Response to "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'" [Appl. Phys. Lett. 99, 196101 (2011)]

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

(Received 14 September 2011; accepted 16 October 2011; published online 11 November 2011)

Quantum key distribution (QKD) has been proven theoretically secure at the protocol level. However, the security may be compromised through deviation from theoretical models in device implementation or operation. For each deviation, thorough understanding must be achieved in order for subsequent construction of robust countermeasures.

In Ref. 1, we have studied the effectiveness of bright illumination attacks, a group of attacks targeting gated InGaAs avalanche photodiodes (APDs).[2,3] We found that gated APDs are naturally resilient against continuous-wave (CW) attacks through the gain modulation effect.[4] The finding is contrary to the claim by Lydersen *et al.*[2] that "the loophole is likely to be present in most QKD systems using APDs to detect single photons." The detector loophole reported by Lydersen *et al.*[2] was in fact due to inappropriate settings in the discrimination level of single photon APDs. Furthermore, we discussed the respective effectiveness for temporally tailored bright illumination[3] and after-gate attacks,[5] as summarized in Table I. Against bright illumination attacks, "monitoring the photocurrent" was proposed as a counter-measure, which was based on the vast difference in the measured APD currents as compared with normal operation, see Fig. 1.

In the preceding comment,[6] we note that Lydersen *et al.* do not dispute that bright light attacks[2,3] would be ineffective if the detector parameters were set correctly, which was our main finding. Instead, they challenge the robustness of the counter-measure we proposed. To serve this challenge, they have designed a new attack[7] that uses faint optical pulses ($\leq$120 photons/pulse) only. The attack exploits the super-linear count dependence achieved by restricting the avalanche duration.[8,9] In the absence of bright illumination, Lydersen *et al.* claim, unfortunately without experimental elaboration, that the attack "would not be detectable[6]" by monitoring the current and "the afterpulsing is negligible."[7] It should be pointed out that Lydersen *et al.* reported a high quantum bit error ratio (QBER) of $>$12% during the attack, which would be easily detected by the legitimate users of the system, even for a 100 kHz clock rate which significantly favours the attacker.

Although the illumination during the attack is weak, Lydersen *et al.* have overlooked the fact that the APD gain is still large, and thus, the attack generates a sizable photocurrent that can easily be detected by the users. We prove this with a simple experiment. A gated InGaAs APD is subjected to faint illumination by a 50 ps pulsed laser. The APD is gated with 2 MHz pulses of 4 V amplitude and 3.5 ns duration, a gating condition identical to previously used in an actual QKD system.[10] Its single photon detection efficiency is measured to be 15% with a dark count probability of 3.5×10^{-5} per gate. In the attack, the pulse delay is optimized to have a minimum QBER that the attack would have caused with a flux of 120 photons. Under this optimized delay, the count probability and photocurrent are measured as a function of attacking flux, as shown in Fig. 1. Super-linearity regime used in the faint after-gate attack is identified as occurring at fluxes between 70–300 photons/pulse. Within this flux range, the APD current is macroscopic and actually easily detectable. At around 9 μA, this current is more than 40 times stronger than would be under normal QKD operation for this APD,[11] see Fig. 1.

Macroscopic current causes afterpulsing.[12] In Fig. 1, for an attacking flux less than 60 photons/pulse, the count probability shows a slightly sub-linear dependence, closely resembling that of the photocurrent. This sub-linear behavior can be explained only by the dominance of afterpulsing, and this assignment has been verified by the gated afterpulse measurement technique.[13–15] As can be extrapolated from the linear dependence, the afterpulsing is *not* negligible in the super-linear regime. Therefore, contrary to the intuitive claims by Lydersen *et al.*, the faint after-gate attack not only causes significant current, but also produces non-negligible afterpulses. In addition to the resultant QBER,[7] monitoring the APD current is an effective counter-measure against this attack, although it was initially proposed for bright illumination attacks.[1]

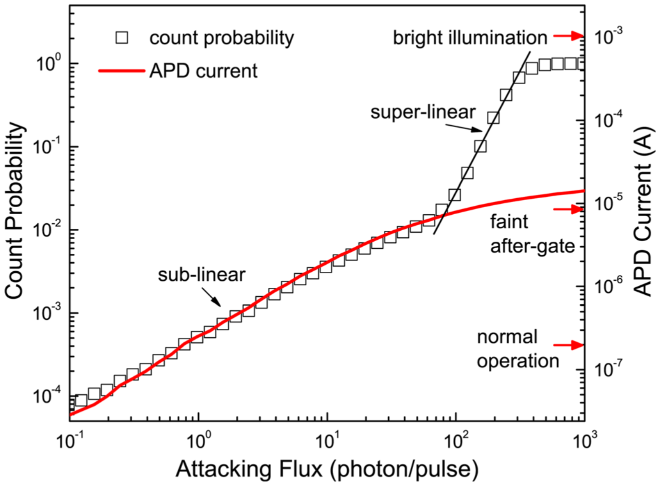

FIG. 1. (Color online) Count probability and photocurrent, when under the faint after-gate attack, as a function of photon flux. Arrows in the right axis label respective currents measured for normal operation, faint after-gate attack, and bright illumination attacks.

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

TABLE I. Summary of attacks targeting the photocurrent mode of gated InGaAs APDs.

Attack	Effectiveness (without counter-measure)	Fingerprint	Counter-measure
CW blinding[2]	Ineffective to correctly operated devices	High photocurrent	Monitor the current
CW thermal blinding[3]	Ineffective to correctly operated devices	High photocurrent	Monitor the current
Thermal blinding of frames[3]	Limited effectiveness to burst-mode systems	High photocurrent; Giveaway photon clicks	Monitor the current
Sink-hole blinding[3]	Limited effectiveness to APDs with an AC-coupled output; Ineffective to DC-coupled APDs	High photocurrent; Giveaway photon clicks	Monitor the current
After-gate[5]	Limited effectiveness to burst-mode systems	Photon arrival timing; High QBER due to afterpulses	Use of narrow modulation and/or detection acceptance window
Faint after-gate[7]	Ineffective due to high QBER	High photocurrent; High QBER due to finite count super-linearity and afterpulses	Monitor the current

Similarly to Ref. 1, the experiment shown in Fig. 1 illustrates again the importance of careful analysis of any proposed attack. Careful analysis is the very foundation, upon which a robust, effective counter-measure can be constructed. Against an attack, two strategies are usually adopted: (1) bounding the information leakage, followed by privacy amplification and (2) deterministic detection or exclusion. Only attacks that are not easily detected on a properly implemented system need to be accounted for in the privacy amplification analysis, e.g., the photon number splitting attack.[16,17] This is certainly not the case for the various detector blinding attacks which rely upon a poor design of the APD circuit and which generate a large, easily detectable photocurrent in the device.

[1] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011).

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[3] L. Lydersen, C. Wichers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).

[4] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[5] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[6] L. Lydersen, V. Makarov, and J. Skaar, Appl. Phys. Lett. **99**, 196101 (2011).

[7] L. Lydersen, N. Jain, C. Wiechers, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. A **84**, 032320 (2011)

[8] B. E. Kardynal, Z. L. Yuan, and A. J. Shields, Nat. Photonics **4**, 425 (2008).

[9] Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 191107 (2010).

[10] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[11] The APD current is measured to be 200 nA for an arrival flux of 0.1 photons/pulse at 2 MHz in the single-photon counting setting. The arrival flux is appropriate as the upper limit under normal operation.

[12] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, Appl. Phys. Lett. **96**, 071101 (2010).

[13] D. S. Bethune, W. P. Risk, and G. W. Pabst, J. Mod. Opt. **51**, 1359 (2004).

[14] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **91**, 041114 (2007).

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

[16] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[17] H. K. Lo, X. F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).