Practical high-speed light source for decoy-state quantum key distribution

Haibin Du (杜海彬)[1], Yan Liang (梁 焰)[1], Shengxiang Zhang (张盛祥)[1], Xiuliang Chen (陈修亮)[1], Lin Zhao (赵 林)[1], Jie Chen (陈 杰)[2], and Heping Zeng (曾和平)[1,2*]

[1]*State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, China*

[2]*Shanghai Key Laboratory of Modern Optical System, Engineering Research Center of Optical Instrument and System, Ministry of Education, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China*

[*]*Corresponding author: hpzeng@phy.ecnu.edu.cn*

Received January 22, 2014; accepted April 23, 2014; posted online June 26, 2014

High-speed light source is realized for decoy-state quantum key distribution (QKD) at telecom wavelength of 1.55 μm. By implementing two different electrical pulses together and triggering with 100 MHz pseudo-random number to drive the laser diode, the signal-state and the decoy-state pulses are prepared with identical pulse duration of 25 ps and similar spectral characteristics, avoiding the eavesdropper's attack by temporal and spectral analysis. The intensity fluctuation of the light source is quantified to satisfy the practical decoy-state QKD with random intensity error. The characteristics of the light source are analyzed with a high-speed single-photon detector.

OCIS codes: 270.5568, 270.5565, 140.5960, 040.1345.

doi: 10.3788/COL201412.072702.

Quantum key distribution (QKD) provides a reliable way to share secure key between two legitimate users[1,2]. The key is then used for encryption and decryption of the message by one-time pad method through a classical channel, proving unconditional security. Since 1984, various QKD protocols have been put forward and achieved in experiments, such as BB84, B92, and EPR[3−11]. On the other hand, various eavesdropping scenarios were considered against practical experimental implementation of these protocols. Preventing QKD systems from eavesdropping[12−15], such as photon number splitting (PNS) attacks, is always the top research subjects in quantum cryptographic studies. Decoy-state QKD has recently raised quite a lot of research interests especially due to its robustness against eavesdropper for practical implementation[16−19].

In the 3-intensity decoy-state QKD[16,17], the photon source is quite important. The light source should be capable of producing photon pulses of three different photon intensities (u, v_1, v_2) including the signal-state photons for carrying the key information, the decoy-state photons and the vacuum-state photons for verifying the security. The decoy-state and vacuum-state pulses should be lurked among the signal pulses randomly. By estimating the loss of the decoy pulses, Alice and Bob could observe the change on the signal or the error rate if attacks to the system exist. The decoy-state light source should fulfill the following requirements. Firstly, the number proportion of the signal pulse, the decoy pulse, and the vacuum pulse should be fixed. And for each state, the photon number statistic should obey the Poissonian distribution. Secondly, the average photon number for vacuum pulses should be as close to zero as possible for the optimal efficiency of the key distillation. Although in the QKD experiment by Lucamarini *et al.*, the vacuum state pulses were prepared with average photon number of 0.001 and a record secure rate of 1.09 Mbps of 50 km was obtained with special protocol[20], in the standard decoy-state BB84 protocol, the protocol was most efficient when v_2=0[21]. Finally, the temporal and spectral properties of the decoy pulses should be identical to the signal pulses to avoid the identification of the different states by temporal or spectral analysis.

In the original scheme of decoy-state QKD, a weak coherent pulse from an attenuated laser served as the light source[22]. With improvement of the decoy-state QKD toward high security and high speed, various experiments have been carried out in recent years[21,23,24]. Usually, for simplicity, two lasers of different intensities are triggered randomly to generate signal-state and decoy-state photons, respectively[25,26]. However, it is quite difficult to set two separate lasers to output pulses of exactly the same temporal and spectral profiles. The optical difference on the two laser sources unavoidably leaves a security hole to the eavesdropper. On the other hand, optical intensity modulators are often used to enforce the decoy protocol, especially in high speed QKD experiments. As an external modulation method, all the pulses plunged into the intensity modulator are from the same laser diode (LD), thus the temporal and spectral characteristics of signal pulses and decoy pulses could be well kept to avoid the eavesdroppers' attacks. But limited by the finite extinction ratio of the intensity modulator, the vacuum pulses obtained still have photon number fluctuation.

In this letter, we present a practical light source for high-speed decoy-state QKD based on gain-switched LD. The probabilities of signal-state pulses, decoy-state pulses, and vacuum-state pulses in the decoy-state protocol were 6:2:1. Meanwhile, the signal-state and decoy-state pulses were fixed at u = 0.6 photons per pulse and v_1=0.2 photons per pulse and the vacuum-state was v_2=0. The repetition rate of the light source was set at 100 MHz. Compared to other proposals, the decoy-state

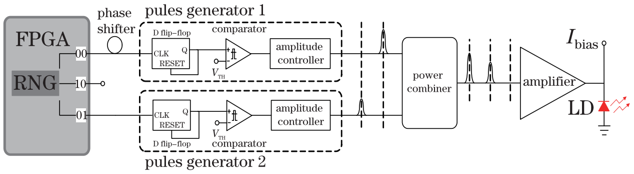

Fig. 1. Schematic setup to produce decoy-state light pulses. I_{bias}: bias current, RNG: random number generator.

light source reported has several advantages. Firstly, with the internal modulation method based on one LD, the vacuum-state could be prepared with high extinction ratio. Secondly, both the decoy pulses and the signal pulses came from the same LD, avoiding the eavesdropper to distinguish the decoy photons from the signal photons by temporal and spectral analysis. As the spectrum of the decoy photons were almost the same as the signal photons, the dispersion difference due to the propagation in the long distance fiber could also be ignored. Finally, the generation rate of the photon pulses reached 100 MHz, fulfilling the requirement of the high-speed QKD system. Such decoy-state laser sources are anticipated to be implemented widely in high-speed QKD systems.

Figure 1 shows the experimental setup of the light source. A pseudo-random numbers of 2-bit based on field programmable gate array (FPGA, Altera Cyclone IV) was generated to trigger either pulse generator or neither. Two electrical pulse generators of the same structure which were composed of a D flip-flop, a high-speed comparator and an amplitude controller produced short pulses of different pulse durations and amplitudes, where the D flip-flops generated short electrical pulse and the high-speed comparators further compressed the pulse duration and the amplitude controllers adjusted the pulse amplitude. The phase shifter was used to calibrate the delay between the two pulses. The outputs from pulse generator 1 and pulse generator 2 were sent to a wideband power combiner followed by cascade radio frequency (RF) amplifier and then were employed to modulate a LD. In particular, if the 2-bit random numbers were 00, pulse generator 1 was triggered on with electrical pulse amplitude of 47 mV and pulse duration of 208 ps which corresponding to the signal-state pulses; if they were 01, pulse generator 2 was triggered on and the electrical pulse amplitude and pulse duration would be 37 mV and 202 ps which would prepare the decoy-state pulses; if they were 10, neither of them was triggered on and the electrical pulse amplitude would be zero which the vacuum-state pulses were produced. In this way, electrical pulses of three different kinds of amplitude could be generated. The (distributed feedback DFB) LD was emitting at 1550.19 nm. Limited by output power of the amplifier used in our setup, a constant bias current of 2 mA was applied on the LD. High extinction ratio could be obtained due to the bias current was much lower than the threshold current (I_{th}=20 mA) of the LD. When the random electrical short pulse was applied on the LD, the LD would produce a laser pulse output due to the gain switch effect, which could also used in fiber laser[27]. Normally, when the modulation current pulse was injected into the LD, stimulated radiation would induce relaxation oscillation after the inverted population density exceeded the threshold value. With the gain switch effect, the inverted population would be consumed at the first peak of the relaxation oscillation and inhibited the afterward. Thus the inverted population emitted within ultra-short time to generate short light pulse. Since the gain switch could be electrically modulated with high speed up to several gigahertzs[28]. And the intensity of light pulse was related to the electrical pulse amplitude. So the decoy-state source of three different intensities was generated at a quite high speed. After attenuation to single-photon level, the decoy-state light source could be used to carry the key information in the QKD system.

We fixed the temperature of the LD at 40 °C. The spectral characteristics of the LD were dependent on the output power when varying the modulation current, as shown in Fig. 2. Normally, as the output optical power increased, the linewidth ($\Delta\lambda$) decreased to the minimum value and increased afterwards, while the central wavelength (λ_c) of the light pulses showed evident blue shift. However, there were a region (marked in red dash ellipse in the Fig. 2) where $\Delta\lambda$ and λ_c almost remained the same. Since the LD was current modulated device and the intensity modulation would introduce phase or frequency chirp to the output light[29], especially under the condition of large signal modulation. The introduced chirp would affect the spectrum parameters and shapes of different intensities. Thus the lower optical power means the LD was working in relatively small signal modulation. The spectrum difference induced by the intensity modulation could be sufficiently inhibited. Accordingly, we could thus select this region as the operating point of the signal-state and decoy-state pulses.

We measured the optical pulse duration when the LD was modulated at different intensities with an optical pulse analyzer (HR150, Southern Photonics), as shown in Fig. 3(a). The pulse duration was measured to be about 25 ps at intensity I. When the intensity was modulated to be $3I$, the pulse duration almost remained the same. And the pulse shape was well retained, ensuring the photon distribution in each pulse of different intensities after attenuation. As the pulse duration was quite short, the detection gate of the InGaAs/InP single-photon detector used in the QKD system could be further shortened, decreasing the afterpulse error counts and dark counts of the detector[30]. Figure 3(b) shows the spectra of the optical pulses recorded by an optical spectrum analyzer (AQ6370, Yokogawa). When the optical intensities were modulated at I and $3I$, the corresponding $\Delta\lambda$ were 0.34

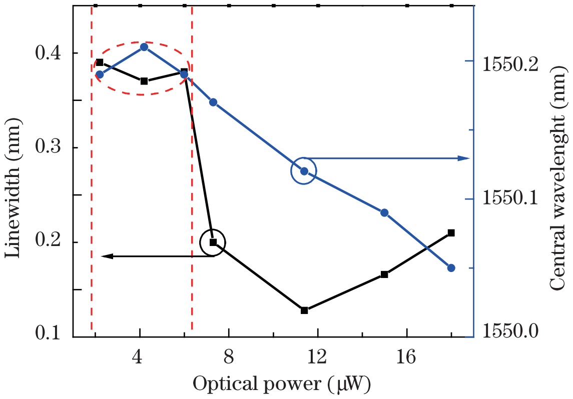

Fig. 2. (Color online) Linewidth and central wavelength as a function of the output optical power.

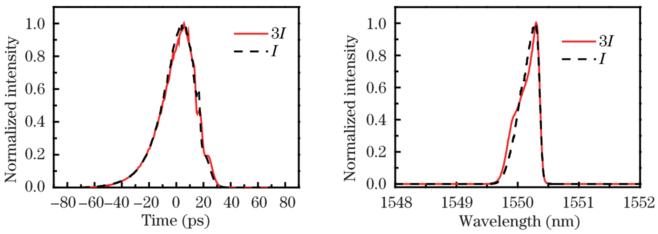

Fig. 3. (Color online) (a) Pulse durations and (b) output spectra at different intensities.

and 0.33 nm, respectively. The center wavelength was located at 1550.19 nm. The spectra were almost remained the same at different intensities as shown in Fig. 3(b), avoiding the eavesdropper's attack by spectral analysis.

To evaluate the similarity of the pulse duration and the output spectrum of different intensities, we calculated the deviation of the two curves using the following equations:

$$\sigma_\tau = \frac{1}{2}\sum_{i=1,2}\int_{\tau_1}^{\tau_2}\frac{\sqrt{[I_i(\tau)-\overline{I}(\tau)]^2}}{\overline{I}(\tau)}\mathrm{d}\tau, \qquad (1)$$

$$\sigma_\lambda = \frac{1}{2}\sum_{i=1,2}\int_{\lambda_1}^{\lambda_2}\frac{\sqrt{[I_i(\lambda)-\overline{I}(\lambda)]^2}}{\overline{I}(\lambda)}\mathrm{d}\lambda, \qquad (2)$$

where σ_τ and σ_λ represent the deviation of the pulse duration and the output spectrum of different intensities, respectively. The deviation of σ_τ was 2.97% indicating the pulse shapes of intensities I and $3I$ were well retained. There were some disparity between the output spectrum shape of the different intensities for the calculated value of σ_λ 7.39%, but the key characteristics of center wavelength and linewidth of the spectrum were almost the same.

To verify the stability of the LD output pulses with random amplitude modulation, we triggered the LD with a high-speed pseudo random number generator based on FPGA of 100 MHz. We detected the optical signals by a fast PIN photodiode (2.5 GHz) and recorded by high-speed oscilloscope (WavePro735Zi, 3.5 GHz, 40 Gbps, Lecroy). Figure 4 shows the amplitude fluctuation histogram of the light pulses with different intensities of $3I$, I, and the vacuum-state. The inset in Fig. 4 shows the waveform recorded by the oscilloscope. The peak amplitudes were 80.1 and 55.5 mV, respectively, corresponding to the signal-state and decoy-state pulses, while the lowest amplitude of 7.6 mV was the vacuum-state pulses which were mainly composed of the background noise. The full width at half maximum (FWHM) fluctuations of the signal-state pulses and the decoy-state pulses were measured to be 3.7% and 4.7%, respectively. Particularly, the fluctuations measured above were mainly contributed by the finite bandwidth of the PIN detector and the limited sampling rate of the oscilloscope. The measured pulse duration was 25 ps with duty cycle of 0.25% which meaned the equivalent bandwidth of the light pulses was up to 40 GHz. So the waveform captured by the oscilloscope could hardly reveal the real undistorted signal while the time jitter and amplitude fluctuation were inevitable. Thus the actual intensity fluctuation would be lower than measured value. And if we simply considered the worst situation, with these random intensity fluctuations, the lower bound of the fraction of untagged bits in the 3-intensity decoy-state protocol could still be verified efficiently[31,32].

The performance of our decoy-state light source was characterized by using a high-speed InGaAs/InP avalanche photodiode based single-photon detector (SPD) based on capacitance balancing technique with gating repetition rate at 100 MHz[33]. The dark count of the SPD was 9×10^{-6} per gate at the detection efficiency of 12%, while the afterpulse probability was 4%. We attenuated the light pulse intensities to μ=0.6, v_1=0.2, and v_2=0. We assumed the light pulses were from a coherent light source and the photon number statistic in the signal pulses and decoy pulses obeyed the Poissonian distribution. The net detection efficiency η could be given by[34]

$$1-e^{-u\cdot\eta} = R(1-P_\mathrm{E})/R_\mathrm{L}(u), \qquad (3)$$

where η is the net detection efficiency, u is the average photon number per pulse, R is the overall counting rate, R_L is the repetition rate of the laser pulse, and P_E is the error counting probability. When the decoy-state light source is detected by the SPD, the overall counting rate R_Decoy can be calculated by

$$R_\mathrm{Decoy} = R_u\cdot P_u + R_{\nu_1}\cdot P_{\nu_1} + R_{\nu_2}\cdot P_{\nu_2}, \qquad (4)$$

where R_x $(x = u, v_1, v_2)$ is the overall counting rate when the detector is triggered by the photon intensities of u= 0.6, v_1=0.2, and v_2=0, respectively. R_Decoy is the theoretical count rate when decoy-state protocol is enforced, and P_x $(x = u, v_1, v_2)$ are the proportion of signal-state, decoy-state, and vacuum-state pulses in the decoy-state protocol. The experimental results were shown in Table 1 together with the theoretical values taking into account of the dark counts and the afterpulse error counts. We first drove the LD to produce pulses of constant intensities of u=0.6 and v_1=0.2. The experimental count rate was almost the same with the theoretical value. The counting rate of v_2=0 was measured to be 1.2×10^3 counts/s. According to the signal pulse counting rate of 7.34×10^6 counts/s as shown in Table 1, the extinction ratio of the signal pulse to vacuum pulse was up to 37 dB. Compared with the normally used external modulation scheme with a maximum extinction ratio of 29 dB[21], there were less photon number fluctuations in our scheme since if no electrical pulses applied on the LD, there was completely no light output, resulting in a higher extinction

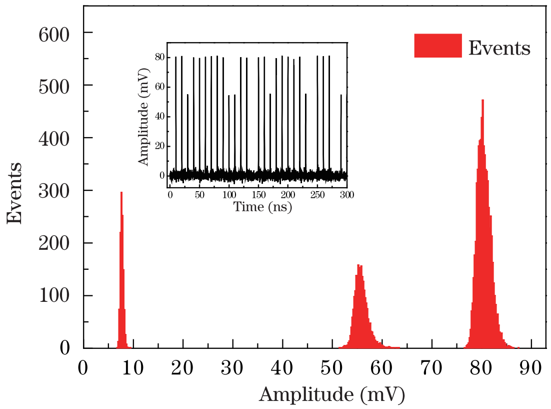

Fig. 4. Amplitude fluctuation histogram and the output waveform of the light pulses.

Table 1. InGaAs/InP SPD Counts of the Decoy-state Light Source

Photon Number (pulse)	Experimental ($\times 10^4$counts/s)					Theoretical ($\times 10^4$counts/s)
	1	2	3	4	Average	
$u = 0.6$	732	735	736	734	734.2±1.7	732
$v_1 = 0.2$	250	254	253	253	252.5±1.7	250
$v_2 = 0.0$	0.12	0.12	0.12	0.12	0.12±0.0	0.09
u : v_1: v_2 = 6:2:1	555	558	554	556	556±1.4	553.6

ratio. Then, we measured the counting rate when the LD was triggered with random signal according to decoy-state protocol. The experimental counting rate agreed well with the theoretical value. Note that all the experimental data measured with the SPD was slightly larger than the theoretical values, which mainly due to the error counting probability P_E used in Eq. (3) was calibrated under the condition of 10 MHz light source, while the actual error counting probability with 100 MHz light source would be larger since the afterpulse probability increased if the repetition of the photon was equivalent to the gating rate of the SPD.

In conclusion, we report on a high-speed light source of 100 MHz at telecom wavelength of 1.55 μm for practical decoy-state QKD. A high modulation rates LD is operated in gain-switching mode to produce ultrashort pulses. By implementing two different short electrical pulses together and triggering with 100 MHz pseudo-random number to drive the LD, the signal-state and decoy-state light pulses are prepared with identical pulse duration of 25 ps and similar spectral characteristics. The intensity fluctuation of the light source is quantified to satisfy the improved 3-intensity decoy-state QKD with random error of light intensity. The characteristics of the decoy-state light source are also analyzed with a high-speed InGaAs/InP avalanche photodiode based SPD. We believe the decoy-state light source is quite useful for the implementation of high-speed QKD systems.

This work was supported by the National Natural Science Foundation of China (Nos. 61127014 and 91221304) and the National Key Scientific Instrument Project of China (No. 2012YQ150092), and the Natural Science Foundation of Shanghai (No. 11ZR1410900).

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74,** 145 (2002).
2. P. Shor and J. Preskill, Phys. Rev. Lett. **85,** 441(2000).
3. C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* **175,** 150 (1984).
4. C. Bennett, Phys. Rev. Lett. **68,** 3121 (1992).
5. A. Ekert, Phys. Rev. Lett. **67,** 661 (1991).
6. J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, Opt. Express **15,** 17928 (2007).
7. Y. Zhang, W. Chen, S. Wang, Z. Yin, F. Xu, X. Wu, C. Dong, H. Li, G. Guo, and Z. Han, Opt. Lett. **35,** 3393 (2010).
8. R. Hughes, G. Morgan, and C. Peterson, J. Mod. Opt. **47,** 533 (2000).
9. Z. Zhao, Y. Luo, Z. Zhao, and H. Long, Chin. Opt. Lett. **9,** 032702 (2011).
10. H. Takesue, K. Harada, K. Tamaki, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S. Itabashi, Opt. Express **18,** 16777 (2010).
11. F. Tang and B. Zhu, Chin. Opt. Lett. **11,** 090101 (2013).
12. N. Lütkenhaus and M. Jahma, New J. Phys. **4,** 44 (2002).
13. D. Gottesman, H. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5,** 325 (2004).
14. X. Peng, B. Xu, and H. Guo, Phys. Rev. A **81,** 042320 (2010).
15. W Liu, S Sun, L Liang, and J Yuan, Phys. Rev. A **83,** 042326 (2011).
16. X. Wang, Phys. Rev. Lett. **94,** 230503 (2005).
17. X. Wang, Phys. Rev. A **87,** 012320 (2013).
18. H. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94,** 230504 (2005).
19. H. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108,** 130503 (2012).
20. M. Lucamarini, K. Patel, J. Dynes, B. FrÖhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penny, and A. Shields, Opt. Express **21,** 24550 (2013).
21. Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, New J. Phys. **11,** 045019 (2009).
22. B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51,** 1863 (1995).
23. K. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, Opt. Lett. **37,** 223 (2012).
24. S. Wang, W. Chen, Z. Yin, Y. Zhang, T. Zhang, H. Li, F. Xu, Z. Zhou, Y. Yang, D. Huang, L. Zhang, F. Li, D. Liu, Y. Wang, G. Guo, and Z. Han, Opt. Lett. **35,** 2454 (2010).
25. C. Peng, J. Zhang, D. Yang, W. Gao, H. Ma, H. Yin, H. Zeng, T. Yang, X. Wang, and J. Pan, Phys. Rev. Lett. **98,** 010505 (2007).
26. Y. Liu, T. Chen, J. Wang, W. Cai, X. Wan, L. Chen, J. Wang, S. Liu, H. Liang, L. Yang, C. Peng, K. Chen, Z. Chen, and J. Pan, Opt. Express **18,** 8587 (2010).
27. J. Yang, Y. Tang, and J. Xu, Photon. Res. **1,** 52 (2013).
28. M. Nakazawa, K. Suzuki and Y. Kimura, Opt. Lett. **15,** 715 (1990).
29. A. Zadok, H. Shalom, M. Tur, W. Cornwell, and I. Andonovic, IEEE Photon. Tech. Lett. **10,** 17091(1998).
30. X. Chen, E. Wu, G. Wu, and H. Zeng, Opt. Express **18,** 7010 (2010).
31. X. Wang, Phys. Rev. A **75,** 052301 (2007).
32. X. Wang, L. Yang, C. Peng, and J. Pan, New. J. Phys. **11,** 075006 (2009).
33. G. Wu, C. Zhou, X. Chen, and H. Zeng, Opt. Commun. **265,** 126 (2006).
34. B. Levine, C. Bethea, and J. Campbell, Electron. Lett. **20,** 596 (1984).