Experimental Demonstration of Passive-Decoy-State Quantum-Key-Distribution with Two Independent Lasers

Shi-Hai Sun[1,2*], Guang-Zhao Tang[1,2], Chun-Yan Li[1,2], and Lin-Mei Liang[1,2,3]
[1] *College of Science, National University of Defense Technology, Changsha 410073, P.R.China*
[2] *Interdisciplinary Center for Quantum Information, National University of Defense Technology, Changsha 410073, P.R.China*
[3] *State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, P.R.China*

Introduction- Quantum key distribution (QKD) [1] admits two parties to share an unconditional secret key, which is guaranteed by the basic principle of quantum mechanics. Until now, high-speed and long-distance QKD have been implemented. However, due to the imperfection of practical electrical and optical setups, potential loopholes in practical QKD systems could be exploited by an eavesdropper (Eve) to spy the final secret key. One of the most famous cat-and-mouse games is the photon-number-splitter (PNS) attack and decoy state method. Due to the unavailability of the single photon source, phase randomized weak coherent source (PR-WCS) is always used in many practical QKD systems. However, the multi photon pulse of the PR-WCS will be exploited by Eve. Then the secret key rate will be dramatically decreased and the maximal secret distance will be limited within tens of kilometers. In order to defeat such loophole, decoy state method was proposed to strictly estimate the yield and error rate of single photon pulses.

In this paper we experimentally demonstrate the phase-encoding passive decoy state QKD with two independent lasers. The visibility of Hong-Ou-Mandel (HOM) interference for the homemade independent lasers reaches 0.53($\pm$0.003). Then different decoy states could be passively generated based on the respondence of Alice's threshold single photon detector (SPD). Finally, the secret key rate about 1.5×10^{-5}/pulse is obtained with about 10km commercial fiber between Alice and Bob. Our results show that the passive decoy state method with practical PR-WCS is possible and has potential applications in practices.

The passive decoy state method was proposed in Ref.[2]. The basic setup of the passive decoy state method is shown in Fig.1(a) (a). Two independent lasers (noted as LD1 and LD2 respectively) with different intensities interfere at a beam splitter (BS1). The transmittance of BS1 is noted as t. Alice measures the light in one mode of the BS (mode b) with a SPD (noted as SPDa). When the SPD clicks, Alice notes the pulses in mode a of the BS1 as signal state, otherwise, she notes them as decoy state. The density matrixes of LD1 and LD2 are given by

$$\rho=e^{-\mu_1}\sum_{n=0}^{\infty}\frac{\mu_1^n}{n!}|n\rangle\langle n|,\ \ \sigma=e^{-\mu_2}\sum_{n=0}^{\infty}\frac{\mu_2^n}{n!}|n\rangle\langle n|, \tag{1}$$

here μ_1 and μ_2 are the average intensities of LD1 and LD2, respectively. The joint probability that n photons in mode a of BS1 and m photons in mode b of BS1 can be written as

$$P_{n,m}=\frac{\nu^{n+m}e^{-\nu}}{2\pi n!m!}\int_0^{2\pi}\gamma^n(1-\gamma)^m d\theta, \tag{2}$$

where

$$\begin{aligned}\nu&=\mu_1+\mu_2,\\ \gamma&=\frac{\mu_1 t+\mu_2(1-t)+\xi\cos(\theta)}{\nu},\\ \xi&=2\sqrt{\mu_1\mu_2(1-t)t}.\end{aligned} \tag{3}$$

Then the joint probability that n photons in mode a of BS1 and no click in SPDa, and the joint probability that n photons in mode a of BS1 and SPDa clicks are given by

$$\begin{aligned}P_n^{nc}&=(1-\epsilon)\sum_{m=0}^{\infty}(1-\eta_d)^m P_{n,m},\\ P_n^{c}&=\sum_{m=0}^{\infty}P_{n,m}-P_n^{nc}\equiv P_n^t-P_n^{nc}.\end{aligned} \tag{4}$$

Here the subscript nc (or c) means the SPD of Alice doesn't click (or clicks). ϵ and η_d are the dark count rate and efficiency of SPDa. It is easy to check that the probability distributions of P_n^{nc} and P_n^c are non-Poisson.

Then Alice and Bob could estimate the secret key rate by combining the the GLLP formula [**?**] and the idea of decoy state method, which is given by Ref.[2]

$$R\geq\sum_l\max\{R^l,0\}, \tag{5}$$

where $l\in\{c,nc\}$ which means SPDa clicks or doesn't

*shsun@nudt.edu.cn

click, and

$$R^l \geq q\{-Q^l f(E^l)H(E^l) + (P_1^l Y_1^L + P_0^l Y_0^L)[1 - H(e_1^U)]\}. \tag{6}$$

Here q is the efficiency of the QKD protocol ($q = 1/2$ for BB84 protocol [1]); $f(E^l)$ is the efficiency of the error correction protocol; Q^l (E^l) is the total gain(error rate); Y_1^L (e_1^U) is the lower bound of yield (upper bound of error rate) of the single photon pules. Y_0^L is the lower bound of dark count rate of Bob's SPD. P_1^l (P_0^l) is the probability of single photon pules (vacuum pulse).

Finally, according to theoretical analysis of Ref.[2], the lower bound of yield and the upper bound of the error rate for the single photon pulse are given by

$$\begin{aligned} P_1^l Y_1^L + P_0^l Y_0^L =& \max\{\frac{P_1^l(P_2^t Q^{nc} - P_2^{nc} Q^t)}{P_2^t P_1^{nc} - P_2^{nc} P_1^t} \\ &+ [P_0^l - P_1^l \frac{P_2^t P_0^{nc} - P_2^{nc} P_0^t}{P_2^t P_1^{nc} - P_2^{nc} P_1^t}] Y_0^U, 0\}, \end{aligned} \tag{7a}$$

$$\begin{aligned} e_1^U =& \min\{\frac{E^c Q^c - P_0^c Y_0^L e_0}{P_1^c Y_1^L}, \frac{E^{nc} Q^{nc} - P_0^{nc} Y_0^L e_0}{P_1^{cn} Y_1^L}, \\ & \frac{P_0^{nc} E^t Q^t - P_0^t E^{nc} Q^{nc}}{(P_1^t P_0^{nc} - P_1^{nc} P_0^t) Y_1^L}\}, \end{aligned} \tag{7b}$$

where $e_0 = 1/2$ is the error rate of background, and

$$\begin{aligned} Y_0^U &= \min\{\frac{E^c Q^c}{P_0^c e_0}, \frac{E^{nc} Q^{nc}}{P_0^{nc} e_0}\}, \\ Y_0^L &= \max\{\frac{P_1^t Q^{nc} - P_1^{nc} Q^t}{P_1^t P_0^{nc} - P_1^{nc} P_0^t}, 0\}, \\ Q^t &= Q^c + Q^{nc}, \\ Q^t E^t &= Q^c E^c + Q^{nc} E^{nc}. \end{aligned} \tag{8}$$

Experiment- The non-Poisson source is generated with two PR-WCS. The generation setups of the non-Poisson is shown in Fig.1, in which two PR-WCS interfere at a beam splitter (BS1). One mode of BS1 (noted as mode b) is measured with a SPD (noted as SPDa in experiment since the detector belongs to Alice), and the other mode of BS1 (note as mode a) is used as signal state or decoy state depending the click of the SPDa. Note that although two weak coherent lights are used to passively generate the signal state and decoy state in our experiment, it is still possible to generate the non-Poisson source with strong coherent light combining with classical threshold detector [2].

In order to ensure that the pulses from LD1 and LD2 could interfere at the BS1, the photons should be indistinguishable in polarization, spectrum, time. Any mismatch in these dimensions will affect the photon number distribution of different decoy states, and then worsen the performance of the passive decoy state QKD protocol.

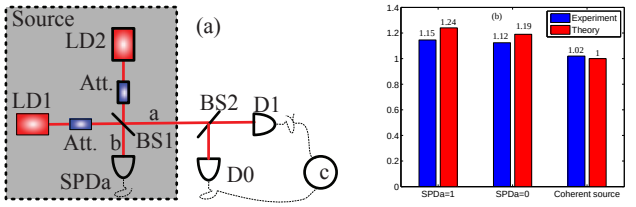

FIG. 1: (Color online) Non-Poisson source generation and HBT experiment. (a) shows the setups for the non-Poisson source generation and the scheme for HBT experiments. (b) shows the measured g^2 for the generated non-Poisson source. Here $SPDa = 1$ (and $SPDa = 0$)means the SPDa clicks (and non-clicks). The standard deviation of the experimental results are 0.06, 0.03 and 0.03 for $SPDa = 1$, $SPDa = 0$ and the coherent source, respectively. For each case, the blue bar (right) and the red bar (left) show the experimental results and theoretical values, respectively. The accumulated time for each bar is 600s.

The polarization is automatically matched using polarization maintain fiber from the laser diodes to the BS1 in our experiment. Although, strictly speaking, the axes of the fiber may mismatch in practical experiment, the error introduced by it is small. The butterfly DFB laser diode is used in our experiment, whose 3dB width of spectrum is about 60pm. By carefully modulating the temperature of the laser diode, the difference of the center wavelength between LD1 and LD2 can be set small enough. In our experiment, the center wavelength of laser diodes is set as 1559nm with difference less than 10pm, which is less than the spectrum of the laser diodes. The major difficult for the HOM interference between two independent lasers is the arriving time of the photons. In order to increase the visibility of HOM interference, a homemade electrical delay with step 10ps is used to adjust the trigger time of LD1 and LD2. With the technologies given above, the visibility of HOM interference 0.53 ± 0.003 is measured.

To evaluate the non-Poisson statistics of the two kinds of pulses, signal state for SPDa click and decoy state for SPDa non-click, a HBT experiment is performed with two SPDs (ID201, Idquantique). Here, we use the correlation function of optical pulses, $g^{(2)}$, to characterize the non-Poisson statistics of the pules. In our experiment, the average intensity of LD1 (and LD2) is set as 0.64 (and 0.08). Then the theoretical predictions of $g^{(2)}$ for signal state (SPDa click) and decoy state (SPDa non-click) are 1.24 and 1.19, respectively. With the experimental setups of Fig.1, the measured $g^{(2)}$ is 1.15 with standard deviation 0.06 for the pulses that SPDa clicks, and 1.12 with standard deviation 0.03 for the pulses that SPDa non-clicks. All the results are shown in Fig.1(b). Here we also measure $g^{(2)}$ for the coherent state. The measured $g^{(2)}$ is 1.02 with standard deviation 0.03, which is very close the theoretical prediction of 1.

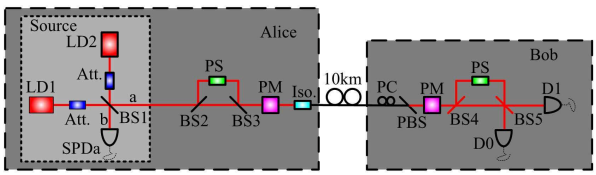

FIG. 2: (Color online) Schematic setup for QKD protocol. LD1 and LD2 are distributed feedback laser diodes. Att. is attenuator used to modulate the intensity of signal pulses from LD1 and LD2. BS: beam splitter; PS: phase shift; PM: phase modulator; Iso.: isolator; PC: polarization controller; PBS: polarization beam splitter. SPDa is the single photon detector of Alice, which is used to determine that the pulse is signal state or decoy state depending on the click of it. D0 and D1 are single photon detectors of Bob. The red lines are polarization maintain fiber. Alice and Bob are connected with about 10km commercial fiber.

Then with the non-poisson source given above, we perform the QKD based on BB84 protocol. The setups are shown in Fig.2. The pulses on mode a pass through the UMZI, in which a phase shift (PS) is used to compensate the phase between the long arm and short arm. The encoding phase of Alice is modulated on the pulses that pass through the short-arm of the UMZI with a phase modulator (PM). At the same time, in order to remove the Trojan-horse attack [3], an isolator is used to stop any light to be injected into Alice's zone form channel. When the pulses arrive at Bob's zone, the polarization is controlled by combing a polarization controller (PC) and a polarization beam splitter (PBS). The decoded phase of Bob is modulated on the pulsed that pass through the long arm of Alice's UMZI. Then Bob uses a UMZI and two SPDs (D0 and D1) to measure Alice's information.

The repetition frequency of our system is 2.5MHz, which is limited by the maximal repetition of Bob's SPD (iD201, Idquantique). The intensities of LD1 and LD2 are set as about 0.64 and 0.08, respectively. And the transmittance of BS1 is 0.5 in our experiment. Then pulses on mode b of BS1 are detected by Alice's SPD, whose dark-count rate is about 1.2×10^{-5}/pulse with a gate width of 2.5ns and an efficiency of 10%. Then final secret key rate is estimated. All the experimental results are listed in Table I. Note that strictly speaking, the statistical fluctuation of the intensity of LD1 and LD2 should be taken into in the estimation of final key rate. However, as a proof-of-principle proof, we assume the intensities of LD1 and LD2 are stable in this paper. By controlling the temperature of laser diodes, the intensities of LD1 and LD2 are very stable. In fact, the measured standard deviations in one hour for LD1 and LD2 are 0.005 and 0.001, respectively.

In our experiment, the estimated final secret key rate is about 1.50×10^{-5}/pulse with only 10km commercial fiber between Alice and Bob. The secret key rate is much lower than the active decoy state QKD experiment. The main reason is that, in passive decoy state method, the intensity of Alice's pulses should be attenuated to weak light before the BS1, but not at the end port of Alice (after the Iso.). Thus the loss of Alice's optical setups should be taken into account in the passive decoy state method (generally speaking, the loss of Alice's optical setups could be ignored in the active decoy state method). This drawback could be improved to enhance the performance of the passive decoy state method. First, the loss of Alice's optical setups is about 9dB in our experiment, which could be reduced by using low loss optical devices. Second, as a proof-of-principle experiment, the parameters are not optimized in our experiment, thus the final key rate could be increased by optimizing all the experimental parameters. Third, the legitimate parties could use the strong coherent light scheme to replace the weak coherent light scheme [2].

TABLE I: Experimental results of our experiment. Here, N is the length of collected data; t is the transmittance of BS1; μ_1 (μ_2) is the average photon number of LD1 (LD2); E^c (E^{nc}) is the total error rate given that Alice's SPD clicks (does not click); Q^c (Q^{nc}) is the total gain given that Alice's SPD click (does not click); R is the final secret key rate. $f(E) = 1.22$. The accumulated time for the experiment that measures the stability of lasers is one hour.

Parameter	Result	Parameter	Result
μ_1	$0.64(\pm0.005)$	μ_2	$0.08(\pm0.001)$
E^c	$6.13(\pm3.42)\%$	E^{nc}	$5.55\ (\pm0.52)\%$
Q^c	$2.54(\pm0.35)\times10^{-6}$	Q^{nc}	$8.18(\pm0.21)\times10^{-5}$
R	1.50×10^{-5}		

Conclusion- In this paper, the phase-encoding passive decoy state QKD has been experimentally implemented with only linear optical setups and threshold SPDs. The different decoy states could be generated based on the HOM interference with two homemade independent pulsed lasers. The visibility of HOM interference reaches $0.53(\pm0.003)$ by modulating the central wavelength with temperature controller and the arriving time with electrical delay chip. The final secret key rate 1.50×10^{-5}/pulse is obtained.

[1] C. H. Bennett, and G. Brassard. *International Conference on Computers, Systems and Signal Processing*, Bangalore, India. New York: IEEE. p.175-179 (1984).
[2] M. Curty, X. F. Ma, B. Qi, and T. Moroder. *Phys. Rev. A* **81**, 022310 (2010).
[3] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. *Phys. Rev. A* **73**, 022320 (2006).