Breakdown Flash From InGaAs Avalanche Photodiodes*

Shi Yicheng[1], Lim Zheng Jie Janet[1], Poh Hou Shun[1], Tan Peng Kian[1],
Tan Peiyu Amelia[1,3], Ling Euk Jin Alexander[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 promise secure point-to-point communications. Many QKD schemes use single photons as carriers of information. Avalanche photodiodes (APDs) are often used in such implementations to detect the single photons. However, certain unintended features may constitude vulnerabilities that can be exploited by eavesdroppers. It was observed that these APDs emit light during the avalanche breakdown process after detecting a photon, as shown in Fig. 1. This happens in Silicon APDs, as well as Indium Gallium Arsenide (InGaAs) APDs which are core components in QKD systems at telecom wavelengths (1260∼1625 nm).

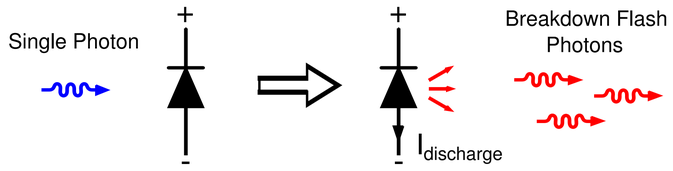

Figure 1

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. 2, an eavesdropper may gain timing or other information of the detected photons by observing the breakdown flash leaked back to the optical channel.

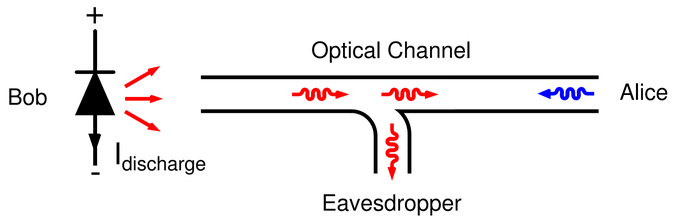

Figure 2

Detection Of Breakdown Flash

We utilize the setup shown in Fig. 3 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.

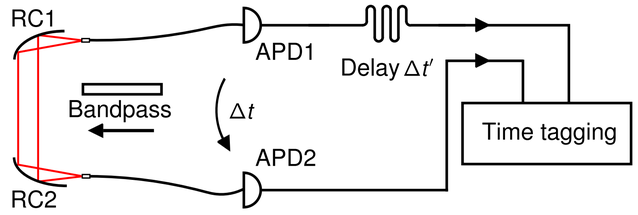

Figure 3

The histogram of the signal arrival times is shown in Fig. 4(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. 4(b).

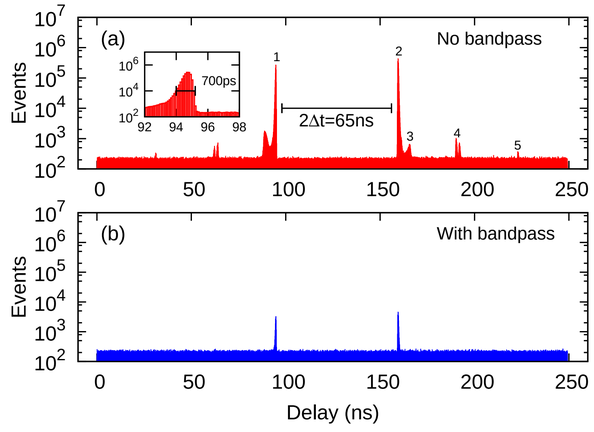

Figure 4

Spectral Distribution

We measure the spectral distribution of the breakdown flash light using a grating monochrometer shown in Fig. 5. The APDs are coupled through the reflective collimators RC1 and RC2 via a blazed reflection grating. An electrical delay is applied to APD1(2) to match the optical delay Δt for flash photons to travel from APD1(2) to APD2(1). The grating is oriented at different angles to record coincidence events at different wavelengths.

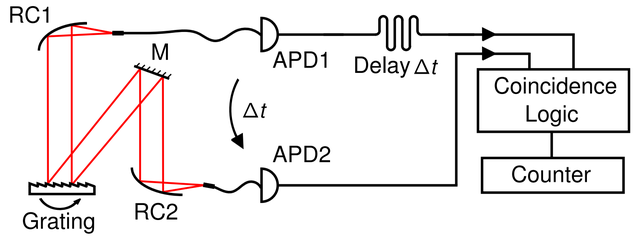

Figure 5

Figure. 6 shows the spectral distribution of the breakdown flash. The spectra range from 1000 nm to 1600 nm and peaks at about 1300 nm.

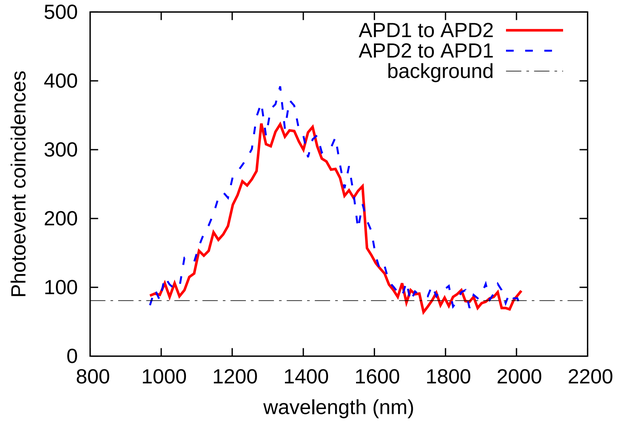

Figure 6

Conclusion

The breakdown flash emitted from InGaAs APDs is a potential vulnerability of QKD systems operating at telecom wavelengths. We characterized its spectral distribution and demonstrated a hardware countermeasure that reliably suppresses the breakdown flash by applying spectral filtering.

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