



# Repeated radiation damage and thermal annealing of avalanche photodiodes

Ian DSouza<sup>1,2</sup>, Jean-Philippe Bourgoin<sup>1,2,3</sup>, Brendon L. Higgins<sup>1,2\*</sup>, Jin Gyu Lim<sup>1,4</sup>, Ramy Tannous<sup>1,2</sup>, Sascha Agne<sup>1,2</sup>, Brian Moffat<sup>1</sup>, Vadim Makarov<sup>5,6,7,2</sup> and Thomas Jennewein<sup>1,2</sup>

\*Correspondence:

[brendon.higgins@uwaterloo.ca](mailto:brendon.higgins@uwaterloo.ca)

<sup>1</sup>Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada

<sup>2</sup>Department of Physics and Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada  
Full list of author information is available at the end of the article

## Abstract

Avalanche photodiodes (APDs) are well-suited for single-photon detection on quantum communication satellites as they are a mature technology with high detection efficiency without requiring cryogenic cooling. They are, however, prone to significantly increased thermal noise caused by in-orbit radiation damage. Previous work demonstrated that a one-time application of thermal annealing reduces radiation-damage-induced APD thermal noise. Here we examine the effect of cyclical proton irradiation and thermal annealing. We use an accelerated testing environment which emulates a realistic two-year operating profile of a satellite in low-Earth-orbit. We show that repeated thermal annealing is effective at maintaining thermal noise of silicon APDs within a range suitable for quantum key distribution throughout the nominal mission life, and beyond. We examine two strategies—annealing at a fixed period of time, and annealing only when the thermal noise exceeds a pre-defined limit. We find both strategies exhibit similar thermal noise at end-of-life, with a slight overall advantage to annealing conditionally. We also observe that afterpulsing probability of the detector increases with cumulative proton irradiation. This knowledge helps guide design and tasking decisions for future space-borne quantum communication applications.

**Keywords:** Avalanche photodiodes; Single-photon detectors; Satellite; Low-Earth orbit; Proton radiation; Annealing; Quantum key distribution; Quantum communications

## 1 Introduction

Distributing secret keys to users of a communication network enables them to exchange messages securely using cryptographic protocols. To do so, conventional cryptosystems utilize algorithms that provide data security under assumptions of computational complexity. Quantum computers, however, are in principle capable of efficiently solving problems that are foundational to some of these algorithms (by using, e.g., Shor's factoring algorithm [1]). "Post-quantum" encryption protocols such as the McEliece protocol [2] attempt to be immune to attacks by a quantum computer, but their robustness to cryptanalysis is not well established—in some cases being prone to even classical attacks [3]. Quantum key distribution (QKD) protocols [4–6] make use of public quantum channels

© The Author(s) 2021. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

to securely distribute symmetric keys by exchange of quantum bits. Fundamentally, security is obtained through the no-cloning theorem: any measurement of a quantum bit by an eavesdropper risks changing the state of that bit, through which the eavesdropper's presence is revealed.

QKD is typically implemented using photons which travel through optical fibers or over atmospheric free space. Both experience high losses as transmission distances increase, with the dominant losses scaling exponentially. This makes it impossible to distinguish transmitted signals above intrinsic photon detector noise beyond distances of a few hundred kilometers. In contrast, orbiting satellites have the advantage that optical transmission through the vacuum of space is dominated by beam divergence, where loss scales quadratically. Thus, quantum satellites, acting as nodes, can help extend the range of QKD. Moreover, placing photon detectors on such a satellite (as opposed to on the ground) has advantages of relaxing its pointing, computational, and memory requirements. The same detector apparatus can additionally be used in a wider range of scientific experiments [7]. Such an approach has been trialled with the Micius satellite [8] and is being pursued by the QEYSSat satellite [9, 10].

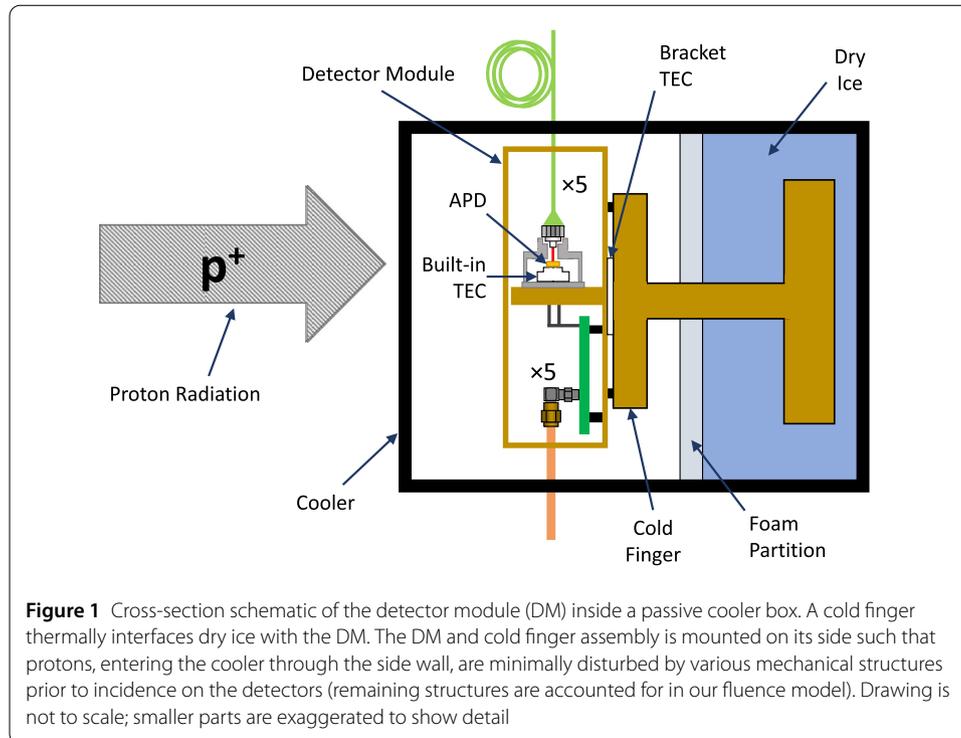
For single-photon detection, silicon avalanche photodiodes (Si APDs) have the advantage of low dark count rates, high maximum count rates, and high photon detection efficiencies when coupled to the near-infrared wavelengths around 800 nm that are a good compromise between atmospheric transmittance and diffraction [7]. In addition, Si APDs do not require cryogenic cooling, as competing detector technologies do, greatly simplifying support systems that would be required to operate on a space-borne platform. However, proton irradiation due to solar particle events [11] can induce displacement damage [12] that causes defects in the Si APD substrate placed in low-Earth orbit (LEO). This leads to noise in the form of dark counts within these detectors, thereby decreasing their signal-to-noise ratios throughout the operational lifetime of a spacecraft payload. Thermal annealing—where a detector's active area is heated to remove crystalline defects—has been proposed as a technique to mitigate such radiation damage and decrease dark count rates. This has shown to be effective in single-shot experiments [13] when coupled with operating the detectors at cold temperatures, e.g.,  $-80^{\circ}\text{C}$ . For a satellite platform, such cold operation can be achieved by thermoelectric cooling supported by passive thermal radiation to deep space. At the same time, annealing temperatures can be achieved by thermoelectric heating supported by resistive electric heating and orbital manoeuvres.

In this work, we examine the effects of repeated thermal annealing on detector parameters over the emulated life of a satellite payload detector apparatus. We irradiate Si APDs with protons over several stages and measure the detector performance at each stage, accumulating dosage equivalent to at least two years in LEO. We demonstrate the efficacy of repeated thermal annealing to reduce dark count rates to within operational range.<sup>1</sup>

To determine suitable criteria for engaging annealing, we study two strategies. The first is to anneal the APDs periodically, regardless of current performance. The second is to only anneal when the dark count rate exceeds a pre-determined threshold value (here 2 kcps, kilo counts per second). We thus irradiate two identical sets of detectors using these two approaches and compare the resulting detector performance. Our results show

---

<sup>1</sup>Many parameters, which vary according to the orbital environment and mission requirements, influence the operational performance of a QKD system. The scenario we consider follows that of Ref. [7].



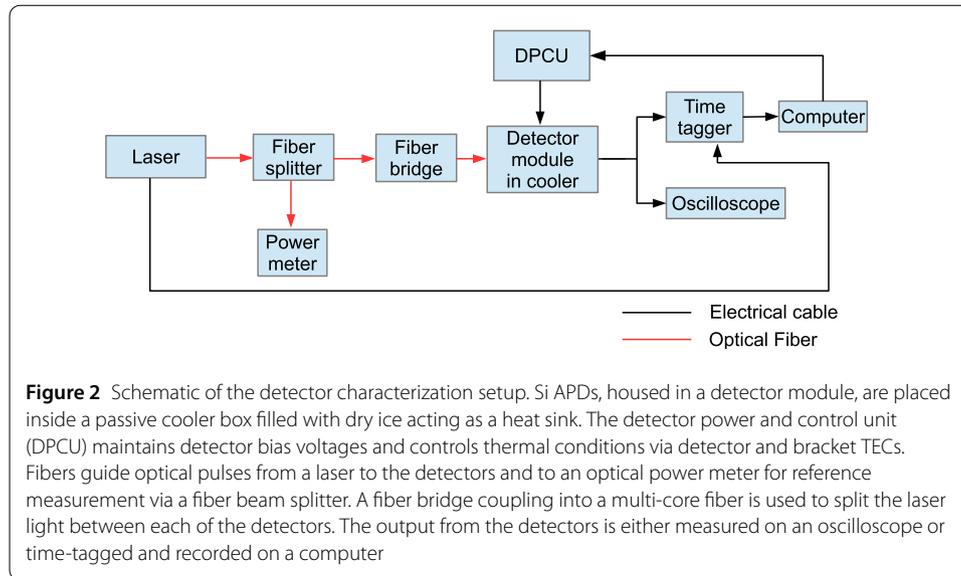
that although both approaches achieve similar outcomes, the case where the detectors are annealed only when the dark count rate exceeds a threshold value generally achieves slightly lower post-annealed dark count rates at the end of the two-year life of the satellite.

This paper is organized as follows. In Sect. 2, we describe the experimental setup to irradiate the detectors and monitor detector parameters. We present our test methodology in Sect. 3 to examine the effects of irradiation and annealing on detector parameters. In Sect. 4, we present our results and inferences of the irradiation and annealing experiments. Concluding remarks are given in Sect. 5.

## 2 Experimental setup

Five silicon APDs manufactured by Excelitas (the packaged APD unit normally found inside the commercial detector module SPCM-AQRH-12-FC) are housed in a custom enclosure together with supporting electronics designed for operating in space. This unit is called the detector module (DM). The APDs are mounted on a bracket which is thermally isolated from the enclosure and connected to a heat sink. Each APD's active area is temperature stabilized using a thermo-electric cooler (TEC) that is housed inside the APD package. The detector TEC is thermally interfaced to the bracket and driven by closed-loop control based on thermistor readout. Another TEC mounted between the bracket and the heat sink serves to stabilize the temperature of the bracket and helps achieve a wider range of APD operating temperatures.

Nominally the heat sink would be mounted to a radiator pointed towards deep space to maintain a low temperature. We emulate this for our tests—the heat sink is maintained at a temperature of about  $-78.5^{\circ}\text{C}$  by thermally interfacing it to one end of a copper cold finger whose other end is embedded in dry ice. This whole setup is housed inside a passive cooler box (Fig. 1) to thermally isolate it from the ambient environment. The DM enclosure and



dry ice are physically separated by an insulating foam partition. The detectors are typically operated around  $-80^{\circ}\text{C}$ , but for annealing they are heated by operating the bracket and APD TECs in reverse, to  $-40^{\circ}\text{C}$  and  $+80^{\circ}\text{C}$ , respectively.

A fiber-coupled pulsed laser emitting 785 nm wavelength light is used to characterize APD performance (Fig. 2). A fiber beam splitter placed in the optical path diverts a small portion of the laser power to a pre-calibrated optical power meter that monitors the incident laser power, while the remaining signal is coupled via a free-space fiber bridge into a 1-to-19 fiber bundle. Five outputs of the fiber bundle which have relatively matched optical powers are used such that attenuated laser power is applied uniformly to each APD. As our primary objective is to detect the relative change of efficiency due to irradiation, we need only ensure the same fiber configuration is used throughout the measurement.

The APDs are run in Geiger mode, biased 20 V above their respective breakdown voltages, and use a passive quenching circuit [13–17]. Electrical output pulses of each APD are measured either on an oscilloscope or using a time tagging unit. The oscilloscope is used to measure breakdown voltage, output pulse amplitude and width, and recharge time. The time tagging unit measures the arrival time of each output pulse. Appropriate post-processing algorithms applied to the recorded time tags then allow evaluation of the detector dark count rate, photon detection efficiency, timing jitter, maximum count rate (saturation), and afterpulsing probability.

We consider the scenario of two years in LEO at 600 km altitude, and assume 10 mm aluminum shielding from the spacecraft walls. Following Ref. [18], which used a commonly accepted silicon damage deposition model [19], under these conditions the cumulative fluence incident on the detectors is equivalent to about  $4 \times 10^9$  protons/cm<sup>2</sup> (p/cm<sup>2</sup>) at 100 MeV energies [13, 20]. We expose DMs to various proton fluences at the Tri-University Meson Facility (TRIUMF), producing protons with energies of about 105 MeV. In our apparatus, an incoming proton will deposit some of its energy in the surrounding material—namely, the cooler box, which would be absent on the satellite, and a metal fiber coupler—prior to reaching an APD. Consequently, a 105 MeV incident proton reduces to 92.8 MeV at the APD [20]. The reduced velocity leads to increased travel time through the APD substrate, where the proton then deposits a greater amount of energy, and the corresponding

displacement damage is 1.052 times greater than what would be obtained with an incident proton energy of 100 MeV at the APD.

### 3 Methodology

Three detector modules were constructed and brought to TRIUMF for testing conducted May 1–6, 2017. Two of these modules, DM1 and DM2, underwent multiple rounds of proton irradiation to emulate the gradual damage accumulation and cyclical usage that would be experienced in orbit. The third DM was not irradiated and acts as a control.

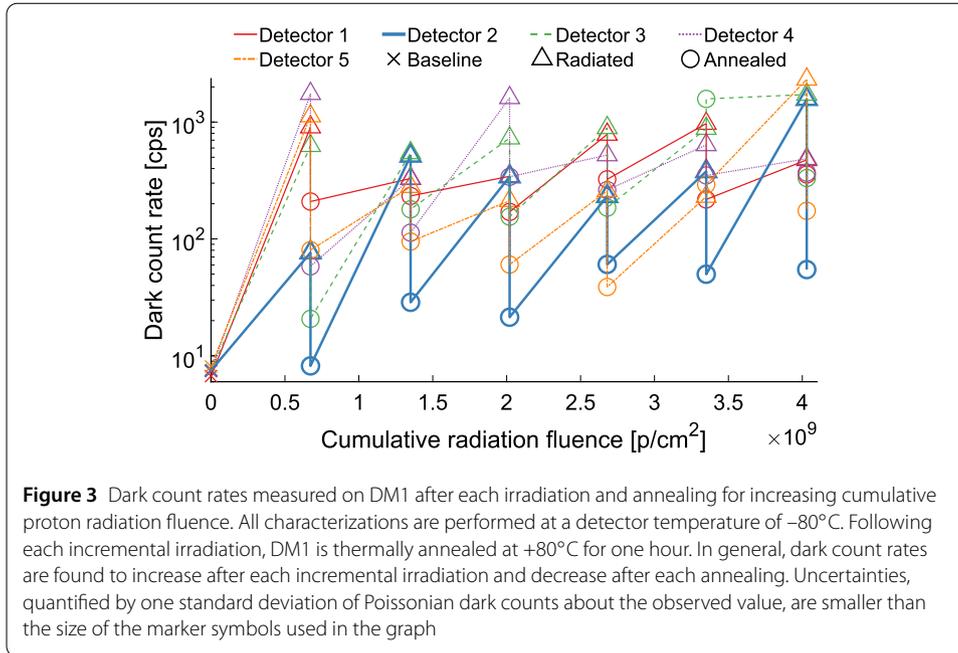
Proton fluences were applied to DM1 in regular increments of nominally  $6.67 \times 10^8$  p/cm<sup>2</sup>, corresponding to 4.2 months equivalent in LEO after adjusting for energy loss in materials surrounding our APDs. We thermally annealed DM1 for one hour between each irradiation. (For more on the annealing duration, see [Appendix](#).) In contrast, thermal annealing of DM2 (also one hour) was only performed if the dark count rate exceeded 2 kcps in each of two or more detectors, to mitigate against outliers. The dark count rate threshold is chosen in view of QKD performance projected for our modelling of ground to space link—see Ref. [7]. Taking this approach, we can compare the effects of the two annealing strategies, periodic and conditional. To allow more fine-grained observation of the dark count rate, proton fluences were applied to DM2 in irregular, initially smaller increments.

DM1 was irradiated to a total fluence of  $4 \times 10^9$  p/cm<sup>2</sup> (2.1 year equivalent in LEO) while DM2 was irradiated to a total fluence of  $2 \times 10^{10}$  p/cm<sup>2</sup> (10.5 year equivalent in LEO), with annealing performed at the nominal two-year mission end as a matter of course for comparison to DM1. We subjected DM2 to greater cumulative fluence—well beyond the nominal mission duration—and colder operating temperatures to explore potential late-life performance of the system. All three DMs were characterized before and after shipping to TRIUMF, while DM1 and DM2 were also characterized at TRIUMF before initial irradiation, after each irradiation (prior to annealing, if any), and again after each annealing (where applicable). Each characterization comprised measuring breakdown voltage, output pulse amplitude and full width at half maximum (FWHM), recharge time, dark count rate, photon detection efficiency, timing jitter, saturation, and afterpulsing probability, for each detector at  $-80^\circ\text{C}$ .

Characterization of each DM proceeded as follows: the breakdown voltage of each detector was measured by observing the presence of pulses on an oscilloscope. At 20 V above the breakdown voltage, the detector's output pulse amplitude and FWHM, and recharge time were then observed by eye over the oscilloscope and recorded. Time-tags of output pulses were then recorded (for all detectors at once) with and without the pulsing laser active. Finally, time-tags were recorded while the input laser power was slowly swept through saturation.

Dark count rates and detection efficiencies of each detector were determined from counts rates observed in inactive- and active-laser data, respectively. Detector timing jitter was extracted from the active-laser data by producing a histogram of time differences between detection events and laser reference pulses. The overall system timing jitter was taken as the FWHM of a Gaussian curve fit of this distribution, and jitter contributions of the laser and time tagging unit were then subtracted (in quadrature).

The active-laser data consists of photon and dark count detections, and afterpulses caused by each of those. Because the afterpulsing time constant is greater than the laser



pulse period, this results in a time-delta histogram with a (roughly Gaussian) photon detection peak on top of an approximately constant noise floor. By performing similar analysis of the inactive-laser data, we determined the combined dark-count and associated afterpulsing contribution to this noise floor. Subtracting this from the active-laser time-delta histogram, we are left with contributions from only incident photons, at a rate  $R_{\text{photons}}$ , and a residual noise floor due to their associated afterpulses. We define the afterpulsing probability as

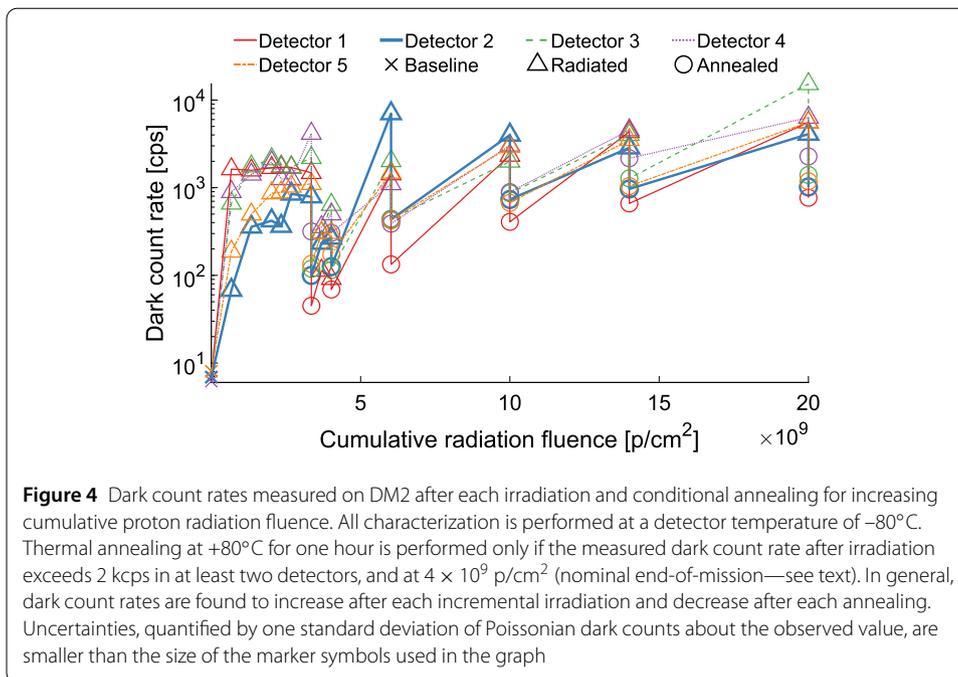
$$P_A = \frac{R_{\text{afterpulsing}}}{R_{\text{photons}} + R_{\text{afterpulsing}}},$$

where the afterpulsing rate  $R_{\text{afterpulsing}}$  includes only afterpulses that are caused by photon detection events. Numerator and denominator are evaluated from suitable off-peak and on-peak locations (respectively) in the time-delta histograms. The above definition corresponds to the average number of afterpulses directly arising due to the avalanche corresponding to any arbitrarily chosen output pulse. Although  $P_A$  is mathematically evaluated with respect to the photon rate here, it can be generalized to any output pulse (including, e.g., afterpulses of afterpulses) on the assumption that all avalanches in the detector substrate are statistically indistinguishable from each other.

#### 4 Results and discussion

As expected, no property of the control DM showed any significant change for the duration of the experiment. For DM1 and DM2, we find that breakdown voltage, output pulse amplitude and FWHM, recharge time, photon detection efficiency, timing jitter, and saturation characteristics are generally uncorrelated with cumulative proton radiation fluence and thermal annealing. This is consistent with the results of previous studies [18, 21].

Figure 3 shows dark count rates measured after each incremental irradiation and fixed-period annealing of DM1. As expected, proton irradiation increases dark count rates, and

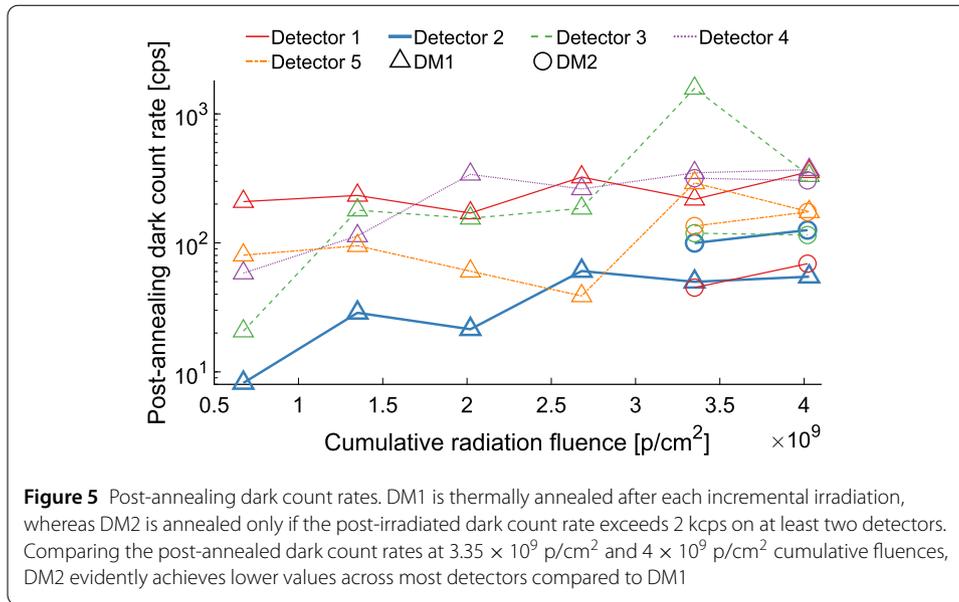


we observe a decrease in dark count rates after each annealing, discounting two statistical anomalies at  $3.35 \times 10^9 \text{ p/cm}^2$  cumulative fluence. A general increase in post-annealed dark count rates with the cumulative fluence is apparent, indicating accumulated damage that annealing cannot repair. Nevertheless, this strategy maintains post-annealing dark count rates under 500 cps throughout the 2.1-year-LEO-equivalent fluence for four of the five detectors. (The outlying detector experienced a post-annealing dark count rate increase, reaching about 1.6 kcps at  $3.35 \times 10^9 \text{ p/cm}^2$  cumulative fluence.) From prior analysis we may infer that these sub-500 cps dark count rates would lead to reduced QKD key rates by a few percent to a few tens of percent, relative to the nominal value (see Table 2 of Ref. [7] and Table 2.6 of Ref. [22]).

Figure 4 shows dark count rates measured after each irradiation and conditional annealing of DM2. We again observe a general increase in dark count rates after each irradiation, although unlike for DM1, some instances of decreased dark count rate can be seen. (For example, three of the five detectors see a dark count rate decrease immediately after irradiation at  $2.35 \times 10^9 \text{ p/cm}^2$  cumulative fluence. Absent any indication of a causative mechanism, we attribute this to statistical fluctuations.<sup>2</sup>) Notably, the conditional annealing strategy saw annealing only once prior to the cumulative fluence equivalent to the two-year nominal mission life, at which point DM2 was annealed as a matter of course.

Like DM1, dark count rates decrease when annealing is applied. We find that thermal annealing is effective in maintaining dark count rates below 500 cps for cumulative fluence up to  $6 \times 10^9 \text{ p/cm}^2$ , 3.15-year-LEO-equivalent dosage. However, at the next cumulative fluence,  $1 \times 10^{10} \text{ p/cm}^2$  or 5.25-year-LEO-equivalent, the post-annealed dark count rate increases to over 800 cps in two of the detectors.

<sup>2</sup>It is notable that six such anomalous results occur following a relatively small fluence increment of nominally  $3.33 \times 10^8 \text{ p/cm}^2$ , three occur following a  $6.67 \times 10^8 \text{ p/cm}^2$  fluence increment, and none are observed for higher fluence increments.

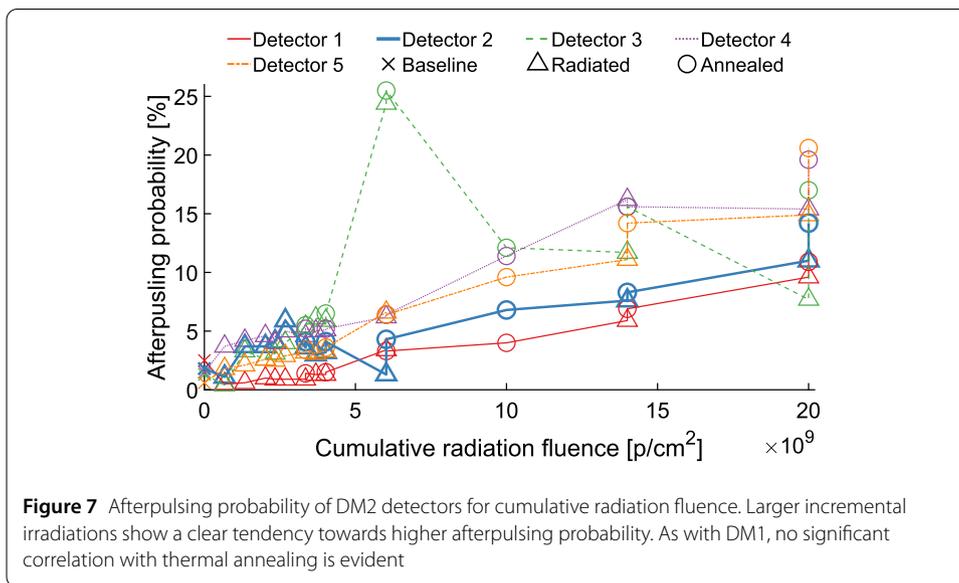
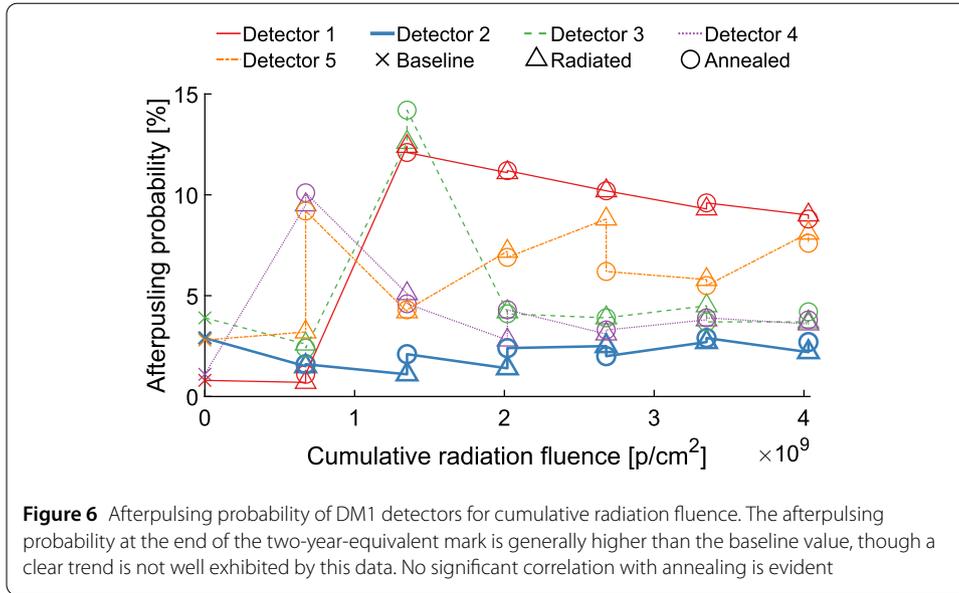


We define the dark count reduction factor (DCRF) as the ratio of the dark count rate before annealing to that after annealing. Most DCRF values cluster between 2 and 5; the largest DCRF found is 32 on DM2. Annealing tends to have the largest DCRF when applied for the first time, when there is the least permanent radiation damage. After this the DCRF values are largely uncorrelated with cumulative fluence. The DCRF also did not show any correlation with the dark count rates measured before the annealing process.

Figure 5 shows the post-annealed dark count rates for both DMs irradiated up to a cumulative fluence of  $4 \times 10^9$  p/cm<sup>2</sup>. The relative performance of the two annealing strategies can be assessed from observations at the two cumulative fluences at which both DMs are annealed. The results indicate that DM2 has slightly lower post-annealed dark count rates across most detectors, despite both DMs being subjected to the same cumulative fluence. Due to the limited samples, it is possible that this originates from statistical variation; alternately, if real, then DM1 experienced worse performance as a consequence of being annealed more times. This suggests that it may be wise to anneal with some conservatism. Given that conditional annealing, with a suitably chosen threshold, will at least achieve the same overall dark count rates that are maintained using periodic annealing, it thus follows that conditional annealing should be preferred.

Irradiating DM2 into late-life condition, with a cumulative fluence equivalent to 10.5 years in LEO ( $2 \times 10^{10}$  p/cm<sup>2</sup>), we observe a mean detector dark count rate following annealing of 1.3 kcps. It is remarkable that the dark count rate can be maintained below the annealing threshold after such significant exposure. Despite worsening performance, prior calculations [7, 22] indicate that DM2's dark count rates would still be low enough to perform QKD even at this well-past-nominal late-life stage.

Afterpulsing probabilities are calculated for both DMs by evaluating the distribution of time deltas between detection events and the corresponding laser reference pulse (Sect. 3). Figures 6 and 7 show the afterpulsing probabilities evaluated corresponding to the characterizations performed after each incremental irradiation and annealing cycles for DM1 and DM2. Afterpulsing probability is seen to generally increase with each incremental irradiation, particularly for the higher fluences of DM2. Thermal annealing has no consis-



tent effect on the afterpulsing probability. For DM1, afterpulsing probabilities are higher at  $4 \times 10^9$  p/cm<sup>2</sup> cumulative fluence than the corresponding baseline (unirradiated) values for three of the five detectors. This effect is more pronounced in DM2, which is radiated up to  $2 \times 10^{10}$  p/cm<sup>2</sup> cumulative fluence, where all the detectors registered higher afterpulsing probabilities compared to their baseline values.

Increased afterpulsing probability tends to increase the dark count rate, which could in part explain the increase of post-annealed dark count rates with higher cumulative fluence in Fig. 5. Because of this tendency, high afterpulsing probabilities can undermine the usability of the detectors if the corresponding signal to noise ratio drops below a critical value. This may ultimately limit the lifetime of the satellite since it appears thermal annealing cannot mitigate the radiation-induced afterpulsing.

Afterpulsing arises from trapped charge carriers in defects of the detector substrate—proton radiation may increase the density of these defect sites. We note that the apparent increase in afterpulsing probability due to the radiation exposure does not appear to improve with annealing, unlike the dark count rate. To our knowledge, there is no established mechanism to explain this behaviour, and more research will be needed to identify this afterpulsing mechanism. While our detectors are passively quenched, the afterpulsing could be mitigated using methods established for telecom single-photon detectors, either using a gated operation (e.g., Ref. [23]), or free-running operation with active afterpulsing suppression (e.g., Ref. [24]). Although we do not explore it here, these and related system parameters may be optimized for QKD key transmission.

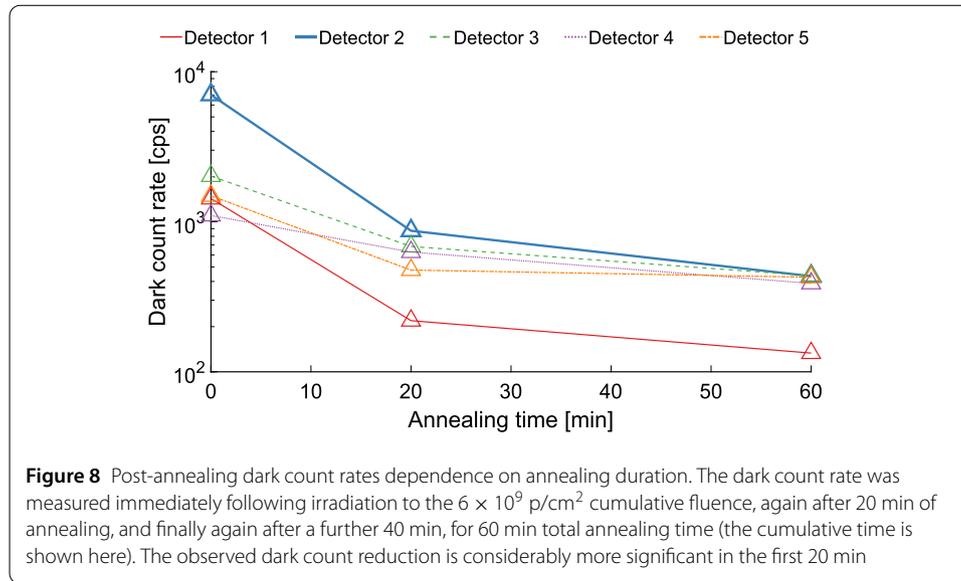
## 5 Conclusions

The dark count rates of Si APD detectors increase substantially due to proton radiation experienced in low-Earth orbit. This can be mitigated by low (but well above cryogenic) temperature operation, and thermal annealing. By measuring the properties of detectors throughout multiple cumulative exposures to varying proton fluences, equivalent to different stages of a LEO life-cycle, and applying thermal annealing at some of these stages, we have established a profile representative of realistic operational scenarios of a quantum communication apparatus on a LEO space platform.

Our results show that even after repeated applications, annealing after irradiation is capable of achieving detector dark count rates suitable to perform QKD—below 500 cps after radiation exposure of a nominal two-year mission lifetime, and potentially sufficiently low after even 10.5 years exposure, albeit with reduced performance in the latter case. Afterpulsing probability was shown to increase with cumulative fluence—however, thermal annealing had no significant effect on the afterpulsing probability. All other detector parameters were unaffected by both cumulative fluence and annealing.

Our observations further suggest that annealing conditionally—only when the dark count rate exceeds a threshold value (here 2 kcps)—may achieve slightly lower post-annealed dark count rates over time in orbit than annealing at fixed periodic intervals. It should be noted that the optimal choice of threshold would depend significantly on the design and operational parameters of the QKD satellite platform that determine the expected channel losses and noise caused by background light. Further, a trade-off between lifetime and key rate can be made: applications interested in high performance over a short term could employ a lower threshold, thus performing annealing more frequently, compared to applications that can accept more moderate performance in exchange for a longer lifetime. Determining the appropriate balance would require additional quantitative analysis incorporating such details—the nonlinear response of the lifetime amount of generated key to the operating conditions may imply an interesting optimization problem. We leave this for future work.

We have demonstrated that thermal annealing is an effective strategy for mitigating radiation-induced dark counts, is feasible under the continuous radiation environment of a low-Earth orbit, and can be applied at appropriate times as a device maintenance procedure. This knowledge helps guide future developments, including the QEYSSat mission and beyond, towards cost-effective, high-performance, and long-lived quantum devices in space.



### Appendix: Annealing time

We chose a baseline annealing time of one hour, following results of previous work [18]. However, for the sake of reproducibility, we also confirmed that our expectations were justified by taking an intermediate measurement at a shorter time while annealing DM2 at a total fluence of  $6 \times 10^9$  p/cm<sup>2</sup>. Figure 8 shows the measured dark count rates corresponding to 20 minutes of annealing followed by an additional 40 minutes of annealing. The decrease in the dark count rate has significantly greater magnitude during the first 20 min compared to the subsequent 40 min, with the dark count rates beginning to stabilize by the 60 minute mark—indicating further annealing time would have little impact. This is consistent with the previous work [18].

### Acknowledgements

We thank Excelitas Technologies for discussions and for providing selected APD samples. We also thank NEPTec Design Group for discussions, designing and building the DM.

### Funding

This work was supported by the Canadian Space Agency (STDP and FAST programs), Industry Canada, Canada Foundation for Innovation (CFI), Ontario Research Fund (ORF), Natural Sciences and Engineering Research Council (NSERC; programs Discovery and CryptoWorks21), and the Ontario Ministry of Research, Innovation and Science (MRIS).

### Availability of data and materials

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

### Competing interests

The authors declare that they have no competing interests.

### Authors' contributions

The study was conceived by TJ with VM. BM provided planning and logistical support. The test procedure and apparatus containing the DM was developed by JPB, supervised by TJ and assisted by ID and BLH. ID, JPB, BLH, JGL, RT, SA, VM and TJ conducted the experiment. ID analyzed the data and prepared the manuscript with BLH, assisted by JPB, RT, VM, and TJ. All authors read and approved the final manuscript.

### Author details

<sup>1</sup>Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada. <sup>2</sup>Department of Physics and Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada. <sup>3</sup>Aegis Quantum, Waterloo, ON, Canada. <sup>4</sup>Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada. <sup>5</sup>Russian Quantum Center, Skolkovo, Moscow, 121205, Russia. <sup>6</sup>Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China,

Shanghai, 201315, People's Republic of China. <sup>7</sup>NTI Center for Quantum Communications, National University of Science and Technology MISIS, Moscow, 119049, Russia.

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 20 December 2020 Accepted: 5 May 2021 Published online: 17 May 2021

## References

1. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* 1999;41(2):303–32. <https://doi.org/10.1137/S0036144598347011>.
2. McEliece RJ. A public-key cryptosystem based on algebraic. *DSN Progress Rep.* 1978;44:114–6.
3. Canteaut A, Sendrier N. Cryptanalysis of the original McEliece cryptosystem. In: International conference on the theory and application of cryptology and information security. Berlin: Springer; 1998. p. 187–99. [https://doi.org/10.1007/3-540-49649-1\\_16](https://doi.org/10.1007/3-540-49649-1_16).
4. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proc. International conference on computers, systems, and signal processing. Bangalore, India. New York: IEEE Press; 1984. p. 175–9. <https://doi.org/10.1016/j.tcs.2014.05.025>.
5. Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. *Phys Rev Lett.* 1992;68(5):557. <https://doi.org/10.1103/PhysRevLett.68.557>.
6. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Rev Mod Phys.* 2009;81(3):1301. <https://doi.org/10.1103/RevModPhys.81.1301>.
7. Bourgoin J, Meyer-Scott E, Higgins BL, Helou B, Erven C, Hübel H, Kumar B, Hudson D, D'Souza I, Girard R, Laflamme R, Jennewein T. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J Phys.* 2013;15(2):023006. <https://doi.org/10.1088/1367-2630/16/6/069502>.
8. Liao S-K, Cai W-Q, Liu W-Y, Zhang L, Li Y, Ren J-G, Yin J, Shen Q, Cao Y, Li Z-P, Li F-Z, Chen X-W, Sun L-H, Jia J-J, Wu J-C, Jiang X-J, Wang J-F, Huang Y-M, Wang Q, Zhou Y-L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y-A, Liu N-L, Wang X-B, Zhu Z-C, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-to-ground quantum key distribution. *Nature.* 2017;549:43. <https://doi.org/10.1038/nature23655>.
9. Jennewein T, Bourgoin JP, Higgins B, Holloway C, Meyer-Scott E, Erven C, Heim B, Yan Z, Hübel H, Weihs G, Choi E, D'Souza I, Hudson D, Laflamme R. QEYSSAT: a mission proposal for a quantum receiver in space. *Proc SPIE.* 2014;8997:89970–1. <https://doi.org/10.1117/12.2041693>.
10. Quantum Encryption and Science Satellite (QEYSSat). <https://www.asc-csa.gc.ca/eng/sciences/qeyssat.asp>. Accessed 27 November 2020.
11. Chancellor J, Scott G, Sutton J. Space radiation: the number one risk to astronaut health beyond low Earth orbit. *Life.* 2014;4(3):491–510. <https://doi.org/10.3390/life4030491>.
12. Srour J, Marshall CJ, Marshall PW. Review of displacement damage effects in silicon devices. *IEEE Trans Nucl Sci.* 2003;50(3):653–70. <https://doi.org/10.1109/TNS.2003.813197>.
13. Anisimova E. Single-photon detectors for long distance quantum communications. PhD thesis. University of Waterloo; 2018. <http://hdl.handle.net/10012/12935>.
14. Gallivanoni A, Rech I, Ghioni M. Progress in quenching circuits for single photon avalanche diodes. *IEEE Trans Nucl Sci.* 2010;57(6):3815–26. <https://doi.org/10.1109/TNS.2010.2074213>.
15. Lim JG, Anisimova E, Higgins BL, Bourgoin J-P, Jennewein T, Makarov V. Laser annealing heals radiation damage in avalanche photodiodes. *EPJ Quantum Technol.* 2017;4(1):11. <https://doi.org/10.1140/epjqt/s40507-017-0064-x>.
16. Kim Y-S, Jeong Y-C, Sauge S, Makarov V, Kim Y-H. Ultra-low noise single-photon detector based on Si avalanche photodiode. *Rev Sci Instrum.* 2011;82:093110. <https://doi.org/10.1063/1.3641294>.
17. Tan YC, Chandrasekara R, Cheng C, Ling A. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *Opt Express.* 2013;21(14):16946–54. <https://doi.org/10.1364/OE.21.016946>.
18. Anisimova E, Higgins BL, Bourgoin J-P, Cranmer M, Choi E, Hudson D, Piche LP, Scott A, Makarov V, Jennewein T. Mitigating radiation damage of single photon detectors for space applications. *EPJ Quantum Technol.* 2017;4(1):10. <https://doi.org/10.1140/epjqt/s40507-017-0062-z>.
19. Dale CJ, Chen L, McNulty PJ, Marshall PW, Burke EA. A comparison of Monte Carlo and analytic treatments of displacement damage in Si microvolumes. *IEEE Trans Nucl Sci.* 1994;41(6):1974–83. <https://doi.org/10.1109/23.340532>.
20. Lim JG. Laser annealing irradiated silicon single-photon avalanche photodiodes for quantum satellite receiver. Master's thesis. University of Waterloo; 2018. <http://hdl.handle.net/10012/13284>.
21. Sun X, Dautet H. Proton radiation damage of Si APD single photon counters. In: Radiation effects data workshop, 2001 IEEE. New York: IEEE Press; 2001. p. 146–50. <https://doi.org/10.1109/REDW.2001.960462>.
22. Bourgoin J-P. Experimental and theoretical demonstration of the feasibility of global quantum cryptography using satellites. PhD thesis. University of Waterloo; 2014. <http://hdl.handle.net/10012/8897>.
23. He D-Y, Wang S, Chen W, Yin Z-Q, Qian Y-J, Zhou Z, Guo G-C, Han Z-F. Sine-wave gating InGaAs/InP single photon detector with ultralow afterpulse. *Appl Phys Lett.* 2017;110(11):111104. <https://doi.org/10.1063/1.4978599>.
24. Lunghi T, Barreiro C, Guinnard O, Houlmann R, Jiang X, Itzler MA, Zbinden H. Free-running single-photon detection based on a negative feedback InGaAs APD. *J Mod Opt.* 2012;59(17):1481–8. <https://doi.org/10.1080/09500340.2012.690050>.