using EPR pair block as detection particles will be 50%; while the proposed strategy's detection rate will be 75%. In the end, the security of the proposed protocol is discussed. The analysis results show that the eavesdropping detection strategy presented is more secure.

For simplicity, we suppose that the protocol presented in [21] is shortened as DPP and the improved protocol in this paper is shortened as FPP.

1 DPP Protocol

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

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

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

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

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

If the state of a single photon being measured, the Bell state will collapse and the state of the other particle will be completely determined if we know the measurement result of the first photon. As is known to us all, the basic principle of the original "ping-pong" protocol is that one bit information can be encoded in the states $\left|\psi^{\pm}\right\rangle$, which is completely unavailable to anyone who only has access to either of the particles. To extract secret message from Alice, Bob must own both particles, for no experiment performed on only one particle can distinguish these states from each other [28].

Let us start with a brief description of the DPP protocol.

(S1) Alice prepares an ordered N EPR pairs in state $\left|\psi^-\right\rangle$, extracts all the first particles, and forms the sequence A in order. The remainder particles are formed the sequence B in order.

(S2) Alice sends the sequence A to Bob. Alice and Bob then check eavesdropping by the following procedure: (a) Bob chooses randomly a number of the photons from the sequence A and tells Alice which particle he has chosen. (b) Bob chooses randomly one of the two sets of MBs, say σ_z and σ_x to measure the chosen photons. (c) Bob tells Alice the MB he has chosen for each photon and the outcomes of his measurements. (d) Alice uses the same MB as Bob to measure the corresponding photons in the sequence B and checks the results with Bob. If no eavesdropper exists, their results should be completely opposite. This is the first eavesdropping check. After that, if the error rate is small, Alice and Bob can conclude that there is no eavesdropper in the line. Alice and Bob continue to perform step (S3); otherwise, they have to discard their transmission and abort the communication.

(S3) Alice encodes her messages on the sequence B and transmits them to Bob. Before the transmission, Alice must encode the EPR pairs. In order to guard for eavesdropping in this transmission, Alice has to add a small trick in the sequence B. She selects randomly in the sequence B some particles and performs on them randomly one of the four operations. The number of such particles will not be big as long as it can provide an analysis of the error rate. Only Alice knows the positions of these sampling particles and keeps them secretly until the communication is completed. The remaining sequence B particles are used to carry the secret message directly. To encode the message, they use the dense coding scheme of Bennett and Wiesner [8], where the information is encoded on an EPR pair with a local operation on a single particle. Here, the dense coding idea was generalized into secure direct communication. Different from dense coding, in this protocol, both the particles in an EPR pair are sent from Alice to Bob in two steps, and the transmission of EPR pairs is done in block. Explicitly, Alice makes one of the four unitary operations (U_0, U_1, U_2 and

U_3) to each of her particles:

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

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

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

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

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

(S4) After the transmission of sequence *B*, Alice tells Bob the positions of the sampling pairs and the type of the unitary operations on them. Bob performs the Bell-basis measurement on the sequence *A* and *B* simultaneously. By checking the sampling pairs that Alice has chosen, he will get an estimate of the error rate in the sequence *B* transmission. In fact, in the second transmission, Eve can only disturb the transmission and cannot steal the information because she can only get one particle from an EPR pair.

(S5) If the error rate of the sampling pairs is reasonably low, Alice and Bob can then entrust the process, and continue to correct the error in the secret message using error correction methods. Otherwise, Alice and Bob abandon the transmission and repeat the procedure from the beginning.

(S6) Alice and Bob do error correction on their results. This procedure is exactly the same as that in QKD. However, to preserve the integrity of the message, the bits preserving correction code, such as CASCADE [29], should be used.

2 FPP Protocol

2.1 The process of the FPP protocol

In the protocol presented in [13], the transmission is managed in batches of *N* EPR pairs. An advantage of block transmission scheme is that we can check the security of the transmission by measuring some of the decoy photons [30,31] in the first step, where both Alice and Bob contain a particle sequence at hand, which means that an eavesdropper has no access to the first particle sequence, and then no information will be leaked to her whatever she has done to the second particle sequence. Follow this method using block transmission. The FPP scheme is proposed and shown in Figure 1.

Define

$$|\psi\rangle = \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle\right). \quad (9)$$

Now let us give an explicit process for the FPP.

(S1) Bob prepares a large enough number (*N*) of Bell states $|\varphi^+\rangle$ in order. He extracts all the first particles in these Bell states, forming the sequence *A* (the travel qubits) in order. The sequence *A* is used to transmit secure message. Then the remaining particles form the sequence *B* (the home qubits) in order.

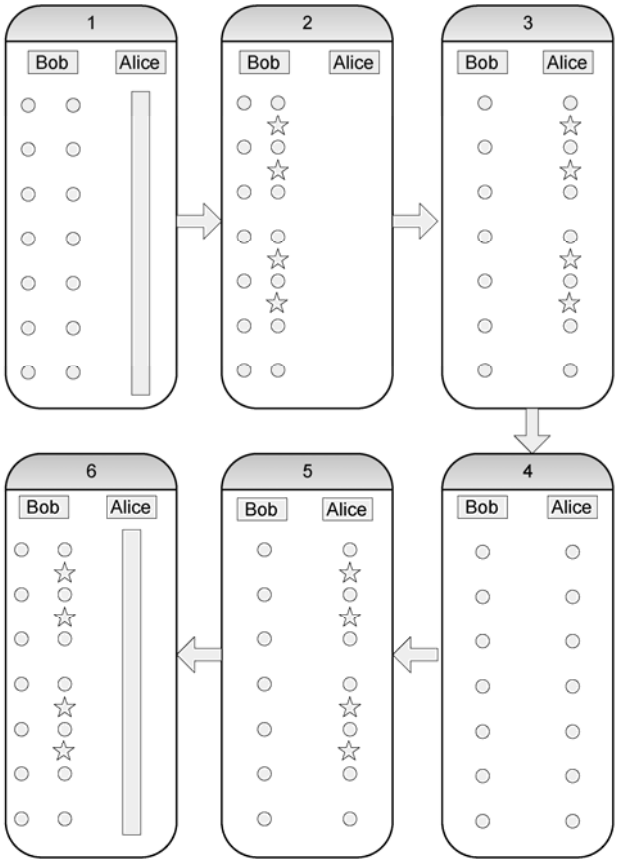

Figure 1 The process of the FPP.

(S2) Bob prepares a large number ($cN/(1-c)$) of four-particle cluster states $|\psi\rangle$ and forms the sequence *C* to detect eavesdropping. Here, *c* expresses the probability of switching to the control mode in the original "ping-pong" protocol [28]. Note that the sequence *C* includes $4cN/(1-c)$ qubits. Bob inserts the decoy photons *C* to the sequence *A* randomly, forming a new sequence *D*. Only Bob knows the positions of these decoy photons.

(S3) Bob stores the sequence *B* and sends the sequence *D* to Alice.

(S4) After Alice received the sequence *D*, Bob tells her the positions where the decoy photons are. Then, Alice extracts the decoy photons from the sequence *D* and performs four-particle cluster state measurement. This is the first eavesdropping check. If there is no eavesdropper, every result should be in the four-particle cluster state, and they continue to execute the next step (S5), the FPP protocol keeping on. Otherwise, the communication is interrupted, and the FPP protocol switches to (S1).

(S5) Alice discards the decoy photons, then the sequence *D* becomes to the sequence *A* again. Alice encodes her

messages on the sequence *A* and transmits it to Bob. In order to guard for eavesdropping in this transmission, Alice has to insert some four-particle cluster state particles in the sequence *A* before the transmission. Only Alice knows the positions of these decoy photons and keeps them secret until the communication is completed. The remaining sequence *A* are used to carry the secret message directly. To increase the transmission capacity, the dense coding scheme be used to encode the secret message. Different from dense coding, in this protocol, the transmission of EPR pairs is done in block. Explicitly, Alice makes one of the four unitary operations (U_0, U_1, U_2 and U_3) to each of her particles, and they transform the state $|\varphi^+\rangle$ into $|\varphi^+\rangle$, $|\varphi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$, respectively. These operations correspond to 00, 01, 10 and 11, respectively. Then Alice transmits the sequence *A* which carries decoy photons to Bob.

(S6) After transmitting the sequence *A*, Alice tells Bob the positions of the decoy photons. Bob performs Bell-basis measurement on the sequences *A* and *B* simultaneously. By checking the decoy photons that Alice insert, Bob will get an estimate of the error rate in the sequence *A* transmission. In fact, Eve can only disturb the transmission and cannot steal the information because she can only get one particle from an EPR pair. If the error rate of the decoy photons is reasonably low, Alice and Bob can then entrust the process, and continue to transmit the secret message. Otherwise, Alice and Bob abandon the transmission and repeat the procedures from the beginning.

As discussed above, the secret message can be transmitted securely between Alice and Bob, and the eavesdropper will be found out if she disturbs the quantum line. Eve cannot read out the information from the EPR pairs even if she captures the sequence *A*, because no one can read the information from one particle of the EPR pair alone. Therefore, the improved protocol is secure.

2.2 The security analysis of the protocol

In the original "ping-pong" protocol, the author calculated the maximal amount of the information $I(d_{lO})$ that Eve can eavesdrop and the probability d_{lO} that Eve is detected [28]. And the function $I(d_{lO})$ is provided. When p_0=p_1=0.5,

$$I(d_{lO}) = -d_{lO}\log_2 d_{lO} - (1-d_{lO})\log_2(1-d_{lO}). \tag{10}$$

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

Now, let us analyze the efficiency of eavesdropping detection in FPP protocol. In order to gain the information that Alice operates on the travel qubits, Eve performs the unitary attack operation $\hat{E}$ on the composed system firstly. Then Alice takes a coding operation on the travel qubits. Eve performs a measurement on the composed system at last. Note that, all transmitted particles are sent as block before detecting eavesdropping, which is different from the original "ping-pong" protocol. For Eve does not know which particles are used to detect eavesdropping, so what she can do is only performing 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, supposing there is a group of decoy photons at the four-qubit cluster states $|\psi\rangle$, and after performing the attack operation $\hat{E}$, the states $|0\rangle$ and $|1\rangle$ become

$$|\varphi_0'\rangle = \hat{E}\otimes|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle, \tag{11}$$

$$|\varphi_1'\rangle = \hat{E}\otimes|1x\rangle = m|0y_0\rangle + n|1y_1\rangle, \tag{12}$$

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

$$|\alpha|^2 + |\beta|^2 = 1, \quad |m|^2 + |n|^2 = 1. \tag{13}$$

Then let us calculate the detection probability. Attacked by Eve, the state of composed system becomes

$$\begin{aligned}
|\psi\rangle_{\text{Eve}} &= E\otimes E\otimes E\otimes E\left[\frac{1}{2}\left(|0x0x0x0x\rangle + |0x0x1x1x\rangle + |1x1x0x0x\rangle - |1x1x1x1x\rangle\right)\right] \\
&= \frac{1}{2}\Big[\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)\otimes\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)\otimes\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)\otimes\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right) \\
&\quad + \left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)\otimes\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)\otimes\left(m|0y_0\rangle+n|1y_1\rangle\right)\otimes\left(m|0y_0\rangle+n|1y_1\rangle\right) \\
&\quad + \left(m|0y_0\rangle+n|1y_1\rangle\right)\otimes\left(m|0y_0\rangle+n|1y_1\rangle\right)\otimes\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right)\otimes\left(\alpha|0x_0\rangle+\beta|1x_1\rangle\right) \\
&\quad - \left(m|0y_0\rangle+n|1y_1\rangle\right)\otimes\left(m|0y_0\rangle+n|1y_1\rangle\right)\otimes\left(m|0y_0\rangle+n|1y_1\rangle\right)\otimes\left(m|0y_0\rangle+n|1y_1\rangle\right)\Big] \\
&= \frac{1}{2}(\alpha^4|0x_00x_00x_00x_0\rangle + \alpha^3\beta|0x_00x_00x_01x_1\rangle + \alpha^3\beta|0x_00x_01x_10x_0\rangle + \alpha^2\beta^2|0x_00x_01x_11x_1\rangle \\
&\quad + \alpha^3\beta|0x_01x_10x_00x_0\rangle + \alpha^2\beta^2|0x_01x_10x_01x_1\rangle + \alpha^2\beta^2|0x_01x_11x_10x_0\rangle + \alpha\beta^3|0x_01x_11x_11x_1\rangle \\
&\quad + \alpha^3\beta|1x_10x_00x_00x_0\rangle + \alpha^2\beta^2|1x_10x_00x_01x_1\rangle + \alpha^2\beta^2|1x_10x_01x_10x_0\rangle + \alpha\beta^3|1x_10x_01x_11x_1\rangle
\end{aligned}$$

$$
\begin{aligned}
&+\alpha^2\beta^2\left|1x_1 1x_1 0x_0 0x_0\right\rangle+\alpha\beta^3\left|1x_1 1x_1 0x_0 1x_1\right\rangle+\alpha\beta^3\left|1x_1 1x_1 1x_1 0x_0\right\rangle+\beta^4\left|1x_1 1x_1 1x_1 1x_1\right\rangle\\
&+\alpha^2m^2\left|0x_0 0x_0 0y_0 0y_0\right\rangle+\alpha^2mn\left|0x_0 0x_0 0y_0 1y_1\right\rangle+\alpha^2mn\left|0x_0 0x_0 1y_1 0y_0\right\rangle+\alpha^2n^2\left|0x_0 0x_0 1y_1 1y_1\right\rangle\\
&+\alpha\beta m^2\left|0x_0 1x_1 0y_0 0y_0\right\rangle+\alpha\beta mn\left|0x_0 1x_1 0y_0 1y_1\right\rangle+\alpha\beta mn\left|0x_0 1x_1 1y_1 0y_0\right\rangle+\alpha\beta n^2\left|0x_0 1x_1 1y_1 1y_1\right\rangle\\
&+\alpha\beta m^2\left|1x_1 0x_0 0y_0 0y_0\right\rangle+\alpha\beta mn\left|1x_1 0x_0 0y_0 1y_1\right\rangle+\alpha\beta mn\left|1x_1 0x_0 1y_1 0y_0\right\rangle+\alpha\beta n^2\left|1x_1 0x_0 1y_1 1y_1\right\rangle\\
&+\beta^2m^2\left|1x_1 1x_1 0y_0 0y_0\right\rangle+\beta^2mn\left|1x_1 1x_1 0y_0 1y_1\right\rangle+\beta^2mn\left|1x_1 1x_1 1y_1 0y_0\right\rangle+\beta^2n^2\left|1x_1 1x_1 1y_1 1y_1\right\rangle\\
&+\alpha^2m^2\left|0y_0 0y_0 0x_0 0x_0\right\rangle+\alpha\beta m^2\left|0y_0 0y_0 0x_0 1x_1\right\rangle+\alpha\beta m^2\left|0y_0 0y_0 1x_1 0x_0\right\rangle+\beta^2m^2\left|0y_0 0y_0 1x_1 1x_1\right\rangle\\
&+\alpha^2mn\left|0y_0 1y_1 0x_0 0x_0\right\rangle+\alpha\beta mn\left|0y_0 1y_1 0x_0 1x_1\right\rangle+\alpha\beta mn\left|0y_0 1y_1 1x_1 0x_0\right\rangle+\beta^2mn\left|0y_0 1y_1 1x_1 1x_1\right\rangle\\
&+\alpha^2mn\left|1y_1 0y_0 0x_0 0x_0\right\rangle+\alpha\beta mn\left|1y_1 0y_0 0x_0 1x_1\right\rangle+\alpha\beta mn\left|1y_1 0y_0 1x_1 0x_0\right\rangle+\beta^2mn\left|1y_1 0y_0 1x_1 1x_1\right\rangle\\
&+\alpha^2n^2\left|1y_1 1y_1 0x_0 0x_0\right\rangle+\alpha\beta n^2\left|1y_1 1y_1 0x_0 1x_1\right\rangle+\alpha\beta n^2\left|1y_1 1y_1 1x_1 0x_0\right\rangle+\beta^2n^2\left|1y_1 1y_1 1x_1 1x_1\right\rangle\\
&-m^4\left|0y_0 0y_0 0y_0 0y_0\right\rangle-m^3n\left|0y_0 0y_0 0y_0 1y_1\right\rangle-m^3n\left|0y_0 0y_0 1y_1 0y_0\right\rangle-m^2n^2\left|0y_0 0y_0 1y_1 1y_1\right\rangle\\
&-m^3n\left|0y_0 1y_1 0y_0 0y_0\right\rangle-m^2n^2\left|0y_0 1y_1 0y_0 1y_1\right\rangle-m^2n^2\left|0y_0 1y_1 1y_1 0y_0\right\rangle-mn^3\left|0y_0 1y_1 1y_1 1y_1\right\rangle\\
&-m^3n\left|1y_1 0y_0 0y_0 0y_0\right\rangle-m^2n^2\left|1y_1 0y_0 0y_0 1y_1\right\rangle-m^2n^2\left|1y_1 0y_0 1y_1 0y_0\right\rangle-mn^3\left|1y_1 0y_0 1y_1 1y_1\right\rangle\\
&-m^2n^2\left|1y_1 1y_1 0y_0 0y_0\right\rangle-mn^3\left|1y_1 1y_1 0y_0 1y_1\right\rangle-mn^3\left|1y_1 1y_1 1y_1 0y_0\right\rangle-n^4\left|1y_1 1y_1 1y_1 1y_1\right\rangle).
\end{aligned}
\tag{14}
$$

Obviously, when Alice performs four-qubit cluster state measurement on the decoy photons, the probability without eavesdropper is

$$
\begin{aligned}
p(|\psi\rangle)=\frac{1}{4}\big(&|\alpha^4|^2+|\alpha^2\beta^2|^2+|\alpha^2\beta^2|^2+|\beta^4|^2\\
&+|\alpha^2m^2|^2+|\alpha^2n^2|^2+|\beta^2m^2|^2+|\beta^2n^2|^2\\
&+|\alpha^2m^2|^2+|\alpha^2n^2|^2+|\beta^2m^2|^2+|\beta^2n^2|^2\\
&+|m^4|^2+|m^2n^2|^2+|m^2n^2|^2+|n^4|^2\big).
\end{aligned}
\tag{15}
$$

So the lower bound of the detection probability is

$$
\begin{aligned}
d_{lF}&=1-p(|\psi\rangle)\\
&=1-\frac{1}{4}\big(|\alpha^4|^2+|\alpha^2\beta^2|^2+|\alpha^2\beta^2|^2+|\beta^4|^2\\
&\quad+|\alpha^2m^2|^2+|\alpha^2n^2|^2+|\beta^2m^2|^2+|\beta^2n^2|^2\\
&\quad+|\alpha^2m^2|^2+|\alpha^2n^2|^2+|\beta^2m^2|^2+|\beta^2n^2|^2\\
&\quad+|m^4|^2+|m^2n^2|^2+|m^2n^2|^2+|n^4|^2\big).
\end{aligned}
\tag{16}
$$

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

$$
\begin{aligned}
d_{lF}&=1-p(|\psi\rangle)\\
&=1-\frac{1}{4}\big(|\alpha^4|^2+|\alpha^2\beta^2|^2+|\alpha^2\beta^2|^2+|\beta^4|^2\\
&\quad+|\alpha^2m^2|^2+|\alpha^2n^2|^2+|\beta^2m^2|^2+|\beta^2n^2|^2\\
&\quad+|\alpha^2m^2|^2+|\alpha^2n^2|^2+|\beta^2m^2|^2+|\beta^2n^2|^2\\
&\quad+|m^4|^2+|m^2n^2|^2+|m^2n^2|^2+|n^4|^2\big)\\
&=1-\frac{1}{4}\big(a^4+2a^2b^2+b^4+s^4+2s^2t^2+t^4\\
&\quad+2a^2t^2+2b^2t^2+2a^2s^2+2b^2s^2\big)\\
&=-(a^4-2a^3+3a^2-2a+t^4-2t^3+3t^2\\
&\quad-2t+2a^2t^2-2at^2-2ta^2+2at).
\end{aligned}
\tag{17}
$$

However, in DPP, authors have calculated the efficiency of eavesdropping detection. Here donot analyze it again, and the efficiency is

$$
d_{lD}=|\beta|^2=|\beta'|^2=1-|\alpha|^2=1-|\alpha'|^2.
\tag{18}
$$

Now, let us analyze how much information Eve can gain maximally when there is no control mode. First, Alice takes measurement on the photon in her hand with signal-photon detector and the state is $|0\rangle$ supposing that the quantum state of the photon in the hand of Alice is $|0\rangle$, which is similar to that in [21]. Then the state of the system composed of Bob's photon is

$$
\begin{aligned}
|\psi'\rangle&=\hat{E}|0,E\rangle\equiv\hat{E}|0\rangle|E\rangle=\alpha|0\rangle|\varepsilon_{00}\rangle+\beta|1\rangle|\varepsilon_{01}\rangle\\
&\equiv\alpha|0,\varepsilon_{00}\rangle+\beta|1,\varepsilon_{01}\rangle,
\end{aligned}
\tag{19}
$$

and Eve's probe can be described by

$$
\begin{aligned}
\rho'=&|\alpha|^2|0,\varepsilon_{00}\rangle\langle 0,\varepsilon_{00}|+|\beta|^2|1,\varepsilon_{01}\rangle\langle 1,\varepsilon_{01}|\\
&+\alpha\beta^*|0,\varepsilon_{00}\rangle\langle 1,\varepsilon_{01}|+\alpha^*\beta|1,\varepsilon_{01}\rangle\langle 0,\varepsilon_{00}|.
\end{aligned}
\tag{20}
$$

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

$$
\begin{aligned}
\rho''=&(p_0+p_3)|\alpha|^2|0,\varepsilon_{00}\rangle\langle 0,\varepsilon_{00}|\\
&+(p_0+p_3)|\beta|^2|1,\varepsilon_{01}\rangle\langle 1,\varepsilon_{01}|\\
&+(p_0-p_3)\alpha\beta^*|0,\varepsilon_{00}\rangle\langle 1,\varepsilon_{01}|\\
&+(p_0-p_3)\alpha^*\beta|1,\varepsilon_{01}\rangle\langle 0,\varepsilon_{00}|
\end{aligned}
$$

$$
\begin{aligned}
&+(p_1+p_2)|\alpha|^2\,|1,\varepsilon_{00}\rangle\langle 1,\varepsilon_{00}| \\
&+(p_1+p_2)|\beta|^2\,|0,\varepsilon_{01}\rangle\langle 0,\varepsilon_{01}| \\
&+(p_1-p_2)\alpha\beta^*\,|1,\varepsilon_{00}\rangle\langle 0,\varepsilon_{01}| \\
&+(p_0-p_3)\alpha^*\beta\,|0,\varepsilon_{01}\rangle\langle 1,\varepsilon_{00}|
\end{aligned} \tag{21}
$$

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

$$
\rho''=\begin{pmatrix}
(p_0+p_3)|\alpha|^2 & (p_0-p_3)\alpha\beta^* & 0 & 0 \\
(p_0-p_3)\alpha^*\beta & (p_0+p_3)|\beta|^2 & 0 & 0 \\
0 & 0 & (p_1+p_2)|\alpha|^2 & (p_1-p_2)\alpha\beta^* \\
0 & 0 & (p_0-p_3)\alpha^*\beta & (p_1+p_2)|\beta|^2
\end{pmatrix}, \tag{22}
$$

with

$$
p_0+p_1+p_2+p_3=1. \tag{23}
$$

The information I_0 that Eve can get is equal to the Von Neumann entropy

$$
I_0=\sum_{i=0}^{3}-\lambda_i\log_2\lambda_i, \tag{24}
$$

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

$$
\begin{aligned}
\lambda_{0,1}&=\frac{1}{2}(p_0+p_3)\pm\frac{1}{2}\sqrt{(p_0+p_3)^2-16p_0p_3|\alpha|^2|\beta|^2} \\
&\frac{1}{2}(p_0+p_3)\pm\frac{1}{2}\sqrt{(p_0+p_3)^2-16p_0p_3\left(d-d^2\right)},
\end{aligned} \tag{25}
$$

$$
\begin{aligned}
\lambda_{2,3}&=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2|\alpha|^2|\beta|^2} \\
&\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2\left(d-d^2\right)}.
\end{aligned} \tag{26}
$$

In the case of p_0=p_1=p_2=p_3=0.25, where Alice encodes exactly 2 bits, expressions (25)–(26) simplify to $\lambda_0=0.5d$, $\lambda_1=0.5(1-d)$, $\lambda_2=0.5d$ and $\lambda_3=0.5(1-d)$. Interestingly, the maximal information gain is equal to the Shannon entropy of a binary channel:

$$
\begin{aligned}
I_0(d)=&-\frac{1}{2}d\log_2\left(\frac{1}{2}d\right)-\left(\frac{1}{2}-\frac{1}{2}d\right)\log_2\left(\frac{1}{2}-\frac{1}{2}d\right) \\
&-\frac{1}{2}d\log_2\left(\frac{1}{2}d\right)-\left(\frac{1}{2}-\frac{1}{2}d\right)\log_2\left(\frac{1}{2}-\frac{1}{2}d\right).
\end{aligned} \tag{27}
$$

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

$$
\begin{aligned}
I_1(d)=&-\frac{1}{2}d\log_2\left(\frac{1}{2}d\right)-\left(\frac{1}{2}-\frac{1}{2}d\right)\log_2\left(\frac{1}{2}-\frac{1}{2}d\right) \\
&-\frac{1}{2}d\log_2\left(\frac{1}{2}d\right)-\left(\frac{1}{2}-\frac{1}{2}d\right)\log_2\left(\frac{1}{2}-\frac{1}{2}d\right).
\end{aligned} \tag{28}
$$

So the maximal amount of information that Eve can obtain is

$$
I=0.5(I_0+I_1)=1-d\log_2 d-(1-d)\log_2(1-d). \tag{29}
$$

After some simple mathematical calculations in FPP, when a=t, get

$$
d_{IF}=-4a^4+8a^3-8a^2+4a, \tag{30}
$$

and the maximum I is

$$
I(d_{IF})=1+H\left(\frac{1}{2}+\frac{1}{2}\times\sqrt{-1+2\sqrt{1-d_{IF}}}\right), \tag{31}
$$

where

$$
H(x)=-x\log_2 x-(1-x)\log_2(1-x). \tag{32}
$$

However, in DPP, the maximum I is

$$
\begin{aligned}
I(d_{ID})&=1-d_{ID}\log_2 d_{ID}-(1-d_{ID})\log_2(1-d_{ID}) \\
&=1+H(d_{ID}).
\end{aligned} \tag{33}
$$

The above analysis shows that function $I(d_{ID})$ and $I(d_{IF})$ have the similar algebraic properties. If Eve wants to gain the full information (I=2), the probabilities of eavesdropping detection are $d_{ID}(I=2)$=0.5 in DPP and $d_{IF}(I=2)$=0.75 in FPP.

In order to contrast the two functions, Figure 2 is given. As are shown in Figure 2, if Eve wants to gain the full information, she must face a larger detection probability in

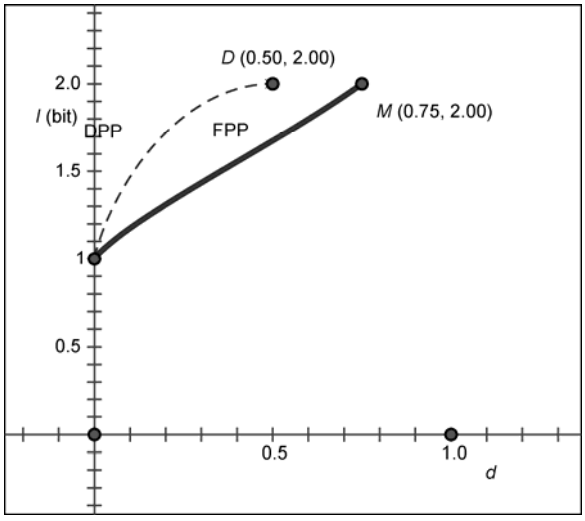

Figure 2 The comparison of the two detection results. The dotted line expresses the function $I(d_{ID})$ in DPP and the thick line expresses the function $I(d_{IF})$ in FPP. Obviously, if Eve wants to get the full information, she must encounter the higher detection efficiency in FPP.

FPP than DPP. This also indicates that FPP is more secure than DPP.

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

$$s(c,d) = (1-c) + c(1-d)(1-c) + c^2(1-d)^2(1-c) + \ldots = \frac{1-c}{1-c(1-d)}. \quad (34)$$

Then the probability of successful eavesdropping $I=nI(d)$ bits is $s(I,c,d) = s(c,d)^{I/I(d)}$. Therefore

$$s(I,c,d) = \left(\frac{1-c}{1-c(1-d)}\right)^{I/I(d)}, \quad (35)$$

where

$$I(d) = 1 + H\left(\frac{1}{2} + \frac{1}{2}\times\sqrt{-1+2\sqrt{1-d}}\right). \quad (36)$$

Now let us analyze the security of the FPP. In the limit $I \to \infty$ (a message or key of infinite length) get $s \to 0$, so the presented protocol 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 decoy mode is c=0.5. In Figure 3, the eavesdropping success probability as a function of the information gain I is plotted, 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 she has got. So, the FPP protocol is proved secure.

3 Conclusion and further work

In summary, an improved eavesdropping detection strategy based on four-particle cluster state in quantum direct communication protocol has been introduced, and two eavesdropping detection strategies are compared quantitatively using the constraint between the information that eavesdropper obtains and the interference introduced. The key idea of FPP is same to the controlled order rearrangement encryption, which is to implement encryption and detect eavesdropping by disorganizing the cluster state particles. In FPP, the sequence B is always in hands of Bob and Eve can only touch the sequence A. Any useful message will not be leaked to the potential eavesdropper. So the security message can be securely transmitted to the receiver. Compared with the DPP, in the FPP protocol, the four-particle cluster state particles are used to detect eavesdropping which increases the efficiency of detection eavesdropping.

In the analysis, if the eavesdropper obtains the full information, she must face a larger detection probability in the FPP than DPP, which shows that the efficiency of eavesdropping detection in FPP is higher than DPP. Therefore it can ensure that the quantum direct communication protocol is more secure. In order to detect eavesdropping, Bob sends more decoy photons than DPP, while this method reduces the number of measurement. That is, Bob gains the better security at the cost of sending more particles.

Compared with the existing research working [32,33] based on the four-particle cluster state, the goal of utilizing the four-particle cluster state is different. The four-particle cluster state is not only used as the decoy photon, but also used to transmit secret message in [32,33]. And the four-particle cluster states are divided into two groups. Only one group was transmitted in the whole communication. However, the four-particle cluster state is only used as the decoy photon. The secret message is transmitted by Bell states. Moreover, the four-particle cluster state is randomly inserted in the travel particles together.

The preparation process of four-particle cluster state is complex relatively and the creating probability based on the present technology is lower. However, experimentally, Walther et al. [34,35] have used nonlinear optics to directly produce four-particle cluster state. Then, in 2008, Zhang et al. [36] and Tokunaga et al. [37] presented a simple scheme for generating such a cluster state and measuring it in the basis FMB, respectively. Moreover, as cluster state has been applied to one-way quantum computer [38]. Thus, the presented protocol is feasible in recent technology.

As we know, the quantum direct communication protocol can also be used as an efficient QKD protocol. In this paper, only the situation that the improved protocol is used as a QKD strategy is considered. So the weaknesses which the quantum direct communication protocol must be faced, such as the noise channel [39,40], the Dos attack [41,42] and so on, may not be considered. In the further work, the other QSDC protocol will be researched.

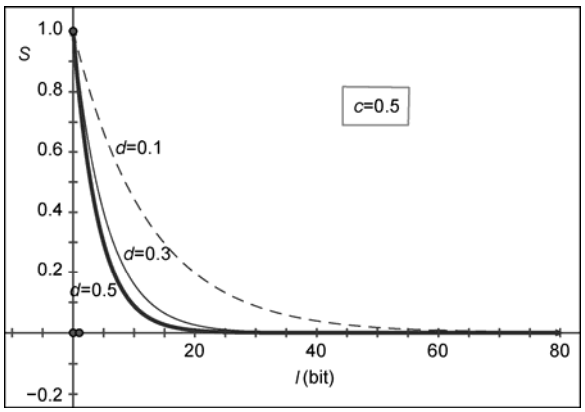

Figure 3 Eavesdropping success probability as a function of the maximal eavesdropped information, plotted for different detection probabilities d.

The work was supported by the National Natural Science Foundation of China (61100205).

1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceeding of the IEEE International Conference on Computer, Systems and Signal Processing, Bangalore, 1984. 175–179
2 Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895–1899
3 Peng F, Xie G J, Wu T H. Optimizing quantum teleportation circuit using genetic algorithm. In: Proceeding of 2009 IEEE International Conference on Granular Computing, 2009. 466–470
4 Pan J W. Recent progress in quantum teleportation experiments. In: Proceeding of 2011 Conference on Lasers and Electro-Optics (CLEO), 2011. 1–2
5 Prakash H. Quantum teleportation. In: Proceeding of 2009 International Conference on Emerging Trends in Electronic and Photonic Devices & Systems, 2009. 18–23
6 Hari P. Quantum teleportation. In: Proceedings of the International Conference on Emerging Trends in Electronic and Photonic Devices & Systems, 2009
7 Akira F. Quantum teleportation and quantum information processing. In: Proceedings of the Quantum Electronics and Laser Science Conference, 2010
8 Li C Y, Li X H, Deng F G, et al. Complete multiple round quantum dense coding with quantum logical network. Chin Sci Bull, 2007, 59: 1162–1165
9 Zhao Y H, Wen X J. A covert communication protocol based on quantum dense coding. In: Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology, 2011. 3376–3379
10 Li C Y, Li X H, Deng F G, et al. Complete multiple round quantum dense coding with quantum logical network. Chin Sci Bull, 2007, 52: 1162–1165
11 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
12 Yang Y G, Wen Q Y. Threshold quantum secret sharing between multi-party and multi-party. Sci China Ser G: Phys Mech Astron, 2008, 51: 1308–1315
13 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
14 Li J, Jin H F, Jing B. Improved quantum "ping-pong" protocol based on GHZ state and classical XOR operation. Sci China Phys Mech Astron, 2011, 54: 1612–1618
15 Shimizu K, Imoto N. Communication channels secured from eavesdropping via transmission of photonic Bell states. Phys Rev A, 1999, 60: 157–166
16 Yuan H, Song J, Zhou J, et al. High-capacity deterministic secure four-qubit W state protocol for quantum communication based on order rearrangement of particle pairs. Int J Theor Phys, 2011, 50: 2403–2409
17 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. Acta Phys Pol A, 2002, 101: 357
18 Yang Y G, Wen Q Y. Threshold quantum secure direct communication without entanglement. Sci China Ser G: Phys Mech Astron, 2008, 51: 176–183
19 Li X H, Deng F G. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A, 2006, 74: 054302
20 Li X H, Li C Y, Deng F G, et al. Quantum secure direct communication with quantum encryption based on pure entangled states. Chin Phys Lett, 2007, 16: 2149–2153
21 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
22 Nguyen B A. Quantum dialogue. Phys Rev A, 2004, 328: 6–10
23 Wang D, Chai X C, Zha X W, et al. Bidirectional quantum secure communication based on cluster state. In: Proceeding of 2010 International Symposium on Information Science and Engineering, 2010. 267–270
24 Zhang X J, Xie S C, Wang D. Three-party quantum secure direct communication base on partially entangled states. In: Proceedings of 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, 2011. 1555–1558
25 Man Z X, Xia Y J. Improving of security of three-party quantum secure direct communication based on GHZ states. Chin Phys Lett, 2007, 24: 15–18
26 Chen Y, Man Z X, Xia Y J. Quantum bidirectional secure direct communication via entanglement swapping. Chin Phys Lett, 2007, 24: 19–22
27 Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons. Sci China Ser G-Phys Mech Astron, 2007, 50: 558–562
28 Boström K, Felbringer T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902
29 Brassard G, Salvail L. Secret-key reconciliation by public discussion. Lect Notes Comput Sci, 1994, 765: 410–423
30 Zhou Y Y, Zhou X J, Yang S J. Study on passive decoy-state protocol for quantum key distribution. In: Proceeding of 3rd International Conference on Advanced Computer Theory and Engineering, 2010. 91–94
31 Li C Y, Li X H, Deng F G, et al. Efficient quantum cryptography network entanglement and quantum memory. Chin Phys Lett, 2006, 23: 2897–2899
32 Cao W F, Yang Y G, Wen Q Y. Quantum secure direct communication with cluster states. Sci China Phys Mech Astron, 2010, 53: 1271–1275
33 Wang G Y, Fang X M, Tan X H. Quantum secure direct communication with cluster state. Chin Phys Lett, 2006, 23: 2658
34 Walther P, Pan J W, Aspelmeyer M, et al. De Broglie wavelength of a non-local four-photon state. Nature, 2004, 429: 158–161
35 Walther P, Resch K J, Rudolph E, et al. Experimental one-way quantum computing. Nature, 2005, 434: 169–176
36 Zhang W, Liu Y M, Wang Z Y, et al. Discriminating 16 mutually orthogonal 4-atom cluster states via cavity QED in teleporting arbitrary unknown two-atom state with a 4-atom cluster state as quantum channel. Int J Mod Phys C, 2008, 19: 741–747
37 Tokunaga Y, Kuwashiro S, Yamamoto T, et al. Generation of high-fidelity four-photon cluster state and quantum-domain demonstration of one-way quantum computing. Phys Rev Lett, 2008, 100: 210501
38 Raussendorf R, Briegel H J. One-way quantum computer. Phys Rev Lett, 2001, 86: 5188–5191
39 Wójcik A. Eavesdropping on the "ping-pong" quantum communication protocol. Phys Rev Lett, 2003, 90: 157901
40 Deng F G, Li X H, Li C Y, et al. Eavesdropping on the "ping-pong" quantum communication protocol freely in a noise channel. Chin Phys Lett, 2007, 16: 277–281
41 Cai Q Y. The "ping-pong" protocol can be attacked without eavesdropping. Phys Rev Lett, 2003, 91: 109801
42 Zhang Z J, Man Z X. The improved Boström-Felbinger protocol against attacks without eavesdropping. Int J Quant Inform, 2004, 2: 521–527