Editors' Suggestion

Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution

A. Koehler-Sidki,[1,2] J. F. Dynes,[1] M. Lucamarini,[1] G. L. Roberts,[1,2] A. W. Sharpe,[1] Z. L. Yuan,[1,*] and A. J. Shields[1]

[1]*Toshiba Research Europe Ltd., Cambridge Research Laboratory, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom*

[2]*Engineering Department, University of Cambridge, 9 J. J. Thomson Avenue, Cambridge CB3 0FA, United Kingdom*

(Received 14 November 2017; revised manuscript received 23 February 2018; published 18 April 2018)

Fast-gated avalanche photodiodes (APDs) are the most commonly used single photon detectors for high-bit-rate quantum key distribution (QKD). Their robustness against external attacks is crucial to the overall security of a QKD system, or even an entire QKD network. We investigate the behavior of a gigahertz-gated, self-differencing (In,Ga)As APD under strong illumination, a tactic Eve often uses to bring detectors under her control. Our experiment and modeling reveal that the negative feedback by the photocurrent safeguards the detector from being blinded through reducing its avalanche probability and/or strengthening the capacitive response. Based on this finding, we propose a set of best-practice criteria for designing and operating fast-gated APD detectors to ensure their practical security in QKD.

DOI: 10.1103/PhysRevApplied.9.044027

I. INTRODUCTION

Quantum key distribution (QKD) is a method of secure communication whose security is guaranteed by the laws of physics and does not depend on any assumption of an eavesdropper's (Eve's) computational power [1,2]. In its implementation, semiconductor avalanche photodiodes (APDs) are the most used single-photon detectors because they can operate at temperatures obtainable by thermoelectric cooling, or even at room temperature [3,4]. For this reason, they have naturally attracted intensive scrutiny in the QKD community [5]. The blinding attack, in particular, has been demonstrated to be the most effective. Here, Eve first shines bright light onto the receiver's detectors, which brings them under her control [6–8] and then uses a faked state attack in an intercept and resend configuration, which ensures that the receiver's detectors click only when he chooses the same basis as hers [9]. Under a favorable setting [10], Eve can gain all information on the final key without introducing a quantum bit error.

With advances in fast-gating techniques [11–17], APD detectors can count single photons at gigahertz rates [18], and their importance in QKD has grown considerably [19–23]. Gigahertz-clocked self-differencing (SD) detectors have enabled a secure key rate exceeding 10 Mbit/s [24] and can support a communication distance over 200 km of fiber [25], while their robustness for real-world deployment has been routinely proven in field trials [26–28]. However, little scrutiny has been devoted so far to the security of these fast-gated detectors, except a recent study on a moderate-speed SD detector [29]. A set of best-practice criteria for designing and operating these detectors is still lacking, although an incorrectly designed or ill-set detector will be guaranteed to bring vulnerability into a QKD system [30].

All fast-gating techniques use high-frequency gating to periodically switch on the detector for single-photon detection, although they may differ in how the signal is processed after optical detection, i.e., how the strong capacitive response to the fast-gating signal is removed. Here, we investigate the behavior of a gigahertz-gated SD detector under strong illumination to gain insights into the behavior of fast-gated detectors. While an appropriately set detector shows resilience against blinding attacks, we explore the detector parameter space where the device becomes prone to blinding. Our analysis reveals that the negative feedback by the photocurrent of a properly set SD APD prevents the detector from being blinded, and this conclusion is further supported by theoretical modeling. The feedback reduces the avalanche probability and increases the detector capacitance, with a combined effect that safeguards the detector from the blinding attacks. Our findings enable us to propose a set of best-practice criteria for designing and operating these detectors to ensure their practical security in QKD.

II. EXPERIMENTAL SETUP

The device under test is a fiber-coupled $(\mathrm{In,Ga})\mathrm{As/InP}$ APD which is thermoelectrically cooled to $-30\,^{\circ}\mathrm{C}$ and has

*zhiliang.yuan@crl.toshiba.co.uk

 © 2018 American Physical Society

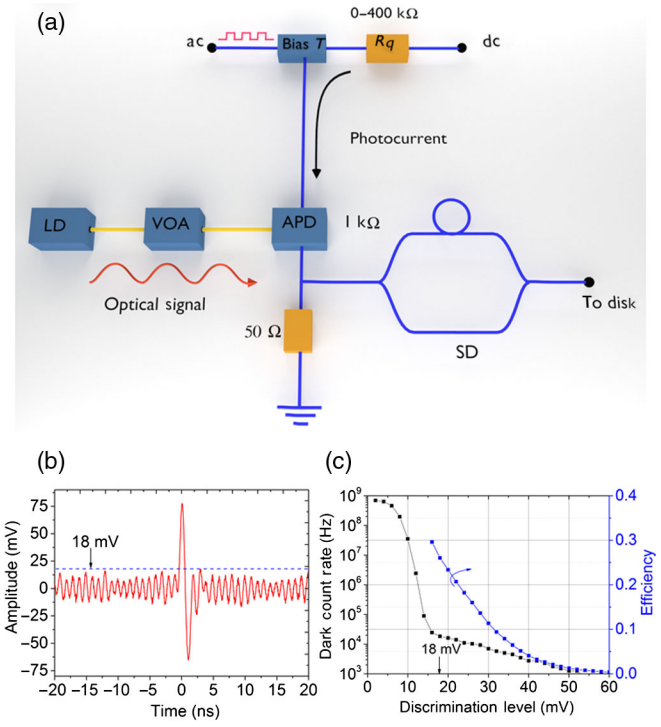

FIG. 1. (a) Setup for characterizing the self-differencing detector under bright illuminations. LD, laser diode; VOA, variable optical attenuator; SD, self-differencer; R_q, quenching resistor. (b) A SD output waveform showing a single avalanche rising above the capacitive response residual. (c) Detection efficiency and dark count rate as a function of the discrimination level. 18 mV is marked as our chosen appropriate discrimination level.

a breakdown voltage of 51.8 V. Generic electronics in the form of a dc voltage source and pulse generator are used to provide the SD APD with a constant dc bias of 51.6 V and a 1-GHz square wave with a peak-to-peak amplitude of 4.6 V, respectively. This bias condition results in an excess voltage of $V_{\mathrm{ex}}^{0} = 2.1$ V over its breakdown voltage. The series resistance of the APD is measured to be 1.0 kΩ. A variable quenching or biasing resistor is applied in the biasing circuit for later convenience, and its initial value is set to zero. A continuous-wave distributed-feedback *C*-band laser is used to illuminate the APD, and the output is amplified by two 20-dB amplifiers before being measured using a 16-GHz oscilloscope. The overall experimental setup is given in Fig. 1(a).

Under fast gating, an APD produces a strong capacitive response which can be much stronger than the avalanche signals arising from photon detections. To suppress such a response and enable photon detection, the SD circuit splits the output of the APD in half, shifting one of those halves by a gating period and then recombining the two halves in order to cancel the strong capacitive response of the detector [12]. Figure 1(b) shows a typical waveform of a SD output, with an avalanche signal rising above the residual, uncanceled background of the detector capacitive response. It is important to choose an appropriate discrimination level that rejects the residual capacitive background while accepting photon-induced avalanches with a maximal probability. Figure 1(c) shows the detector efficiency and dark count rate as a function of the discrimination level. The dark count rate shows a kink at the discrimination level of 16 mV, indicating the threshold above which the dark avalanches have replaced the capacitive residuals to be the dominant contribution to the measured dark count rate. While we could use this level, we set the discrimination level about 10% higher at 18 mV in order to have a tolerance margin. The detector is measured to have a single-photon detection efficiency of 26% for pulsed light and a dark count rate of approximately 23 kHz for this discrimination level. Setting a higher discrimination leads to a lower detection efficiency and dark count rate. More detrimentally, doing so can also favor blinding, as we show later, and therefore goes against the best practice of using SD APDs.

III. SD APD UNDER STRONG ILLUMINATION

Gated APDs are often simplified as a binary detector; i.e., their avalanche amplitude is independent of the number of photons that triggered it [31]. Under such a simplification, a SD detector's count rate (f_C) can be written as

$$f_C = f(1 - P_{\mathrm{click}})P_{\mathrm{click}} = fe^{-\mu\eta}(1 - e^{-\mu\eta}), \qquad (1)$$

where P_{click} is the probability of an avalanche being generated, f is the gating frequency, μ is the photon flux per gate, and η is the probability that a photon initiates a macroscopic avalanche.

Equation (1) highlights the nature of the self-differencing circuit, which requires an avalanche to be followed by no avalanche in order to be registered as a count. If two subsequent counts occur, then the cancellation effect causes one of them not to be counted. If $P_{\mathrm{click}} = 1$, then every gate contains an avalanche and they all cancel each other out, resulting in a count rate of zero. Therefore, under blinding conditions, we expect a count rate of zero when $\mu\eta \gg 1$, translating to a blinding power of about 100 nW for the current detector under continuous-wave excitation; see Fig. 2 (the dashed line). This blinding power is 3 to 4 orders of magnitude lower than that required for conventional gated APDs [6], and this finding has lead to the concern that such intrinsic imperfection threatens the security of a high-bit-rate QKD system using SD detectors [29].

To examine this prediction, we subject our detector to continuous-wave illumination from the laser diode. Figure 2 shows the detector count rate as a function of the incident optical power for various discrimination levels. We first look at the result obtained with the appropriate discrimination level of 18 mV. In the weak illumination regime ($\lesssim 10$ nW), the detector behaves like a typical single-photon detector. Its count rate is initially dominated by dark count noise, then increases linearly due to a

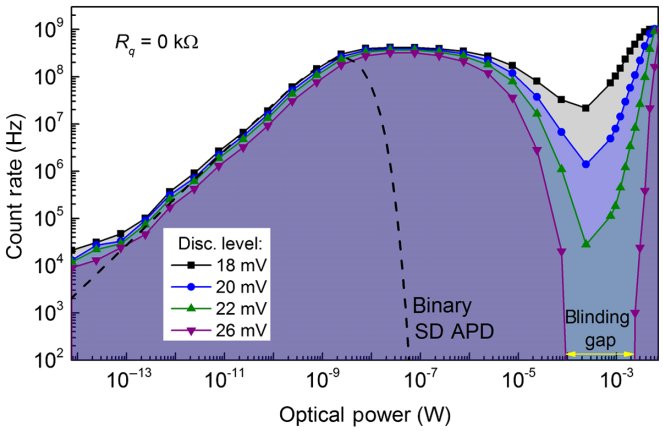

FIG. 2. Detector count rates as a function of incident optical power from a continuous-wave C-band laser diode with different discrimination levels. The variable quenching resistor is set to 0 Ω. The dashed line represents Eq. (1) with a constant $\eta = 0.028$ for continuous-wave illumination.

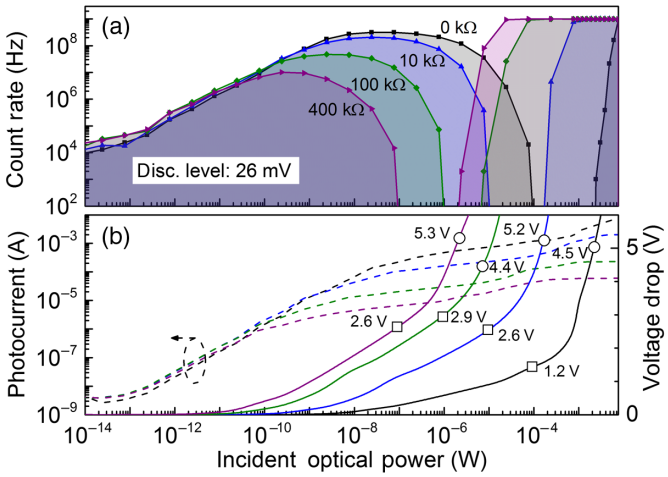

FIG. 3. Detector behavior with different quenching resistor values. (a) Detector count rates as a function of the incident optical power at an ill-set discrimination level of 26 mV. (b) Measured photocurrents and calculated voltage drop in the detector bias. The same color codes are used in (a) and (b) to represent different quenching resistor values.

detection of incoming photons before saturation at about 4 nW. Beyond saturation, the detector exhibits a count-rate plateau between 10 nW to 2 μW, while Eq. (1) predicts an immediate, sharp drop in the count rate. When the optical power is greater than 2 μW, the count rate starts to fall noticeably because of the SD cancellation between neighboring gates. However, the fall only creates a shallow dip with a local minimum of 21.4 MHz at approximately 0.23 mW. We do not observe detector blinding, i.e., the count rate falling to zero, for incident power up to 7 mW.

By increasing the discrimination level, both the detection efficiency and the saturation count rate become lower, as a higher discrimination level rejects a larger fraction of self-differenced signals. More strikingly, the count-rate dip becomes deeper. At 26 mV, the detector registers a zero count rate with an incident power between 0.1 and 2.5 mW. The existence of this blinding gap makes Eve's blinding attack feasible, and this result leads to an unsurprising conclusion that an inappropriately set SD detector is vulnerable, just like its low-speed counterparts [30]. We note that the minimum blinding power is still more than 3 orders of magnitude larger than that predicted by Eq. (1).

To understand the origin of the discrepancy, we perform another experiment by varying the resistance value of the quenching resistor in the dc path of the detector biasing circuit. While use of a quenching resistor is common for free-running APD detectors [32], it is unnecessary for gated APDs because an avalanche is automatically quenched after a detection gate. Figure 3(a) shows the count-rate dependencies for different resistance values together with that obtained without a quenching resistor. Here, we choose to use the ill-set discrimination level of 26 mV to enhance the blinding effect. A blinding gap exists for all resistance values, but the gap shifts to lower power regions as the resistance value increases. With 400 kΩ, the blinding power is just 100 nW, which is 3 orders of magnitude lower than in the 0 kΩ case.

Figure 3(b) shows the measured detector photocurrent (the dashed lines) as a function of the incident optical power. Flowing through the resistive components, including both the quenching resistor and the APD itself, the photocurrent creates a voltage drop and therefore lowers the detector reverse bias; see Fig. 3(b) (the solid lines). This voltage drop has two direct effects. First, it reduces the avalanche probability (η). The higher the incident power, the lower the excess bias and avalanche probability. This outcome explains why the detector requires a much higher optical power to become blinded than that expected from Eq. (1) and the formation of the count-rate plateau. Second, it lowers the avalanche signal amplitude and, consequently, the differential signal between adjacent detector gates. A larger quenching resistor makes the detector excess bias drop faster, as shown in the following equation:

$$V_{\mathrm{ex}} = V_{\mathrm{ex}}^{0} - IR, \tag{2}$$

where V_{ex}^{0} is the excess bias under dark conditions, I is the photocurrent, and R is the total series resistance, including both the intentional quenching resistor and the internal series resistance of the detector. The larger the value of R, the smaller the required photocurrent to reduce the excess bias, V_{ex}, to zero, which results in an earlier blinding. The voltage drop corresponding to blinding is marked in Fig. 3(b) with empty squares.

A third effect caused by the photocurrent can explain the count-rate recoveries shown in Fig. 3(a). We mark in the figure the voltage values corresponding to the recovery point after each blinding gap with an empty circle. The voltage

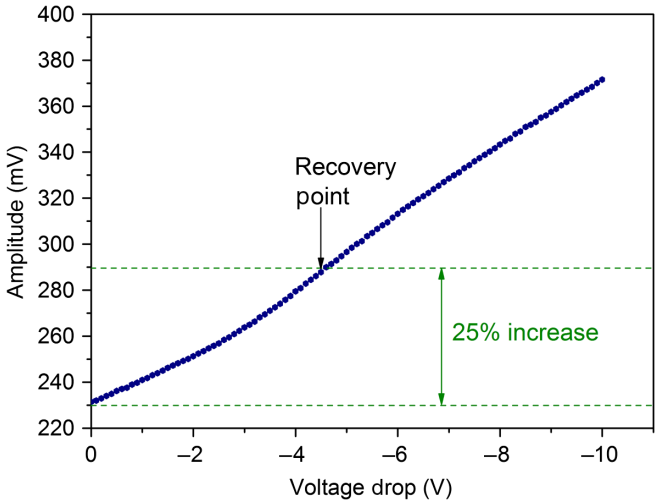

FIG. 4. APD capacitive response measured before the self-differencing circuit as a function of the dc bias reduction below its normal value. We mark the point corresponding to the count-rate recovery as shown in Fig. 3.

drop values are all around 5 V. This observation provides a key to understanding the count-rate recoveries, as we explain here. A SD circuit suppresses the detector capacitive response but will always leave a residual background due to its finite performance. The amplitude of such background is proportional to the APD capacitance [see Fig. 1(b)], which depends on the thickness of its depletion layer that is reverse-bias dependent [33]. A voltage drop leads to an increase in the capacitance and hence the amplitude of the residual background, which eventually overcomes the discrimination level and revives the counting rate. This explanation agrees with the count rate reaching 1 GHz for all quenching resistor values; see Fig. 3(a).

To provide further support to this argument, we measure the APD capacitive amplitude under dark conditions before the SD circuit as we reduce the dc bias applied to the device. As shown in Fig. 4, we find that, at the point of recovery, the response increases in amplitude by 25% of its original value, where there is a bias reduction of 4.5 V. This quantity of bias reduction can be realized using 2.3 mW of optical illumination for the case of the biasing resistor being set at zero. Because of the imperfect cancellation of the SD, the increased capacitance of the APD translates to a larger background after the SD circuit. This measurement result also justifies our choice of the appropriate discrimination level as being only 10% above the capacitive background (see our previous discussion), as this level can easily be overcome by such a dramatic increase in the residual capacitive signal. We note that the measured increase of the capacitive signal is applicable to all fast-gated APDs [11–17].

With both sides of each blinding gap accounted for, it is natural to understand the gradual disappearance of the blinding gap when lowering the discrimination level (Fig. 2). In a "blinding" gap, the SD output signal is made up of two components with opposing trends. The differential output of the SD circuit becomes smaller as the incident power increases because each detector gate is more likely to produce an avalanche with a saturated amplitude or the amplitude itself is reduced by the lowered excess bias. Concurrently, the residual capacitive background gains strength due to the reduction of the APD reverse bias. The latter can overcome an appropriately set discrimination level before the photon-induced signal falls completely under.

The above explanation is distinctively different from the gain modulation that has prevented conventional gated APDs from blinding [30]. Although still present, the modulation of the photocurrent by detector gating is periodical and considerably weaker than the capacitive response, and therefore its contribution to the self-differencer output is negligible. Laser intensity fluctuations can also produce self-differencing signals that can overcome a detector discrimination level at high illumination power, particularly when pulsed optical excitation is used [29]. However, this mechanism does not play the dominant role in our case using continuous-wave illumination. First, it is incompatible with our observation in Fig. 3 that the recovery power can vary over 3 orders of magnitude for the same detector and blinding laser, with the lowest recovery power being merely 2 μW. Second, the intensity fluctuation should produce a maximum count rate that is half of the gating frequency, while we observe a maximum count rate of 1 GHz.

IV. MONTE CARLO SIMULATION

We perform a Monte Carlo simulation to reproduce the experimental observation shown in Fig. 2. For each APD gate, we compute its avalanche current $(i_1, i_2, i_3, \ldots)$ and then determine the current difference between neighboring gates $(\Delta_n = i_n - i_{n-1})$. Together with the capacitive residual background (σ_{SD}), this differential current represents the self-differencing output, and we compare the value of $\Delta_n + \sigma_{\mathrm{SD}}$ against the discrimination level (δ) to decide whether a gate produces a count. In the simulation, we take into account the negative feedback of the photocurrent. This effect lowers the avalanche probability, which is related to the excess voltage described in Eq. (2). This reduced excess bias increases the capacitive residual σ_{SD}, which is a result of the reduction of the APD's charge layer depletion. The photon-number-dependent [34] avalanche amplitude that is saturated at a high photon number is also accounted for.

Figure 5 shows the Monte Carlo simulation results using the above model and a typical set of parameters (see the caption), with the exception of various discrimination levels. For comparison, we replot the experimental data (the symbols) showing a blinding gap and obtained with a 26-mV discrimination level, as well as the analytical calculation (the dashed line) for a binary detector using

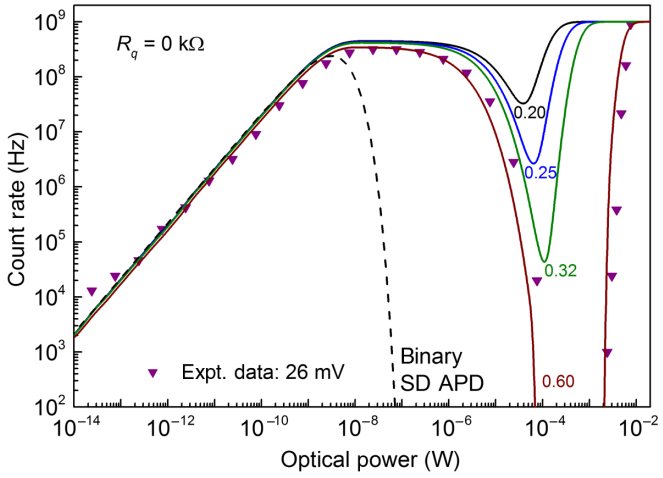

FIG. 5. Monte Carlo simulation results (the solid lines) of the detector count rate as a function of incident optical power with different discrimination levels. Experimental data for a 26-mV discrimination level is shown for comparison. The dashed line shows the expected count rate for a binary detector, i.e., an APD with a constant avalanche probability and an avalanche amplitude that is photon-number independent. Parameters are $V_{ex} = 2.1$ V, $R_{APD} = 1$ kΩ. $\sigma^0_{SD} = 0.64$, and $\eta(0) = 0.028$. The discrimination levels shown in the figure and σ_{SD} are in units of I_0, which is the average current of single-photon-induced avalanches in the absence of a noticeable photocurrent.

Eq. (1) with a constant η. We are able to see that the Monte Carlo simulation successfully reproduces the experimental observations. First, the simulation confirms the detector blinding at a high discrimination level and the subsequent count recovery due to the increased capacitive response. Second, it replicates the blinding power being 3 orders of magnitude higher than expected for the binary detector. Finally, the blinding gap disappears with lower discrimination levels and the count-rate dip becomes shallower. Although the simulation is based on a simple and intuitive model, it confirms again the effects of negative feedback on the detector photocurrent.

Having understood the effect of the negative feedback of the photocurrent, we can reliably discuss the impact of Eve's blinding attacks on self-differencing detectors. To succeed in blinding attacks, Eve has to blind all single-photon detectors in a system, i.e., each of them registering zero or finite count rates that are negligible when compared with that expected by the legitimate QKD users. To keep hidden, her attack must not introduce detectable changes. It is fair to say that an Eve using the same equipment as we use, i.e., a continuous-wave laser at 1606 nm with 1-GHz-clocked semiconductor SD APDs, achieves neither when SD detectors are appropriately set. As shown in Fig. 2, Eve's attack laser produces a count rate exceeding 10 MC/s, comparable to the state-of-the-art raw key rates. At the same time, Eve's attack produces a detectable photocurrent on the order of 1 mA, thereby underlining that correctly set SD detectors are resilient to a certain type of blinding attack.

V. BEST-PRACTICE CRITERIA

We propose below a list of best-practice criteria to be followed in either designing or operating self-differencing detectors to mitigate blinding attacks.

(a) Monitor the photocurrent. The blinding current is still on the order of 1 mA, which can easily be sensed using a resistor of 1 kΩ.

(b) Avoid use of a quenching or biasing resistor of high resistance value because it can provide overly strong feedback to the excess bias and therefore severely limit the maximum count rate. We recommend a value less than 50 kΩ when a biasing resistor is desired to limit the current for protecting the APD detector. This resistance value still allows a maximum count rate of over 30 MC/s and has a negligible effect on the QKD key rate.

(c) Set an appropriate discrimination level. Doing so not only gives an optimal detection efficiency but also enables protection by sensing the excess voltage reduction through the residual capacitive background.

(d) Use different resistance values in a QKD system that contains more than one detector. A careful choice of resistance values can prevent an overlap of the detectors' blinding gaps (see Fig. 3) when their discrimination levels are inadvertently ill set.

(e) Verify whether the capacitive response residual can overcome the detector discrimination level when the APD's reverse bias is lowered below its breakdown. If not, detune the self-differencing circuit slightly and/or reset the detector discrimination level.

(f) Model the behavior of the detector, as in Fig. 5, to ensure that it behaves as expected in the protected environment of a laboratory.

Compliance with the above criteria does not introduce a significant increase in system complexity or a reduction in the secure key rate. This is an advantage as compared with the countermeasure of monitoring the detector efficiency [35], which offers a higher level of assurance, but at the expense of the system simplicity and key rate. We note that the applicability of the proposed criteria is not limited to SD detectors but extends to other types of high-speed gated APD detectors, as discussed earlier. They can all improve their resilience from the negative feedback of the photocurrent, despite their use of different signal cancellation techniques.

VI. CONCLUSION

In summary, we experimentally study and theoretically model in this paper the behavior of an (In,Ga)As self-differencing detector under bright illumination from a continuous-wave laser. We show that the intrinsic, negative

feedback of the photocurrent prevents not only an early blinding but also a complete blinding at very high attacking powers by strengthening the residual capacitive background. We show the importance of setting an appropriate discrimination level, as doing so has a direct impact on the detector's behavior under Eve's blinding attack. Our findings allow us to outline a set of best-practice criteria to ensure the most secure conditions to operate these detectors in QKD systems.

ACKNOWLEDGMENTS

A. K.-S. gratefully acknowledges financial support from the Engineering and Physical Sciences Research Council (EPSRC) and from Toshiba Research Europe Ltd.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[3] N. Walenta, T. Lunghi, O. Guinnard, R. Houlmann, H. Zbinden, and N. Gisin, Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature, J. Appl. Phys. **112**, 063106 (2012).

[4] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, Room temperature single-photon detectors for high bit rate quantum key distribution, Appl. Phys. Lett. **104**, 021101 (2014).

[5] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

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

[7] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, Controlling an actively-quenched single photon detector with bright light, Opt. Express **19**, 23590 (2011).

[8] 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).

[9] V. Makarov and D. R. Hjelme, Faked states attack on quantum cryptosystems, J. Mod. Opt. **52**, 691 (2005).

[10] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Avoiding the blinding attack in QKD, Nat. Photonics **4**, 800 (2010).

[11] N. Namekata, S. Sasamori, and S. Inoue, 800 MHz Single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating, Opt. Express **14**, 10043 (2006).

[12] 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).

[13] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes, Appl. Phys. Lett. **95**, 091103 (2009).

[14] Y. Nambu, S. Takahashi, K. Yoshino, A. Tanaka, M. Fujiwara, M. Sasaki, A. Tajima, S. Yorozu, and A. Tomita, Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution, Opt. Express **19**, 20531 (2011).

[15] Y. Liang, E. Wu, X. Chen, M. Ren, Y. Jian, G. Wu, and H. Zeng, Low-timing-jitter single-photon detection using 1-GHz sinusoidally gated InGaAs/InP avalanche photodiode, IEEE Photonics Technol. Lett. **23**, 887 (2011).

[16] A. Restelli, J. C. Bienfang, and A. L. Migdall, Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz, Appl. Phys. Lett. **102**, 141104 (2013).

[17] D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, Y.-J. Qian, Z. Zhou, G.-C. Guo, and Z.-F. Han, Sine-wave gating InGaAs/InP single photon detector with ultralow afterpulse, Appl. Phys. Lett. **110**, 111104 (2017).

[18] K. A. Patel, J. F. Dynes, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, Gigacount/second photon detection with InGaAs avalanche photodiodes, Electron. Lett. **48**, 111 (2012).

[19] 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).

[20] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes, Opt. Express **19**, 10632 (2011).

[21] K. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, High-speed wavelength-division multiplexing quantum key distribution system, Opt. Lett. **37**, 223 (2012).

[22] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza *et al.*, A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing, New J. Phys. **16**, 013047 (2014).

[23] L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, Long-distance copropagation of quantum key distribution and terabit classical optical data channels, Phys. Rev. A **95**, 012301 (2017).

[24] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Lucamarini, Y. Tanizawa, H. Sato, and A. Shields, 10 Mb/s quantum key distribution, http://2017.qcrypt.net/scientific-program/ (unpublished).

[25] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).

[26] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Field test of quantum key distribution in the Tokyo QKD Network, Opt. Express **19**, 10387 (2011).

[27] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert *et al.*, Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber, Opt. Express **22**, 23121 (2014).

[28] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, Quantum key distribution with hacking countermeasures and long term field trial, Sci. Rep. **7**, 1978 (2017).

[29] 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).

[30] 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).

[31] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, A high speed, postprocessing free, quantum random number generator, Appl. Phys. Lett. **93**, 031109 (2008).

[32] R. E. Warburton, M. Itzler, and G. S. Buller, Free-running, room temperature operation of an InGaAs/InP single-photon avalanche diode, Appl. Phys. Lett. **94**, 071116 (2009).

[33] T. Lee and S. Sze, Depletion layer capacitance of cyclindrical and spherical *p-n* junctions, Solid State Electron. **10**, 1105 (1967).

[34] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, O. Thomas, and A. J. Shields, Probing higher order correlations of the photon field with photon number resolving avalanche photodiodes, Opt. Express **19**, 13268 (2011).

[35] 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).