Breakdown Flash From 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]Center for Quantum Technologies, National University of Singapore, [2]Department of Physics, National University of Singapore
[3]Singapore Telecommunications Limited

Breakdown Flash In InGaAs APDs

Quantum Key Distribution (QKD) schemes, which promise secure point-to-point communications, use single photons as carriers of information. Avalanche photodiodes (APDs) are often used in QKD implementations to detect the single photons. However, certain unintended features may constitute vulnerabilities that can be exploited by eavesdroppers. It was observed that these APDs emit light during the avalanche breakdown process after detecting a photon. This happens in Silicon APDs [1], as well as Indium Gallium Arsenide (InGaAs) APDs [2, 3] which are core components in QKD systems at telecom wavelengths (1260∼1625 nm). This fluorescence light (referred to as "breakdown flash") gives rise to potential eavesdropping attacks and poses real threat to telecom QKD systems. As shown in Fig. 1, an eavesdropper may gain timing or other information of the detected photons by observing the breakdown flash leaked back to the optical channel.

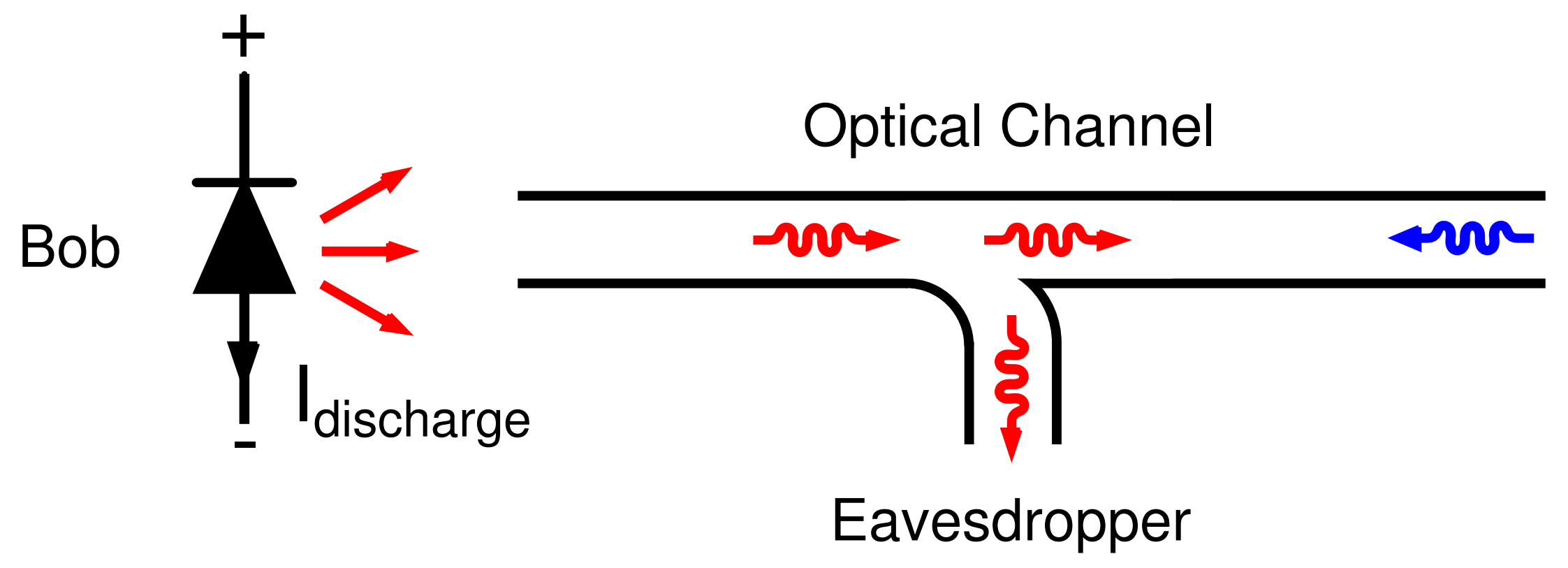

Figure 1: Schemes for eavesdropping on a QKD channel by exploiting the breakdown flash from APDs.

Detection Of Breakdown Flash

We utilize the setup shown in Fig. 2 to detect breakdown flash from APDs. Two commercial APDs are optically coupled through a pair of reflective collimators. The APDs are connected to a time tagging device which is triggered upon receiving a signal from APD2. Once triggered, the device records the arrival times of signals from APD1. We also inserted an optical bandpass filter (1300±6 nm) as an attempt to suppress the breakdown flash.

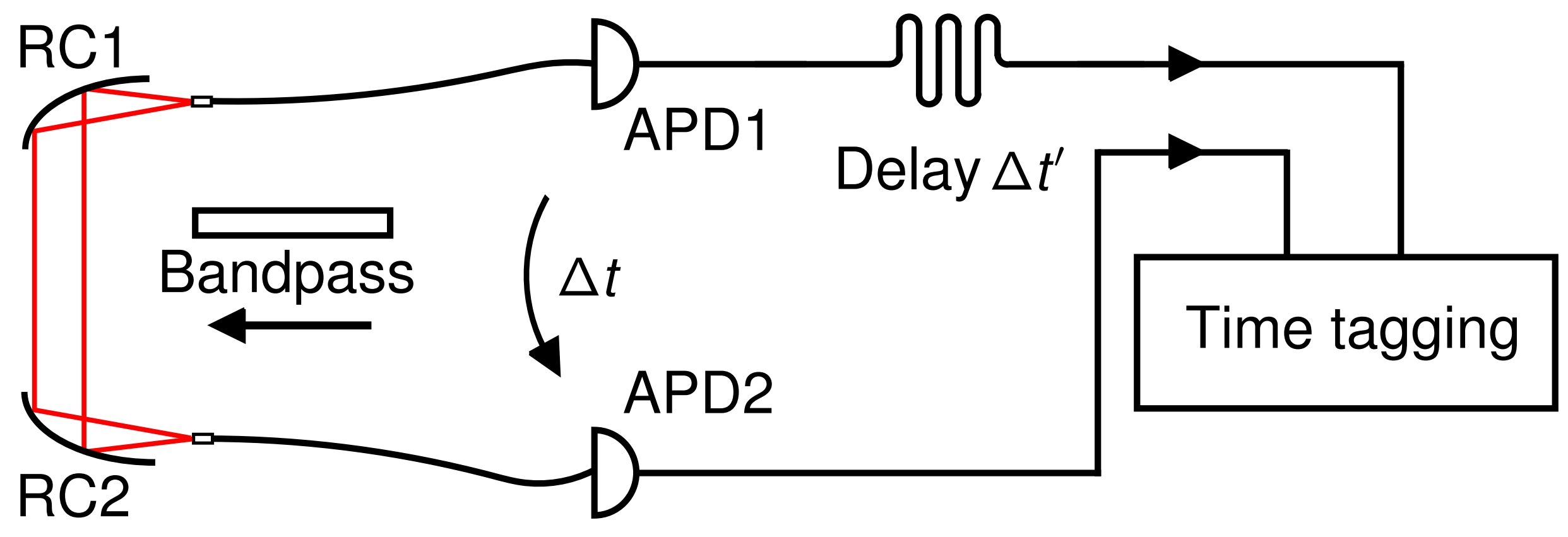

Figure 2: Setup for detecting the breakdown flash from two InGaAs APDs.

The histogram of the signal arrival times is shown in Fig. 3(a). Peak 1 and peak 2 corresponds to cases where APD1(2) emits a breakdown flash detected by APD2(1). Each peak has a full width at half maximum (FWHM) of 700 ps. The timing seperation between the two peaks is 65ns. Peak 3, 4 and 5 are due to the APD after pulsing and photon back reflection at fibre joints. When an optical bandpass filter was inserted between RC1 and RC2, the number of breakdown flash events could be suppressed by a factor of about 100, as shown in Fig. 3(b).

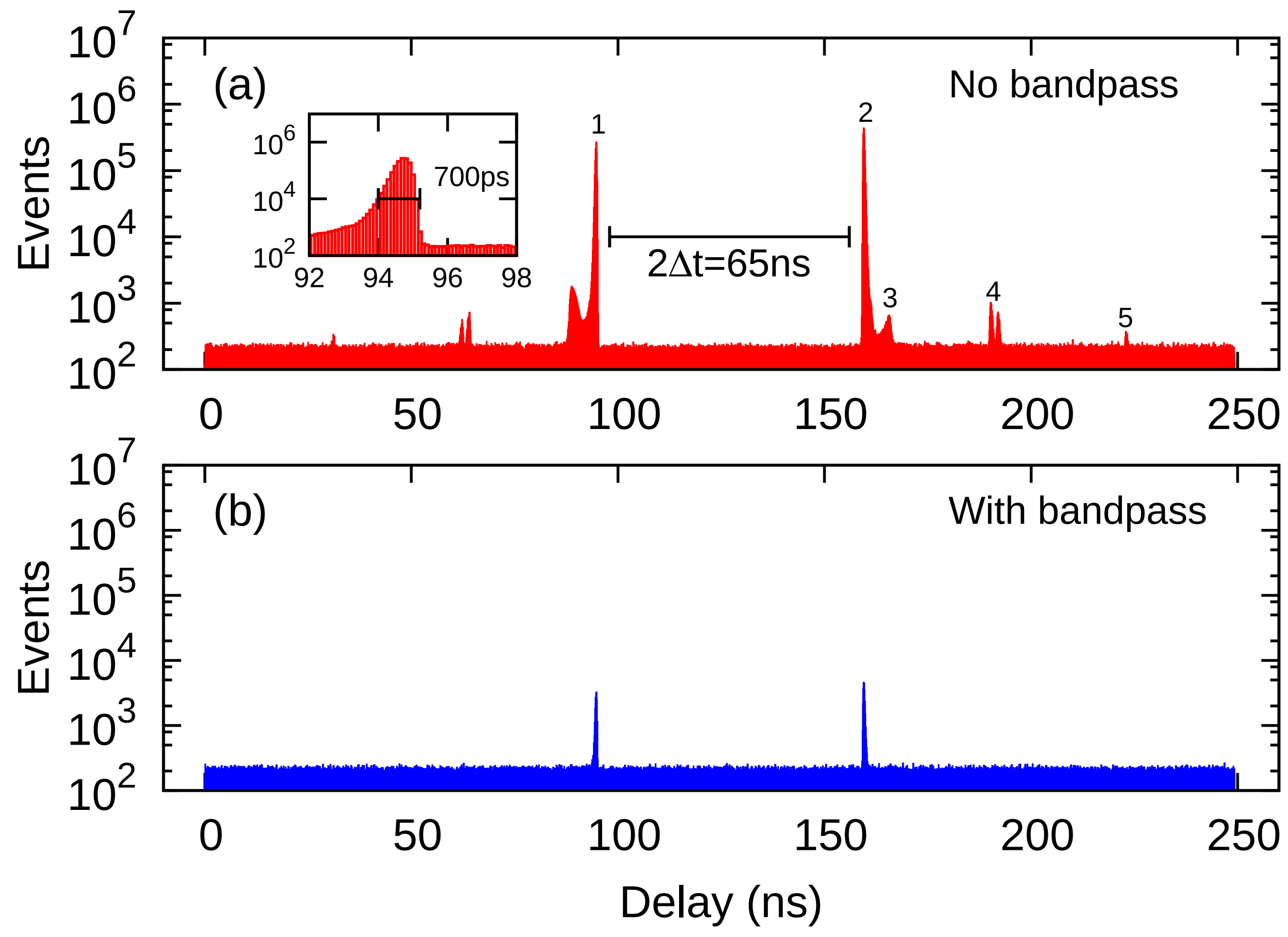

Figure 3: (a) Histogram of the signal arrivial times. (b) Histogram of the signal arrival times, with bandpass filter applied.

We also measured the probability of detecting a breakdown flash by replacing the time tagging unit with a coincidence counter. A breakdown flash is registered as a coincidence event from the two detectors and after normalization with the dark count rate of the detectors, we obtained a lower bound probability of 0.4% of detecting a breakdown flash. This probability drops to 0.005% once we inserted the bandpass filter.

Spectral Distribution

We analyze the spectral distribution of the breakdown flash light with the setup shown in Fig. 4. 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.

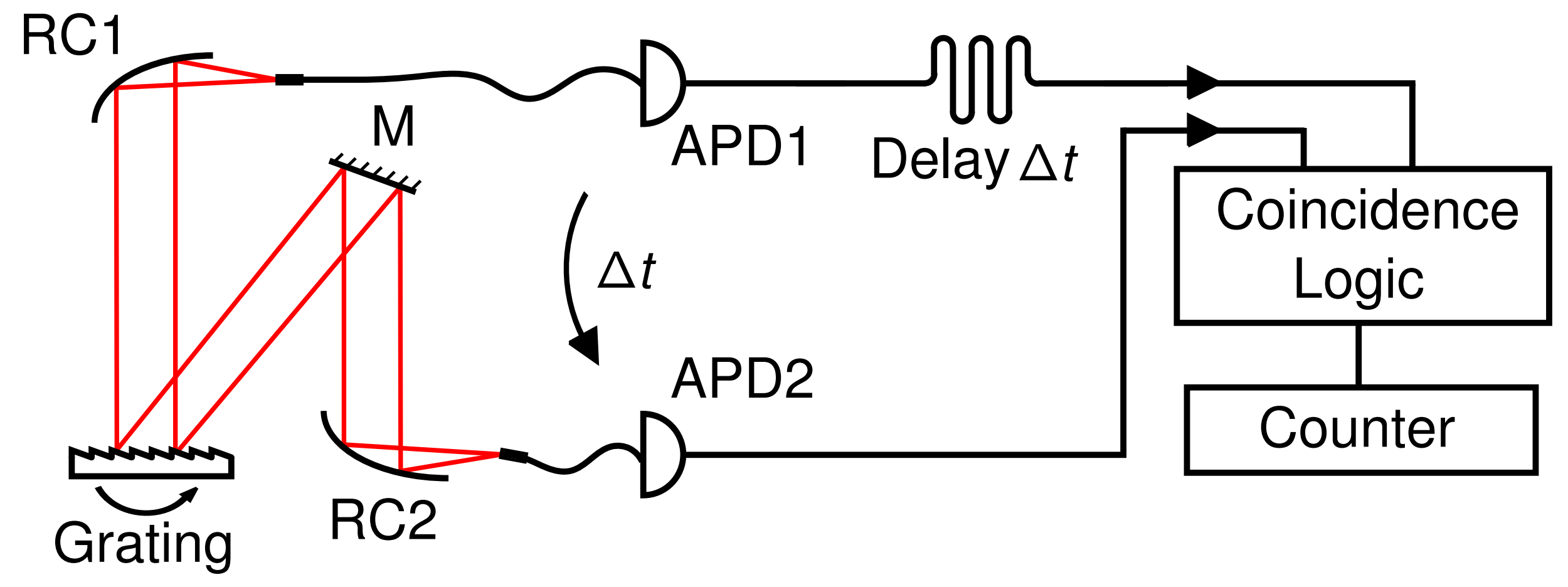

Figure 4: Setup for measuring the spectrum of breakdown flash.

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. 5. 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.

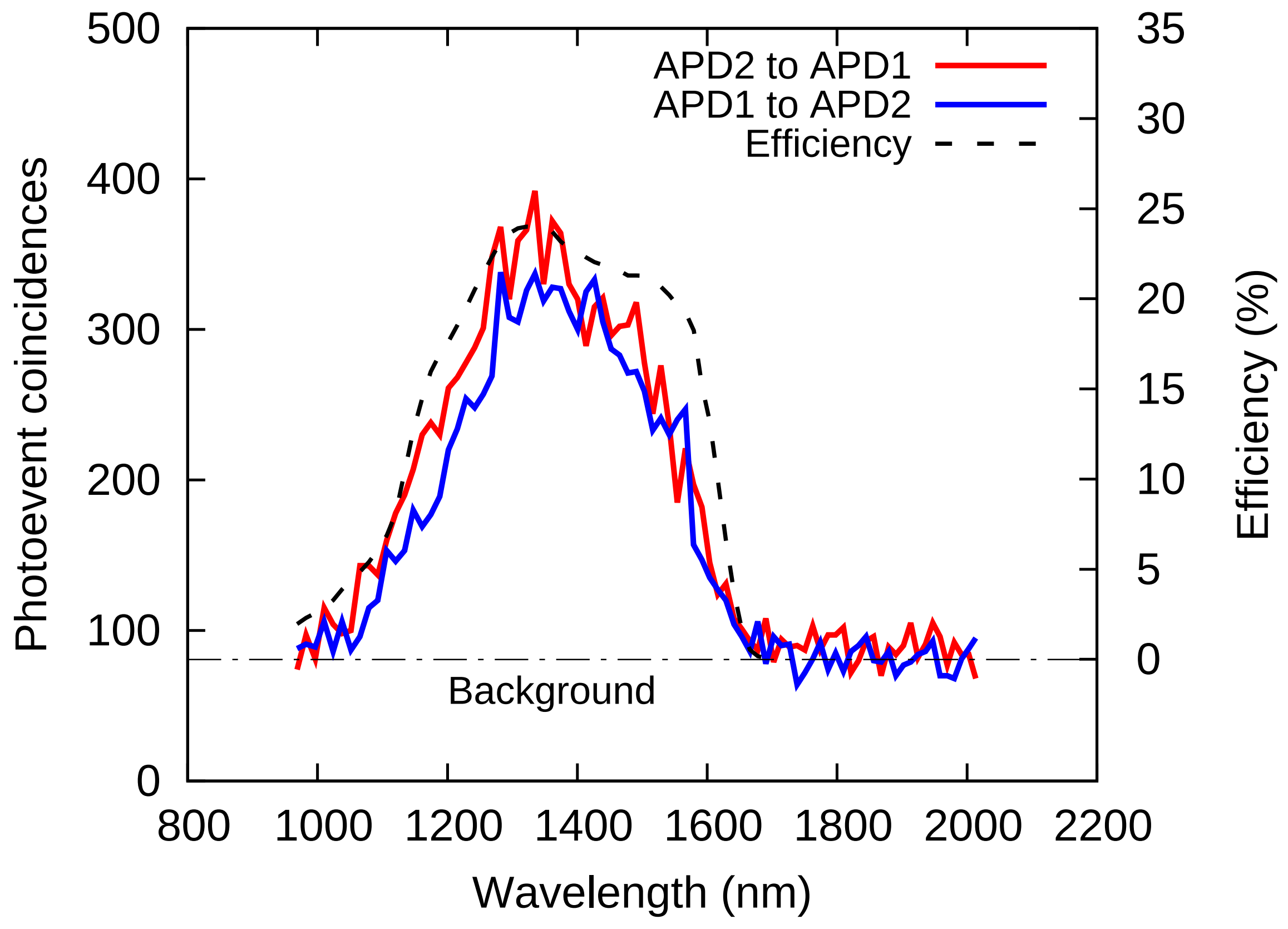

Figure 5: Spectral distribution of the breakdown flash.

The observed spectra (Fig. 5, left axis) follow closely the spectral dependency of the nominal quantum efficiency (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.

Conclusion

Commercial InGaAs single-photon counting modules show breakdown flash upon photon detections, similar to their silicon counterparts. This constitudes potential vulnerability to QKD systems implemented over telecom wavelengths as the emitted breakdown flash may cause information leakage back to the optical channel.

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 $\approx 0.4\%$. We measured the spectral distribution of the breakdown flash which is relatively wide ($1000\,\mathrm{nm} \sim 1600\,\mathrm{nm}$). We also demonstrated that 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.

Acknowledgement

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.

References

[1] Kurtsiefer et al., *Journal of Modern Optics*, 48(13):2039–2047, Nov 2001.

[2] Marini et al., *Photonics and Fiber Technology 2016 (ACOFT, BGPP, NP)*, 2016.

[3] Meda et al., *Light: Science & Applications*, 6(6):e16261, dec 2016.

---

[*] This research is performed at the NUS-Singtel Cyber Security Research & Development Laboratory.