White Rose Research Online

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk
Universities of Leeds, Sheffield and York

Deposited via The University of York.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/167275/

Version: Published Version

Article:
Koehler-Sidki, A., Dynes, J. F., Martinez, A. et al. (2019) Intrinsic mitigation of the after-gate attack in quantum key distribution through fast-gated delayed detection. Physical Review Applied. 024050. ISSN: 2331-7019

https://doi.org/10.1103/PhysRevApplied.12.024050

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Intrinsic Mitigation of the After-Gate Attack in Quantum Key Distribution through Fast-Gated Delayed Detection

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

[1] *Cambridge Research Laboratory, Toshiba Research Europe Ltd., 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 29 March 2019; revised manuscript received 15 July 2019; published 23 August 2019)

The information-theoretic security promised by quantum key distribution (QKD) holds as long as the assumptions in the theoretical model match the parameters in the physical implementation. The superlinear behavior of sensitive single-photon detectors represents one such mismatch and can pave the way to powerful attacks hindering the security of QKD systems, a prominent example being the after-gate attack. A long-standing tenet is that trapped carriers causing delayed detection can help mitigate this attack, but despite intensive scrutiny, it remains largely unproven. Here we approach this problem from a physical perspective and find evidence to support a detector's secure response. We experimentally investigate two different carrier-trapping mechanisms causing delayed detection in fast-gated semiconductor avalanche photodiodes, one arising from the multiplication layer and the other arising from the heterojunction interface between absorption and charge layers. The release of trapped carriers increases the quantum bit error rate measured under the after-gate attack above the typical QKD security threshold, thus favoring the detector's inherent security. This represents a significant step to avert quantum hacking of QKD systems.

DOI: 10.1103/PhysRevApplied.12.024050

I. INTRODUCTION

Quantum key distribution (QKD) promises secure distribution of cryptographic digital keys [1], spurring significant development of the technology. This has rapidly matured and is now stepping out of the laboratory and into deployment in optical fiber networks [2–8]. Contributing to its maturity, a great deal of research has been devoted to quantum hacking [9–13], which identifies imperfections of QKD components from their theoretical models and evaluates their implications for QKD security. Best-practice criteria and countermeasures can then be developed [14–21] to reinforce the identified weak components and reclaim implementation security.

Because of their exposure to the quantum channel, single-photon detectors in QKD systems have been subjected to most hacking attacks in the past decade [22–24]. Weak detectors have been demonstrated to be under full control of an eavesdropper (Eve), resulting in a collapse of security [25]. Detector loopholes can be completely closed by novel protocols that achieve measurement-device-independent security [26–28]. However, these protocols require an intermediate relay and therefore their deployment in the network is unfavorably complex when compared with that of standard point-to-point QKD links. A solution to regain detector security is thus highly desirable for relayless QKD links.

Single-photon detectors based on semiconductor (In,Ga)As avalanche photodiodes (APDs) serve the majority of links in existing QKD networks [2–7] because they operate at temperatures that are easily within reach of thermoelectric cooling [29] or even room temperature [30]. The state-of-the-art systems can offer a key rate exceeding 10 Mb/s [31] and operate over 200 km of fiber [32].

Attacks on (In,Ga)As APDs have revealed their vulnerabilities, most of which have been dealt with because Eve's attack either changes the detector characteristics or produces a detectable fingerprint. However, as a special class of faked state attack [9], the faint after-gate attack [33] remains an open threat. This is because detectors under such an attack will maintain their single-photon sensitivity and will not produce a massive photocurrent [34] as in bright-illumination attacks.

When a photon is absorbed by an (In,Ga)As APD it generates an electron-hole pair. The hole can then become trapped in defects or at barriers and is released with a certain probability related to the characteristic time

*amks31@outlook.com
†james.dynes@crl.toshiba.co.uk

 © 2019 American Physical Society

constant of the trap. As opposed to trapped carriers arising from macroscopic avalanches, whose lifetimes are on the order of microseconds, the trapped-hole lifetime at the material interface is of subnanosecond order. Such trapping, therefore, does not have an effect in megahertz-gated detectors [33,34]. However, under gigahertz gating, the trapping time becomes comparable with the the detector gating period and the release of such carriers in subsequent gates can result in substantial numbers of delayed detection events. This could provide a means to mitigate the faint after-gate attack. Hence, it is natural to look at fast gigahertz-gated APDs [29] as a potential countermeasure to this attack. So far, however, there is no study supporting this conjecture. Earlier investigations were largely concerned with megahertz-gated detectors, where the time between gates is significantly longer than the decay time of trapped carriers. Furthermore, the analysis of the quantum bit error rate (QBER) previously focused solely on Eve's target gate [33,34], due to the contribution from delayed detection events being negligible.

In this work, we investigate two sources of carrier trapping in fast-gated (In,Ga)As APDs, one from the multiplication layer and the other from the heterointerface between the two materials, and find that both cause a non-negligible delayed-detection probability.

This previously perceived drawback of single-photon (In,Ga)As APDs can be used to detect an after-gate attack. The delayed photodetection introduces an increase in the QBER of the QKD system that unveils the attack, thus promoting fast-gated devices as a means of mitigating this potential vulnerability. In addition to that, we show that the amount of induced QBER in Eve's absence is not excessive and still allows efficient QKD operation if the appropriate gating frequency is chosen.

II. CARRIER TRAPPING

To give some notion of the trapping mechanism, we provide a schematic of a typical (In,Ga)As avalanche photodiode in Fig. 1(a). An incoming photon is absorbed in the intrinsic (In,Ga)As region, where an electron-hole pair is generated and subsequently separated by the electric field in this region. The hole needs to overcome the potential barrier that arises from the valence-band mismatch [35] [the shaded purple area in Fig. 1(a)] to reach the InP multiplication region so as to have a finite probability of initiating a macroscopic avalanche that can be electronically registered. During the generation of a macroscopic avalanche, some of the avalanche carriers may become trapped and can subsequently be released at a later time, causing a secondary avalanche, known as an "afterpulse." The release timescale is on the order of several microseconds or greater [36–38].

We stress that the term "afterpulse" or "afterpulsing" refers only to clicks that are correlated with a previous

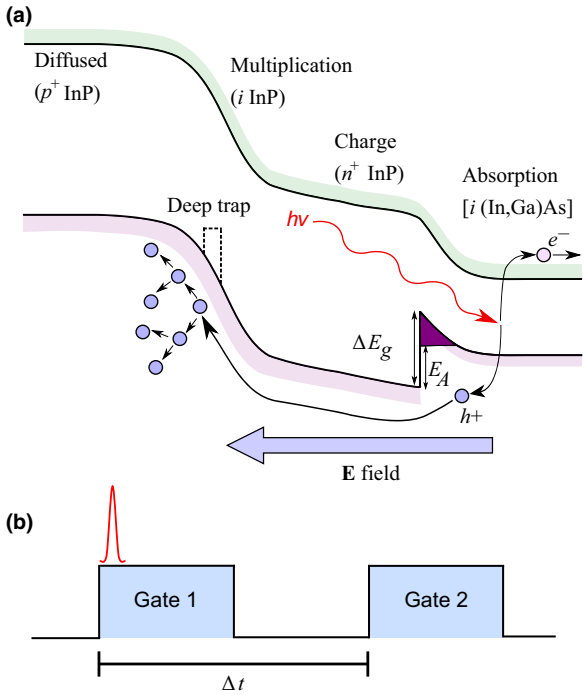

FIG. 1. (a) Typical band diagram of separate absorption, charge, and multiplication structure of an (In,Ga)As/InP APD, where E_g is the band-gap offset and E_A is the effective barrier height arising at the interface between the APD absorption and charge regions. (b) Gating scheme. Electron-hole pairs are generated at the start of gate 1 when the laser is timed to arrival and experience an exponential decay between the two gates. The proportion of holes left over at gate 2 is related to the decay constant, which is in turn related to the activation energy given by the barrier height, E_A.

detection event. The notion of "delayed detection," on the other hand, is more general and it encompasses afterpulsing. It refers to *all* detection events originating from trapped carriers, even those that did not give rise to a detected avalanche in a previous gate.

The ability of the hole to overcome the valence-band discontinuity, which is a potential barrier, directly affects device characteristics such as detection efficiency and timing response [39]. However, it is reasonable to conclude that the hole trap time is significantly shorter than 1 ns because subnanosecond gated APDs still show detection efficiencies as high as 55% [29]. If the decay time were longer than 1 ns, then fewer than half of the generated carriers would overcome the barrier and the detection efficiency would not be able to exceed 50%. We can infer from this analysis that the hole-trap lifetime is at least 3 orders of magnitude shorter than that of deep traps causing afterpulses and we specially devised an experiment to study it, which is schematically illustrated in Fig. 1(b). We optically excite an APD at the start of a gate. When a hole fails to overcome the potential barrier within gate 1, it will have a finite probability to overcome the barrier and initiate a

macroscopic avalanche in subsequent gates within several nanoseconds.

III. TRAPPING AT THE MATERIAL INTERFACE

For this study we operate the (In,Ga)As APDs in gated Geiger mode at a clock frequency of 1 GHz. The avalanche signals are discriminated with the help of self-differencing circuits that remove the capacitive response to the applied gate [40]. A telecom-C-band passively-mode-locked laser synchronized to the APD gating frequency and with a repetition frequency of 20 MHz and a pulse width of 3 ps is used to illuminate the APD via its single-mode-fiber pigtail. We follow the best-practice criteria [20] to set the discrimination level of the self-differencing APD. Time-tagging electronics with a dead time of 50 ns are used to record the photon-detection histogram [29]. We measure several (In,Ga)As APDs with different active diameters: 50 and 16 μm. In this paper we present results from two 16-μm devices: namely, APD 1 and APD 2. The 50-μm devices show similar behavior. Unless otherwise stated, the data presented are from APD 1.

We first examine the effect of the interface on the APD. The APD is characterized as having a single-photon-detection efficiency of 28% and an afterpulsing probability of 4% at room temperature. Here the optical flux μ is maintained at 0.1 photons per pulse and the laser delay is set to enable the photon arrival at the beginning of the illuminated gate [schematically shown in Fig. 1(b)], thus allowing an avalanche to have sufficient time to grow above the discrimination level and hence have a maximum detection efficiency. Figure 2(a) shows a typical photon-detection histogram under such illumination conditions. The illuminated gate gives a pronounced peak arising from single-photon detection events. Immediately after this peak, the count rate experiences a fast decay before reaching an approximately flat background at the fifth gate. The flat background is attributed to detector dark and afterpulsing counts. The elevated count rates between 2 and 4 ns (gates 2–4) cannot be attributed to detector afterpulsing because the time tagger has a dead time of 50 ns. Moreover, the subnanosecond decay time is orders of magnitude faster than typical lifetimes of deep traps that are responsible for afterpulsing. We attribute the elevated count rates at these gates to delayed photon detection caused by hole trapping at the absorption-charge interface.

The above conclusion is supported by temperature-dependent measurements. It is possible to extract the interface trapping lifetime by comparing counts in gates 1 and 3 in the histogram data (gate 2 is ignored due to the possibility of cancellation from the self-differencer). Plotting these lifetimes at different temperatures in an Arrhenius configuration, where the excess bias as a proportion of the breakdown voltage is kept constant for each temperature, allows us to extract the effective barrier height, E_A, at the material interface [35], shown in Fig. 2(b), where the gradient is equal to E_A/k_BT. The activation energies (tens of millielectronvolts, corresponding to lifetimes of several hundreds of picoseconds) and the trend of higher excess biases resulting in overall shorter lifetimes, and consequently lower activation energies, are consistent with the literature [35,41]. This implies that carriers with decays of several hundred picoseconds are dominated by trapping at the heterointerface when the APD is illuminated with fluxes on the order of single photons.

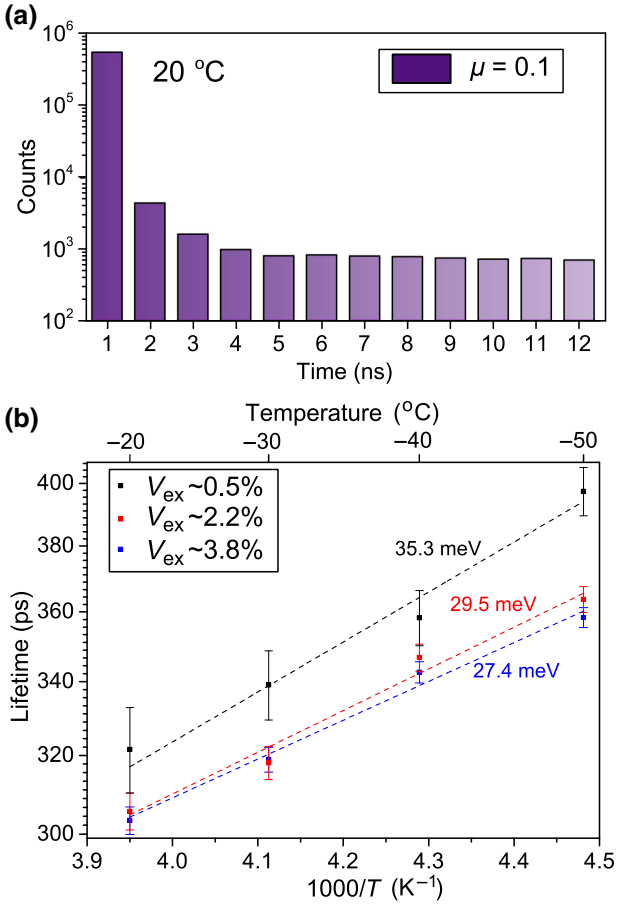

FIG. 2. (a) Time-resolved histogram of detected counts of the APD under illumination by a pulsed laser with flux $\mu = 0.1$, clearly demonstrating an exponential decay in counts after the initial illuminated gate. (b) Arrhenius plot showing the single-photon detection efficiency as a function of the inverse of the temperature, where the respective gradients allow the extraction of the hole activation energy.

IV. MITIGATING THE FAINT AFTER-GATE ATTACK

Carriers with decays of several hundred picoseconds could be used to mitigate the faint after-gate attack. This is because Eve's attempt to mount such an attack using moderately high fluxes would result in delayed detection

events that would alert the users to her presence. The subnanosecond separation between gates in gigahertz-clocked APDs is sufficiently narrow to allow delayed detection as a result of carriers with a decay on the order of several hundred picoseconds to be observed, where they would be missed in slower, megahertz-clocked systems [33,34]. However, we find that in this regime, traps in the multiplication region become the dominant contribution to delayed detection events, which we now examine.

In more detail, the after-gate attack is a class of faked state attack, which itself is a type of intercept-and-resend attack [9]. Eve measures the photons sent by the transmitter, Alice, with a copy of Bob's apparatus. She then sends her own pulses to Bob, which are detected only if he chooses the same measurement basis as Eve, otherwise he registers nothing. In this way, after Alice and Bob have exchanged basis information, Eve has a string that is perfectly correlated with that held by Alice and Bob. The aim for Eve is thus to send a pulse that at full power registers a click with a detection probability of 1 and at half power (corresponding to incompatible bases) registers with probability 0. More generally, when the probability at full power exceeds twice that at half power in this manner, the detector behavior is said to be "superlinear." If Eve sends attack pulses toward the end of Bob's APD gate, she can maximize the ratio of detection probabilities of full-power and half-power pulses such that she learns most of the key and also generates a sufficiently low QBER to go undetected. The original demonstration [33] involved sending pulses of moderately high photon flux (approximately 40 photons per pulse) at the end of the APD gate.

By obtaining the detection probability at full power and half power, one can derive the resultant QBER using the following equation from Ref. [33]:

$$Q = \frac{2p_h - p_h^2}{2p_f + 2(2p_h - p_h^2)}, \tag{1}$$

where p_f is the detection probability at full power and p_h is the detection probability at half power. This equation ignores any errors arising from dark counts or afterpulsing and thus focuses only on the detection probability at the target gate. If the QBER drops below approximately 21%, this indicates superlinearity as $p_f > 2p_h$.

We demonstrate here that gigahertz-gated APDs could also show superlinear behavior when the delayed photon-detection events are not considered (i.e., the situation when only the target gate is considered). Here we measure the detection probability at full power (80 photons per pulse) and half power(40 photons per pulse) of an optical trigger pulse as a function of the arrival time of the laser pulse on the APD (these values are chosen due to their use in the original demonstration in Ref. [33], but other optical powers are also investigated, the results of which are given in the Appendix). We do this by varying the delay on the pulse generator providing the ac signal to the APD. The result is given for two APD temperatures (20 and −30 °C) as the black lines in Figs. 3(a) and 3(c). At a certain temporal separation from maximum detection, the QBER drops below 11% (illustrated as the dotted red line), reaching a minimum of approximately 7% at around 153 ps at room temperature, suggesting Eve could mount such an attack at this delay and remain undetected. Either side of this trough, the QBER is 25% since either $p_f = p_h = 1$ around the center of the gate or $p_f = p_h \approx 0$ outside the gate.

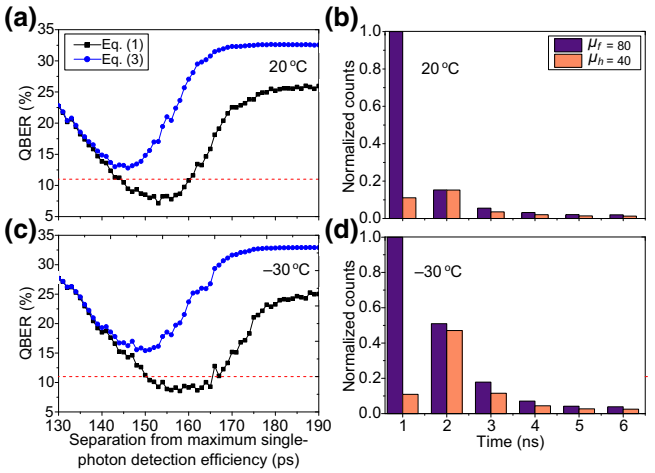

FIG. 3. (a) QBER as a function of temporal separation from the maximum single-photon detection efficiency. The black line indicates the case where delayed detection is ignored and the QBER is calculated with Eq. (1) and Eve appears not to introduce a QBER greater than 11% and thereby remains undetected. When delayed detection is taken into account, as shown by the blue line calculated with Eq. (2), the QBER rises above 11% and she can be detected. (b) Histograms taken at minimum QBERs showing the detection probabilities in each gate at 20 °C. Under half-power illumination of $\mu = 40$ (in orange), gate 2 is always larger than gate 1, which would result in a QBER of 50% in that gate. (c) As (a) but measured with the APD at −30 °C. (d) As (b) but measured with the APD at −30 °C.

To probe the effect of delayed detection, we examine the histograms in the vicinity of the superlinear regime (i.e., corresponding to the conditions of an after-gate attack), as shown in Figs. 3(b) and 3(d). For the cases where Eve is using the after-gate attack, a higher proportion of clicks occur in the gate adjacent to the target gate (gate 2 as opposed to gate 1) when she chooses an incompatible basis to Bob, shown as the salmon-colored bars. Delayed detection events would have a 50% QBER as they are uncorrelated with Alice's qubit preparation. Since a higher proportion of clicks occur in the adjacent gate for incompatible bases, this corresponds to an afterpulsing probability of more than 100%, which is significantly greater than the 4% afterpulse probability measured for the single-photon case. For compatible bases, the detection probability in gate 2 is approximately 15% of that in

gate 1, which is in stark contrast to the single-photon case shown in Fig. 2(a), where gate 2 is approximately 1% of the size of gate 1.

The degree of trapping is greater in the multiphoton case than in the single-photon case for two reasons. First, more carriers are generated in the absorption region for the multiphoton case; therefore, the probability of a carrier becoming "trapped" at the material interface is greater. Second, as pulses are sent at the end of the gate, the electric field in the device is lower; therefore, carriers that are generated and subsequently trapped in the multiplication region have a smaller probability of escaping the traps within the initial gating period and are consequently more likely to be released in the following gating period when the electric field is raised again.

This underlines the importance of incorporating delayed detection events into the calculation of the QBER. To this end, we estimate the delayed-detection probabilities under full-power and half-power pulses and add them to the detection probability without delayed detection. This leads us to the following expression for the QBER:

$$Q' = \frac{2p'_h - (p'_h)^2}{2p'_f + 2[2p'_h - (p'_h)^2]}, \tag{2}$$

$$p'_{f\,(h)} = p_{f\,(h)} + \overline{p}_{\mathrm{DD}}, \tag{3}$$

$$\overline{p}_{\mathrm{DD}} = \frac{1}{4}p_{\mathrm{DD}|f} + \frac{1}{2}p_{\mathrm{DD}|h}. \tag{4}$$

Q' in Eq. (2) represents the QBER measured in the presence of the after-gate attack when delayed detection is taken into account. This is accounted for with the term $\overline{p}_{\mathrm{DD}}$, which represents the average probability per gate of a one-gate-delayed detection. The factor 1/4 (1/2) in the expression is due to their being a click in Bob's detectors when his basis matches (does not match) Eve's basis in the previous gate. In Eq. (4), $p_{\mathrm{DD}|f}$ ($p_{\mathrm{DD}|h}$) is the probability of a delayed detection in gate n when a full-power (half-power) pulse impinges on the detector at gate $n-1$, represented as a violet-colored (salmon-colored) bar in Fig. 3(b) [Fig. 3(d)].

Using this result, we plot the resulting QBER from Eq. (2) with blue lines in Figs. 3(a) and 3(c). As is apparent from the figures, the 11% security threshold, typical of the BB84 protocol, is now overcome. This result highlights the effectiveness of the delayed detection at mitigating the faint after-gate attack.

By including contributions from delayed detection in Eq. (2), we assume Eve mounts her attack all of the time. We therefore address the case where Eve attacks only a fraction of the gates. In this case, the overall QBER will be smaller than the 11% tolerance, and thus Alice and Bob will not abort their key exchange. However, Eve's information will also be smaller. In a worst-case scenario, we can reason as follows [17]. We assume for simplicity that Eve attacks "every other gate," so she introduces errors in the odd gates and no errors in the even gates. Therefore, the users can notice an odd-even pattern in the measured QBER and could draw two different key rates, one extracted from odd gates and one extracted from even gates. The resulting key rate will be given by the sum of the two partial key rates. Because of the convexity dependence of the key rate on the QBER [42,43], the resulting key rate when Eve attacks every other gate will always be greater than the key rate when she attacks every gate, thus confirming that it would be best for Eve to attack every gate. This conclusion can be generalized to different attacking patterns and holds under the assumption that the users can recognize such patterns from a detailed analysis of their QBER. However, we also notice that the above rationale overestimates Eve's chances to gain information because it assumes that the QBER is zero for the cases where Eve does not attack, whereas in the real case it is clearly larger than zero due to the delayed-detection effect.

We also consider the case where Eve attempts to conduct a hybrid attack, where she attempts to blind counts in gate 2 and thus suppress any erroneous counts as a result of her after-gate attack on gate 1. While it has been shown that blinding attacks are ineffective against appropriately operated self-differencing APDs [20], this places the onus on the user, and such devices are often improperly used. However, for Eve to blind gate 2, because of the cancellation nature of the self-differencing circuit, she would also have to shine strong light on gate 1, thereby negating her original attack.

V. TRAPPING IN THE MULTIPLICATION REGION

Differently from the interface trapping effect, the origin of the delayed detection is predominately due to carrier trapping in the multiplication region. Consequently these delayed detection events feature longer lifetimes compared with that of interface trapping events. At 20 °C, the lifetimes extracted from Fig. 3(b) are comparable to the those in the case shown in Fig. 2(b). However, at −30 °C, the lifetimes become much longer than those shown in Fig. 2(b) for the same temperature, by approximately 2–3 times. This suggests the existence of deeper traps and that these traps, rather than the material interface, are responsible for the delayed detection in the after-gate attack. We believe these deeper traps are located in the multiplication region.

This is supported by our measuring the detection probability in the adjacent gate [gate 2 in Fig. 1(b)] as a function of separation from the maximum detection for APD 2, as shown in Fig. 4. From left to right, the optical photon pulse is moving away from the end of gate 1 and approaching the start of gate 2. The detection probability initially decreases as the laser approaches gate 2. Here

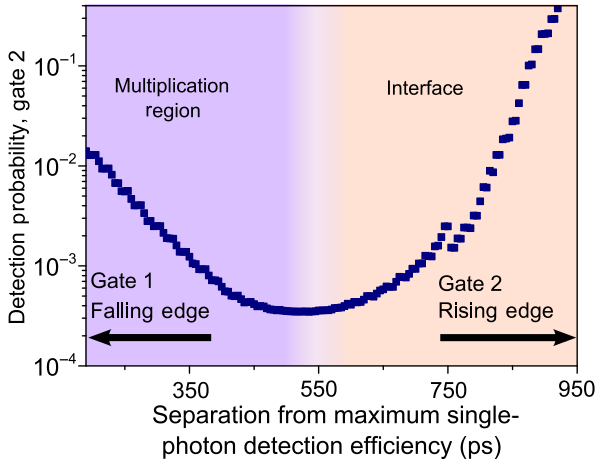

FIG. 4. Detection probability in gate 2 as a function of temporal separation from the maximum single-photon detection efficiency for APD 2. The increased detection probability on the left-hand side can be explained by the dominance of trapping in the multiplication region.

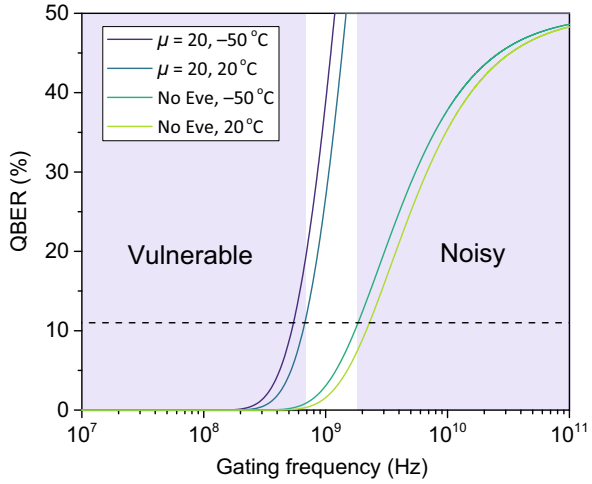

FIG. 5. QBER as a function of gating frequency at 20 and −50 °C. The central white region indicates suitable operation, where the APD is both safe from the after-gate attack and has sufficiently low noise to make QKD possible.

impact ionization is occurring and therefore carriers are multiplied and a portion of these multiplied carriers are trapped in the multiplication region, shown in purple. The high detection probability on the left-hand side roughly coincides with the QBER dip, underlining that delayed detection largely arises from trapping in the multiplication layer. If the interface were the major contributor, the detection would continue to increase the closer to gate 2 the optical pulse is as the carriers have a progressively shorter time to decay before gate 2 is activated. However, at a certain point the probability flattens and then begins to increase, an observation which is consistent with interface trapping, suggesting it starts to take over once carriers cease to become trapped in deep levels at the multiplication region.

Using the discovery of delayed detection allows us to define the best practice for choosing a suitable gating frequency for QKD. For this analysis at two different temperatures, 20 and −50 °C, we consider trapping only at the material interface. This is the more-conservative definition from a security point of view, as it requires higher gating frequencies to maintain the delayed detection required to preserve the protection against the after-gate attack. This range of gating frequencies fulfills two criteria: (i) the gating frequency is low enough to separate adjacent gates temporally such that a click in the first gate has a small enough probability to have a delayed detection in the second gate without raising the QBER above the tolerance threshold of 11% under operation in the absence of Eve; (ii) equally, the gating frequency is high enough such that Eve would cause clicks in the gate adjacent to her target gate with a large enough probability to raise the QBER above the aforementioned threshold, which we examine for a conservative attacking flux of $\mu = 20$ photons per pulse that is favorable for hiding Eve's presence (see the Appendix). Our simulation result is shown in Fig. 5, with the narrow white band indicating a regime where the APD is neither too "noisy" nor "vulnerable." Because of the longer carrier decays at lower temperatures, lower temperatures are more favorable for slower gating, whereas higher temperatures are more suited to faster gating. Most significantly, gating frequencies of around 1 GHz, which are commonly used for QKD experiments (e.g., Refs. [5,31,44]) as well as in this study, fall in the white region, suggesting these are optimal values for QKD.

VI. CONCLUSION

In conclusion, we investigate two sources of trapping of carriers in (In,Ga)As APDs: at the valence-band mismatch arising at the interface between the APD absorption and charge regions, and at deep traps in the multiplication region. In characterizing the carrier lifetime at the heterojunction, we provide an explanation for short decays observed in fast-gated APDs. We determine that in the after-gate regime, however, the major contribution to delayed detection events that can provide enhanced security arises from traps in the multiplication region. We provide evidence that fast-gated APDs can be used to mitigate the after-gate attack due to the additional contribution to the QBER that arises from delayed detection events. By exploiting the intrinsic imperfection of the material interface, we are able to bound the appropriate APD gating frequency suitable for use in QKD.

ACKNOWLEDGMENTS

A.K.-S. gratefully acknowledges financial support from Toshiba Research Europe Ltd. and the Engineering and Physical Sciences Research Council through an Industrial CASE studentship.

APPENDIX

For the demonstration of the attack presented in this paper, we chose $\mu_f = 80$ and $\mu_h = 40$ as the full-power and half-power fluxes, respectively, as these were values used in the original proposal in Ref. [33]. By expanding our measurement to examine a range of fluxes at room temperature, we are able to obtain a more-general picture of the parameters that Eve could use, as shown in the measurement performed with a fast oscilloscope in Fig. 6.

The dark-purple regions within the dotted line indicate a flux and delay combination that produces a QBER that is lower than 11% when calculated with Eq. (1), within which Eve will choose to operate. The pale-yellow parts in the top left of Fig. 6 indicate a QBER of 25%, which occurs when $p_f = p_h = 1$. This overall trend in Fig. 6 implies that the closer to the center of the gate Eve moves, the smaller the flux she should use to mount her attack. This suggests that this is an extension of the original proposed after-gate attack [45], where the APD is operating in linear mode and strong pulses of power P_{th} overcome the discrimination level and cause the detector to click, whereas pulses of power $P_{\text{th}}/2$ often do not overcome the discrimination level and therefore rarely cause a click. By our focusing on the edge of the gate, a smaller flux is required to generate the same effect, which is the most-favorable case for Eve. The smallest attacking flux of $\mu = 20$ is therefore used in determining the appropriate gating frequencies in Fig. 5.

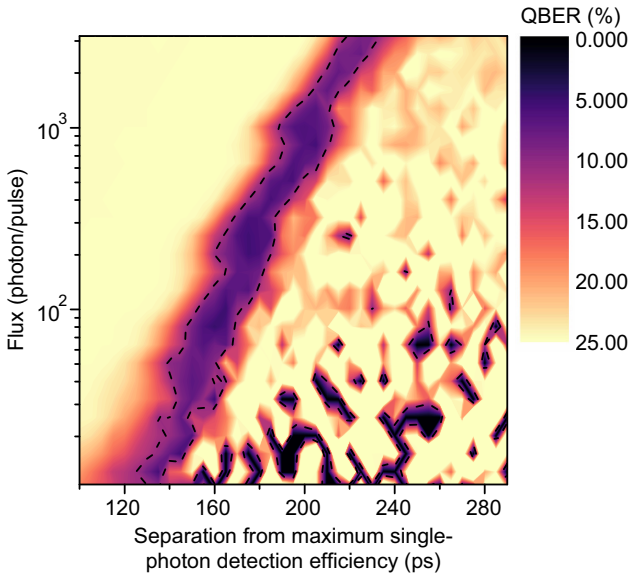

FIG. 6. Contour plot of the QBER calculated with Eq. (1) as a function of the flux of the trigger pulse and APD gate delay with respect to the laser. The region inside the dotted line indicates where the QBER is lower than 11% and thus Eve can mount a successful attack in this parameter space if delayed detection events are ignored.

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

[2] M. Peev *et al.*, The SECOQC quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[3] M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[4] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, Stability of high bit rate quantum key distribution on installed fiber, Opt. Express **20**, 16339 (2012).

[5] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, Integrating quantum key distribution with classical communications in backbone fiber network, Opt. Express **26**, 6010 (2018).

[6] 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).

[7] W. Sun, L.-J. Wang, X.-X. Sun, Y. Mao, H.-L. Yin, B.-X. Wang, T.-Y. Chen, and J.-W. Pan, Experimental integration of quantum key distribution and gigabit-capable passive optical network, J. Appl. Phys. **123**, 043105 (2018).

[8] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, Metropolitan Quantum key Distribution with Silicon Photonics, Phys. Rev. X **8**, 021009 (2018).

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

[10] 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).

[11] A. Vakhitov, V. Makarov, and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. **48**, 2023 (2001).

[12] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[13] 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).

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

[15] 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).

[16] L. Lydersen, V. Makarov, and J. Skaar, Secure gated detection scheme for quantum cryptography, Phys. Rev. A **83**, 032306 (2011).

[17] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

[18] 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**, 192 (2015).

[19] T. Ferreira da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Safeguarding quantum key distribution through detection randomization, IEEE J. Sel. Top. Quantum Electron. **21**, 159 (2014).

[20] 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).

[21] A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation, Phys. Rev. A **98**, 022327 (2018).

[22] 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).

[23] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Creation of backdoors in quantum communications via laser damage, Phys. Rev. A **94**, 030302 (2016).

[24] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Eavesdropping and countermeasures for backflash side channel in quantum cryptography, Opt. Express **26**, 21020 (2018).

[25] 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).

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

[27] S. L. Braunstein and S. Pirandola, Side-channel-free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[28] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[29] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm, J. Appl. Phys. **117**, 083109 (2015).

[30] 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).

[31] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, 10-Mb/s quantum key distribution, J. Lightwave Technol. **36**, 3427 (2018).

[32] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Simple 2.5 GHz time–bin quantum key distribution, Appl. Phys. Lett. **112**, 171108 (2018).

[33] L. Lydersen, N. Jain, C. Wittmann, O. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Superlinear threshold detectors in quantum cryptography, Phys. Rev. A **84**, 032320 (2011).

[34] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Hacking the Quantum Key Distribution System by Exploiting the Avalanche-transition Region of Single-photon Detectors, Phys. Rev. Appl. **10**, 064062 (2018).

[35] S. R. Forrest, O. K. Kim, and R. G. Smith, Optical response time of $In_{0.53}Ga_{0.47}As/InP$ avalanche photodiodes, Appl. Phys. Lett. **41**, 95 (1982).

[36] X. Jiang, M. A. Itzler, R. Ben-Michael, and K. Slomkowski, InGaAsP–InP avalanche photodiodes for single photon detection, IEEE J. Sel. Top. Quantum Electron. **13**, 895 (2007).

[37] M. Liu, C. Hu, X. Bai, X. Guo, J. C. Campbell, Z. Pan, and M. M. Tashima, High-performance InGaAs/InP single-photon avalanche photodiode, IEEE J. Sel. Top. Quantum Electron. **13**, 887 (2007).

[38] X. Jiang, M. A. Itzler, R. Ben-Michael, K. Slomkowski, M. A. Krainak, S. Wu, and X. Sun, Afterpulsing effects in free-running InGaAsP single-photon avalanche diodes, IEEE J. Quantum Electron. **44**, 3 (2008).

[39] F. Zappa, A. Lacaita, S. Cova, and P. Webb, Nanosecond single-photon timing with InGaAs/InP photodiodes, Opt. Lett. **19**, 846 (1994).

[40] 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).

[41] S. Pellegrini, R. E. Warburton, L. J. J. Tan, J. S. Ng, A. B. Krysa, K. Groom, J. P. R. David, S. Cova, M. J. Robertson, and G. S. Buller, Design and performance of an InGaAs-InP single-photon avalanche diode detector, IEEE J. Quantum Electron. **42**, 397 (2006).

[42] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[43] M. Koashi, Efficient quantum key distribution with practical sources and detectors, arXiv:quant-ph/0609180 (2006).

[44] 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).

[45] 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).