Ability of strong-pulse illumination to hack self-differencing avalanche photodiode detectors in a high-speed quantum-key-distribution system

Binwu Gao,[1] Zhihao Wu,[1] Weixu Shi,[1] Yingwen Liu,[1] Dongyang Wang,[1] Chunlin Yu,[2] Anqi Huang,[1,*] and Junjie Wu[1,†]

[1] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China*

[2] *China Greatwall Research Institute, China Greatwall Technology Group Co., Ltd., Shenzhen 518057, China*

(Received 9 May 2022; accepted 31 August 2022; published 29 September 2022)

Implementation of high-speed quantum key distribution (QKD) has become one of the major focuses in the field, which produces a high key-generation rate for applications. To achieve high-speed QKD, tailored techniques are developed and employed to quickly generate and detect quantum states. However, these techniques may introduce unique loopholes to compromise the security of QKD systems. In this paper, we investigate the loopholes of the self-differencing (SD) avalanche photodiode (APD) detector, typically used for high-speed detection in a QKD system, and demonstrate experimental testing of the SD APD detector under strong-pulse-illumination attack. This attack presents blinding stability and helps an eavesdropper to learn the secret key without introducing extra quantum bit rate error. Based on this testing, we propose a set of criteria for protecting SD APD detectors from the strong-pulse-illumination attack.

DOI: 10.1103/PhysRevA.106.033713

I. INTRODUCTION

Quantum key distribution (QKD), whose security is guaranteed by the laws of quantum mechanics, allows two remote and legitimate users to share a private and secret key [1–4]. Nowadays, for the need of high-speed key-generation rate, prepare-and-measure QKD protocols [1,5–7] are the common choice, instead of measurement-device-independent (MDI) QKD protocol [4] that removes all security loopholes in measurement devices but has a relatively low rate. In order to achieve high key-generation rate with the help of the system's high repetition frequency, a traditional gated avalanche photodiode (APD) detector might not be suitable due to the effect of afterpulse noise that is produced by trapped avalanche charge. To reduce the afterpulse noise, it is required that the weaker avalanche signal shall be sensed, which can be satisfied by employing self-differencing (SD) technique to an APD. Therefore, the SD APD detector is commonly used in gigahertz high-speed QKD systems [8,9].

Although QKD has been proved to be information-theoretically secure in theory, there are still some loopholes in practical implementation [10–23]. For example, the single-photon detectors (SPDs), which are the core devices in BB84 QKD systems, may be hacked by the eavesdropper Eve via the after-gate attack [24], the time-shift attack [25,26], the detector-blinding attack [11,13], and so on. In order to defend against these attacks on the detection devices, security patches [27–29] are effective countermeasures. That is, once a new type of attack is discovered, a corresponding countermeasure against this attack may be proposed and realized in an existing QKD system [30]. Recently, in order to ensure the most secure conditions to operate SD APD detectors in QKD systems, a set of so-called "best-practice criteria" for practical security of SD APD detectors has been proposed [31].

Continuous-wave (cw) light is usually regarded to achieve a reliable eavesdropping, such as for the best-practice criteria that only considers the case of cw blinding attacks [31]. Instead, the power fluctuation of optical pulse may expose the hacking behavior of an eavesdropper [31,32]. However, in this study, we find that strong-pulse-illumination attack presents blinding stability. By using strong optical pulse, an eavesdropper can blind the SD APD detector continuously and steadily without introducing extra quantum bit rate error (QBER).

In this paper, under the practice criteria [31], we experimentally demonstrate that the SD APD detector in a QKD system can be directly blinded by using strong optical pulses with the repetition frequency the same as the gating frequency of the SD APD detector. Then we trigger the SD APD detector when it is completely blinded and realize the control in the detection probability of the detector from 0% to 100%. This study shows that the SD APD detector can be successfully hacked by the pulse-illumination attack, which might compromise the security of a high-speed QKD system with SD APD detectors. Afterward, we propose a set of criteria for practical security of SD APD detectors by taking the threat of pulse-illumination attack into account.

The paper is structured as follows. Section II introduces the operation principle of SD APD detectors, the general process of strong-pulse-illumination attack, and the difference between cw blinding attack and pulsed-illumination attack. The experimental setup and selection criteria of the discrimination level of the tested SD APD detector are described in Sec. III. Under the practice criteria, the methodology and

[*] angelhuang.hn@gmail.com

[†] junjiewu@nudt.edu.cn

testing results of the pulse-illumination attack are presented in Sec. IV. In Sec. V, we show the difference between the pulse-illumination attack in this work and the previous attack on the SD APD detector disclosed in Ref. [32], analyze the incomprehensiveness of practical criteria in Ref. [31], and propose a list of practical criteria to resist pulse-illumination attack. Finally, we conclude in Sec. VI.

II. WORKING PRINCIPLE OF SD APD DETECTORS AND STRONG-PULSE-ILLUMINATION ATTACK

In this part, we first introduce the operation principle of SD APD detectors by taking the SD APD detector tested in this study as an example. Then we introduce the general process of strong-pulse-illumination attack that is proposed in this work. Finally, we clarify the difference between cw blinding attack and pulsed-illumination attack.

Figure 1(a) shows the schematic circuit of the tested SD APD detector. A dc bias voltage combined with the periodic gating signals is reversely loaded on the APD. When the reversed bias voltage is higher than the breakdown voltage, the APD works on Geiger mode, where a single photon can result in detectable macroscopic avalanche current. However, the repetition rate of the gating signal is so fast that weak avalanche signals are often buried within the APD's capacitive response [33]. In order to remove the capacitive response, the SD technique is applied. That is, first divide the response of APD into two halves, then shift one of them by one gate period, and recombine the two halves to cancel the strong capacitive response. The weak avalanche signal processed after the SD technique is shown in Fig. 1(b). Through SD technique, only weak avalanche signals and capacitive response residual remain, which can be distinguished by setting a discrimination level.

Due to the intrinsic imperfection of SD APD detectors, under the strong cw light illumination, the SD APD detector might be blinded [31]. To eliminate the threat of cw blinding attack, Ref. [31] investigated the behavior of a SD APD under cw bright-light illumination and proposed practice criteria for practical security of SD APD detectors employed in a QKD system. Under the proposed practice criteria, once Eve uses cw bright light to blind SD APD detectors, the large blinding photocurrent exposes the existence of Eve. In addition, the increase of error rate caused by residual capacitive background can also help Bob discover Eve. Therefore, SD APD detectors under this practice criteria can defend cw bright-light illumination.

However, the effectiveness of this practical criteria under pulsed-illumination attack is not fully investigated yet. In this work, we thoroughly test the behavior of the SD APD detector under strong-pulse illumination. Figure 2 shows the general process of strong-pulse-illumination attack. During the attack, Eve's operation is divided into two steps. Before explaining the specific process, we denote the strong optical pulse sent by Eve in the first step as blinding pulse, which is used to blind the SD APD. After the SD APD is blinded, the optical pulse sent by Eve in the second step is denoted as trigger pulse to control the detection response of SD APD. By using the strong optical pulses with the same repetition rate of the gated signal applied to the SD APD detector, each optical pulse triggers a stable avalanche photocurrent. The stable and periodic avalanche photocurrent is canceled out after the SD processing. Therefore, the remaining avalanche photocurrent is lower than the discrimination threshold. As a result, the SD APD detector is blinded and its output detection can be controlled by Eve's classical trigger pulses with tailored energy, which triggers a click only when Bob selects the same basis as Eve.

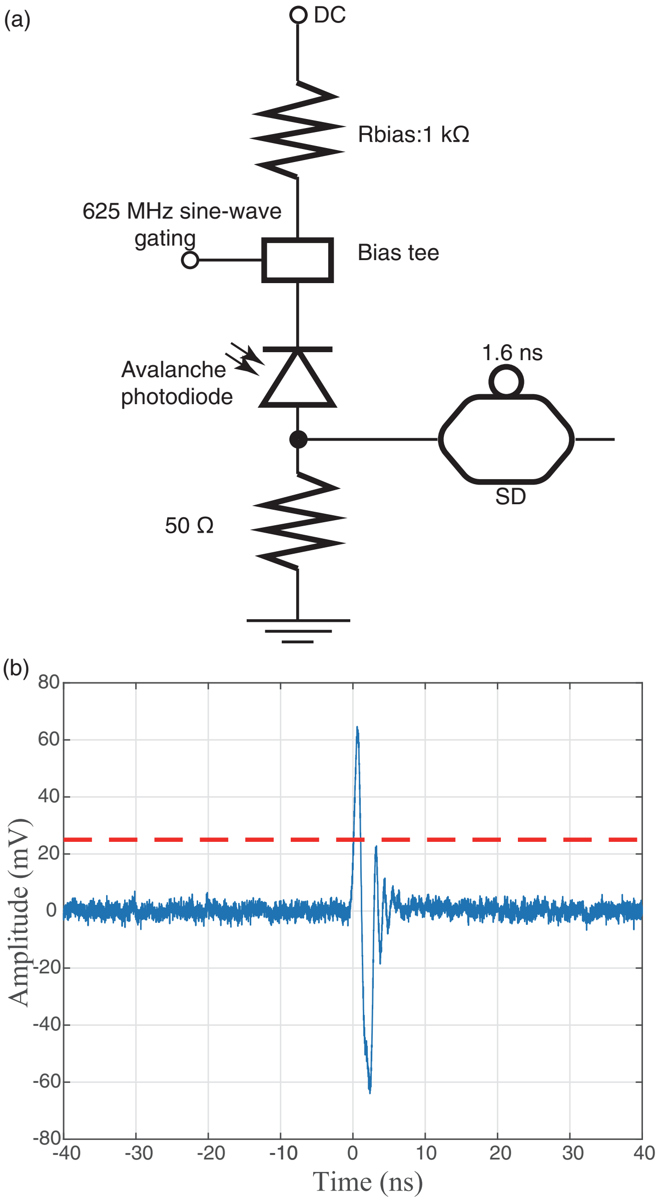

FIG. 1. (a) Schematic circuit of the tested SD APD detector. (b) Output waveform of the tested SD APD detector shows a single avalanche rising above the capacitive response residual. The red dashed line represents the discrimination level, which is set to be 25 mV.

The pulse-illumination attack also is beneficial to bypass the countermeasures against the cw bright-light blinding attack. Regarding the cw blinding atttack, the eavesdropper, Eve, uses cw light to illuminate APD to cause a large constant photocurrent through APD, which lowers the bias voltage on

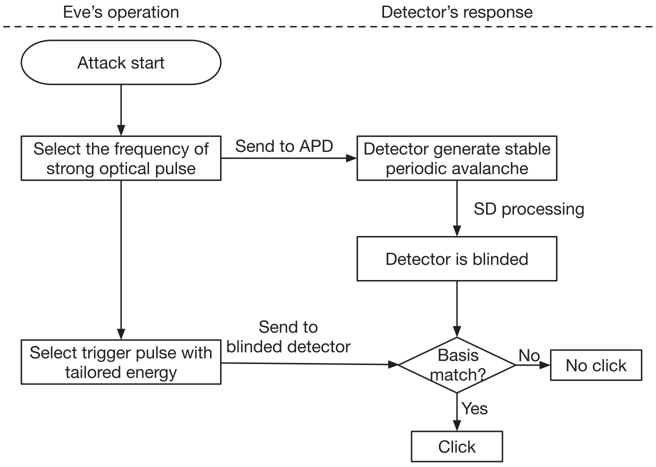

FIG. 2. General process of strong-pulse-illumination attack.

APD to be below the breakdown voltage and pulls APD back to the linear mode that is not sensitive to a single photon [11], whereas the pulse-illumination attack accumulatively introduces a high photocurrent that varies over time to lower the bias voltage, so as to achieve blinding. The drop of bias voltage under the pulse-illumination attack is not as much as that under the cw bright-light blinding attack, which keeps the capacitive response residual lower than the discrimination threshold and introduces no detection. Furthermore, the photocurrent monitor as an alarm of the cw bright-light blinding attack may be muted under the pulse-illumination attack [34]. This is because the photocurrent monitor may contain a low-pass filter or have limited bandwidth, which causes the pulsed photocurrent to be treated as high-frequency noise and filters out most of it.

III. EXPERIMENTAL SETUP

In order to experimentally explore the behavior of SD APD detectors under strong-pulse illumination, the test is conducted using the setup shown in Fig. 3. An arbitrary wave generator (AWG) is used to drive laser diodes. The laser diode 1 (LD1) is driven to emit blinding pulses at 1550 nm, whose repetition frequency 625 MHz is the same as that of the gating signal applied to the SD APD detector under test. Similarly, the laser diode 2 (LD2) is driven by the AWG to generate 312.5- MHz trigger pulses used to control the blinded SD APD detector. The laser diode 3 (LD3) emits pulses, denoted as synchronization pulses, with repetition frequency of 100 kHz to synchronize the attacking setup and the SD APD detector under test to ensure that blinding pulses and trigger pulses can stably illuminate inside the gating period of the SD APD. Variable optical attenuators (VOAs) and erbium-doped fiber amplifiers (EDFAs) are used to tune the optical intensity of blinding pulses and trigger pulses. The optical power meter 1 (OPM1) monitors the optical power of the blinding pulses and the optical power meter 2 (OPM2) serves to monitor the optical power of the trigger pulses. Meanwhile, the 50:50 beam splitter 1 (BS1) merges the blinding pulses and the trigger pulses.

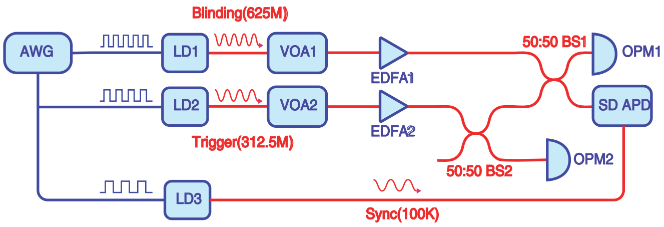

FIG. 3. Schematic diagram of experimental setup. The red lines represent the optical signal and the blue lines represent the electrical signal. AWG, arbitrary wave generator; LD, laser diode; VOA, variable optical attenuator; EDFA, erbium-doped fiber amplifier; BS, beam splitter; OPM, optical power meter; SD APD, self-differencing avalanche photodiode detector. As the testing target, the SD APD connected in series with a 1 kΩ bias resistor works at gating frequency of 625 MHz.

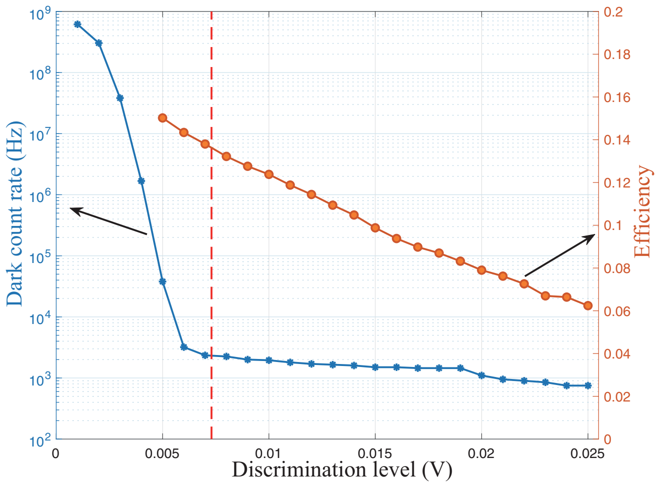

FIG. 4. Dark count rate and detection efficiency as a function of discrimination level. When the discrimination level is lower than 6 mV, the dark count rate mainly comes from the capacitive response residual. Otherwise, the dark avalanches are the major source of the dark count rate. The red dashed line represents the minimum average value of peak amplitude when the SD APD detector is blinded.

The SD APD detector under testing is cooled down to −40 °C and applied by 64.2 V bias voltage. As shown in Fig. 1(a), the gating frequency of the APD is 625 MHz and the bias resistor connected in series is 1 kΩ. The resistance value of the bias resistor satisfies the requirement b) of the practice criteria in Ref. [31], which recommends to avoid using a bias resistor exceeding 50 kΩ. It is important to note that we realize the SD operation of avalanche signals by means of software processing instead of the practical SD circuit. Compared to the physical realization, software processing can remove the effect of the timing jitter, which makes the result of the SD more precise.

Setting an appropriate discrimination level cannot only improve the detection efficiency of the SD APD detector, but also perceive the reduction of excess voltage [31]. Therefore, the choice of discrimination level of a SD APD detector is important. Figure 4 shows the dark count rate and detection efficiency as a function of discrimination level. As observed from Fig. 4, there is a kink at discrimination level of 6 mV, indicating the dark avalanches replace the capacitive response

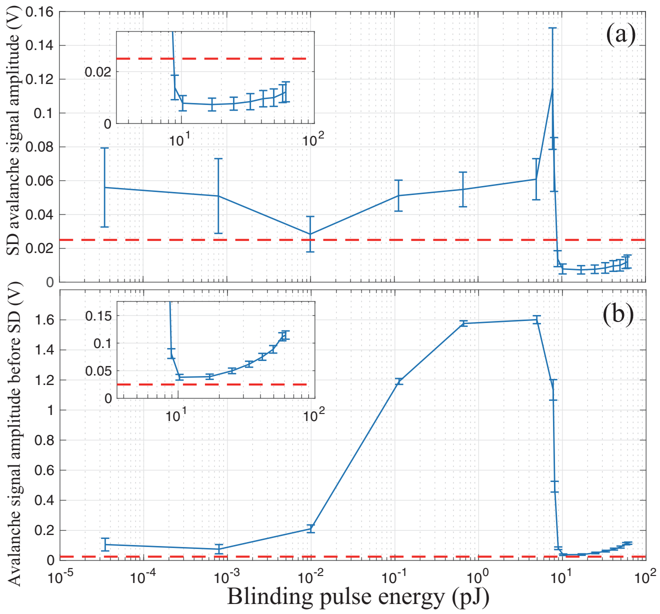

FIG. 5. Average value and standard deviation (a) of the SD avalanche signal's peak amplitude and (b) of the avalanche signal's peak amplitude before SD processing as a function of the blinding pulse energy. The blue dashed line represents the discrimination level. When the peak amplitude of the SD avalanche signal is lower than it, the detector is blinded.

residual to be the dominant contribution to the measured dark count rate when the discrimination level is higher than 6 mV. Therefore, weak avalanche signal and capacitive response residual can be distinguished when the discrimination voltage is higher than 6 mV. However, for a SD APD detector working in a real QKD system, the change of working environment may introduce extra electronic noise and the detection noise of the SD APD may increase during long-time running. Thus the set discrimination level not only needs to distinguish between capacitive response residual and weak avalanche signal, but also needs to resist the noise caused by the above reasons. To enhance noise resistance of the SD APD detector, the discrimination level is set to 25 mV by the third party who provides the SD APD detector. Under this setting, the afterpulse probability is 7.69%, which is relatively high because we do not add the dead time in the calculation.

IV. EXPERIMENT RESULTS

In this study, we conduct an attacking experiment on Bob's SD APD detector with strong optical pulse. LD3 is first turned on to send 100 kHz synchronizing pulses to the SD APD detector for synchronizing the whole testing setup. Then, LD1 is switched on to generate 625- MHz blinding pulses, whose intensity is modulated by VOA1 and EDFA1, to illuminate the SD APD detector. Under each intensity of the incident pulses, we measure the avalanche signal after SD processing, collect 480 consecutive periods, and make statistics on the peak amplitude in each period.

Figure 5(a) shows the average value of peak amplitude $\bar{V}_{\text{peak}}^{\text{SD}}$ and standard deviation σ^{SD} of the SD avalanche signal depending on the energy of each blinding pulse. When the blinding pulse energy is small, the $\bar{V}_{\text{peak}}^{\text{SD}}$ of the SD avalanche signal is higher than the discrimination level, 25 mV. By gradually increasing the blinding pulse energy, the $\bar{V}_{\text{peak}}^{\text{SD}}$ of the SD avalanche signal first decreases and then starts increasing at 0.01 pJ blinding pulse. Remarkably, there is a dip when the blinding pulse energy is 0.01 pJ. It is because, for this amount of energy, each optical pulse triggers an avalanche, whose amplitude is relatively stable in each period, resulting in a smaller amplitude remaining after SD processing. When the blinding pulse energy increases from 0.01 pJ to 7.76 pJ, the amplitude consistently increases, which is due to the stable avalanche response under high gain factor of secondary electron-hole pairs. When the blinding pulse energy is higher than 7.76 pJ, the $\bar{V}_{\text{peak}}^{\text{SD}}$ of the SD avalanche signal begins to decrease rapidly. Finally, the $\bar{V}_{\text{peak}}^{\text{SD}}$ of the SD avalanche signal is lower than the discrimination level when the blinding pulse energy is higher than 8.92 pJ. It means that the SD APD detector can be directly blinded by lowering the amplitude of the SD avalanche signal under the strong-pulse illumination. After the SD APD detector is blinded, even though the average power of the blinding pulse is increased to 61.09 pJ, the count rate of the SD APD detector still does not recover, indicating that the SD APD detector can be blinded stably.

To further understand the blindness of the SD APD detector, we conduct the same statistics on the avalanche signal after the filtering circuit but before SD processing. Figure 5(b) shows the $\bar{V}_{\text{peak}}$ and σ of the avalanche signal after the filtering circuit but before SD processing as a function of each blinding pulse's energy. With the increasing energy of blinding pulse, $\bar{V}_{\text{peak}}$ of the avalanche signal after the filtering circuit but before SD processing first increases and then rapidly decreases to 81 mV at 8.92 pJ, in which case the SD APD detector is blinded. Figures 6(a) and 6(c) respectively show in detail the amplitude of the avalanche signal after the filtering circuit but before SD processing when blinding pulse energy is 8.09 pJ and 10.24 pJ, which are the cases right before and after blinding happened. In Fig. 6(a), amplitude is relatively large and the waveform is very unstable, which results in the SD amplitude being higher than the discrimination level. With the increase of energy, the amplitude of the avalanche signal after the filtering circuit but before SD processing in each period becomes smaller and is very stable in Fig. 6(c). It means strong-pulse illumination lowers amplitude and fluctuation of the avalanche signal after the filtering circuit but before SD processing, consequently blinding the SD APD detector. After the SD APD detector is blinded, in order to control detection outcome of the SD APD detector, LD2 is turned on to send 312.5- MHz trigger pulses to the SD APD detector. The trigger pulses are superimposed on blinding pulses through BS1. For each trigger pulse energy, LD2 sends 960 trigger pulses to provide sufficient samples for statistically analyzing the detection probability of the blinded SD PD detector. The number of the SD avalanche signal's amplitude exceeding the discrimination level is immediately afterwards counted, so as to obtain the detection probability. Figure 7 shows the detection probability as the function of trigger pulse energy under different amounts of blinding pulse energy, which indicates that the detection probability can vary from 0% to 100% with the increase of trigger pulse energy.

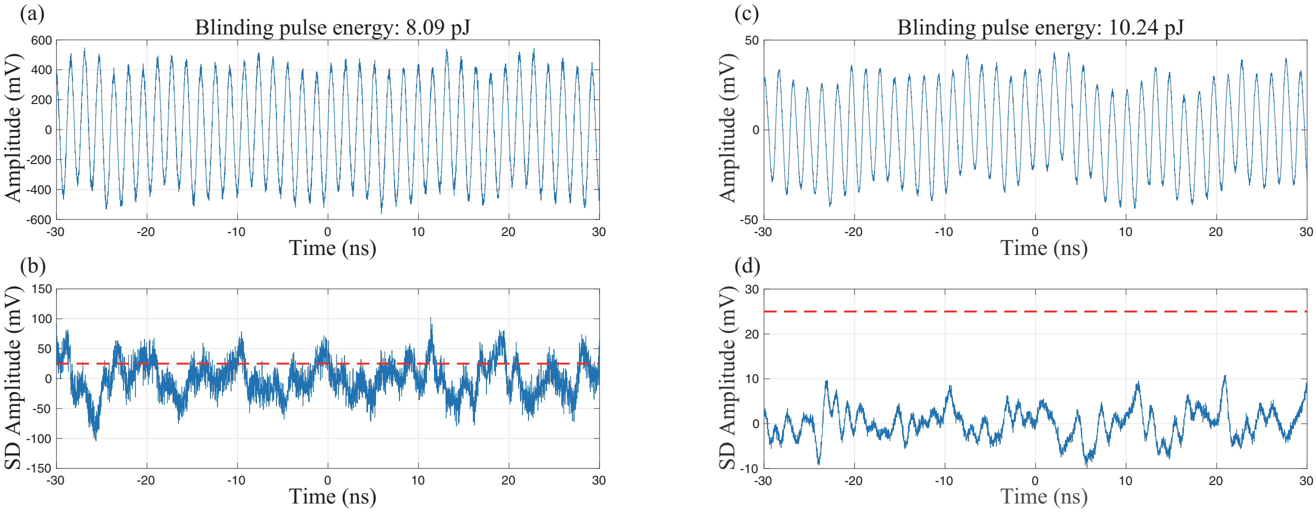

FIG. 6. Amplitude of the avalanche signal under specific blinding pulse energies. (a) The waveform of the avalanche signal after the filtering circuit but before SD processing and (b) the waveform of the SD avalanche signal when the blinding pulse energy is 8.09 pJ, in which case the SD APD detector is not blinded. (c) The waveform of the avalanche signal after the filtering circuit but before SD processing and (d) the waveform of the SD avalanche signal when the blinding pulse energy is 10.24 pJ, in which case the SD APD detector is blinded. The red dashed line represents the discrimination level.

Therefore, for a polarization-encoding BB84 QKD systems with passive basis choice Eve can obtain the key by conducting a fake-state attack [11]. Specifically, Eve first intercepts the single photon sent by Alice and randomly selects a basis to measures it as Bob does. Then she resends Bob a trigger pulse superimposed on the blinding pulse according to the measurement result. If Bob's basis choice is consistent with Eve's, only one of the four detectors responds and the detection event is the same as that measured by Eve. Otherwise, since the energy of the trigger pulse is divided into two parts, no SD APD detector clicks. Here we simply assume that all four SD APD detectors follow the same functional behavior. Finally, Eve can acquire the identical final key by monitoring the classical channel between Alice and Bob.

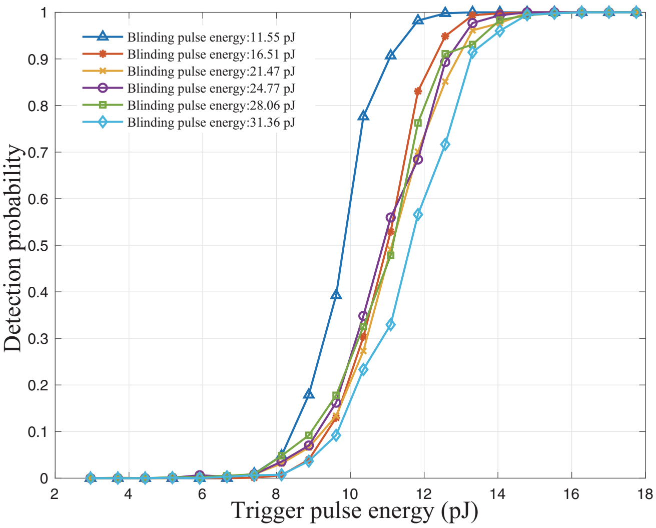

FIG. 7. Detection probability as the function of trigger pulse energy under different amounts of blinding pulse energy.

Although the trigger pulse enables the detection probability to reach 100% in the case of high energy, in order to conduct a perfect eavesdropping, the energy of the trigger pulse needs to satisfy the requirement in a BB84 QKD system proposed in Ref. [11], which can be expressed as

$$E_{\text{always}} \leqslant 2 \times E_{\text{never}}, \tag{1}$$

where E_{always} and E_{never} represent the energy of a trigger pulse when the detection probability is 100% and 0%, respectively. In the experiment, the case that the blinding pulse energy is 11.55 pJ satisfies this requirement. When the trigger pulse energy is lower than 6.656 pJ the detection probability is 0%. At the same blinding pulse energy, the maximum energy of the trigger pulse that Eve can send is 13.312 pJ, and the corresponding detection probability of the SD APD detector is 100%. Therefore, Eve can completely control the output of SD and does not increase the error rate of the final key, which does not expose the existence of Eve. Similarly, for blinding pulse energy of 16.51 pJ, 21.47 pJ, 24.77 pJ, 28.06 pJ, and 31.36 pJ, the corresponding maximum detection probability is 99.37%, 27.3%, 7.08%, 9.2%, and 3.67%, respectively, when no QBER is introduced. It is notable that these non-100% detection probabilities can be hidden by the channel loss during the fake-state attack. We remark that this testing is a proof-of-principle demonstration to disclose the threat of strong-pulse-illumination attack on the SD APD detector. For a real QKD system with multiple SD APD detectors, strong-pulse illumination shall be tested for all the SD APD detectors, whose various responses shall be thoroughly considered to conduct the attack, similar to that in Refs. [11,13,15].

V. DISCUSSION

So far, some investigations have contributed to the security of SD APD detectors. In Ref. [32], researchers disclosed a type of pulsed blinding method, in which $\bar{V}_{\text{peak}}^{\text{SD}}$ is a relatively large value. Therefore, fluctuation in the blinding pulses may cause avalanche signal amplitude to overcome the discrimination level, making the detector resume counting again. However, in our experiment, by using blinding pulse with higher energy, we directly lower the $\bar{V}_{\mathrm{peak}}^{\mathrm{SD}}$ of the avalanche signal. Compared to the previous blinding attack, the pulse-illumination attack demonstrated in this work drastically reduces the influence of optical power fluctuation and causes the detector to be blinded more stably.

Significantly, the pulse-illumination attack might partially invalidate practice criteria proposed in Ref. [31]. First, for the criterion of monitoring the photocurrent [31], although it is an effective method to defend cw bright-light attack, it may be bypassed by a group of blinding pulses that are used in the pulse-illumination attack. Specifically, a group of blinding pulses accumulatively introduces a high photocurrent, which varies over time and may be filtered out by a photocurrent monitor that contains a low-pass filter or has limited bandwidth [34]. Thus the instant high photocurrent may lower the bias voltage across the APD to blind the SD APD detector. Second, for the criterion of avoiding use of a quenching or biasing resistor with resistance value higher than 50 kΩ [31], even though the bias resistance of the tested SD APD detector is only 1 kΩ, which satisfies the requirement, the strong-pulse illumination still blinds the SD APD detector.

Third, according to the requirements c) and e) proposed in Ref. [31], setting a well-selected discrimination level can perceive the reduction of excess voltage through the residual capacitive background, because the capacitive response residual can overcome the discrimination level when the APD's reverse bias voltage decreases [31]. However, for the tested SD APD detector, the capacitive response residual does not greatly increase to overcome the discrimination level with the reduction of excess voltage. We perform an experiment to explore the relationship between voltage drop and the SD APD capacitive response measured before SD processing. By varying the reverse bias voltage of the APD, the capacitive response of the APD is measured under dark condition. For each set voltage drop, the capacitive amplitude of 1920 consecutive periods is recorded, and we make statistics on the peak values of the capacitive amplitude in each period. As shown in Fig. 8, by decreasing the bias voltage of SD APD, the amplitude of APD's capacitive response does not increase greatly and is far below the discrimination level. It is different from the explanation proposed in Ref. [31]. To understand the origin of the discrepancy, we analyze the internal circuit of the SD APD detector. The failure to recover the count rate may be due to the existence of a filter in the circuit. The capacitive response is filtered in advance, thus reducing the influence of the capacitive response residual. Although the filter can help better distinguish weak avalanche signal from the capacitive response, it also leads to the SD APD being blinded under the strong-pulse illumination.

Based on the experimental testing, we propose a list of criteria as follows to resist the pulse-illumination attack on SD APD detectors.

(a) Use a bias resistance with a proper value. The resistance only slightly lowers the bias voltage, helping stop the avalanche, whereas it shall not let the bias voltage rapidly decrease, avoiding a potentially blinding effect.

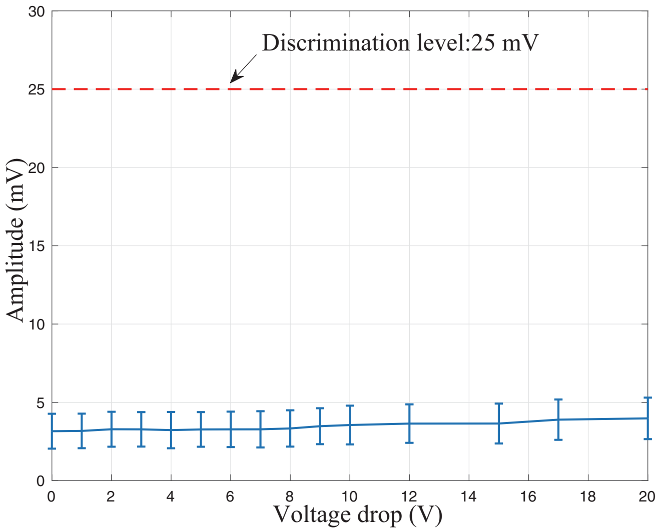

FIG. 8. APD capacitive response measured before the SD processing as a function of the dc bias reduction below its normal value. The red dashed line represents discrimination level and the blue line represents average amplitude and standard deviation of capacitive response.

(b) Use an optical power limiter or an optical fuse. Adding a special passive component, such as an optical power limiter [35] or an optical fuse [36], to sense and respond to instant high-optical power at the SD APD detector's input can prevent the strong pulse from passing through.

(c) If a filter is applied, use one with an appropriate passband. The used filter shall filter out the noise but partially show the capacitive response in the filtered signal, which may help the SD APD detector to defend against the strong-pulse-illumination attack without significantly weakening the performance of the SD APD detector.

(d) Set an appropriate discrimination level. No matter the temperature change of the working environment or long time running, doing so not only ensures that the SD APD is not disturbed by noise, but also enables the capacitive response residual overcoming the discrimination level when excess voltage reduces.

(e) Carefully monitor temporally the avalanche signal after the filtering circuit but before SD processing or the one after SD. Cautiously design the monitor to sense the temporal change of the signals and verify that no other loophole is introduced.

VI. CONCLUSION

In summary, we experimentally investigate the behavior of the SD APD under the strong-pulse illumination. We show that the strong-pulse illumination can hack SD APD detectors in high-speed quantum-key-distribution systems to learn the secret key without introducing extra QBER. Based on the testing results, we find that the strong-pulse-illumination attack presents blinding stability and the strong optical pulse can be used as an alternative tool for an eavesdropper to blind the SD APD detector. Moreover, we propose a list of criteria to enhance the practical security of SD APD detectors. This work greatly contributes to improving the security of the practical high-speed QKD system.

ACKNOWLEDGMENTS

We thank K. Zaitsev, V. Makarov, P. Xu, C. Wu, and Q. Zheng for helpful discussions. This work was funded by the National Natural Science Foundation of China (Grants No. 61901483 and No. 62061136011), the National Key Research and Development Program of China (Grant No. 2019QY0702), and the Research Fund Program of State Key Laboratory of High Performance Computing (Grant No. 202001-02).

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)* (IEEE Press, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[4] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[5] K. Inoue, E. Waks, and Y. Yamamoto, Differential Phase Shift Quantum Key Distribution, Phys. Rev. Lett. **89**, 037902 (2002).

[6] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, Phys. Rev. Lett. **92**, 057901 (2004).

[7] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. **87**, 194108 (2005).

[8] Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, Gigahertz quantum key distribution with InGaAs avalanche photodiodes, Appl. Phys. Lett. **92**, 201104 (2008).

[9] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, Opt. Express **16**, 18790 (2008).

[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[12] F. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12**, 113026 (2010).

[13] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[14] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser Damage Helps the Eavesdropper in Quantum Cryptography, Phys. Rev. Lett. **112**, 070503 (2014).

[15] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, IEEE J. Quantum Electron. **52**, 8000211 (2016).

[16] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, Insecurity of Detector-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **117**, 250505 (2016).

[17] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-Seeding Attack in Quantum Key Distribution, Phys. Rev. Appl. **12**, 064043 (2019).

[18] V. Chistiakov, A. Huang, V. Egorov, and V. Makarov, Controlling single-photon detector id210 with bright light, Opt. Express **27**, 32253 (2019).

[19] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution, Phys. Rev. Appl. **13**, 034017 (2020).

[20] S. Sun and A. Huang, A review of security evaluation of practical quantum key distribution system, Entropy **24**, 260 (2022).

[21] P. Chaiwongkhot, J. Zhong, A. Huang, H. Qin, S.-C. Shi, and V. Makarov, Faking photon number on a transition-edge sensor, EPJ Quantum Technol. **9**, 23 (2022).

[22] A. Huang, A. Mizutani, H.-K. Lo, V. Makarov, and K. Tamaki, Characterisation of state preparation uncertainty in quantum key distribution, arXiv:2205.11870.

[23] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, Protecting fiber-optic quantum key distribution sources against light-injection attacks, arXiv:2201.06114.

[24] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, After-gate attack on a quantum cryptosystem, New J. Phys. **13**, 013043 (2011).

[25] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).

[26] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[27] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography, Appl. Phys. Lett. **98**, 231104 (2011).

[28] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems, Opt. Express **20**, 18911 (2012).

[29] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution, IEEE J. Sel. Top. Quantum Electron. **21**, 6601305 (2015).

[30] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[31] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, Best-Practice

Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution, Phys. Rev. Appl. **9**, 044027 (2018).

[32] M.-S. Jiang, S.-H. Sun, G.-Z. Tang, X.-C. Ma, C.-Y. Li, and L.-M. Liang, Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems, Phys. Rev. A **88**, 062335 (2013).

[33] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, High speed single photon detection in the near infrared, Appl. Phys. Lett. **91**, 041114 (2007).

[34] Z. Wu, A. Huang, H. Chen, S.-H. Sun, J. Ding, X. Qiang, X. Fu, P. Xu, and J. Wu, Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination, Opt. Express **28**, 25574 (2020).

[35] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim, Securing practical quantum communication systems with optical power limiters, PRX Quantum **2**, 030304 (2021).

[36] S.-i. Todoroki and S. Inoue, Observation of blowing out in low loss passive optical fuse formed in silica glass optical fiber circuit, Jpn. J. Appl. Phys. **43**, L728 (2004).