Experimental demonstration of passive decoy state quantum key distribution*

Zhang Yang(张 阳), Wang Shuang(王 双)†, Yin Zhen-Qiang(银振强)‡, Chen Wei(陈 巍), Liang Wen-Ye(梁文烨), Li Hong-Wei(李宏伟), Guo Guang-Can(郭光灿), and Han Zheng-Fu(韩正甫)

Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Sciences, Hefei 230026, *China*

(Received 12 April 2012; revised manuscript received 21 June 2012)

Passive decoy state quantum key distribution (PDS-QKD) has advantages in high-speed scenarios. We propose a modified model to simulate the PDS-QKD with a weak coherent light source based on Curty's theory [*Opt. Lett.* **34** 3238 (2009)]. The modified model can provide better performance in a practical PDS-QKD system. Moreover, we report an experimental demonstration of the PDS-QKD of over 22.0-dB channel loss.

Keywords: quantum key distribution, passive decoy state method

PACS: 03.67.Dd **DOI:** 10.1088/1674-1056/21/10/100307

1. Introduction

Quantum key distribution (QKD)[1−3] provides a method to exchange keys between two legal parties (Alice and Bob), regardless of the computational and technological power of the eavesdropper (Eve). The security is guaranteed by quantum mechanics. Many research groups have realized point-to-point QKD systems or QKD networks,[2−9] and focus on the analysis and simulation of practical QKD systems and imperfect devices.[3,10.11]

The QKD protocols of BB84 class are based on a single-photon source, which is still beyond the practical implementation capabilities at present. As a result, weak coherent light sources are used instead in practical QKD systems. This kind of light source occasionally emits multiple-photon pulses, which is vulnerable to the photon-number-splitting attack.[12−14] Hwang *et al.* have proposed the decoy state method to overcome the photon-number-splitting attack.[15−18] Most decoy state QKD experiments employ the variable optical attenuator to modulate the intensity of the light pulse actively. By contrast, the decoy state QKD schemes based on passive optical elements[19−22] reduce electronic controller difficulty, and have advantages especially in high-speed QKD scenarios. In addition, it is less possible for Eve to distinguish between decoy and signal states in the passive decoy state method.[21] In 2009, Curty *et al.* proposed a convenient method to obtain a non-Poissonian light source,[23,24] which could be a crucial element to realize the passive decoy state QKD (PDS-QKD). Our preliminary work experimentally implemented an intrinsic-stable non-Poissonian light source based on Curty's theory.[25] In this paper, we modify the simulation model for a practical PQS-QKD system based on Curty's protocol when employing a weak coherent light source, and obtain a better key generation rate under the same condition. Then an experimental PDS-QKD system is accomplished over 22.0-dB channel loss.

2. Modified model

The modified model of a practical PDS-QKD system is shown in Fig. 1. The part inside the dashed square is the non-Poissonian light source scheme proposed in Ref. [23]. The interference of two Fock diagonal states at the beam splitter makes the pulses out

*Project supported by the National Basic Research Program of China (Grants Nos. 2011CBA00200 and 2011CB921200), the National Natural Science Foundation of China (Grant Nos. 60921091 and 61101137), and the China Postdoctoral Science Foundation (Grant Nos. 20100480695 and 2012M511419).

†Corresponding author. E-mail: wshuang@ustc.edu.cn

‡Corresponding author. E-mail: yinzheqi@mail.ustc.edu.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

of port a obey a non-Poissonian distribution. Monitoring the detection results in port b, Alice and Bob can treat no-click and click events differently to employ the decoy state QKD.[23] Before the pulses enter into the public channel, they will be attenuated in the practical PDS-QKD system by some optical elements, such as the phase modulator, to encode the pulses. The loss in Alice's side cannot be ignored as the active decoy state method usually does. Curty *et al.* have analyzed the setup in the dashed square while using a weak coherent light source.[23,24] However, an attenuator of transmittance t_2 should be added into the model of transmitter. Then the modified model can be analyzed as follows.

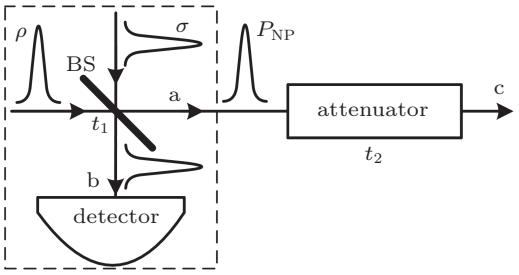


Fig. 1. Modified model, where BS stands for the beam splitter, and the transmittance is $t_1 = 1/2$.

In Fig. 1, two phase-randomized weak coherent laser pulses,

$$\rho = \mathrm{e}^{-\mu_1} \sum_{n=0}^{\infty} \frac{{\mu_1}^n}{n!} |n\rangle\langle n|$$

and

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

interfere at the beam splitter, where μ_1 and μ_2 denote the mean photon numbers. The joint probability of having n photons in port c and m photons in port b is

$$p_{n,m} = \frac{1}{2\pi} \int_0^{2\pi} \frac{(\nu\gamma t_2)^n \, \mathrm{e}^{-\nu\gamma t_2}}{n!} \times \frac{[\nu(1-\gamma)]^m \, \mathrm{e}^{-\nu(1-\gamma)}}{m!} \mathrm{d}\theta, \quad (1)$$

where $\nu = \mu_1 + \mu_2$, $\gamma = [\mu_1 t_1 + \mu_2(1-t_1) + \xi\cos\theta]/\nu$, and $\xi = 2\sqrt{\mu_1\mu_2(1-t_1)t_1}$. The probability of having n photons in port c obeys the non-Poissonian distribution, which can be given as

$$p_n^t = \sum_{m=0}^{\infty} p_{n,m} = \frac{\nu^n}{n!} \frac{1}{2\pi} \int_0^{2\pi} (\gamma t_2)^n \, \mathrm{e}^{-\nu\gamma t_2} \, \mathrm{d}\theta. \quad (2)$$

As the threshold detector produces no click in port b, the joint probability of finding n photons in port c can be expressed as

$$p_n^{\bar{c}} = (1-\epsilon) \sum_{m=0}^{\infty} (1-\eta_d)^m p_{n,m} = (1-\epsilon) \frac{\nu^n \, \mathrm{e}^{-\eta_d \nu}}{n!} \frac{1}{2\pi} \int_0^{2\pi} (\gamma t_2)^n \, \mathrm{e}^{-\nu\gamma(t_2-\eta_d)} \mathrm{d}\theta, \quad (3)$$

where η_d and ϵ indicate the quantum efficiency and the dark count rate of the monitor detector, respectively.

Conversely, we obtain the joint probability of finding n photons in port c and a click in the monitor detector as $p_n^c = p_n^t - p_n^{\bar{c}}$. The conditional photon number distribution in port c varies owing to the monitor's results

$$q_n^c = p_n^c/(1-N_W), \qquad q_n^{\bar{c}} = p_n^{\bar{c}}/N_W, \quad (4)$$

$$N_W = \sum_{n=0}^{\infty} p_n^{\bar{c}} = (1-\epsilon) \, \mathrm{e}^{-\eta_d[\mu_1(1-t_1)+\mu_2 t_1]} \, \mathrm{I}_{0,\eta_d\xi}, \quad (5)$$

where

$$\mathrm{I}_{q,z} = \frac{1}{2\pi} \int_0^{2\pi} \cos(q\theta) \, \mathrm{e}^{z\cos\theta} \, \mathrm{d}\theta$$

stands for the modified Bessel function of the first kind.

Consequently, the gain Q and the quantum bit error rate (QBER) E can be calculated in the following equations

$$Q^{\bar{c}} = \sum_{n=0}^{\infty} p_n^{\bar{c}} Y_n = N_W - (1-\epsilon)(1-Y_0) \times \mathrm{e}^{(\eta_d - \eta_{\rm sys} t_2)\omega - \eta_d \nu} \, \mathrm{I}_{0,(\eta_d - \eta_{\rm sys} t_2)\xi}, \quad (6)$$

$$Q^{\bar{c}} E^{\bar{c}} = \sum_{n=0}^{\infty} p_n^{\bar{c}} Y_n e_n = (e_0 - e_d) Y_0 N_W + e_d Q^{\bar{c}}, \quad (7)$$

$$Q^t = \sum_{n=0}^{\infty} p_n^t Y_n = 1 - (1-Y_0) \, \mathrm{e}^{-\eta_{\rm sys}\omega t_2} \, \mathrm{I}_{0,\eta_{\rm sys} t_2 \xi}, \quad (8)$$

$$Q^t E^t = \sum_{n=0}^{\infty} p_n^t Y_n e_n = (e_0 - e_d) Y_0 + e_d Q^t, \quad (9)$$

where $\omega = \mu_1 t_1 + \mu_2(1-t_1)$, $Y_n = 1-(1-Y_0)(1-\eta_{\rm sys})^n$, and $Y_n e_n = Y_0 e_0 + (Y_n - Y_0) e_d$. The parameter $\eta_{\rm sys} = \eta_{\rm Bob} 10^{-\alpha d/10}$ is the overall transmittance, which includes the loss in Bob's apparatus and the public channel, and we assume $\alpha = 0.21$ dB/km in the simulation. The Y_n and e_n represent the yield rate and the error rate of an n-photon signal, respectively. And e_d is the probability that a signal hits Bob's detector by mistake due to the misalignment of the interferometer. All these parameters are the same as those in Refs. [18] and [24].

The key generation rate Eqs. (4), (5), (A5), (A10), (A12), (A16), and (A18) in Ref. [24] are still valid in

our modified model. We provide explicit expressions for p_n^t and $p_n^{\bar{c}}$ with $n = 0, 1, 2$

$$p_0^t = \mathrm{e}^{-\omega t_2}\, \mathrm{I}_{0,\xi t_2}, \tag{10}$$

$$p_1^t = t_2\, \mathrm{e}^{-\omega t_2}(\omega\, \mathrm{I}_{0,\xi t_2} - \xi\, \mathrm{I}_{1,\xi t_2}), \tag{11}$$

$$p_2^t = \frac{t_2^2\, \mathrm{e}^{-\omega t_2}}{2}\left[\left(\omega^2 + \frac{\xi^2}{2}\right)\mathrm{I}_{0,\xi t_2} - 2\omega\xi\, \mathrm{I}_{1,\xi t_2} + \frac{\xi^2}{2}\, \mathrm{I}_{2,\xi t_2}\right], \tag{12}$$

$$p_0^{\bar{c}} = \tau\, \mathrm{I}_{0,(t_2-\eta_d)\xi}, \tag{13}$$

$$p_1^{\bar{c}} = \tau t_2[\omega\, \mathrm{I}_{0,(t_2-\eta_d)\xi} - \xi\, \mathrm{I}_{1,(t_2-\eta_d)\xi}], \tag{14}$$

$$p_2^{\bar{c}} = \frac{\tau t_2^2}{2}\left[\left(\omega^2 + \frac{\xi^2}{2}\right)\mathrm{I}_{0,(t_2-\eta_d)\xi} - 2\omega\xi\, \mathrm{I}_{1,(t_2-\eta_d)\xi} + \frac{\xi^2}{2}\, \mathrm{I}_{2,(t_2-\eta_d)\xi}\right], \tag{15}$$

where $\tau = (1-\epsilon)\, \mathrm{e}^{-[\eta_d \nu + (t_2-\eta_d)\omega]}$.

We assume that $t_2 = 0.2$ and the standard BB84 protocol is adopted,[1] the simulation is based on the parameters of the GYS experiment.[4] The results in Fig. 2 indicate that the optimized parameters μ_1 and μ_2 prolong the secure distance, and the maximum secure distance is about 128.25 km. Note that the optimal parameters should be analyzed based on the value of t_2 in different QKD protocols.

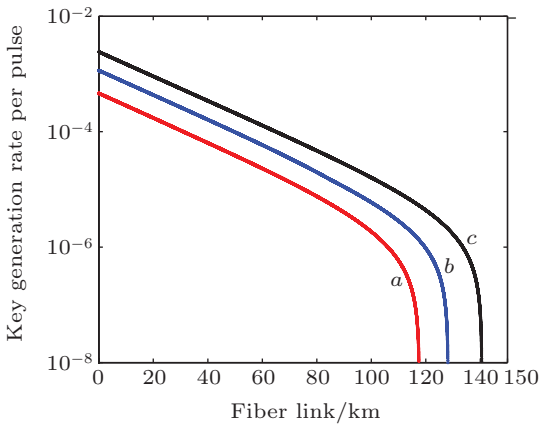


Fig. 2. (colour online) Simulation results for the practical QKD system: curve a for PDS-QKD, $\mu_1 = 0.5$, $\mu_2 = 10^{-4}$, the optimal parameters proposed in Ref. [24]; curve b for PDS-QKD, $\mu_1 = 1.7$, $\mu_2 = 10^{-4}$, based on the modified model; curve c for active two-decoy-state QKD with weak coherent pulse.[18]

3. Proof-of-principle experiment

To demonstrate this scheme, we performed the PDS-QKD experiment based on the non-Poissonian light source[25] and the Faraday–Michelson system (FMI),[5–9] as shown in Fig. 3. The non-Poissonian light source is inside the dashed square. The 1550-nm laser emitted the light pulses at the frequency of 1 MHz. The 1:99 beam splitter (BS_1) transmitted most of the power to the synchronous detectors (Syn), which were designed to trigger the single photon detectors (SPD). The pulses were attenuated by an electronic variable optical attenuator (EVOA) to guarantee that $\mu_1 = 2$, $\mu_2 = 0.5$. To reveal the physical process clearly, the optimal parameters μ_1 and μ_2 were not chosen to avoid the situation that the yield rates of click and no-click events cannot be distinguished obviously.[24] The monitor detector, IDQ id200 $\mathrm{SPD_M}$, had a quantum efficiency of 6.6% and a dark count rate of 8.1×10^{-6} per 2.5-ns gate. Since Faraday rotator mirrors (FM) can change any incoming polarization state into its orthogonal state, they were employed to solve the instability owing to the polarization-dependent loss and the polarization mode dispersion of the single mode communication fiber.[2,5] Half of the pluses were blocked by the intensity modulator (IM),[24] so the security analysis in Ref. [10] can be applied in this scheme.

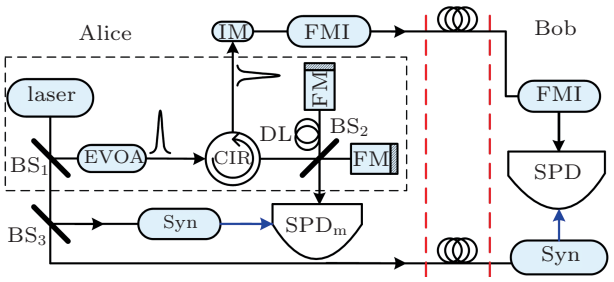


Fig. 3. (colour online) PDS-QKD system, where CIR stands for the circulator, and DL is the 200-m delay line.

The BB84 phase-coding protocol[1,2] was realized in the system. The pulses through Alice's FMI were encoded randomly by one of $\{\{0, \pi\}, \{\pi/2, 3\pi/2\}\}$. The transmittance between the light source and the public channel was $t_2 = 0.187$. Bob also decoded the pulses randomly by one of $\{\{0, \pi\}, \{\pi/2, 3\pi/2\}\}$, and employed only one IDQ id200 SPD. The quantum efficiency was 6.16%, and the dark count rate was 1.2×10^{-6} per 2.5-ns gate. After declaring the basis set selected in every time bin when Bob detected photons, the sifted keys with the same basis sets were kept. The experimental results are listed in Table 1. We tested the system over different channel losses respectively, then distilled the secret keys from both click and no-click events. The experiment finally got the key generation rate based on the GLLP formula[10,24] and the modified model, which indicated the feasibility of the PDS-QKD protocol. Figure 4 shows the experimental results and the simulation results based on the parameters in our experiment.

Table 1. QKD experiment results, where CL is the channel loss, and KGR is the key generation rate per pulse.

CL/dB	Monitor	Ratio	Yield rate	QBER	KGR
10.3	click	8.0%	7.57×10^{-5}	1.21%	–
	no-click	92.0%	1.10×10^{-4}	0.99%	–
	total	100%	1.07×10^{-4}	1.00%	3.85×10^{-5}
14.9	click	8.1%	2.59×10^{-5}	2.91%	–
	no-click	91.9%	3.91×10^{-5}	2.15%	–
	total	100%	3.80×10^{-5}	2.19%	8.85×10^{-6}
22.0	click	8.0%	6.14×10^{-6}	6.40%	–
	no-click	92.0%	8.68×10^{-6}	5.77%	–
	total	100%	8.48×10^{-6}	5.81%	6.23×10^{-7}

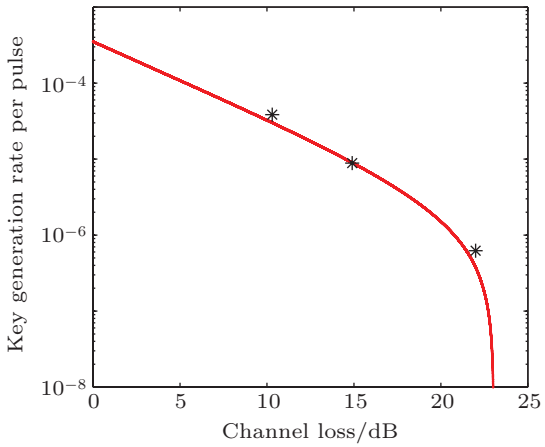


Fig. 4. (colour online) Simulation and experiment results, where the red line is the simulation result based on experimental parameters, and $e_d = 0.006$, $\eta_{\rm Bob} = 0.00516$; the star points are obtained directly from experiment.

4. Conclusion

In summary, we proposed a modified model for a practical passive decoy state QKD system employing the non-Poissonian light source produced from a weak coherent light source. The simulation results showed that the modified model could provide a better reference to set parameters in the experiments. Combining the intrinsic-stable light source with the Faraday–Michelson system, we performed a proof-of-principle demonstration of the passive decoy state QKD. This kind of QKD protocol is attractive because of its potential and advantage for high-speed applications.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE Int. Conf. on Computers, Systems and Signal Processing* Bangalore, India, p. 175

[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[3] Scarani V, Bechmann-Pasquinucci H, Cerf M, Dušek N J, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[4] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[5] Mo X F, Zhu B, Han Z F, Gui Y Z and Guo G C 2005 *Opt. Lett.* **30** 2632

[6] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L and Guo G C 2008 *Chin. Phys. Lett.* **25** 3547

[7] Chen W, Han Z F, Zhang T, Wen H, Yin Z Q, Xu F X, Wu Q L, Liu Y, Zhang Y, Mo X F, Gui Y Z, Wei G and Guo G C 2009 *IEEE Photon. Technol. Lett.* **21** 575

[8] Xu F X, Chen W, Wang S, Yin Z Q, Zhang Y, Liu Y, Zhou Z, Zhao Y B, Li H W, Liu D, Han Z F and Guo G C 2009 *Chin. Sci. Bull.* **54** 2991

[9] Wang S, Chen W, Yin Z Q, Zhang Y, Zhang T, Li H W, Xu F X, Zhou Z, Yang Y, Huang D J, Zhang L J, Li F Y, Liu D, Wang Y G, Guo G C and Han Z F 2010 *Opt. Lett.* **35** 2454

[10] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Infor. Comput.* **4** 325

[11] Liu D, Yin Z Q, Wang S, Wang F M, Chen W and Han Z F 2012 *Chin. Phys.* B **21** 060202

[12] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863

[13] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[14] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[15] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[16] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[17] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[18] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326

[19] Mauerer W and Silberhorn C 2007 *Phys. Rev.* A **75** 050305

[20] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503

[21] Ma X and Lo H K 2008 *New J. Phys.* **10** 073018

[22] Xu F X, Wang S, Han Z F and Guo G C 2010 *Chin. Phys.* B **19** 100312

[23] Curty M, Moroder T, Ma X and Lütkenhaus N 2009 *Opt. Lett.* **34** 3238

[24] Curty M, Ma X, Qi B and Moroder T 2010 *Phys. Rev.* A **81** 022310

[25] Zhang Y, Chen W, Wang S, Yin Z Q, Xu F X, Wu X W, Dong C H, Li H W, Guo G C and Han Z F 2010 *Opt. Lett.* **35** 3393