Commun. Theor. Phys. (Beijing, China) **53** (2010) pp. 67–70

Vol. 53, No. 1, January 15, 2010

Deterministic Quantum Key Distribution with Pulsed Homodyne Detection*

WANG Chuan (王川),[1] WANG Wan-Ying (王婉莹),[2] AI Qing (艾清),[2] and LONG Gui-Lu (龙桂鲁)[2,3]

[1]School of Science and Key Laboratory of Optical Communication and Lightwave Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2]Key laboratory of Atomic and Molecular NanoSciences and Department of Physics, Tsinghua University, Beijing 100084, China

[3]Tsinghua National Laboratory of Information Science and Technology, Beijing 100084, China

(Received November 24, 2008)

Abstract *In this paper, we propose a deterministic quantum communication protocol using weak coherent states and pulsed homodyne detection. In this protocol, the communication parties exchange their secret information deterministically in two rounds. The devices and efficiency of the protocol are discussed respectively. We also show the security of the protocol against intercept-resend and Trojan-Horse eavesdropping attacks.*

PACS numbers: 03.67.Dd, 03.67.Hk
Key words: deterministic quantum key distribution, pulsed homodyne detection

1 Introduction

The main goal of cryptography is to make secret message not readable to eavesdropper but intelligible to the two authorized parties of the communication, conventionally called Alice and Bob. During the past few years, quantum key distribution (QKD) is thought to be one ideal technology which meets the requirement.[1−13] These protocols encode information on either single photons or entangled photon pairs. However, practical conditions limit the QKD communication distance and the key rates. For example, the loss of single photon during transmission is high. To overcome this difficulty, people have been looking for a new information carrier. In 1999, Ralph first proposed a protocol of quantum cryptography using continuous variables.[14] Different from discrete variable communication, the two communication parties choose to modulate or measure the phase and amplitude quadratures of a coherent state $|\alpha\rangle$. If Alice chooses to modulate one of the two quadratures and Bob happens to choose the same quadrature, then they get certain results of the coherent state. After the security checking process and error correction procedures, secure keys are then generated. The intensity of coherent state is much stronger than single photon source, so it seems to be a better resource in QKD realizations. Now continuous variable QKD has attracted much attention.[15−23] In continuous variable QKD, nonclassical beams are used as information carriers, such as squeezed states, EPR correlated continuous variables, and so on. The security of continuous variable quantum communication is guaranteed by the commutation relation between the quadrature amplitude of light field. Ever since then, rapid experiment progress has been made in continuous variable quantum cryptography. In 2003, Grosshans *et al.* finished their experiment on quantum cryptography using coherent state.[24]

In 2003, Hirano *et al.* proposed a quantum cryptography protocol using weak pulsed coherent state and pulsed homodyne detection.[25] They also experimentally realized BB84 QKD protocol using this method. The hybrid protocol encodes the keys on the phases of a coherent state and reads out by pulsed homodyne detection. The security of this protocol has also been discussed.[26−28] In this study, we generalize a deterministic quantum key distribution protocol using pulsed coherent state and homodyne detection. Our hybrid protocol combines the idea of continuous variable quantum cryptography and quantum deterministic communication with faint laser pulses. Therefore, the quantum keys are generated deterministically, and homodyne detection measurement lessens the limitation of single photon detection.

The paper is organized as follows. In Sec. 2, we first review the idea of deterministic quantum communication and quantum cryptography using pulsed homodyne detection, and propose the idea of hybrid deterministic quantum key distribution protocol. In Sec. 3, we analyze the security of our protocol against intercept-resend and Trojan-Horse attacks. And the last section is our conclusion.

2 Deterministic Quantum Key Distribution Using Pulsed Homodyne Detection

The idea of deterministic quantum communication using discrete variables was first proposed in Refs. [5, 29] in which the keys were generated deterministically. In Ref. [29], the protocol contains two-round communication. At first, Bob produces a series of single pho-

*Supported by the National Fundamental Research Program under Grant No. 2006CB921106, the National Natural Science Foundation of China under Grant Nos. 10874098 and 10775076

tons randomly in one of the following states: $|H\rangle$, $|V\rangle$, $|+\rangle = (1/\sqrt{2})(|H\rangle + |V\rangle)$, $|-\rangle = (1/\sqrt{2})(|H\rangle + |V\rangle)$, here H and V represent the horizontal and vertical polarizations of the photons respectively. Then the photons are sent to Alice. For each photon, Alice chooses to perform control procedure or coding procedure randomly. If she chooses the control procedure, she performs measurements on the photon in either X or Z basis. Otherwise, she performs $U_0 = |H\rangle\langle H| + |V\rangle\langle V|$ or $U_1 = |H\rangle\langle V| - |V\rangle\langle H|$ operations in the coding procedure. Then Alice and Bob publicly compare the security checking photons and estimate the error rate in communication. If the error rate is lower than the security bound, Alice sends the remaining photons back to Bob. Bob chooses to measure the photons according to the original basis when he prepares them and reads out the results of coding qubits. Then the two communication parties share a key series deterministically.

In the QKD protocol proposed by Hirano *et al.*,[25] the communication parties generate keys by producing and measuring the coherent states: $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$. The measuring basis chosen by Bob are either $X_1 = (a + a^\dagger)/2$ or $X_2 = (a - a^\dagger)/2i$ quadratures. The coherent states are the eigenstates of X_1 and X_2. When Alice and Bob happen to choose the same basis, their results are in correspondence with each other and a key is generated between them.

By combining the features in both the above-mentioned protocols, we propose here a deterministic quantum key distribution using pulsed continuous variable. The setup of the protocol is depicted in Fig. 1 and detailed procedure is shown as follows:

(i) Bob produces weak coherent laser pulses in coherent state $|\alpha\rangle$. The pulses pass the interferometer on Bob's side. The light in the upper path is used as the local oscillator light and the light in the path below is used as the signal light. Bob modulates the signal light randomly using a phase modulator by $\theta = 0, \pi/2, \pi, 3\pi/2$ and the state transforms to $|\alpha e^{i\theta}\rangle$. By proper time delay, the two light pulses are combined together and propagate to Alice.

(ii) When coherent pulses arrive at Alice's side, with probability p_1 she chooses the encoding path and modulates the signal light of the pulses with phase $\phi_A = 0, \pi$. With probability $1 - p_1$, Alice chooses the control path and measures the pulse quadratures of X_1 or X_2 using homodyne detections and saves the results. The coding pulses are delayed by some extending lines.

(iii) Alice announces publicly the results of security checking qubits. If their results are in agreement, they confirm that the channel is safe. Alice returns the remain coded pulses back to Bob. Bob then measures the coded pulses using homodyne detection with X_1 or X_2 basis according to their original states.

(iv) For these security checking pulses, Alice compares the results with Bob's preparation. They can build a correspondence with each other. For the cases they choose the same basis but get the wrong result, they define them as errors. If the error rate is lower than the security bound, they can confirm that the communication is secure.

(v) Bob then applies $\theta_B = \{0, \pi/2\}$ to the local oscillator light and measures the coding pulses using balanced homodyne detection. He then compares the corresponding phase differences with his original state and gets the phase information $\theta = \theta_A - \theta_B$ deterministically and reads out the phase θ_A that Alice adds. Bob then selects some of the results and compares them with Alice to prohibit Eve's attack in the second-round communication. If they confirm this step is secure, the two parties finish their deterministic communication process.

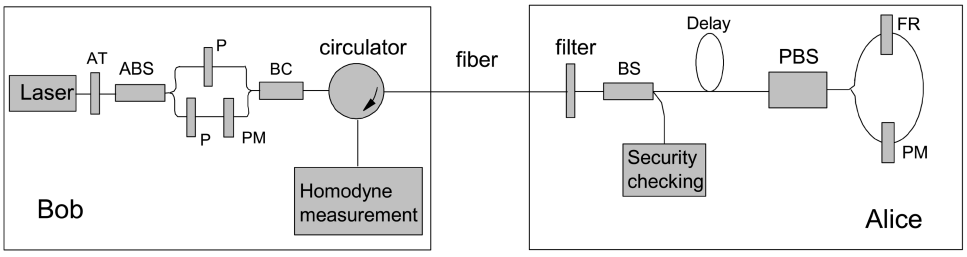

Fig. 1 Deterministic quantum communication setups. ABS is asymmetric beam splitter which reflects most of the light and transmits only a small portion. BC is the polarization beam combiner, and PBS is a polarizing beam splitter. AT is an attenuator. PM and P are phase modulator and polarization filter respectively. Faraday rotator (FR) and the PBS, play the role as a Faraday mirror.

The normalized quadrature amplitude of the signal X_θ is related to the results of the photodiodes N_θ and the average photon numbers $n_{\rm LO}$: $X_\theta = N_\theta/2\sqrt{n_{\rm LO}}$. For a coherent state with proper α, the distribution of X_θ obeys the Gaussian function in the X basis homodyne measurement. As analyzed in Ref. [25], the state $|\pm i\alpha\rangle$ and the state $|\pm\alpha\rangle$ cannot be distinguished by X_1 measurement in the region $-X_0 < x < X_0$. On condition that Alice chooses the correct basis, Bob sets a threshold of X_0. He defines the bit value as 0 if $x < -X_0$ and 1 if $x > X_0$. In this protocol, only Bob knows the initial states. Alice only performs a phase shift on the unknown state to encode the message. In this way, Alice needs not to know what the incoming states are while Bob knows Alice's message deterministically after the two-round communications. Quantum key distribution and quantum deterministic communication can both be realized using the apparatus shown in Fig. 1.

In the first round communication, when Alice receives the pulses, she chooses to encode the key message with phase $\phi_A = \{0, \pi\}$. Bob's signal state is in the coherent state $|\alpha e^{i\theta}\rangle$, here $\theta = \{0, \pi/2, \pi, 3\pi/2\}$. The encoding procedure divides Bob's signal states into two groups: $\{|\alpha\rangle, |-\alpha\rangle\}$ and $\{|i\alpha\rangle, |-i\alpha\rangle\}$. The states transformation takes place in their groups respectively after Alice's phase encoding.

After the security checking procedures, she returns the pulses back to Bob if the channel is secure. The states $|\alpha\rangle$ and $|-\alpha\rangle$ can only be distinguished when Bob applies a phase shift 0 on the local oscillator light and using balanced homodyne detection which is X_1 basis measurement. The phase difference $\theta = \theta_A - \theta_B$ can be read out when $\theta = \{0, \pi\}$. The states $|i\alpha\rangle$ and $|-i\alpha\rangle$ can only be distinguished when Bob chooses the phase shift $\pi/2$ on the local oscillator light and then performs the balanced homodyne detection, which is the X_2 basis measurement. The phase difference can be read out when $\theta = \{\pi/2, 3\pi/2\}$. The correspondence between the measuring bases and phase difference is shown in Table 1.

Table 1 Correspondence between bases and phase difference.

Phase	B_0	$B_{\pi/2}$	B_π	$B_{3\pi/2}$
A_0	X_1	X_2	X_1	X_2
A_π	X_1	X_2	X_1	X_2

In Bob's decoding process, he sets a range of the value x of the homodyne measurement result: $x < -X_0$ or $x > X_0$. In this distribution area, we can distinguish the classical information 0 (when $x < -X_0$) or 1 (when $x > X_0$). In the area $-X_0 < x < X_0$, the state $|\pm i\alpha\rangle$ are overlapped and cannot be distinguished. This would induce an increasing of bit errors, so we omit it in our communication protocol. For the purpose of high efficiency and low error rate, we expect to set a proper X_0 in the range of pulsed continuous variable to avoid the overlapping of distribution function which cannot be distinguished by homodyne detection.

3 Security Analysis

The security of continuous variable quantum communication is guaranteed by the commutation relations of quadrature amplitudes. In our protocol, any eavesdropping behavior will be discovered in the security checking procedures. In the communication process, Alice chooses randomly part of her pulses with probabilities $p = 1 - p_1$ to check the security of communication and compare these results publicly with Bob in the two-round transmission. If the error rate is higher than the security bound, they believe that the channel is insecure, and the weak coherent pulses may be eavesdropped. Now we will discuss the two main kinds of eavesdropping strategies and show that our protocol is secure against them.

As analyzed in Ref. [26], the eavesdropper, so called Eve, performs an intercept-resend attack on the coherent states. She has two kinds of strategies:

(i) Eve blocks the coherent state pulses in the first round, measures them and sends fake pulses to Alice in certain states according to her results. She chooses to measure X_1 or X_2 basis, with half of the probabilities she gets the wrong results and increases the error rate in Alice's security checking procedures. Alice will discover Eve's existence by security checking and abort the transmission.

(ii) Eve eavesdrops the pulses which carries phase shift information added by Alice on them in the second round. Eve has to guess Alice's phase shift and choose to perform either X_1 or X_2 measurement. It is obvious that Eve cannot differentiate phase shift correctly. Since she did not know the original state, the result is completely random to her. Also this behavior will induce errors in the result when Bob performs his security checking in the last step of the protocol.

Next we will consider the Trojan-Horse attack in deterministic quantum key distribution. In this attack, since pulses are in the state $|\alpha e^{i\theta}\rangle$, Eve modulates a coherent pulse in the same state as the probe pulse. She then attaches her coherent pulses into each signal pulse with the same frequency in the time slot. The security checking process is similar to BB84 QKD.[1] Eve cannot modulate her pulses similar to Bob's signal pulses since the original phases of the signal coherent states are completely random for her. The signal state then becomes a mixed

coherent state. With probability $1-p_1$, her Trojan-Horse pulses pass the control path and been measured by Alice. If Alice happens to choose the same basis with Bob on such state and they should generate consistent results, i.e. the phase of signal pulse is $\pi/2$ at the time slot and Eve's pulse is $3\pi/2$. With $(1-p_1)/2$ probability, Alice chooses the right measuring basis which fits Bob's original state. Eve's pulses would induce errors during measurement on Alice's side. With $(1-p_1)/4$ probability, the legitimate parties find an increase of error rate and discover the existence of Eve.

4 Conclusion

In this study, we propose a protocol of deterministic quantum communication with pulsed homodyne detection. The coding strategy depends on the choice of phase difference on the local oscillator light and signal light. Keys are generated deterministically on Bob's side. It is a more practical method for quantum communication since the photodiodes are used instead of single photon detectors to perform homodyne detection. Moreover the efficiency depends on the threshold of X_0 and average photon number of weak laser pulses. Two-way security checking is needed in this protocol. The security is also discussed against intercept-resend and Trojan-Horse attacks. Eavesdropping behavior will increase the bit error rate on the communication parties and will be discovered.

References

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

[2] A.K. Ekert, Phys. Rev. Lett. **67** (1991) 661.

[3] C.H. Bennett, Phys. Rev. Lett. **68** (1992) 3121.

[4] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68** (1992) 557.

[5] G.L. Long and X.S. Liu, Phys. Rev. A **65** (2002) 032302.

[6] F.G. Deng and G.L. Long, Phys. Rev. A **68** (2003) 042315.

[7] G.L. Long, F.G. Deng, C. Wang, X.H. Li, K. Wen, and W.Y. Wang, Frontiers of Physics in China **2** (2007) 251.

[8] F. Gao, F.Z. Guo, Q.Y. Wen, and F.C. Zhu, Sci. in China G**51** (2008) 1853.

[9] C. Wang, F.G. Deng, Y.S. Li, X.S. Liu, and G.L. Long, Phys. Rev. A **71** (2005) 044305.

[10] C. Wang, F.G. Deng, and G.L. Long, Opt. Comm. **252** (2005) 15.

[11] P. Chen, Y.S. Li, F.G. Deng, and G.L. Long, Commun. Theor. Phys. **47** (2007) 49.

[12] W. Chen, Z.F. Han, X.F. Mo, F.X. Xu, G. Wei, and G.C. Guo, Chin. Sci. Bull. **53** (2008) 1310.

[13] C.Y. Li, X.H. Li, F.G. Deng, P. Zhou, and H.Y. Zhou, Chin. Sci. Bull. **52** (2007) 1162.

[14] T.C. Ralph, Phys. Rev. A **61** (1999) 010303.

[15] M. Hillery, Phys. Rev. A **61** (2000) 022309.

[16] M. Reid, Phys. Rev. A **62** (2000) 062308.

[17] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam, Phys. Rev. A **73** (2006) 0222316.

[18] T.C. Ralph, Phys. Rev. A **62** (2000) 062306.

[19] J.T. Jing, J. Zhang, Y. Yan, F.G. Zhao, C.D. Xie, and K.C. Peng, Phys. Rev. Lett. **90** (2003) 167903.

[20] F. Grosshans, Phys. Rev. Lett. **94** (2005) 020504.

[21] C.D. Xie, J. Zhang, Q. Pan, X.J. Jia, and K.C. Peng, Frontiers of Physics in China **1** (2006) 383.

[22] H.Y. Fan and X.T. Liang, Commun. Theor. Phys. **44** (2005) 833.

[23] D.H. Wu, P. Dong, M. Yang, and Z.L. Cao, Commun. Theor. Phys. **49** (2008) 877.

[24] F. Grosshans, G. Van. Assche, and J. Wenger, Nature (London) **421** (2003) 238.

[25] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68** (2003) 042331.

[26] R. Namiki and T. Hirano, Phys. Rev. A **67** (2003) 022308.

[27] R. Namiki and T. Hirano, Phys. Rev. Lett. **92** (2004) 117901.

[28] R. Namiki and T. Hirano, Phys. Rev. A **72** (2005) 024301.

[29] F.G. Deng and G.L. Long, Phys. Rev. A **70** (2004) 012311.