

Controlling a sine wave gating single-photon detector by exploiting its filtering loophole

Lin-Xi Feng(冯林溪), Mu-Sheng Jiang(江木生), Wan-Su Bao(鲍皖苏), Hong-Wei Li(李宏伟), Chun Zhou(周淳), Yang Wang(汪洋)

Citation: Chin. Phys. B . 2018, 27(8): 080305. **doi:** 10.1088/1674-1056/27/8/080305

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Continuous-variable quantum key distribution based on continuous random basis choice

Weiqi Liu(刘维琪), Jinye Peng(彭进业), Peng Huang(黄鹏), Shiyu Wang(汪诗寓), Tao Wang(王涛), Guihua Zeng(曾贵华)

Chin. Phys. B . 2018, 27(7): 070305. **doi:** 10.1088/1674-1056/27/7/070305

Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation

Yingming Zhou(周颖明), Xue-Qin Jiang(蒋学芹), Weiqi Liu(刘维琪), Tao Wang(王涛), Peng Huang(黄鹏), Guihua Zeng(曾贵华)

Chin. Phys. B . 2018, 27(5): 050301. **doi:** 10.1088/1674-1056/27/5/050301

Improved quantum randomness amplification with finite number of untrusted devices based on a novel extractor

Ming-Feng Xu(徐明峰), Wei Pan(潘炜), Lian-Shan Yan(闫连山), Bin Luo(罗斌), Xi-Hua Zou(邹喜华), Peng-Hua Mu(穆鹏华), Li-Yue Zhang(张力月)

Chin. Phys. B . 2018, 27(1): 010305. **doi:** 10.1088/1674-1056/27/1/010305

Decoy-state reference-frame-independent quantum key distribution with both source errors and statistical fluctuations

Kang Liu(刘康), Jian Li(李剑), Jian-Rong Zhu(朱建荣), Chun-Mei Zhang(张春梅), Qin Wang(王琴)

Chin. Phys. B . 2017, 26(12): 120302. **doi:** 10.1088/1674-1056/26/12/120302

Balancing four-state continuous-variable quantum key distribution with linear optics cloning machine

Xiao-Dong Wu(吴晓东), Qin Liao(廖骏), Duan Huang(黄端), Xiang-Hua Wu(吴湘华), Ying Guo(郭迎)

Chin. Phys. B . 2017, 26(11): 110304. **doi:** 10.1088/1674-1056/26/11/110304

Controlling a sine wave gating single-photon detector by exploiting its filtering loophole*

Lin-Xi Feng(冯林溪)[1,2,†], Mu-Sheng Jiang(江木生)[1,2,†], Wan-Su Bao(鲍皖苏)[1,2,‡], Hong-Wei Li(李宏伟)[1,2], Chun Zhou(周淳)[1,2], and Yang Wang(汪洋)[1,2]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou* 450001, *China*
[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 24 February 2018; revised manuscript received 10 May 2018; published online 10 July 2018)

GHz single-photon detector (SPD) is a crucial part in the practical high speed quantum key distribution (QKD) system. However, any imperfections in a practical QKD system may be exploited by an eavesdropper (Eve) to collect information about the key without being discovered. The sine wave gating SPD (SG-SPD) based on InGaAs/InP avalanche photodiode, one kind of practical high speed SPD, may also contain loopholes. In this paper, we study the principle and characteristic of the SG-SPD and find out the filtering loophole of the SG-SPD for the first time. What is more, the proof-of-principle experiment shows that Eve could blind and control Bob's SG-SPD by exploiting this loophole. We believe that giving enough attention to this loophole can improve the practical security of the existing QKD system.

Keywords: quantum key distribution, sine wave gating single-photon detector, quantum hacking, practical security

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/27/8/080305

1. Introduction

Quantum key distribution (QKD)[1–4] with high speed has already been put into use in recent years, and the single-photon detector (SPD) plays an important role in the quantum key distribution system,[5–10] but there are many kinds of attacks aimed at the SPD threaten the quantum key distribution system.[11–18] Finding and eliminating loopholes in the single-photon detector is crucial to obtain provable practical security. The sine wave gating single-photon detector (SG-SPD)[19–21] is one kind of high speed single-photon detector based on InGaAs/InP avalanche photodiode (APD), but the research on the security of the sine wave gating single-photon detector is still incomplete. In this paper, we analyze the working principle of the sine wave gating single-photon detector firstly, then we find a filtering loophole of the sine wave gating single-photon detector and propose a kind of attack, which can experimentally blind the sine wave gating single-photon detector in principle. What is more, by adding a controlling laser pulse with suitable light intensity, we can control the response of the sine wave gating single-photon detector. Finally, we discuss the countermeasures of this attack, so as to improve the security of the quantum key distribution system.

The SG-SPD has been investigated for about ten years. Here, we would like to review the operation principle of the SG-SPD. As shown in Fig. 1, a direct current (DC) power source and a sine-wave gating signal are loaded on the avalanche photodiode (APD) reversely through a bias tee, then the avalanche photodiode can work under the Geiger mode and the linear mode alternately. Thus the dark count and the afterpulse could be reduced obviously, especially in high speed applications. However, the sine-wave gating signal will cause an obvious noise, which is caused by the responding of the parasitic capacitance in the avalanche photodiode and will overwhelm the weak single-photon avalanche signal. Differently from the traditional gating mode, the capacitive noise outputted by the avalanche photodiode under the sine-wave gating signal is simple, which is composed with the gating frequency and its higher harmonics. Therefore, the noise can be filtered by the band-stop filter (BSF) and the low-pass filter (LPF) easily, and finally, the avalanche signal could be extracted. When a single-photon arrives at the avalanche photodiode under the Geiger mode, it will be absorbed and cause a weak avalanche signal. Then, the mixed signals, including the weak avalanche and the capacitive noise of the circuit, pass through the band-stop filter and the low-pass filter, which can filter the capacitive noise. Thus the avalanche signals, which previously completely buried in the capacitive response, become detectable. Finally, the avalanche signals are amplified by the amplifier and then transformed to the processing circuit. We can also observe the single-photon avalanche signal by the oscilloscope, which is shown in Fig. 1, the subgraph (c).

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61605248 and 61505261).
†These authors contributed equally.
‡Corresponding author. E-mail: 2010thzz@sina.com
© 2018 Chinese Physical Society and IOP Publishing Ltd

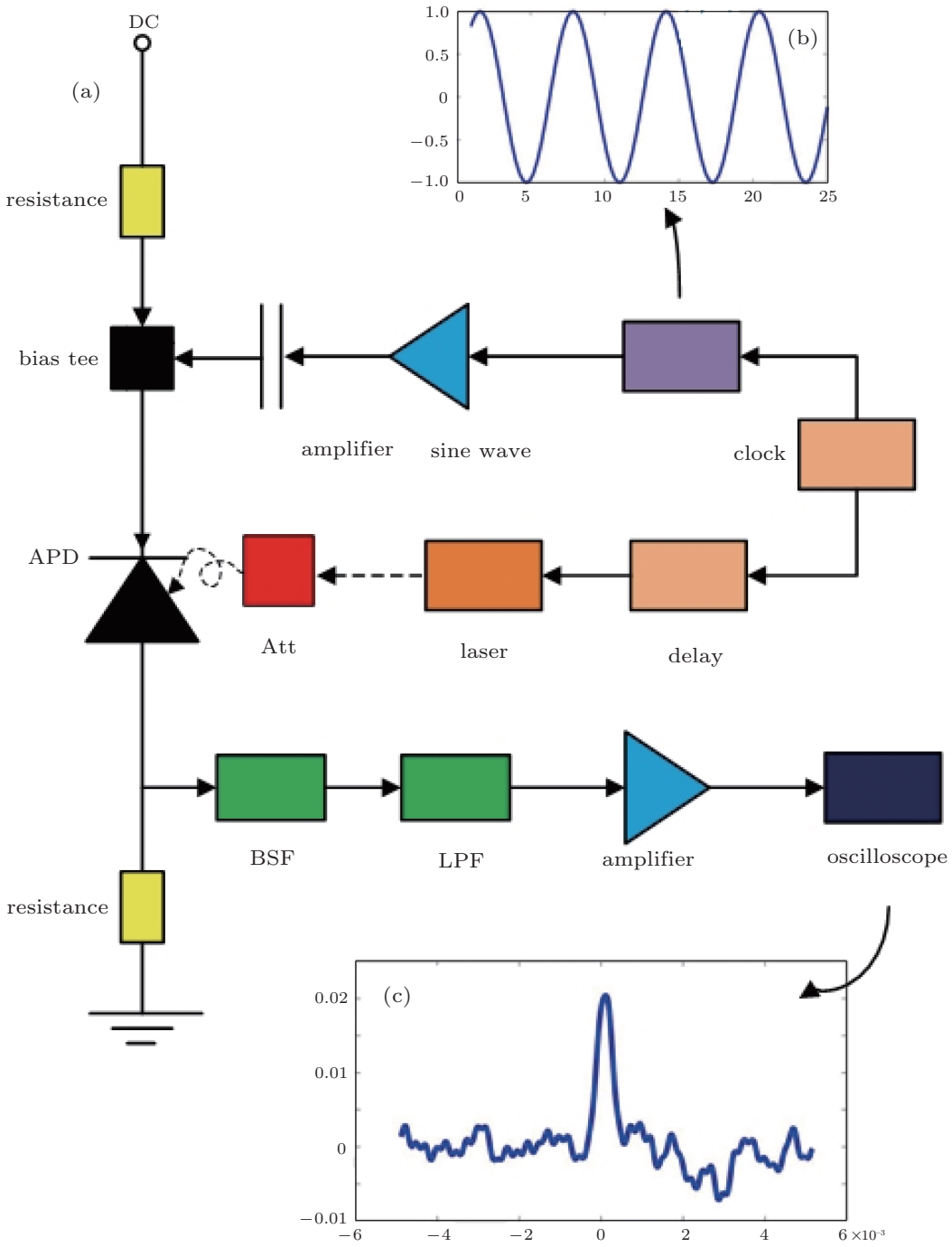


Fig. 1. (color online) The operating principle of the sine-wave gating single-photon detector(SG-SPD). DC: DC power source; APD: avalanche photodiode; Att: variable attenuator; BSF: band-stop filter; LPF: low-pass filter. APD's model is JDS Uniphase X00408052-005. In our experiment, the laser is a pulse laser with external trigger function, the full width at half maximum of the laser pulse is 80 ps, the delayer's adjusting precision is 10 ps, the gain of the amplifier is 20 dB, and the bandwidth of oscilloscope is 8 GHz. The dotted line represents the light connections, accordingly, the solid line represents the electrical connections. (a) Schematics of the SG-SPD, in which the APD under testing is cooled electrically to -50 °C, the bias DC voltage is 49.7 V, the detection efficiency η is 11.7% with a corresponding dark count rate of 18.6 kHz, and the discrimination level of the avalanche signal after 20-dB amplification is 66 mV in our experiment. (b) The sine wave gating signal with frequency of ω. Here we set $\omega = 1$ GHz, and correspondingly we choose a band-stop filter with 10MHz bandwidth and the stop-band central frequencies of 1 GHz, 2 GHz, and 3 GHz, while the low-pass filter with a cut-off frequency of 3.5 GHz. (c) Schematics of a single photon signal captured by the oscilloscope.

2. The filtering loophole of the SG-SPD

Since the SG-SPD has a simple suppression circuit with excellent performance in noise suppression, it is widely used in high speed QKD systems. In the practical QKD system, the average intensity of incident light arrived at the SG-SPD is very weak. Therefore, the generation of the avalanche signal is random, sudden, and independent, resulting a broadband distribution in spectrum. Thus, the avalanche signal can be extracted by filtering the sine-wave noise based on the BSF and the LPF, which has been mentioned in former section. How-

ever, with the incident flux rising, the light pulse with the same frequency of the SG-SPD gating will trigger an avalanche signal in each gating pulse. And the spectrum of the avalanche signal will behave discrete spectral lines, with the gating frequency and its higher harmonics, just like the spectrum of the capacitive noise. Actually, we indeed demonstrate this phenomenon when we test our homemade SG-SPD. As shown in Fig. 2, the average voltage of avalanche signal is increasing slowly and approaching to saturation, while its standard deviation (σ) rises first and then falls with the increase of the average photon number μ. When μ is larger than 10^5, the avalanche signal is almost saturated with a negligible standard deviation, and the periodicity of the avalanche signal is more and more obvious. So, it is easy to understand that once a signal is periodic, it can be decomposed to a certain sine wave and its higher harmonics based on the fourier transform. In other words, when we apply a periodic bright light pulse to the SG-SPD, in which both the light pulse and the sine-wave gating have the same frequency of ω (in our experiment, we set $\omega = 1$ GHz), then, if the average photon number μ is larger enough, the avalanche signal could be decomposed into ω, 2ω, 3ω, ..., and so on.

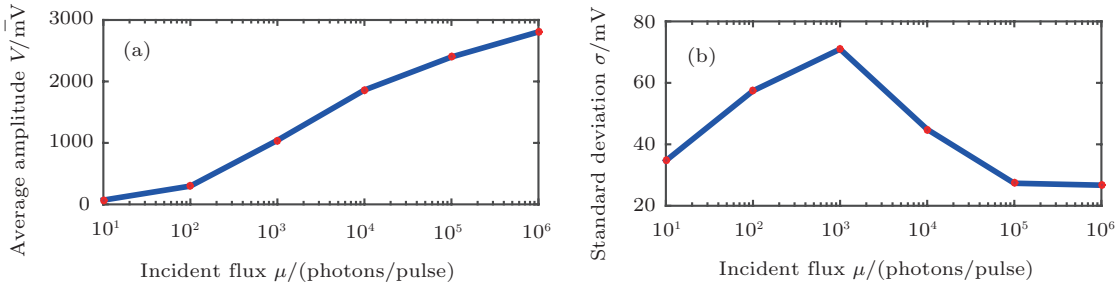


Fig. 2. (color online) (a) The average voltage ($\bar{V}$) of avalanche signal as the function of the incident flux (μ). (b) The standard deviation (σ) of the average voltage ($\bar{V}$) as the function of the incident flux (μ). With the increase of incident flux, the average voltage increases, the standard deviation of the voltage firstly increases and then decreases to almost 0, that is to say, the voltage is becoming saturated in this process. Here, we measure the amplitude of avalanche signal (V) of the SD-SPD for different incident fluxes by the setup shown in Fig. 1(a) with η setting to 11.7% and the trigger rate of the light pulse setting to $\omega/100$ by a prescaler. A large number of V for a certain incident flux are recorded in the oscilloscope, and $\bar{V}$ and σ are obtained by statistical analysis of V, but the effect of the afterpulse of the SG-SPD and the background noise of the oscilloscope have been subtracted. It must be pointed out that the power fluctuation of our incident light pulse is measured to be 15%, so the σ.

So in practical QKD system with SG-SPD, when the incident light reaches to a certain intensity, the output avalanche signal from the APD will become periodic, which will be filtered when passing through the BSF and LPF, with none response to the incident light. In other words, the SG-SPD has be blinded in this situation. Here, we point out that this loophole is introduced directly by the operating principle of the SG-SPD, and we call this loophole the filtering loophole of the SG-SPD.

3. Blinding of the SG-SPD

To confirm our hypothesis about the blind effect of the SG-SPD, we test our homemade SG-SPD shown in Fig. 1(a). Firstly, we use a single clock source with frequency of 1GHz to trigger both of the pulse laser and sine-wave gating generator in the SG-SPD. Then we enter the pulse laser into the SG-SPD. By adjusting the delayer between the clock source and the pulse laser, we can achieve signal synchronization between the pulse laser and the SG-SPD. And by controlling the variable attenuator between the pulse laser and the SG-SPD, we can obtain different intensities of the incident laser pulse. Based on this experimental platform, we test the count rate of the SG-SPD for different average photon numbers μ_b of the incident laser pulse, which is shown in Fig. 3.

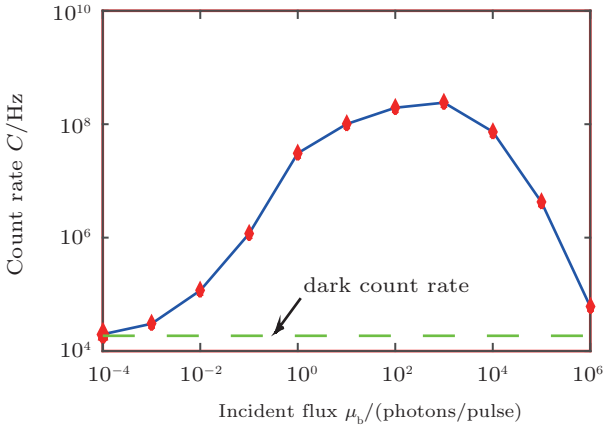


Fig. 3. (color online) The count rate as a function of the average photon number μ_b. Here we use a single clock source with frequency of 1GHz to trigger both of the pulse laser and sine-wave gating generator in the SG-SPD. In Fig. 3, the dotted line represents the dark count rate of the SG-SPD. Limited by our laser source, the biggest μ_b we can obtain is 10^6 photons/pulse, and in this case, the count rate is already very close to the dark count rate.

We can see that, the count rate of the SD-SPD will first increase and then decrease with the increase of the incident flux. Actually, when the incident flux is low, the count rate is proportional to μ_b, but when μ_b is larger than 10^3 photons/pulse, the count rate starts to fall. Specially, when the μ_b reaches to 10^6, the count rate is close to dark count rate, which is meet our expectation that the SG-SPD can ba blinded by a bright pulse laser with frequency of 1 GHz, the same as the sine-wave gat-

ing. It is no doubt that if μ_b keeps increasing, the count rate could decrease below the dark count rate.

4. Controlling experiment of the SG-SPD

Since the SG-SPD can be blinded in certain condition, Eve can insert another pulse with low frequency to control Bob's SG-SPD, then she can get all the secret keys without being discovered by the legitimate parties. As shown in Fig. 4, Alice's laser diode (LD) generates a laser pulse, then the pulse is transformed to Bob by the quantum channel after modulation and attenuation. Bob first demodulates and then detects his received photons using his SG-SPDs. In order to control Bob's SG-SPDs, Eve intercepts the pulse on the quantum channel and then generates fake state to Bob. On the one hand, Eve generates a blinding light pulse by driving the laser diode with frequency of 1GHz, synchronizing with the clock signal from Alice, and the intensity of the blinding laser could be adjusted to an appropriate value. On the other hand, Eve imitates Bob's behavior, she demodulates and detects the photons from Alice, and modulate a controlling light pulse according to her detection results, in the same way, the control pulse could be adjusted to the optimal state by the variable attenuator, finally, the two pulses are mixed with the BS and then transmits to Bob.

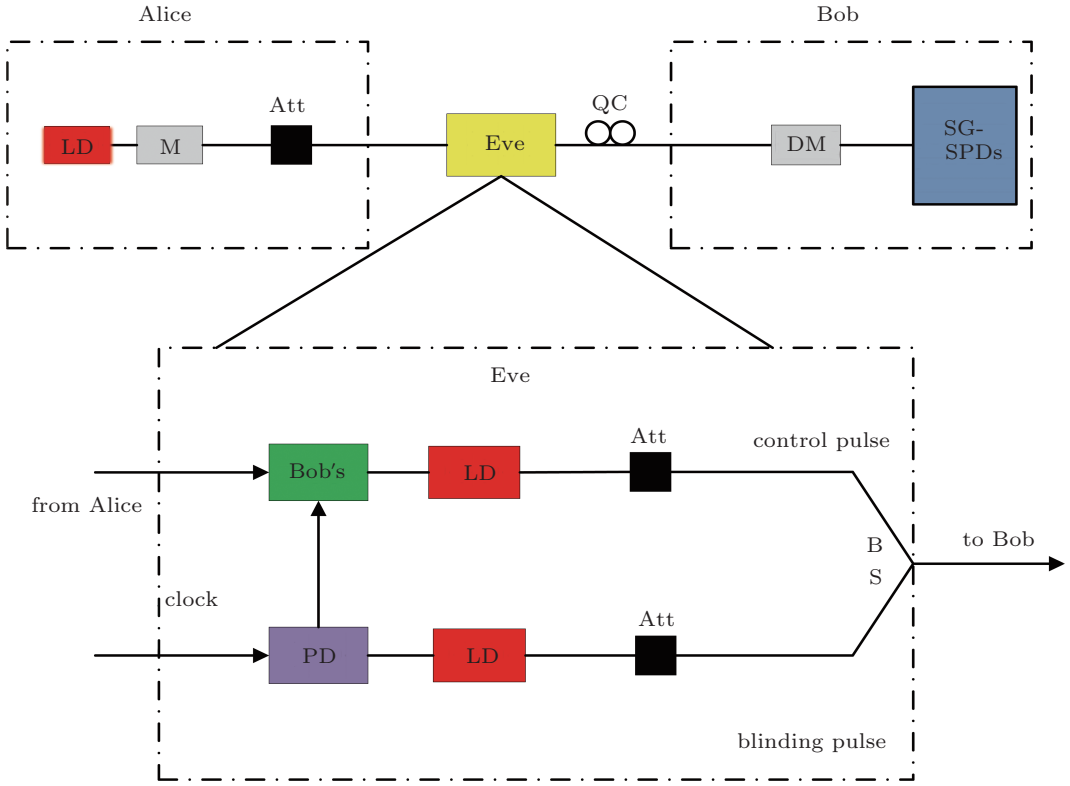


Fig. 4. (color online) The experimental principle diagram of controlling the SG-SPDs. LD: laser diode; M: Alice's modulation process; Att: variable attenuator; QC: the quantum channel; DM: Bob's demodulation process; PD: the photoelectric conversion; BS: the beam splitter. The laser source of control pulse and blinding pulse is EIG1000D and WT-LD100 respectively.

In our paper, without loss the generality, we simplify Bob's equipment and make the blinding pulse and the control pulse enter into the SG-SPD directly, in which the intensity of the blinding pulse is 10^6 photons/pulse, and the control pulse uses the periodic light pulse with 1-MHz repetition frequency. Then we can gain the count rate of the sine-wave gating SPD by changing the controlling pulse intensity, as shown in Fig. 5. Using μ_c to represent the average photon number of the controlling laser pulse, we can see from Fig. 5 that, the count rate increases gradually with the increase of μ_c, especially when μ_c is bigger than 2.5×10^6, the count rate will result in super linear characteristic.[22] In fact, when the controlling flux increases from 2.5×10^6 photon/pulse to 5×10^6 photon/pulse, the detection probability increases from $\eta_h = 15\%$ to $\eta_h = 100\%$ just as shown in Fig. 5. In this way, Eve can control Bob's SPD's detection efficiency following her own wishes.

Since Eve could control the SG-SPD of Bob, she can make an intercept and resent attack just like the conventional gate mode SPD's blinding attack,[23] which can be realized by the following steps. First, Eve intercepts the pulse on the quantum channel and imitates Bob's behavior, she demodulates and detects the photons from Alice, then she resends the detection results and controls Bob's detection events, in which she uses a blinding pulse to blind Bob's SG-SPDs, and a controlling pulse to control Bob's SG-SPDs which has already been

blinded. Under Eve's attack, Bob will certainly have a detection event when his active basis choice coincides with that of Eve, otherwise, the detection probability of Bob's SG-SPDs is only 15%, which decreases the error rate introduced by Eve.

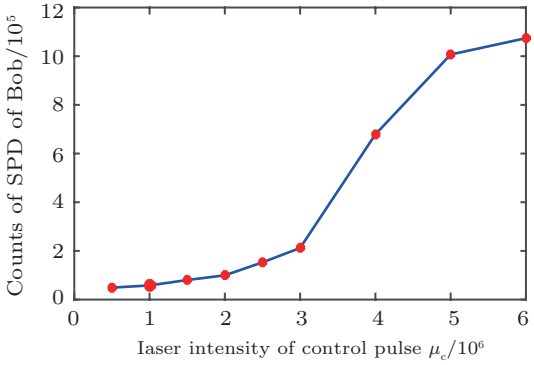


Fig. 5. (color online) Bob's count rate under the control pulse with different light intensity μ_c. In Fig. 5, the intensity of the blinding laser pulse μ_c is 10^6. When μ_c is lower than 2.5×10^6, the counts change slowly, but when μ_c reaches 3×10^6, the counts begin to rise sharply and show the superlinearity character. So Eve can control Bob's SG-SPD by the way without being exposed.

5. Discussion

Here we point out that there are some imperfections in our experiment. Firstly, in our theory analysis, when the blinding laser pulse is periodic strictly with very small jitter both in time and amplitude, the avalanche signal could be triggered periodically by increasing of the blinding laser pulse, and the SG-SPD could be blinded completely. However, there is a gap between our existing experimental conditions and the ideal conditions, our blinding laser pulse's jitter cannot be ignored, which affects our experimental results obviously, resulting in incomplete blinding and controlling of the SG-SPD.

Secondly, in theory, under a blind light with a certain jitter, the count rate of the SG-SPD should be reduce first and then increase with the increasing of the intensity of the blinding pulse, and there is a minimum point of the count rate curve, which could gain the best effect of blinding. Unfortunately, in our experiment, our equipment cannot generate a blinding laser pulse larger than 10^6 photons/pulse, so we cannot reduce the count rate lower than the dark count rate (see Fig. 3).

In addition, the blinding results are affected by the discrimination level of the avalanche signal, which is closely related to the performance of the SG-SPD. In general, the better the filtering effect is, the lower the discrimination level could be set, then the SG-SPD could distinguish the avalanche signal with a lower amplitude, and resulting in a lower after pulse rate. In this case, the dead time of the SG-SPD could be shorter, and the maximum count rate of the SG-SPD will be higher. However, in order to achieve better blinding effect, we need the avalanche signal to be very periodic, in other words, the standard deviation of the avalanche signal should be much lower than the discrimination level. In a word, the discrimination level is lower, the SG-SPD will be more difficult to be blinded.[24] In our experiment, the discrimination level is only 66 mV to get a higher count rate, with such a low discrimination level, the SG-SPD is relatively difficult to be blinded.

We also point out that the filtering loophole of the SG-SPDs is introduced directly by the working principle of the SG-SPD, and it can even be controlled completely under certain specific parameters. We believe that this loophole is threatening in existing QKD system using SG-SPDs. In order to apply the SG-SPD safely, some countermeasures should be taken, such as photocurrent monitoring or setting parameters more carefully. For example, we can add another APD to monitor part of the laser pulse, in this case, we could observe the change of optical signal, which can discover the potential Eve. What is more, other countermeasures are put up in recent years, such as setting appropriate discrimination level to prevent the SG-SPD from being blinded,[24] using an explicit random number generator to prevent the SG-SPD from being blinded by the bright laser pulse,[25] or using a coupler with asymmetric splitting ratio to monitor the bright light attack.[26] Further, the measurement-device-independent (MDI) QKD attracts a lot of attention now, it can fill the loophole caused by the imperfections of measurement devices especially the SPD,[27–29] maybe years later, MDI-QKD could put into use in practical.

6. Summary

At the end of this paper, let us review our experiment simply. Firstly, we obtain an idea of blinding the SG-SPD from its working principle. Secondly, we observed the blinding effect in the experiment when the blinding pulse with incident photon number μ_b exceeds 10^5. And then, we realize the controlling the count rate of Bob's SG-SPD, which could be exploited by Eve to control Bob's SG-SPD. Finally, we analyze the imperfections in our experiment and discuss the countermeasures of this loophole in QKD system using the SG-SPD.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computer Systems and Signal Processing* (New York: IEEE) pp. 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 3121
[4] Zhang Y Y, Bao W S, Zhou C, Li H W, Wang Y and Jiang M S 2017 *Chin. Phys. Lett.* **34** 1
[5] Yuan Z L, Sharpe A W, Dynes J F, Dixon A R and Shields A J 2010 *Appl. Phys. Lett.* **96** 18790
[6] Yuan Z L, Kardynal B E, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **91** 175-179

[7] Restelli A, Bienfang J C and Migdall A L 2013 *Appl. Phys. Lett.* **102** 141104

[8] Comandar L C, Fröhlich B, Dynes J F, Sharpe A W, Lucamarini M and Yuan Z L 2015 *J. Appl. Phys.* **117** 045005

[9] Fujiwara M, Ishizuka H, Miki S, Yamashita T, Wang Z and Tanaka A, *et al.* 2011 *Quantum Electronics Conference and Lasers and Electro-Optics, IEEE* **19** 507

[10] Acín A, Bloch I, Buhrman H, Calarco T, Eichler C and Eisert J, *et al.* 2017 arXiv: 1712.03773 [quant-ph]

[11] Jiang M S, Sun S H, Tang G Z, Ma X C, Li C Y and Liang L M 2013 *Phys. Rev. A* **88** 062335

[12] Jiang M S, Sun S H, Li C Y and Liang L M 2012 *Phys. Rev. A* **86** 197

[13] Yuan Z L, Dynes J F and Shields A J 2011 *Appl. Phys. Lett.* **98** 057901

[14] Jiang M S, Sun S H, Li C Y and Liang L M 2014 *J. Mod. Opt.* **61** 147

[15] Sauge S, Lydersen L, Anisimov A, Skaar J and Makarov V 2011 *Opt. Express* **19** 23590

[16] Weier H, Krauss H, Rau M, Fuerst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 193

[17] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 4702

[18] Tang Y L, Yin H L, Ma X Fung, C H F, Liu Y, Yong H L, Chen T Y, Peng C Z, Chen Z B and Pan J W 2013 *Phys. Rev. A* **88** 5862

[19] Namekata N, Adachi S and Inoue S 2009 *Opt. Express* **17** 6275

[20] Namekata N, Inoue S and Sasamori S 2006 *Opt. Express* **14)** 10043

[21] Liang X L, Liu J H, Wang Q, Du D B, Ma J, Jin G, Chen Z B, Zhang J and Pan J W 2012 *Rev. Sci. Instrum.* **83** 145

[22] Lydersen L, Jain N, Wittmann C, Ø Marøy, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. A* **84** 2372

[23] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686

[24] Koehlersidki A, Dynes J F, Lucamarini M, Roberts G L, Sharpe A W, Yuan Z L and Shields A J 2017 arXiv: 1712.06520 [quant-ph]

[25] Stipčević M 2014 arXiv: 1403.0143 [quant-ph]

[26] Wang J, Wang H, Qin X, Wei Z and Zhang Z 2016 *Eur. Phys. J. D* **70** 1

[27] Mizutani A, Tamaki K, Ikuta R, Yamamoto T and Imoto N 2012 *Phys. Rev. Lett.* **108** 130503

[28] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 *Phys. Rev. A* **85** 281

[29] Liu C Q, Zhu C H, Wang L H, Zhang L X and Pei C X 2016 *Chin. Phys. Lett.* **10** 3