Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes

YICHENG SHI,[1] JANET ZHENG JIE LIM,[1] HOU SHUN POH,[1] PENG KIAN TAN,[1] PEIYU AMELIA TAN,[1,3] ALEXANDER LING,[1,2] CHRISTIAN KURTSIEFER,[1,2,*]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore, 117543*
[2]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore, 117542*
[3]*Singapore Telecommunications Limited, 31 Exeter Road Comcentre #15-00, Singapore 239732*
[*]*phyck@nus.edu.sg*

References and links

1. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984*, pages 175–179, 1984.
2. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283–3286, Oct 1998.
3. Ivan Marcikic, Antia Lamas-Linares, and Christian Kurtsiefer. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.*, 89:101122, 2006.
4. Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7:378–381, October 2012.
5. P. D. Townsend. Quantum cryptography in optical fiber networks. In *OFC/IOOC . Technical Digest. Optical Fiber Communication Conference, 1999, and the International Conference on Integrated Optics and Optical Fiber Communication*, volume 4, pages 141–143, Feb 1999.
6. M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg. Experiments on long wavelength (1550nm) “plug and play” quantum cryptography systems. *Opt. Express*, 4(10):383–387, May 1999.
7. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Fast and user-friendly quantum key distribution. *Journal of Modern Optics*, 47(2-3):517–531, 2000.
8. Richard J. Hughes, George L. Morgan, and C. Glen Peterson. Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547, 2000.
9. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. ”plug and play” systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795, 1997.
10. Damien Stucki, Grégoire Ribordy, André Stefanov, Hugo Zbinden, John G. Rarity, and Tom Wall. Photon counting for quantum key distribution with peltier cooled InGaAs/InP APDs. *Journal of Modern Optics*, 48(13):1967–1981, 2001.
11. Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3(12):696–705, 12 2009.
12. Jun Zhang, Mark A. Itzler, Hugo Zbinden, and Jian-Wei Pan. Advances in InGaAs/InP single-photon detector systems for quantum communication. *Light: Science & Applications*, 4:e286, January 2015.
13. Jeff Bude, Nobuyuki Sano, and Akira Yoshii. Hot-carrier luminescence in Si. *Phys. Rev. B*, 45:5848–5856, Mar 1992.
14. Andrea L. Lacaita, Franco Zappa, Stefano Bigliardi, and Manfredo Manfredi. On the bremsstrahlung origin of hot-carrier-induced photons in silicon devices. 40:577 – 582, 04 1993.
15. Christian Kurtsiefer, Patrick Zarda, Sonja Mayer, and Harald Weinfurter. The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? *Journal of Modern Optics*, 48(13):2039–2047, Nov 2001.
16. Loris Marini, Robin Camphausen, Chunle Xiong, Benjamin Eggleton, and Stefano Palomba. Breakdown flash at telecom wavelengths in direct bandgap single-photon avalanche photodiodes. *Photonics and Fiber Technology 2016 (ACOFT, BGPP, NP)*, 2016.
17. Alice Meda, Ivo Pietro Degiovanni, Alberto Tosi, Zhiliang Yuan, Giorgio Brida, and Marco Genovese. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. *Light: Science & Applications*, 6(6):e16261, dec 2016.
18. F. Acerbi, A. Tosi, and F. Zappa. Avalanche current waveform estimated from electroluminescence in InGaAs/InP SPADs. *IEEE Photonics Technology Letters*, 25(18):1778–1780, Sept 2013.
19. Ivan Rech, Antonino Ingargiola, Roberto Spinelli, Ivan Labanca, Stefano Marangoni, Massimo Ghioni, and Sergio Cova. Optical crosstalk in single photon avalanche diode arrays: a new complete model. *Opt. Express*, 16(12):8381–

8394, Jun 2008.
20. Joseph W. Chludzinski Douglas C. Oakley Leonard J. Mahoney Joseph E. Funk Joseph P. Donnelly S. Verghese Richard D. Younger, K. Alex McIntosh. Crosstalk analysis of integrated geiger-mode avalanche photodiode focal plane arrays. *Proc.SPIE*, 7320:7320 – 7320 – 12, 2009.
21. W. Shockley and W. T. Read. Statistics of the recombinations of holes and electrons. *Phys. Rev.*, 87:835–842, Sep 1952.
22. ID Quantique. *Data sheet for ID220 Infrared Single-Photon Detector*.
23. G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and Roman Sobolewski. Picosecond superconducting single-photon optical detector. *Applied Physics Letters*, 79(6):705–707, 2001.

Abstract: Quantum key distribution (QKD) at telecom wavelengths (1260 − 1625 nm) has the potential for fast deployment due to existing optical fibre infrastructure and mature telecom technologies. At these wavelengths, Indium Gallium Arsenide (InGaAs) avalanche photodiode (APD) based detectors are the preferred choice for photon detection. Similar to their Silicon counterparts used at shorter wavelengths, they exhibit fluorescence from recombination of electron-hole pairs generated in the avalanche breakdown process. This fluorescence may open side channels for attacks on QKD systems. Here, we characterize the breakdown fluorescence from two commercial InGaAs single photon counting modules, and find a spectral distribution between 1000 nm and 1600 nm. We also show that by spectral filtering, this side channel can be efficiently suppressed.

1. Introduction

Quantum key distribution (QKD) enables two distant parties to share a random encryption key without being eavesdropped by a malicious third party. Since the proposal of BB84 protocol by Bennett and Brassard in 1984 [1], years of research effort have been committed to building more efficient and robust QKD systems. These systems can be implemented using photons transmitted over free space [2–4] or over optical fibres [5–7].

QKD implementations over optical fibres receive growing interest due to their compatibility with existing telecom fibre networks [8], but require detection of single photons at telecom wavelengths (1260 − 1625 nm). Avalanche photodiodes (APDs) based on Indium Gallium Arsenide (InGaAs) are the commonly used detectors for this wavelength range [9–11]. Despite their relatively high dark count rate as compared to their Silicon counterparts, InGaAs APDs are able to detect single photons at telecom wavelengths with quantum efficiency up to 20% [11, 12].

One aspect of APD may provide a susceptibility to the so-called side channel attack in QKD implementations: the emission of fluorescence light during the avalanche breakdown process [13, 14]. This light emission is due to the recombination of electrons and holes in the APD junction, and covers a spectrum ranging from 700 nm to 1000 nm in Silicon based APDs [15]. A similar fluorescence has also been observed in InGaAs APDs [16–18] and InGaAs APD arrays [19, 20]. **[In [17] the spectral distribution of the fluorescence was investigated across the range of** 1530 nm **to** 1600 nm**.]** This fluorescence (referred to as 'breakdown flash', 'backflash' or 'electroluminescence') reveals information about the photon detection process to an eavesdropper [15, 17]. Depending on the detection scheme in a quantum communication setting, the eavesdropper may extract timing and/or polarization information of the detected photons by observing the breakdown flash leaked back to the optical channel. Thus, a strategy must be in place to reduce or eliminate this side channel.

In this work, we investigate the breakdown flash from two commercial InGaAs single-photon counting modules (ID220, ID Quantique). In doing so, we obtain a lower bound for the breakdown flash probability. **[We also characterize its spectral distribution over the entire telecom wavelengths]** and find that by spectral filtering, the number of detected breakdown flash

events can be greatly suppressed. Under the conservative assumption on a unit detector efficiency, one can place an upper bound to the information leakage due to the breakdown flash in a QKD scenario.

2. Detection of breakdown flash

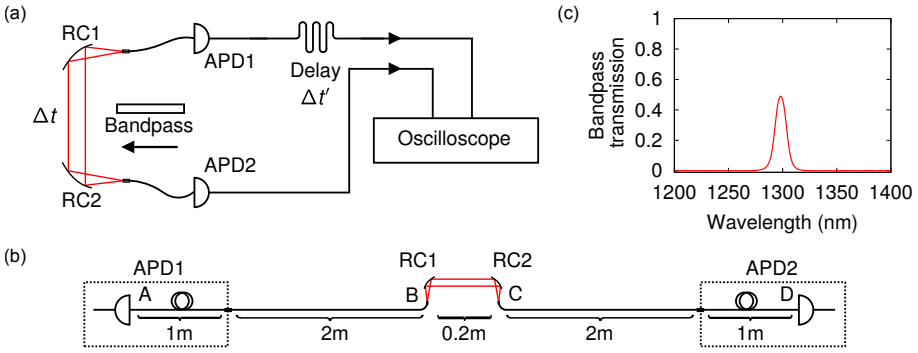

Fig. 1. (a) Setup for detecting the breakdown flash. The two APDs are optically coupled to each other by a pair of reflective collimators (RC1 and RC2). It takes $\Delta t \approx 32.5$ ns for a photon to travel the optical distance between APD1 and APD2. (b) Schematics of the lengths of fibre patchcords. The output signals from APDs are sent to an oscilloscope with an electrical delay $\Delta t' \approx 127$ ns applied to APD1. The oscilloscope triggers on signals received from APD2, and records the arrival times of signals from APD1. We record coincidence both events where APD1 emits a breakdown flash that is detected by APD2, and the other way round. An optical bandpass filter in a another measurement to suppress the number of breakdown flash events. The transmission profile of the bandpass filter is shown in (c).

The devices under test are two InGaAs APD based single-photon counting modules, APD1 and APD2 (ID220, ID Quantique, with fibre input). We use the setup shown in Fig. 1 where each counting module acts as both source and detector. To observe the breakdown flash events, the fibre-coupled detectors APD1 and APD2 are optically coupled through free space by a pair of reflective collimators (RC1 and RC2) with an overall transmission of 89% (including fibre losses). The reflective collimators are placed ≈ 0.2 meters apart and each one is connected to a counting module through 3 meters of optical fibre (2 meters patchcord + 1 meter fibre in the detector module).

The output signals from the two APDs are connected to two channels of an oscilloscope (Lecroy Waverunner 640 Zi), which triggers when a signal is received from APD2. Once being triggered, the oscilloscope records the arrival time of a signal from APD1 with respect to the trigger event within the next 250 ns with a time resolution of 100 ps. An adjustable electrical delay is applied to APD1 to offset the signal arrival time such that only positive time differences for all interesting events are recorded by the oscilloscope.

The experimental setup is kept in the dark such that the breakdown flash is only caused by dark breakdown events in the APDs. A dark breakdown event is a thermally induced avalanche breakdown in the APD, hence it emits the same breakdown flash light as what would be generated in a photodetection event [21]. With the setup shown in Fig. 1(a), we observe single detector event rates of $(1.00 \pm 0.016) \times 10^4\,\mathrm{s}^{-1}$ for APD1, and $(0.533 \pm 0.019) \times 10^4\,\mathrm{s}^{-1}$ for APD2.

When there is a breakdown event in APD2 at $t = 0$ s, the oscilloscope is triggered. Such an event causes a breakdown flash that arrives at APD1 after a traveling time Δt in the optical path.

This generates a signal from APD1 which is delayed by $\Delta t'$ due to the electrical delay connected to APD1. The signal is timestamped by the oscilloscope at $t = \Delta t + \Delta t'$, which indicates a breakdown flash emitted from APD2 and detected by APD1. Alternatively, a breakdown event detected in APD1 at $t = -\Delta t$ causes a breakdown flash that reaches APD2 at $t = 0$ and triggers the oscilloscope. The corresponding breakdown signal from APD1 reaches the oscilloscope and is recorded at $t = \Delta t' - \Delta t$, indicating a breakdown flash event from APD1 detected by APD2.

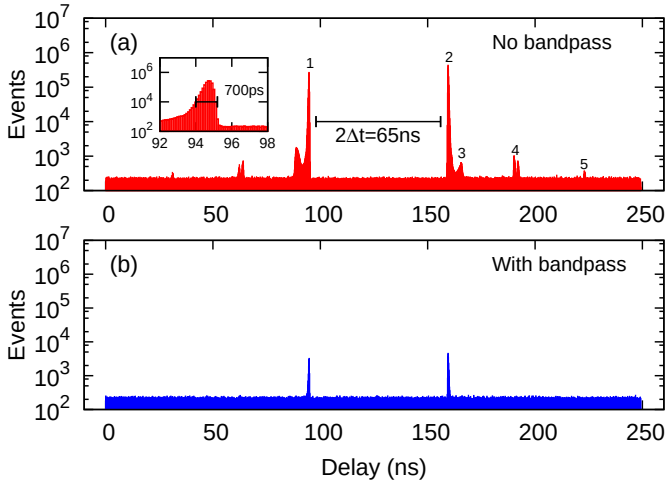

Fig. 2. (a) Histogram of signal arrival times from APD1 recorded by an oscilloscope. Peak 1 corresponds to APD1 emitting a breakdown flash that detected by APD2 (path A-B-C-D), peak 2 to the reverse direction (path D-C-B-A). Peak 3 is suspected to be due to the after-pulsing of APD1. Peaks 4 and 5 are due to the back reflection of breakdown flash light at fibre joints (paths A-B-C-D-C/B-D and D-C-B-A-B/C-A). (b) Same measurement, but with a bandpass filter in the optical path. The number of breakdown flash events is suppressed by a factor of over 100. An integration time of 12 hours is used for both measurements.

Fig. 2 (a) shows the histogram of the event timings recorded by the oscilloscope over an integration time of 12 hours. Peak 1 (located at $t_1 = \Delta t' - \Delta t \approx 95$ ns) and peak 2 (located at $t_2 = \Delta t' + \Delta t \approx 159$ ns) correspond to breakdown flash events between the two APDs along paths A-B-C-D and D-C-B-A, respectively. Each peak has a full width at half maximum (FWHM) of ≈ 700 ps. The timing separation between the two peaks is $t_2 - t_1 = 2\Delta t \approx 65$ ns, matching twice the optical transit time from A to D.

Peak 3 ($t \approx 166$ ns) is suspected to be afterpulsing signals of APD2 [16]. Peak 4 ($t \approx 190$ ns) actually consists of two small peaks. They are possibly due to the back reflections of photons at the reflective collimators from a secondary breakdown flash in APD1 (triggered by flash photons from APD2), i.e., follow a path D-C-B-A-B/C-A. The timing difference between peak 4 and peak 2 is about 31 ns, which corresponds to a fibre length of about 6 meters (from point A to B/C then back to A, Fig. 1(b)). Peak 5 ($t \approx 223$ ns) is suspected to be a tertiary breakdown from APD2 (triggered by photons from the secondary flash in APD1), as it is about 64 ns away from peak 2 and the timing difference matches a fibre length of about 12 meters (from point A to D then back to A, Fig. 1(b)).

This measurement was repeated with a bandpass filter (transmission profile shown in Fig. 1(c)) inserted between RC1 and RC2. The events timing histogram is shown in Fig. 2. The two major peaks (peak 1 and peak 2) are suppressed by factor of about 100, while the other small peaks are no longer observable. This indicates that spectral filtering could be used as a countermeasure to effectively reduce the breakdown flash.

The recording of timing histograms with the oscilloscope does not directly permit the determination of absolute detection rates for breakdown flash photons, as the histogram processing disables data taking for an unpredictable time. We therefore employ a different method involving a hardware coincidence stage to determine the absolute probability of detecting a breakdown flash event. (see Fig. 3(a)). For flash events emitted by APD1 and detected by APD2, the signal from APD1 is electrically delayed by $\Delta t'$, matching the photon traveling time Δt. Then, an initial breakdown signal from APD1, and the breakdown flash signal from APD2 arrive at the coincidence stage within a coincidence window of $\sim$ 500 ps. Such a coincidence event indicates a breakdown flash emitted from APD1 detected by APD2, and is recorded by a hardware counter, avoiding the dead time of the oscilloscope in data processing. The number of breakdown flash events emitted by APD2 is measured in the same manner, except that the same electrical delay is applied to signals from APD2.

For each configuration, we continuously record the number of coincidences for 12 hours. We find a rate of $44.4 \pm 2.2\,\mathrm{s}^{-1}$ from APD1 to APD2, and $22.2 \pm 1.6\,\mathrm{s}^{-1}$ from APD2 to APD1. Normalized by the count rate of the emitting APDs, this yields a probability of $0.44\% \pm 0.02\%$ for APD2 detecting a breakdown flash from APD1, and a probability of $0.42\% \pm 0.03\%$ in the reverse direction.

In comparison, these probabilities drop to $0.0049\% \pm 0.0023\%$ and $0.0057\% \pm 0.0033\%$, respectively, when the bandpass filter is inserted. We estimate the rate of accidental coincidences by blocking the optical path between the APDs, yielding a rate of $0.032 \pm 0.057\,\mathrm{s}^{-1}$, with dark count rates of $(9.55 \pm 0.18) \times 10^3\,\mathrm{s}^{-1}$ and $(5.46 \pm 0.20) \times 10^3\,\mathrm{s}^{-1}$ for APD1 and APD2, respectively. Therefore, applying spectral filtering can effectively suppress the rate of breakdown flash by two orders of magnitude.

3. Spectral distribution of breakdown flash

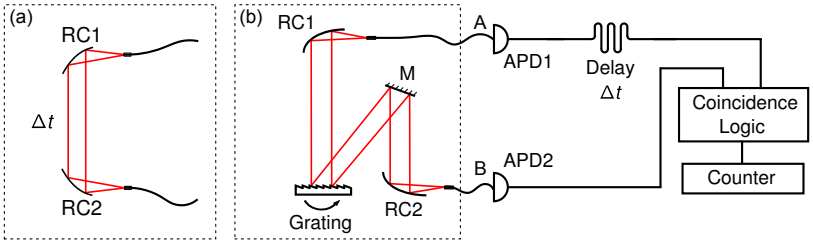

Fig. 3. (a) Setup for a coincidence measurement to determine the rate of detecting breakdown flashes from APD1. An electrical delay is applied to APD1 such that the dark count signal from APD1 and the breakdown flash signal from APD2 arrive at the coincidence stage at the same time. A counter is used to log the number of events per second. The setup can also measure the breakdown flash rates from APD2 with the electrical delay connected to APD2. (b) Setup for measuring the spectral distribution of the breakdown flashes. The working principle is the same as the one in (a), except that the reflective collimators are replaced by a grating monochromator to select different transmission wavelength.

The spectral information available from the bandpass experiment is somewhat limited. We therefore analyze the spectral distribution of the breakdown flash light with the setup shown in Fig. 3(b). A monochromator consisting of a reflective grating (600 lines/mm, blazed at 1.25 μm) and a pair of reflective collimators (RC1 and RC2) is inserted in the optical path between the two APDs. The grating is rotated to select the transmission wavelength between them. To estimate the spectral resolution of the monochromator, we measure the instrument response to a 1310 nm single mode diode laser, and find a full width at half maximum (FWHM) of 3.3 nm. For the first-order diffraction of the same 1310 nm light, we observe a transmission of 51% from point A to

B in Fig. 3(b).

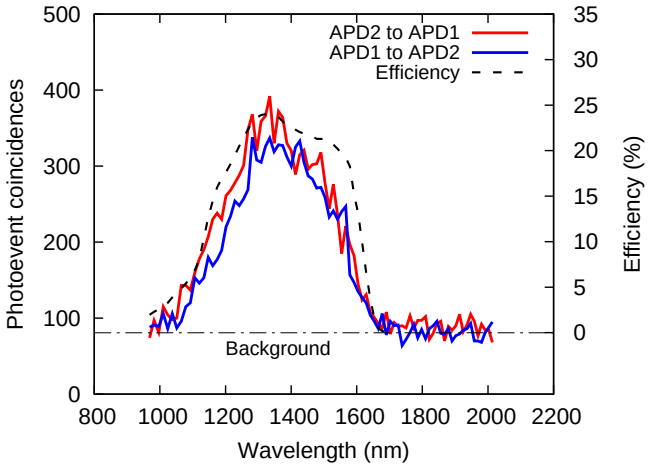

Fig. 4. Spectral distribution of the InGaAs APD breakdown flash. The integration time for each data point is 30 minutes. We record cases where APD1 emits a breakdown flash that is detected by APD2 and vice versa. The two spectra range from 1000 nm to 1600 nm and peak at about 1300 nm. The dashed line indicates the background due to accidental coincidences.

We sampled 84 wavelengths ranging from 1000 nm to 2000 nm with a grating angle incrementation of 0.28 °. We perform same coincidence measurement as with the single bandpass in the optical path, but with an integration time of 30 minutes. The results are shown in Fig. 4. The coincidence events span a wide range from 1000 nm to 1600 nm, with a maximum at about 1300 nm. These results are not corrected for the transmission efficiency of the monochromator, nor the wavelength-dependent detection efficiencies of the two APDs. However, the observed spectra (Fig. 4, left axis) follow closely the spectral dependency of the nominal quantum efficiency [22] (right axis). We are not able to detect spectral components outside the 1000 nm-1650 nm band. The close match of spectral sensitivity and observed spectrum of the flash suggests that the spectrum could be relatively flat over the whole region we are able to observe, and could even extend beyond that sensitivity range. A more comprehensive measurement of the actual spectrum would require more wide-band photodetectors. The recent progress with superconducting nanowire detectors [23] would make these devices a good choice for such a measurement.

4. Conclusion

Commercial InGaAs single-photon counting modules do show breakdown flash, similar to their Silicon counterparts [15]. We characterized the breakdown flash from two such devices using a coincidence measurement, and obtain a lower bound for the probability of detecting a breakdown flash of $\approx 0.4\%$. Given that these APDs have a nominal detection efficiency of about 10%, the breakdown flash could contain at least 0.04 photons emerging from the fiber connector of the devices. This may result in a considerable amount of information leakage that has to be considered in practical QKD implementations.

In some sense, this should not come as a surprise, as light emission for electron-hole recombinations in direct bandgap semiconductors like InGaAs is more likely to happen than in indirect bandgap semiconductors like Silicon. However, a direct comparison with photon numbers due to the breakdown flash in different APD types based on our observation is not directly obvious:

the overall breakdown flash photon number is likely to be proportional to the charge released in a breakdown, which is significantly smaller in InGaAs APD than in Silicon APDs due to the lower excess voltage above breakdown. Another unknown in the experimental observations we have access to is the different coupling efficiencies of the diodes in this experiment (diodes are connected to multi-mode fibers with a small core diameter) and free space diodes used in earlier experiments [15].

The spectral distribution of the breakdown flash appears to be relatively wide. Thus, a spectral filter in front of an APD is a suitable countermeasure to prevent potential information leakage through the breakdown flash in a quantum key distribution scenario. In that narrow spectral window, the detection efficiency can be assumed to be constant. With a conservative estimation of the detector efficiency, the observed detected breakdown flash probability can then be used to provide an upper bound for estimating the number of photons being transmitted to the optical channel due the breakdown flash.

This research is supported by the Ministry of Education, Singapore, and the National Research Foundation, Prime Minister's Office, Singapore, partly under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.