Chinese Journal of Electronics
Vol.21, No.4, Oct. 2012

Improved Eavesdropping Detection Strategy Based on Extended Three-particle Greenberger-Horne-Zeilinger State in Two-step Quantum Direct Communication Protocol*

LI Jian, YE Xinxin, LI Ruifan, ZOU Yongzhong and LU Xiaofeng

(*School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China*)

Abstract — In order to improve the eavesdropping detection efficiency in two-step quantum direct communication protocol, an improved eavesdropping detection strategy using extended three-particle GHZ state is proposed, in which extended three-particle GHZ 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 by using the constraint between the information which eavesdropper can obtain and the interference introduced. If the eavesdroppers intend to obtain all information, the eavesdropping detection rate of the original two-step quantum direct communication protocol by using EPR pair block as detection particles is 50%; while the proposed strategy's detection rate is 59%. In the end, the security of the proposed protocol is discussed. The analysis results show that the eavesdropping detection strategy presented is more secure.

Key words — Quantum key distribution (QKD), Dense coding, Extended three-particle GHZ (Greenberger-Horne-Zeilinger) state, Eavesdropping detection, Entropy.

I. Introduction

Since Bennett and Brassard presented the pioneer QKD protocol[1] (BB84 protocol) in 1984, a lot of quantum information security processing methods have been advanced, such as quantum teleportation[2−13], quantum secret sharing[14,15] and so on. In recent years, a novel concept, Quantum secure direct communication (QSDC)[16−18] was put forward and studied by some groups. The QSDC protocol can be used in some special environments as first proposed by Boström *et al.*[19]. In 2003, Deng *et al.* proposed a two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen (EPR) pair block, which each EPR pair carries two bits of classical information[17].

To improve the efficiency of eavesdropping detection in the two-step quantum direct communication protocol, an improved eavesdropping detection strategy based on extended three-particle Greenberger-Horne-Zeilinger (GHZ) state in two-step quantum direct communication protocol is proposed in which extended three-particle GHZ state is used to detect eavesdroppers. During the security analysis, the method of the entropy theory is introduced, If the eavesdropper gets the full information, the detection rate of the two-step quantum direct communication protocol using the EPR pair block is 50%; the detection rate of the presented protocol using extended three-particle GHZ state is 59%. In the end, the security of the proposed protocol is discussed. The analysis results show that the improved two-step quantum direct communication protocol using extended three-particle GHZ state is more secure.

For simplicity, suppose that the original two-step QSDC using EPR pair in Ref.[17] is referred to as TSE and the improved eavesdropping detection strategy proposed is referred to as TSET.

It should be emphasized that, taking into account the security vulnerability while the quantum "Ping-pong" protocol is used as QSDC, only the situation that the proposed protocol is used as a QKD strategy is analyzed. That is to say, the transmitted information is random key (raw key), not the secret message. After the error correction and the privacy amplification, the random key will become the final key.

II. The TSET Protocol

The basic idea of dense coding is that Alice makes one of the four unitary operations to each of her particles and two bits of classical information can be encoded in each EPR pair. In Ref.[17], the author generalizes the dense coding idea into secure direct communication. But the eavesdropping detection efficiency is not high. In order to improve the eavesdropping detection efficiency, an improved eavesdropping detection strategy based on extended three-particle GHZ state in two-step quantum direct communication protocol is proposed. The specific steps are as follows.

*Manuscript Received Feb. 2012; Accepted Mar. 2012. This work is supported by the Natural Science Foundation of Jiangsu Province (No.BK2011169), the National Natural Science Foundation of China (No.61100205, No.61100208).

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

Define

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

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

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{4}$$

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |110\rangle + |111\rangle) \tag{5}$$

Now let us give an explicit process for the TSET

(S1) Alice and Bob agree that each of the four Bell bases can carry two-qubit classical information and encode $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ as 00, 01, 10 and 11, respectively.

(S2) Bob prepares a large enough number of Bell states, randomly inserts enough the extended three-particle GHZ states and dispenses the Bell states.

Bob prepares a large enough number (N) of Bell states $|\phi^+\rangle$ in sequence. He extracts all the first particles in the Bell states, and forms a series of particles A (the travel qubits) in order. The remainder particles in the Bell states are formed a series of particles B (the home qubits) in order. These particles are used to transmit secure message.

Bob prepares a large number N_0 of the extended three-particles GHZ states $|\psi\rangle$ and forms a series of particles C in order. These particles are used to detect eavesdropping. Note that the C sequence includes $3N_0$ qubits.

For C, Bob reserves particles 3 of the extended three-particle GHZ state, and measures them by Z-bases. After that, Bob inserts particles 1, 2 of the extended three-particle GHZ state to the particles A randomly. So a new sequence D in which there are decoy particles is produced, but only Bob knows their positions.

Bob stores the particles B and sends the particles D to Alice.

(S3) The detection of eavesdropping

After Alice received the particles D, Bob tells her the positions where there are decoy photons and the results of his measurements. Alice extracts the decoy photons from the particles D and performs the measurement. If Bob's measurement result is $|0\rangle$ and Alice's measurement result is $|00\rangle + |11\rangle$, or Bob's measurement result is $|1\rangle$ and Alice's measurement result is $|11\rangle$, they can trust that there is no eavesdropper. This is the first eavesdropping detection. After that, if the error rate is small, Alice and Bob can conclude that there are no eavesdroppers in the line. Alice and Bob continue to perform step **(S4)**; otherwise, they have to discard their transmission and abort the communication.

(S4) Alice encodes her messages on the particles C and transmits them to Bob.

The dense coding scheme of Bennett and Wiesner[8] is used to encode the message, where the information is encoded on an EPR pair with a local operation on a single qubit. Explicitly, Alice makes one of the four unitary operations (u_0, u_1, u_2, u_3) to each of her particles, u_0, u_1, u_2, u_3 as described by Eqs.(1), (2), (3), (4), respectively. And they transform the state $|\phi^+\rangle$ into $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ respectively. These operations correspond to 00, 01, 10, and 11, respectively. In order to ensure the security of this transmission, Alice has to insert some decoy particles in the sequence C. She inserts enough of the extended three-particle GHZ states in the sequence C as Bob does in **(S2)**, and measures them by Z-bases, only Alice knows their positions.

(S5) Bob decrypts Alice's secure message with the Bell-basis measurement on the particles B and C simultaneously.

After the transmission of the encoded particles C, Alice tells Bob the positions of the decoy photons. Bob makes the second eavesdropping detection. If Alice's measurement result is $|0\rangle$ and Bob's measurement result is $|00\rangle + |11\rangle$, or Alice's measurement result is $|1\rangle$ and Bob's measurement result is $|11\rangle$, they can trust that there is no eavesdropper, allowing them to continue. Then Bob performs the Bell-basis measurement on the particles B and C simultaneously, and Bob gets the secure message. 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.

(S6) The TSET protocol is end.

III. The Security Analysis

From the description above, it can be seen that, the most difference between TSE and TSET is the method of the detection of eavesdropping. In Ref.[17], the author computes the maximal amount of the information (I) that Eve can eavesdrop and the probability (d) that Eve is detected. And the function I_0 is provided.

When $p_0 = p_1 = p_2 = p_3 = 1/4$,

$$I_0 = -\sum_{i=0}^{3} \lambda_i \log_2 \lambda_i \tag{6}$$

Such that for $i = 0, 1, 2, 3$,

$$\lambda_{0,2} = \frac{1}{4} + \frac{1}{2}\sqrt{\frac{1}{4} - d(1-d)} \tag{7}$$

$$\lambda_{1,3} = \frac{1}{4} - \frac{1}{2}\sqrt{\frac{1}{4} - d(1-d)} \tag{8}$$

So 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 TSET 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 performs the coding operation on the travel qubits. And finally Eve performs a measurement on the composed system. Note that, all transmitted particles are sent together before detecting eavesdropping. This method is different with the original dense coding. Because Eve does not know which particles are used to detect eavesdropping, she can only 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 $p = 1/2$.

Generally speaking, suppose that there is a group of decoy photons in the extended three-particle GHZ states $|\psi\rangle$. Similar to that in Ref.[20], suppose that after Eve performs the attack operation $\hat{E}$ the states $|0\rangle$ and $|1\rangle$ become

$$|\varphi_0'\rangle = \hat{E}\otimes|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle \tag{9}$$

$$|\varphi_1'\rangle = \hat{E}\otimes|1x\rangle = m|0y_0\rangle + n|1y_1\rangle \tag{10}$$

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

$$|\alpha|^2+|\beta|^2=1, \quad |m|^2+|n|^2=1 \tag{11}$$

Then let us compute the detection probability. After being attacked by Eve, the state of composed system becomes

$$\begin{aligned}
|\psi\rangle_{Eve} =& E\otimes E\otimes I\otimes\frac{1}{\sqrt{3}}(|0x0x\rangle\otimes|0\rangle \\
&+|1x1x\rangle\otimes|0\rangle+|1x1x\rangle\otimes|1\rangle) \\
=&\frac{1}{\sqrt{3}}[(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes|0\rangle \\
&+(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes|0\rangle \\
&+(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes|1\rangle] \\
=&\frac{1}{\sqrt{3}}[(\alpha^2|0x_00x_0\rangle+\alpha\beta|0x_00x_0\rangle+\alpha\beta|1x_10x_0\rangle \\
&+\beta^2|1x_11x_1\rangle)\otimes|0\rangle+(m^2|0y_00y_0\rangle+mn|0y_01y_1\rangle \\
&+mn|1y_10y_0\rangle+n^2|1y_11y_1\rangle)\otimes|0\rangle+(m^2|0y_00y_0\rangle \\
&+mn|0y_01y_1\rangle+mn|1y_10y_0\rangle+n^2|1y_11y_1\rangle)\otimes|1\rangle] \\
=&\frac{1}{\sqrt{3}}(\alpha^2|0x_00x_00\rangle+\alpha\beta|0x_01x_10\rangle+\alpha\beta|1x_10x_00\rangle \\
&+\beta^2|1x_11x_10\rangle+m^2|0y_00y_00\rangle+mn|0y_01y_10\rangle \\
&+mn|1y_10y_01\rangle+n^2|1y_11y_10\rangle+m^2|0y_00y_01\rangle \\
&+mn|0y_01y_11\rangle+mn|1y_10y_01\rangle+n^2|1y_11y_11\rangle)
\end{aligned} \tag{12}$$

Obviously, when Alice performs the extended three-particle GHZ measurement on the decoy photons, the probability without eavesdropper is

$$p(|\psi\rangle_{Eve}) = \frac{1}{3}(|\alpha^2|^2+|\beta^2|^2+|m^2|^2+|n^2|^2+|n^2|^2) \tag{13}$$

So the lower bound of the detection probability is

$$d = 1-p(|\psi\rangle_{Eve}) \tag{14}$$

Now, let us analyze how much information Eve can gain.

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

$$d = 1-(2a^2+3t^2-2a-2t+2)/3 \tag{15}$$

After some simple mathematical calculations, when $a=t$, we can get

$$d = 1-(5a^2-4a+2)/3 \tag{16}$$

Suppose that Bob sends $|0\rangle$ to Alice, the maximal amount of information is equal to the Shannon entropy of a binary channel, when $p_0=p_1=p_2=p_3=1/4$, the information I_0 that Eve can get is

$$I_0 = -\sum_{i=0}^{3}\lambda_i\log_2\lambda_i \tag{17}$$

Such that for $i=0,\,1,\,2,\,3$,

$$\lambda_{0,2} = \frac{1}{4}+\frac{1}{2}\sqrt{\frac{1}{4}-\frac{2+\sqrt{9-15d}}{5}\left(1-\frac{2+\sqrt{9-15d}}{5}\right)} \tag{18}$$

$$\lambda_{1,3} = \frac{1}{4}-\frac{1}{2}\sqrt{\frac{1}{4}-\frac{2+\sqrt{9-15d}}{5}\left(1-\frac{2+\sqrt{9-15d}}{5}\right)} \tag{19}$$

The above analysis shows that function $I(d_E)$ and $I(d_{ET})$ have the similar algebraic properties. In order to compare the two functions, Fig.1 is given.

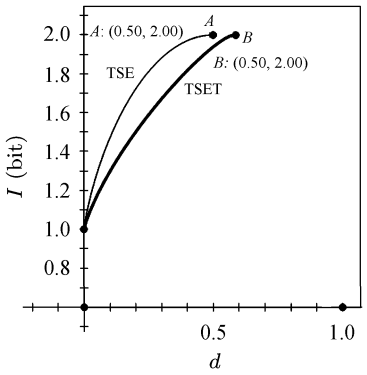

Fig. 1. The comparison of the two detection results

As Fig.1 shows that if Eve wants to gain the full information ($I=2$), the probability of the eavesdropping detection is d_E ($I=2$) $=0.5$ in the TSE. And the probability of the eavesdropping detection is d_{ET} ($I=2$) $=0.59$ in the TSET. Obviously, if Eve wants to get the same amount information, she must encounter the higher detection efficiency in TSET. Also, if there is the same detection efficiency, Eve will eavesdrop less information.

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.

If Eve wants to gain the same amount of information, she must face a larger detection probability in the TSET than the other. This also shows that the TSET is more secure than the other.

IV. Conclusions

In the TSET 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 TSE protocol, the TSET protocol has the following differences:

(1) In the two-step quantum direct communication protocol using the EPR pair block[17], Alice sends the checking-sequence to Bob to make the eavesdropping detection, If the error rate is low, then Alice sends the message-coding sequence to Bob. During this process, Eve can capture the state of particles in both checking-sequence and the message-coding sequence. So a little secret message may be leaked. In the TSET protocol, Bob prepares the particles rather than Alice; Eve cannot capture the states of the home qubits, so the TSET protocol can improve the security of the transmission.

(2) In the TSET protocol, the eavesdropping detection is made twice. The first eavesdropping detection is made to ensure that there is no eavesdropper, so Alice can encode the secret message and the transmission can continue. In fact, in the second transmission, Eve can only disturb the transmission and cannot steal the information. But if Alice and Bob can entrust that there is no eavesdropper by the second eavesdropping detection, those particles which are used to transmit the secure message can be reused.

In this paper, only the situation that the protocol is used as a QKD strategy is considered. So the weaknesses which the TSET protocol necessarily faced as QSDC, such as the noise channel[21,22], may not be considered. In the further work, the other Two-step quantum direct communication protocol's security and its improvement will be researched.

References

[1] C.H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing", *Proceeding of the IEEE International Conference on Computer, Systems and Signal Processing*, Bangalore, India, pp.175–179, 1984.

[2] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wooters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.*, Vol.70, 1993.

[3] Kim. Yoon-Ho, S.P. Kulik and Shih. Yanhua, "Quantum teleportation with a complete Bell state measurement", *J. Mod. Opt.*, Vol.49, pp.221–236, 2002.

[4] J. Li, H.F. Jin and B. Jing, "Improved quantum "Ping-pong" protocol based on GHZ state and classical XOR Operation", *Sci. China Ser. G*, Vol.54, No.9, pp.1612–1618, 2011.

[5] Z.J. Zhang, Y.M. Liu and D. Wang, "Perfect teleportation of arbitrary n-qubit states using different quantum channels", *Phys. Lett. A*, Vol.372, pp.28–32, 2007.

[6] J. Li, D.J. Song, X.J. Guo and B. Jing, "Improved quantum "Ping-pong" protocol based on five-qubit GHZ state and classical CNOT operation", *Int. J. Theor. Phys.*, Vol.51, No.1, pp.292–302, 2012.

[7] H. Yuan, Q. He, X.Y. Hu *et al.*, "Deterministic secure quantum communication with cluster state and bell-basis measurements", *Commun. Theor. Phys.*, Vol.50, 2008.

[8] J. Li, D.J. Song, X.J. Guo and B. Jing, "An improved "Ping-pong" protocol based on four-qubit genuine entangled state", *Chinese Jaurnal of Electronics*, Vol.20, No.3, pp.457–460, 2011.

[9] Prakash. Hari, "Quantum teleportation", *International Conference on Emerging Trends in Electronic and Photonic Devices and Systems*, 2009.

[10] J. Li, D.J. Song, X.J. Guo and B. Jing, "Quantum secure direct communication protocol based on five-particles cluster state and classical XOR operation", *Acta Electronica Sinica*, Vol.36, No.1, pp.31–36, 2012. (in Chinese)

[11] F. Akira, "Quantum teleportation and quantum information processing", *Quantum Electronics and Laser Science Conference*, 2010.

[12] J. Li, H.F. Jin and B. Jing, "Improved security detection strategy for quantum "Ping-Pong" protocol and its security analysis", *Chin. Commun.*, Vol.8, No.3, pp.170–179, 2011.

[13] J. Li, D.J. Song, X.J. Guo and B. Jing, "An improved security detection strategy based on W state in "Ping-pong" Protocol", *Chinese Journal of Electronics,* Vol.21, No.1, pp.117–120, 2012.

[14] M. Hillery, V. Buzek and A. Berthiaume, "Quantum secret sharing", *Phys. Rev. A*, Vol.59, pp.1829–1834, 1999.

[15] S.K. Singh and R. Srikanth, "Generalized quantum secret sharing", *Phys. Rev. A*, Vol.71, pp.012328, 2005.

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

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

[18] G.L. Long, F.G. Deng, C. Wang X.H. Li, K. Wen and W.Y. Wang, "Quantum secure direct communication and deterministic secure quant communication", *Front. Phys. China*, Vol.2, No.3, pp.251–272, 2007.

[19] K. Boström and T. Felbringer, "Deterministic secure direct communication using entanglement", *Phys. Rev. Lett.*, Vol.89, pp.187902, 2002.

[20] F. Gao, F.Z. Guo, Q.Y. Wen *et al.*, "Comparing the efficiency of different detection strategies of the 'Ping-pong' protocol", *Sci. China, Ser. G-Phys Mech. Astron*, Vol.39, No.2, pp.161–166, 2009. (in Chinese)

[21] A. Wójcik, "Eavesdropping on the "Ping-pong" quantum communication protocol", *Phys. Rev. Lett.*, Vol.90, No.5, pp.157901, 2003.

[22] F.G. Deng, X.H. Li, C.Y. Li *et al.*, "Eavesdropping on the "Ping-pong" quantum communication protocol freely in a noise channel", *Chin. Phys. Lett.*, Vol.16, pp.277–281, 2007.

LI Jian Ph.D., Associate Professor of Beijing University of Posts and Telecommunications, interested in research on quantum information, quantum computation, quantum communication security, electronic commerce and artificial intelligence. (Email: lijian@bupt.edu.cn)

YE Xinxin is a M.S. student in the School of Computer at the Beijing University of Posts and telecommunications, China. She received B.S. degree in computer science from Harbin Normal University. Her research interests include quantum information, information security and the security of the Internet of things. (Email: buptyezi@ bupt.edu.cn)

LI Ruifan is a lecturer of Beijing University of Posts and Telecommunications, interested in research on quantum information, quantum computation, quantum communication security, information security and artificial intelligence. (Email: rfli@ bupt.edu.cn)

ZOU Yongzhong is a lecturer of Beijing University of Posts and Telecommunications, interested in research on quantum information, quantum computation, quantum communication security and information security, artificial intelligence.

LU Xiaofeng is a lecturer of Beijing University of Posts and Telecommunications, interested in research on quantum information, quantum computation, quantum communication security, information security and artificial intelligence.