Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography

Z. L. Yuan,[1, a)] J. F. Dynes,[1] and A. J. Shields[1]
Toshiba Research Europe Ltd, Cambridge Research Laboratory, 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, UK

(Dated: 01 March 2011)

Semiconductor avalanche photodiodes (APDs) are commonly used for single photon detection in quantum key distribution. Recently, many attacks using bright illumination have been proposed to manipulate gated InGaAs APDs. In order to devise effective counter-measures, careful analysis of these attacks must be carried out to distinguish between incorrect operation and genuine loopholes. Here, we show that correctly-operated, gated APDs are immune to continuous-wave illumination attacks, while monitoring the photocurrent for anomalously high values is a straightforward counter-measure against attacks using temporally tailored light.

PACS numbers: 85.60.Gz Photo detectors; 85.60.Gw Photodiodes;

As a solution to the key distribution problem, quantum key distribution (QKD) has attracted a great deal of interest, because its underlying security is not reliant on any assumptions about an eavesdropper's (Eve's) power. Although QKD protocols can be proven to be perfectly secure, the differences between a theoretical protocol and its real-world implementation should be carefully analyzed. This helps expose weakness of specific implementations, and thus effective counter-measures can be devised. One example of this is the decoy protocol,[1–3] which not only defeats the photon number splitting attack[4,5] but also allows weak laser systems to achieve the highest key rates.[6,7]

Scrutinizing the security of QKD systems using avalanche photodiodes (APDs) is important, because they are widely used.[6–9] Recently, Lyderson *et al.*[10] used two research QKD systems to demonstrate that continuous-wave (CW) illumination can blind InGaAs APDs so that the count rate falls to zero exactly. Under such induced blindness, Eve can gain full information about the secret key in a modified intercept-resend attack with strong resent pulses. This blinding attack would be a concern for practical QKD systems if proven universally effective. Fortunately, a later experiment showed that the blinding attack is ineffective for APDs that are operated correctly.[11]

In addition to the original blinding attack, Lydersen *et al.* have also proposed a broader range of illumination attacks targeting gated detectors, including thermal blinding, thermal blinding of frames, and "sinkhole" attacks.[12] These attacks need to be carefully analyzed. In particular, efforts must be made to distinguish between incorrect operation and genuine loopholes, only after which counter-measures can be effectively constructed. Here, we study the behavior of gated InGaAs APDs under illumination ranging from 1 fW to >10 mW. Careful analysis reveals that their gain modulation naturally fends off CW bright illumination attacks, without resorting to further countermeasures. Photocurrent monitoring is effective to foil more sophisticated attacks involving temporally tailored illumination.

Figure 1(a) shows a typical circuit for a gated APD. The biasing resistor (R_{bias}) is redundant, included here only for illustrating the blinding attack.[10] A voltage pulse is used to raise the APD bias (V_g) above its breakdown voltage (V_b) [Fig. 1(b)]. Under such excessive bias ($V_{ex} = V_g - V_b > 0$), an APD can probabilistically multiply a single-photon induced charge into a macroscopic current. A detection event is registered when the voltage drop across the sensing resistor (R_s) exceeds the discrimination level (L), as illustrated in Fig. 1(c). It is common and good practice to set L as low as possible, determined here by the capacitive response. A much lower L can be achieved when the capacitive signal is removed.[13–16]

The APDs used here have absolute maximum ratings of 3 mW for optical illumination and 5 mA for reverse current. However, to investigate fully bright illumination of APDs, we exceeded these ratings by manyfold, which inevitably caused damage to the APDs. As a re-

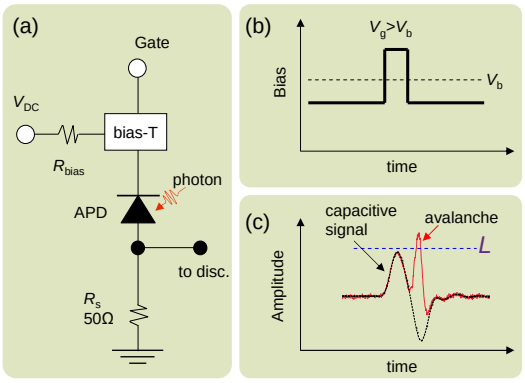

FIG. 1. (a) A schematic diagram for gated mode operation; (b) APD gating; (c) APD output waveforms showing capacitive responses and a single photon-induced avalanche. L: discrimination level.

a) Electronic mail: zhiliang.yuan@crl.toshiba.co.uk

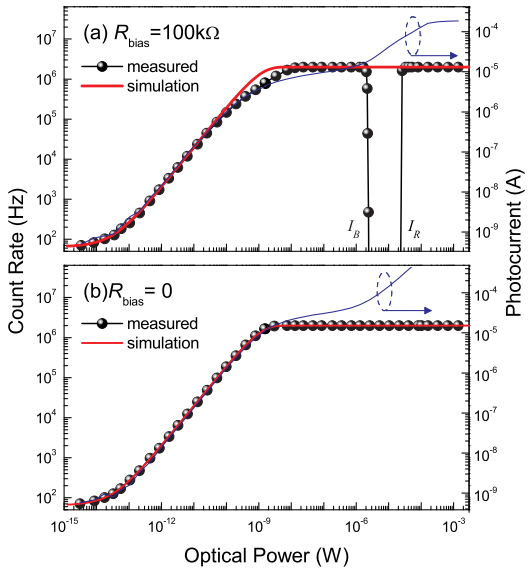

FIG. 2. Measured (symbols) and simulated count rates and photocurrent *vs.* incident optical power for (a) R_{bias} = 100 kΩ and (b) $R_{bias} = 0$.

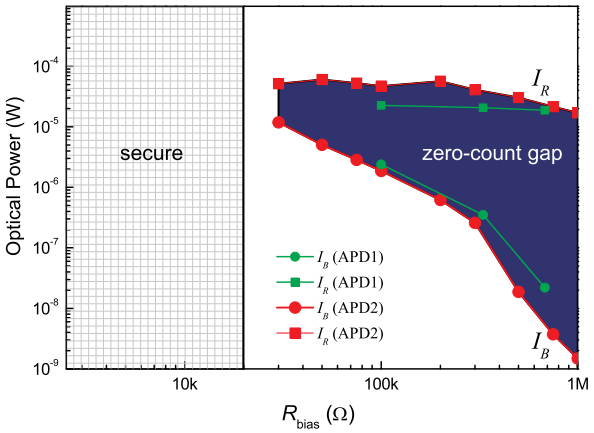

FIG. 3. I_B and I_R as a function of R_{bias}.

sult, two APDs were used to complete this study. Unless explicitly stated, the data shown in this paper refer to APD1. We adopt the same electrical setup as in our QKD experiment.[17] The DC voltage is set 1.5 V below V_b. The gating pulse has 3.5 ns duration, 4 V amplitude (V_{ex}=2.5 V) and 2 MHz repetition rate. Electrically cooled to –30°C, both APDs were measured to have a single photon detection efficiency of 11%; a value typical for InGaAs detectors. A CW laser of 1550-nm is used to illuminate the APD.

We first illustrate the detector blinding by use of a redundant R_{bias} = 100 kΩ. Figure 2(a) shows the dependencies of the count rate and photocurrent as a function of the illumination power. Both are found to have a linear dependence for an optical power of 1 nW or less. Further increasing the illumination intensity, the count rate first saturates, then falls sharply to zero, and remains at zero until it finally recovers abruptly to the saturated rate. The transitions are measured at I_B = 2.5 and I_R = 26 μW for the count rate fall and recovery, respectively. The APD can be blinded by illumination at at any power within the zero-count gap, and then manipulated using short optical pulses.[10]

The zero-count gap in Fig. 2(a) is simply a consequence of the high impedance bias resistor. Removing R_{bias} causes the zero-count gap to disappear throughout the optical power range completely, as shown in Fig. 2(b). Without such a gap, Eve cannot manipulate this detector and hence the APD is secure. The count rate is well simulated with

$$R = f_0[(1 - e^{-\mu\eta}) + P_d - (1 - e^{-\mu\eta}) \cdot P_d)], \qquad (1)$$

where f_0 is the gate repetition rate, μ the photon flux within each detection gate, η the detection efficiency, and P_d is the dark count probability. In contrast, the simulation for R_{bias} = 100 kΩ gives a higher count rate than measured when approaching count rate saturation around 1 nW, suggesting a decreasing photon detection efficiency due to the APD bias reduction via the high impedance resistor.

The zero-count gap in Fig. 2(a) is a result of the bright illumination induced photocurrent causing a voltage drop across R_{bias} and thus reducing the bias applied to the APD. At I_B = 2.5 μW, the photocurrent is measured as 19 μA, corresponding to a voltage drop of 1.9 V across the R_{bias}. Although this voltage drop is smaller than V_{ex}, it is sufficient to prevent the avalanche from evolving above the discrimination level.[18] The count recovery at I_R is due to gain modulation, which is discussed later.

We stress that $R_{bias} = 0$ is not necessary to avoid the zero-count gap. Figure 3 shows the R_{bias} dependence of I_B and I_R. With decreasing R_{bias}, the zero-count gap narrows, as I_B increases more rapidly than I_R. It is determined that for $R_{bias} \leq$ 20 kΩ, no zero-count gap is found: the APD behaves similar to the case of $R_{bias} = 0$ [Fig. 2(b)].

Setting an inappropriate discrimination level also leads to the detrimental zero-count gap. To illustrate this, we plot in Fig. 4 the AC amplitude of the APD output as a function of illumination power for various values of R_{bias}. As the illumination power increases, the AC amplitude declines first, then varies slowly, and finally recovers sharply. While all AC voltages are greater than the capacitive signal, the amplitude minimum increases with decreasing R_{bias}. For $R_{bias} \leq$ 5 kΩ, the minimum is significantly greater than the capacitive signal with clear discrimination from the capacitive signal, thus allowing persistent counting. However, if we deliberately discriminate at a level which is twice the capacitive signal, a detrimental zero-count gap would emerge even for the case of $R_{bias} = 0$.

The AC amplitudes shown in Fig. 4 are provided by the photocurrent modulated by the APD gating. In contrast to single photon detection, this gain modula-

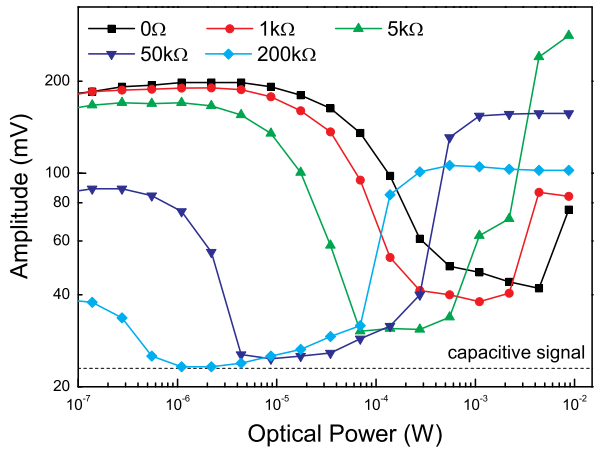

FIG. 4. Signal amplitudes by gain modulation as a function of illumination power for varying R_{bias}. The data were obtained from APD2.

tion signal becomes significant only with bright illumination. The sharp amplitude recovery at high powers is due to the APD bias reaching to its punch-through voltage, below which photon absorption does not produce a photocurrent.[19] At this voltage, electrical gating switches on/off the photocurrent, thus producing a large pulsed current.

Gain modulation might be compensated by a sophisticated Eve using temporally tailored illumination.[12] In this case, monitoring the photocurrent for anomalously high values is a straightforward counter-measure. As shown in Fig. 2, the photocurrent is proportional to the count rate in the single photon regime ($I < 1$ nW). Such a relation is also observed for high speed APDs.[20,21] By constantly monitoring the photocurrent, an anomalously high measured photocurrent, *i.e.*, exceeding the expected photocurrent in the single photon regime, can be used to foil any bright illumination attack. We stress that this measure is effective universally for all APDs, including the non-gated[22] as well as high-speed gated.[15,16,23] In comparison with the previous proposal using a separate power-meter,[22] the present solution does not need a lossy beam splitter which will inevitably deteriorate the bit rate and distance in QKD.

Before commenting on recent attacks, two measures for safeguarding APDs are listed below:

1. Avoid a high impedance biasing resistor and use a low discrimination level;

2. Monitor the photocurrent for anomalously high values.

Measure 1 is actually the very basic rule for correctly operating a gated APD.[11] Following this rule alone will prevent CW bright illumination attacks.

Now, we discuss what has caused the vulnerability in Clavis2, one of the two systems attacked by Lydersen *et al.*[10] We choose this system for discussion simply because it has more experimental details[12] available. While APDs in Clavis2 have an adequate $R_{bias} = 1$ kΩ, their discrimination levels were set at ∼80 mV, which is more than twice the value needed for rejection of the capacitive signal (35 mV).[12] Using such high discrimination level, induced blindness was then demonstrated at an illumination of 397 μW. Later, instead of correcting the discrimination levels, Lydersen *et al.* removed the non-zero R_{bias} to show the induced blindness once again at a much higher power (∼10 mW).[12] This time, the detector heating was suggested as the prime cause. In both cases, we believe the induced blindness should have been avoided if the discrimination levels were correctly set. No matter whether the illumination causes APD bias reduction[10] or device heating,[12] gain modulation always exists and should trigger a discrimination level that is correctly set. In our tests on an APD detector from Clavis2's manufacturer, we saw no evidence of an induced blindness for a CW illumination of up to 14 mW.[24] Nor did we see the induced blindness for an illumination of up to 17.8 mW on our own detector.[11]

Lydersen *et al.* also demonstrated an alternative thermal attack using temporally tailored light.[12] Attacking the Clavis2, which transmits quantum signals in frames, blinding illuminations are switched on only during the intervals between QKD frames. First, this is not a stealth attack. It gives itself away by causing extra photon clicks outside QKD frames. Even if a QKD system ignores such clicks, monitoring the photocurrent for anomalously high value is sufficient to foil this attack. The attack still requires an average optical power of 1.5 mW, the photocurrent of which will significantly exceeds the value expected in the single photon counting regime.

As a more special attack targeting AC-coupled detectors, "sink-hole" attack illuminates between gates, creating a photocurrent valley around each APD gate.[12] As AC coupling re-bases the ground level, the avalanche signal sitting in these valleys will be reduced below the discrimination level, thereby preventing detection of single photons. However, this attack still requires an illumination of around 200 μW, the photocurrent of which remains easily detectable. Moreover, such sink-hole attack is ineffective to detectors using DC coupling, in which no capacitor is used to block the DC signal before the discriminator.

Finally, we discuss the "after-gate" attack, in which Eve exploits the intrinsic linear mode of APD between gates, facilitated by the excessively long modulation gates or detection acceptance window in the QKD setup.[25] As detailed in Ref. [25], this attack induces high levels of detector afterpulsing, and thus works only on frame-based QKD systems with long intervals between frames. This attack is ineffective on continuous-running one-way systems, particularly the high speed ones.[6,7] Moreover, for any QKD systems, either narrowing the modulation gate duration or the detection acceptance window will completely defuse this attack. Nowadays, use of sub-nanosecond modulation pulses or acceptance windows in QKD is not uncommon.[6,7,9,26]

To conclude, correctly-operated, gated APDs are immune to CW bright illumination attacks. For temporally tailored illumination, monitoring the photocurrent for anomalously high values is a straightforward countermeasure.

Partial support from EU project QEssence is acknowledged.

[1] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[2] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[3] H. K. Lo, X. F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[4] M. Dušek, O. Haderka, and M. Hendrych, Opt. Commun. **169**, 103 (1999).
[5] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[6] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Opt. Express **16**, 18790 (2008).
[7] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).
[8] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, New J. Phys. **11**, 075001 (2009).
[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Opt. Express **19**, 10387 (2011).
[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[11] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).
[12] L. Lydersen, C. Wichers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).
[13] D. S. Bethune and W. P. Risk, IEEE J. Quant. Electron. **36**, 340 (2000).
[14] A. Tomita and K. Nakamura, Opt. Lett. **27**, 1827 (2002).
[15] N. Namekata, S. Sasamori, and S. Inoue, Opt. Express **14**, 10043 (2006).
[16] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **91**, 041114 (2007).
[17] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[18] Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 191107 (2010).
[19] For example, see Fig. 2 in X. Jiang, M. A. Itzler, R. Ben-Michael and K. Slomkowski, IEEE. J. Sel. Top. Quant. Electron. **13**, 895 (2007).
[20] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, New J. Phys. **11**, 045019 (2009).
[21] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, Appl. Phys. Lett. **96**, 071101 (2010).
[22] V. Makarov, New J. Phys. **11**, 065003 (2009).
[23] O. Thomas, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **97**, 031102 (2010).
[24] Model: id200. Settings: 4 MHz gating frequency and 2.5 ns gate duration. The discrimination level, as well as the bias impedance, is unknown to end-users.
[25] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[26] X. Tang, L. Ma, A. Mink, T. Chang, H. Xu, O. Slattery, A. Nakassis, B. Hershman, D. Su, and R. F. Boisvert, Proc. SPIE **7092**, 70920I (2008).