Single-photon detectors for satellite based quantum communications

by

Nigar Sultana

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering (Quantum Information)

Waterloo, Ontario, Canada, 2020

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner	NAME	Giuseppe Vallone
	Title	Associate Professor
Supervisor	NAME	Thomas Jennewein
	Title	Associate Professor
Co-Supervisor	NAME	Guoxing Miao
	Title	Associate Professor
Internal Member	NAME	Na Young Kim
	Title	Associate Professor
Internal Member	NAME	Michal Bajcsy
	Title	Assistant Professor
Internal-external Member	NAME	Kazi Rajibul Islam
	Title	Assistant Professor

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of contribution

1. **Chapter 5: CAPSat detector module for in-orbit laser annealing.**
   Contribution: Main lead of the project. Designing, building, and testing the detector module. Also, developing firmware for a programmable system on chip (PSoC) embedded system to control the module functions.
   Publication: Experiment in progress.

2. **Chapter 6: A new readout circuit for NFADs and their characterization.**
   Contribution: Main lead of the project. Designing, building, testing the NFAD readout module, and Characterizing NFADs.
   Publication: N. Sultana, J.-P. Bourgoin, K.B.Kuntz, and T. Jennewein, A simple photon counting module for free-running negative-feedback avalanche diodes with active suppression of afterpulses, (manuscript in preparation).

3. **Chapter 7: Blinding attack on NFADs.**
   Contribution: Performing blinding attack on the two NFADs running under new readout system that is explained in chapter 6.
   Publication: G. Gras, N. Sultana, A. Huang, T. Jennewein, F. Bussières, V. Makarov, and H. Zbinden, Optical control of free running single photon negative feedback avalanche diode detector, arXiv:1911.12742v1, 2019.

4. **Chapter 8: High-speed single-photon source for airborne demonstration of QKD.**
   Contribution: Developing high-speed source modulator. Particularly, finding the appropriate arbitrary waveform generator (AWG) to run four devices (a laser, an intensity, and two phase-modulators) synchronously, writing code in Matlab to generate random voltage sequences for the devices and interfacing them with the AWG, as well as characterizing the sum-frequency generation crystal.
   Publication: C.J. Pugh, S. Kaiser, J.-P Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B.L. Higgins, and others, Airborne demonstration of a quantum key distribution receiver payload, Quantum Science and Technology, 2(2):024009, 2017.

Abstract

With the growing use of online communications in our modern society, information security is becoming a big concern. Along with that, the progress in quantum computers is posing severe threats to such communications. Once powerful quantum computers are available, most of today's encryption schemes, which are based on computationally hard problems, will be broken within a short period. Researchers are therefore making a great effort to establish quantum-safe encryption schemes. One such scheme is quantum key distribution (QKD), which utilizes the laws of quantum mechanics. These cryptography protocols offer unconditional security to the communication between two distant parties by providing a secure way of sharing encryption keys between them.

While over last few decades QKD has continuously progressed, it is limited to a distance of up to several hundred kilometers using terrestrial quantum links. Satellites are therefore being considered to extend the QKD range for global coverage, although implementations of the satellite-based QKD infrastructure are still in their early stage. There are many aspects of QKD that need further assessment and advancement for establishing long-term satellite-based quantum communication (QC). My thesis works were focused on developing advanced systems for single-photon detectors and quantum sources.

Single photon avalanche diodes (SPADs) are the most viable option for satellite-based quantum communications. They must travel to outer space either for receiving quantum-states in the ground-to-satellite QC, or for characterizing the quantum-sources in the satellite-to-ground QC. However, while in space, SPADs exhibit damage caused by the space radiation that gradually increases their dark counts. Performing QKD is not possible when the dark counts exceed a specific threshold. Hence, methods of reducing the detectors' dark counts by mitigating the damages would help to extend the SPADs' in-space useful lifetime. Laser annealing is one such effective method, found in lab experiments, to heal the radiation-induced detector damages. We now aim to carry out this method in low Earth orbit (LEO) to verify its in-orbit effectiveness. On that goal, we are building an annealing payload (APL) for a cube satellite (CubeSat) in collaboration with the University of Illinois at Urbana Champaign (UIUC). We, the University of Waterloo team, built one of the two segments of the APL– a space-qualified detector module containing two

Excelitas C30902SH and Excelitas SLiK detectors. Our miniaturized and compact module integrates the facilities required for the detector operation and laser annealing, as well as an active detector temperature control system. The operation of the detector module is highly flexible and software controllable. Our detector module will work together with the control board containing the laser annealing system (built by the UIUC team). Once the satellite has been launched in 2020, the in-orbit experiment will enable us to study the in-space SPAD radiation damage and their healing using the integrated annealing system.

During a second project, we designed and built a new simple readout circuit for the negative feedback avalanche diodes (NFADs), which are free-running single-photon detectors at telecom wavelengths. These detectors suffer from strong afterpulsing effects, which limits their overall performances. Therefore, our readout system incorporates features to suppress NFAD afterpulses. We also used this custom readout to characterize two NFADs (from Princeton Lightwave) and assessed the performance of the new electronics. Our analysis showed that even at higher detection efficiencies, a 20 μs hold-off time after each avalanche event is enough to extensively reduce the number of afterpulses and to keep the dark count rate below 100 Hz at 192 K temperature. Both the detectors showed timing jitter of less than 75 ps FWHM at their maximum efficiencies. The best figure of merit is found to be 1.6×10^7, which is comparable to that of the high-performing superconducting nanowire single photon detectors. This result demonstrates the suitability of our readout and the NFADs in various quantum optics applications, such as in long-distance quantum key distribution, where the detection rate is usually low.

We then performed a blinding attack, which enables an Eavesdropper in QKD to gain information on the key, on these NFADs using bright illumination. These detectors are usually threshold detectors that generate a click when the optical power is above a certain threshold, otherwise they do not click. Blinding attack utilizes their inability of resolving the photon numbers. During the experiment, we sent controlled optical pulses with a high time resolution to deterministically force detection at the detectors. The result demonstrated the NFADs' susceptibility to this attacks, which tells us to include countermeasures into the system to protect the communications.

Finally, we built a quantum source to produce 785 nm polarized photons to implement decoy-state BB84 QKD. Our source utilized the sum-frequency generation scheme to generate 785 nm laser pulses. Its modulator system includes an intensity modulator and two phase modulators in the Mach-Zehnder configuration to prepare polarized quantum states with different intensities. Our source provides a repetition rate of 500 MHz, which was successfully used in an airborne QKD demonstration with a moving receiver up to 10 km distance.

To summarize, my research projects are a contribution to the development of advanced devices, particularly single-photon detectors for quantum communications.

Acknowledgements

I would like to thank my supervisor Dr. Thomas Jennewein for his guidance, encouragement and support during my PhD. I learned a lot over the past few years and truly enjoyed working with him. His help and discussions made it easier to overcome the issues in the experiments. At the same time, I feel lucky getting the opportunity to be a part of the Canadian satellite quantum communication endeavour. I extend my thanks to my co-supervisor Dr. Guoxing Miao for supporting me whenever I needed him. I thank my other committee members, Dr. Michal Bajcsy, Dr. Na Young Kim and Dr. Kazi Rajibul Islam for their advice. I also thank Dr. Giuseppe Vallone for agreeing to be part my thesis defense committee.

Many thanks to Dr.Vadim Makarov for his valuable advice and providing access to his lab. So many times I could continue my experiments by using resources from his lab. I am also grateful to him for his guidance in the blinding attack experiment, and for useful criticism on my comprehensive report as a committee member.

I extend my gratitude to Dr. Paul Kwiat and his team at the University of Illinois at Urbana Champaign, US. I want to especially thank Eric Alpine and Joe Stahl, who were continuously in touch over the time of developing the detector module for the CAPSat mission. I am grateful to them for their warm welcome during my visits to Illinois and all sorts of support at the time of implementing the detector module for the CAPSat mission using their lab. I thank Dr. Alexander Ling from National University of Singapore for useful discussion on space suitable electronics.

I would like to thank Prof. Hugo Zbinden, Félix Bussières and Gaëtan Gras from ID Quantique, Switzerland for their collaborative efforts in the blinding attack experiment. I acknowledge their patience waiting a long time for us to get ready for the experiment.

Many thanks to all my colleagues in the quantum photonics lab for their contribution to this work either directly or through discussions. An especial thanks to Dr. Brendon Higgins, Ramy Tannous, and Youn Seok Lee for reviewing my thesis and giving useful suggestions. I would like to acknowledge my colleagues who directly contributed to this work. Thanks to Dr. Jean Philippe Bourgoin for his help and valuable discussions during the WCP source implementation and characterization of the NFAD detectors. Next, my heartiest thanks to Katanya, who enormously supported me mentally. Whenever we had a discussion out of research, she shared her experiences and helped me to release my stresses. She and Jean Phillipe assisted me immensely to prepare the manuscript on the experiment of NFAD readout system and detector characterization. I would like to extend my thanks to Dr. Rolf Horn for lending us his SPDC source and making effort to set it up for our use. Many thanks to Dr. Anqi Huang who helped me to initiate the blinding attack experiment.

I also extend my gratitude to the funding supports from the Canada Foundation for Innovation (CFI), the Canadian Space Agency (CSA), the Ontario Research Fund (ORF), the Natural Sciences and Engineering Research Council of Canada (NSERC), and Industry Canada.

I gratefully acknowledge my friends in Waterloo. Their company enormously energised me and helped me to stay out of stress. Next, I express my deep and sincere gratitude to my husband, Dr. Shihan Sajeed for his continuous help and support. Without him, it was not possible to complete this journey with a little daughter. Whenever I needed more time for my research, he was the one who took care of my daughter and took some duties off from me. I cannot express his contribution with words. Finally, I would like to mention my daughter, Sabriyah Sajeed, with lots of love. I cannot imagine my Ph.D. journey without her. She was the greatest source of happiness in this journey.

Dedication

To my loving parents. I can feel how happy my father would have been if he could see my accomplishment. I always hear his proud voice in my heart which gave me the inspiration throughout my Ph.D. journey. Next, my mother's contribution towards my life is impossible to express with words. I simply know without their lessons and hard work, I would not be the person I am today.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In today's modern life, our society is deeply connected through a variety of electronic devices, such as desktops, laptops, smartphones, wearables, or smart cards. Because of the technology advancements of these gadgets, people nowadays rely heavily on online communications in their daily activities. Many of such activities include online data transfer, banking, shopping, email, and data storage in the clouds, which are rendered using public communication channels. Therefore, it is crucial to protect these transmissions using encryption so that an unauthorized entity does not gain access to the information.

Modern cryptography uses two types of encryption schemes: symmetric cryptography (i.e., advanced encryption standard, AES [1], triple data encryption standard, TDES [2]), and asymmetric cryptography (i.e., RSA [3], Diffie-Hellman, DH [4], and elliptical curve, ECC [5, 6]). Most of these schemes do not provide any provable security. They are based on mathematically hard problems, which are assumed to be unsolvable within a certain time frame using conventional computers. The construct of the mathematical problems is such that the computation is easy in one direction while the reverse is difficult. For instance, the popular public-key scheme, RSA utilizes the difficulty of factorizing an integer that is a product of two secret prime numbers. Typically, long integers are chosen so that an adversary needs several decades to break the scheme. The security thus depends on limited computational power of an adversary.

However, the security of these schemes is currently under threat posed by the exponential processing power of quantum computers. These new computers use quantum mechanical effects for information processing. Their fundamental information units are quantum bits, also known as qubits, that can be at both '0' and '1' states concurrently. This property of qubits is called superposition that provides a probabilistic outcome upon measurement. In addition, using another property of qubits – quantum entanglement –

one qubit can influence another at a distance. A combination of superposition and entanglement properties give parallel processing power to quantum computers. Therefore, a quantum computer using n qubits can execute 2^n operations simultaneously. An adversary, having access to such quantum computers can exploit quantum algorithms to optimize certain hard problems. For example, Shor's algorithm [7] would make it possible to factorize a large number in a relatively shorter time. An adversary could also run Grover's algorithm [8] in a quantum machine to break the symmetric cryptography systems. This algorithm would be able to find a particular entry from an unsorted database of size N in $\sqrt{N}$ iterations, while a conventional computer would need N/2 iterations. For instance, in AES-128 symmetric cryptography, an attacker would need a maximum 2^{64} operations in a quantum machine as opposed to that of 2^{128} in classical computer to break the scheme.

The concerning fact – from cryptography's point of view – is that quantum computers are coming into existence very fast. For example, the quantum machine from Rigetti has the capability of up to 128 qubits [9]. However, a study by the National Academies says that quantum computers still need way more processing power to attempt a real attack on the existing classical encryptions. It is stated that a quantum computer would need 20 million qubits to break an RSA-2048 bit system [10]. Now the question is, how long it will take to build a quantum computer with super processing power. Although the advances of these machines are unpredictable, quantum scientists anticipate that quantum computers might come earlier than expected. This is certainly alarming news to any government, defense, or business agencies who want to secure their data for decades. Therefore, it is important to develop a 'quantum-safe' cryptography soon so that defensive measures are ready against the foreseen attacks by the quantum computers.

At this moment there are two possible solutions to this threats: post-quantum cryptography (PQC) [11] and quantum key distribution (QKD) [12, 13]. PQC is also based upon complex mathematical problems that are assumed to be unsolvable, or at least not solvable within a certain time, even by a quantum computer. This scheme is also known as quantum-resistant cryptography. They can be implemented within our existing infrastructures as most of the implementations are software-based. However, PQC schemes do not guarantee security due to the lack of security proofs. On the other hand, QKD guarantees unconditional security (not dependent on any assumptions), as this protocol is based on quantum mechanics. It is a method of generating encryption keys between two end-users (generally referred to as Alice and Bob). In QKD, there is a fundamental limit that an Eavesdropper (Eve) can gain from a quantum system. According to the Heisenberg Uncertainty Principle [14], Eve can only know one parameter with certainty from a conjugate property by measuring a quantum system. In addition, 'No-cloning theorem' [15] says that if Eve tries to copy a quantum state, it will disturb the system. Therefore, Eve's attempt to measure or copy a quantum state will introduce errors in the measurement outcomes. This will reveal her presence to Alice and Bob. The only downside of QKD systems is that it needs a completely different sophisticated infrastructure.

However, QKD being the only provably secure quantum-safe scheme, a great effort has been given to the development of its protocols and the technology required for its infrastructure. QKD was originally proposed in 1984 by Bennet and Brassard (BB84 protocol) [12]. It uses photons as information carriers that are transmitted from Alice to Bob. This protocol can be implemented using various degrees of freedom. In QKD, using polarization degree of freedom, Alice first generates a single-photon in one of the four polarization states: $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$. To prepare the photon-states, she uses two non-orthogonal bases: horizontal/Vertical (H/V) basis and diagonal/anti-diagonal (D/A). The bases are used to encode bit 0 and 1, where $|H\rangle$ and $|D\rangle$ refer to 0, and $|V\rangle$ and $|A\rangle$ refer to 1. After preparing the states, Alice sends them to Bob, who measures the received photons randomly in a horizontal/Vertical (H/V) or a diagonal/anti-diagonal (D/A) basis. If Bob's measurement basis matches with that of Alice, they will have the same outcome with high probability. In contrast, for the non-matching basis choice, their outcome can be different. After completing the transmission of a certain number of qubits, they establish a key, called raw key. Then Alice and Bob communicate over an authenticated public channel. Bob announces his measurement basis that he used for each state, and Alice tells the correct basis choices. At the end of this communication phase, they keep only those states having the matching bases and discard the rest. This process is called sifting and leads to a new shorter key: sifted key. During the sifting process, if Eve tries to listen to the open communications between Alice and Bob, she will only know the basis choices, not the actual bit values. Once a sifted is produced, Alice and Bob next exchange a portion of their sifted key to check the quantum bit error rate (QBER). If the QBER exceeds a certain threshold, the operation is aborted. Otherwise, the sifted key is error corrected and then shortened through a privacy amplification process to reduce the probability of information leakage to Eve. The last two tasks are performed through a classical communication channel and known as classical post-processing. At the end of all processing, Alice and Bob establish a shared secret key between them. This key then can be used with any symmetric encryption algorithm, such as AES or TDES, although to achieve unconditional security, one-time pad (OTP) encryption scheme is required [16].

There is another main stream QKD scheme that utilizes quantum entanglement properties of photons. The scheme was proposed by Artur Ekert in 1991 (E91 protocol) [13], where an intermediate source generates an entangled-photon pair. One photon is then sent towards Alice and another one towards Bob. E91 scheme utilizes singlet states: either $\frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b \pm |V\rangle_a|H\rangle_b)$, or $\frac{1}{\sqrt{2}}(|D\rangle_a|A\rangle_b \pm |A\rangle_a|D\rangle_b)$. When received, Alice and Bob both measure the states at random bases. Both of them next communicate over a public channel to announce their chosen measurement bases for each state. They keep the states for similar bases that give a bit string and forms a raw key. One of them needs to flip their bit value since singlet states are anti-correlated. They also share a small portion of the key to test the Bell's inequality [17, 18] by calculating their correlation value S. When the correlation statistics violate some form of Bell's inequality, it confirms the entanglement, which in turn guarantees the security since there is no classical replication of such correlation. If Eve tries to eavesdrop, her action will simply disturb the correlation of the quantum states, revealing her presence to Alice and Bob. The post-processing of this scheme is similar to that of BB84 scheme.

QKD technology has progressed very fast in the last decade. Commercial QKD systems [19–21] have already been tested in government tasks (e.g., elections in Geneva), banks, as well as Soccer World cup in 2010 [19]. But the QKD links, which are generally established via optical fibers [22–24] or free-space [25–27], have limited range in the Earth. The intrinsic optical loss in fiber imposes the limit [28], while free-space links are restricted due to the possible direct point-to-point links [29]. One of the other reasons for this distance limitation is the nonexistence of quantum repeaters [30], which are still in their early stages of development, and the time of their readiness is quite unknown. Therefore, an intensive effort is being given to alternative solutions in extending the limits of QKD distance and the key rates. At present, satellites are being considered in the QKD infrastructure to extend its range. Towards that goal, China has launched its first quantum communication satellite in 2016 and has been successful in demonstrating the ground-to-satellite entanglement distribution[31], decoy-state QKD [32] and quantum teleportation [33] over 1200 km. Almost a year later, in 2017, Japan was also successful in sending single-photons from a low-cost microsatellite to a ground station [34].

However, there are various other aspects of QKD systems that need further investigation to push the existing technology to make them suitable for long-distance communication. In particular, the two main components of a quantum communication system – quantum sources and receivers – require more improvements. That leads to the direction of my research. In this thesis, I present my works that have been done on single-photon detectors (SPDs), which are the mandatory devices for quantum receivers. I also explain my work that is done on a weak coherent pulsed (WCP) source.

My recent research is developing a single-photon detector (SPD) module that fits in a small satellite – a CubeSat (described in chapter 3). Nonetheless, The detector module is designed incorporating silicon single-photon avalanche photodiodes (SPADs), which are a popular device for free-space quantum links because of their high detection efficiency. However, these SPADs are affected by the space radiation consisting of high energy electron and proton particles. In satellite-quantum communication, when the detectors in a spacecraft orbit the Earth, they come to the exposure of in-orbit radiation. It was found in a satellite mission [35] that proton radiation significantly increases the detectors' background noise by damaging the device material. The noise keeps growing each time they cross through the radiation. If the noise exceeds a certain limit, then it is impossible to perform quantum communication [36]. Therefore, it is important to keep the noise below the threshold to lengthen the mission lifetime. Fortunately, there are several effective solutions: thermal annealing [37, 38] and laser annealing [39, 40]. These methods are investigated in several ground-based experiments [41–46] to mitigate the detector radiation damages. Among these methods, laser annealing was found highly effective in resolving the damages [40, 47]. Therefore, we aim to perform an in-orbit laser annealing on the Si-SPADs within a CubeSat in the CAPSat mission [48]. We designed and implemented a SPAD module incorporating the facilities of doing laser annealing and an active thermal control system. We also developed the firmware to control its operation. Then the developed module will be tested in a thermal vacuum chamber (TVAC) to verify its performance in the space-vacuum environment. The details are discussed in chapter 5.

We have also studied negative feedback avalanche diodes (NFADs) [49], which are a type of InGaAs/InP detector. The NFADs work in a free-running mode at 1550 nm wavelength and are suitable for long-distance fiber-based quantum communication. One of the major issues with these NFADs is their significant afterpulsing probability. The afterpulses are non-photon detection events that are produced subsequently after the photon detections. These false counts adversely affect the real photon counts, and the timing of the detection events. Therefore, it is necessary to incorporate the afterpulse suppression feature in NFADs' readout electronics. From this motivation, we developed a new design of a readout incorporating a circuit for active afterpulse suppression. We then implemented the design and tested it, as well as characterized two NFAD detectors using our readout module. chapter 6 gives the details of this experiment.

Next, we performed a blinding attack [50–53] on the NFADs using bright illumination, explained in chapter 7. Usually, practical single-photon detectors suffer imperfections, exploiting which an eavesdropper can attack SPADs to gain information. Particularly in the blinding attacks, Eve can control detectors' outcomes by sending bright pulses, which enables her to get information on the transmitted quantum bits. Consequently, it is necessary to know if the SPAD devices are susceptible to blinding attacks. If they are, we will need to incorporate countermeasures into the detector systems to prevent information leakage. We therefore performed a similar attack on two NFAD samples, and our result suggests that the detectors are unsafe against the blinding attack.

In one project, I worked on single-photon source. We developed a weak coherent pulsed (WCP) source that are used in many practical realization of quantum communications. A WCP source is required to have high repetition rate for photon transmissions over a lossy links in the long-distance communications, particularly in the ground-to satellite links. High rate source increases the probability of received photons at the receiver. The WCP source that we developed provides maximum repetition rate of 500 MHz. It has phase and intensity modulators that implements BB84 decoy-state protocol [54] by preparing four polarization states at three different intensities, which was used in a successful airborne QKD demonstration up to a $10km$ distance. The design and operation of our WCP source, and the airborne QKD are described in chapter 8. Our source provides a repetition rate of 500 MHz which was also successfully used in an airborne QKD demonstration up to $10km$ distance.

Moreover, in chapter 2, I explained the background and schemes of the satellite quantum communications. Then different types of SPDs and their working principals are discussed in chapter 4. Finally, chapter 9 summarizes the results of my research works.

Chapter 2

Quantum communication satellites

2.1 Introduction

With the rapid technological development in recent years, QKD is now a mature protocol and ready for commercial implementations [20, 55]. QKD systems use either optical fiber or free-space as a medium of photon transmission [56, 57]. Fibers are more commonly used both in proof-of-principle QKD experiments [58] and in implementations of larger-scale quantum networks [59, 60]. However, fiber loss increases exponentially as the QKD distance extends. This loss reduces the signal strength down to the dark count rate of the receiver's single-photon detectors, which increases the quantum bit error rate (QBER). QBER is the percentage of incorrect bits over the total number of received bits that needs to be below a certain threshold (depends on the QKD protocol in use) to generate secure keys. The bounds of QBER (i.e., 11% for BB84 protocol [61]) thus imposes a limit in the maximum possible QKD range. Until now, fiber-based QKD succeed to generate secure keys for the longest distance of up to 421 km [28].

In contrast, QKD links over the terrestrial free-space are limited by the possible line-of-sight locations [56]. These links are also affected by the external atmosphere, especially due to the objects in optical paths, atmospheric turbulence, and weather conditions, which cause beam distortion and beam wandering. The atmospheric absorption increases exponentially and the beam divergence scales quadratically with distance. As of now, the direct free-space QKD has been successful to reach up to 144 km [56, 62].

Consequently, to facilitate long-distance quantum communications, quantum signals would be required to be amplified in the intermediate nodes. But according to no-cloning theorem [63], it is not possible to create an amplified copy of quantum signals. In this context, quantum-repeaters [30] and -satellites [64] are the two potential alternatives for the globalization of quantum communications. Quantum repeaters are very promising for future long-distance QKD, but they are still in the development process [65]. In contrast, satellite QKD is already feasible utilizing current satellite and quantum technologies [54, 66, 67]. As of now, China has already demonstrated satellite QKD in their first quantum satellite Micius [31–33], and few other countries are preparing to launch their own quantum satellites in the upcoming years [68–71].

In the satellite-based quantum links, only a small fraction of the propagation path remains in the atmosphere, less than 10 km [64], while the rest of the long path is empty space. In the empty space, optical signals experiences almost no atmosphere induced losses, due to which the satellite links can potentially connect any two points in the globe. This chapter explains the satellite-based QKD schemes, related challenges, and the efforts that are made until now towards the satellite QKD.

2.2 Satellite QKD schemes

There are several possible satellite-based quantum communication schemes (as seen in Fig. 2.1) for extending distances between two ground stations. For example:

1. Ground-to-satellite, also known as uplink, where a photon source stays on the ground station, and the satellite carries the receiver.
2. Satellite-to-ground, known as downlink, where the satellite carries the quantum source and the receiver locates at the ground station.
3. Satellite carries a entangled-photon source which sends the photon pairs to two ground stations simultaneously.
4. Inter-satellite QKD link.

In an uplink (scheme 1), the ground station streams quantum signals to a receiver located in space, whereas in a downlink (scheme 2), a satellite carrying quantum-source sends signals downwards towards a ground station. Generally, the downlinks exhibit less optical loss since the optical signals experience atmospheric turbulence only at the end of a transmission link. In comparison, optical signals in their uplink propagation experience more loss due to the occurrence of turbulence at the beginning of the path [36]. Therefore, the downlink is capable of generating more key bits than an uplink [36], but operating

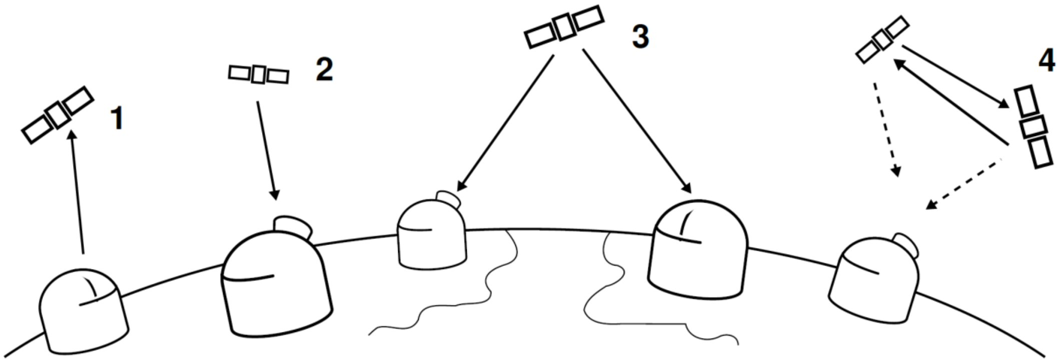


Figure 2.1: Possible configurations for satellite-based QKD. Reprinted from [72]

an in-orbit quantum source is complicated. Because of that, several groups are actively working with the uplink scheme [66, 73–75]. An uplink offers a few advantages over a downlink. For instance, the complex and energy-consuming photon sources stay on the ground that allows flexibility to choose quantum sources among various options, such as entangled photon source or weak coherent photon source. Also, satellite carries the relatively simple single-photon detectors as components of a receiver, whose requirements are comparatively relaxed. Usually, the receiver does not require a high-rate random number generator and high-capacity for data processing and storage since the photon reception rate is considerably low.

In scheme 3, a satellite carries an entangled photon pair source and establish two downlinks with two stations on the ground allowing entanglement-based QKD between the stations [31, 76]. This scenario demands the stations to have simultaneous line-of-sight with the satellite. Chinese satellite was able to distribute entangled-photons over 1200 km [31]. In the last configuration, scheme 4, the inter-satellite QKD [77, 78] can be a fundamental element for a long-distance quantum correlation test. A satellite carrying an entangled-photon source can perform as trusted relay nodes, which are a temporary solution to the quantum repeaters [79]. This scheme will potentially enable to distribute entanglement at much longer distances on the ground [80].

2.2.1 Trusted node QKD scheme

In the near future, the trusted node configuration (Fig. 2.2) is foreseen as the most practical form of satellite-based secret key generation. The satellites in schemes 1 and 2 in Fig. 2.2 function as a trusted node which is demonstrated by the Chinese Micius satellite [82]. In this scheme, an orbiting satellite first performs QKD operation with the ground station A

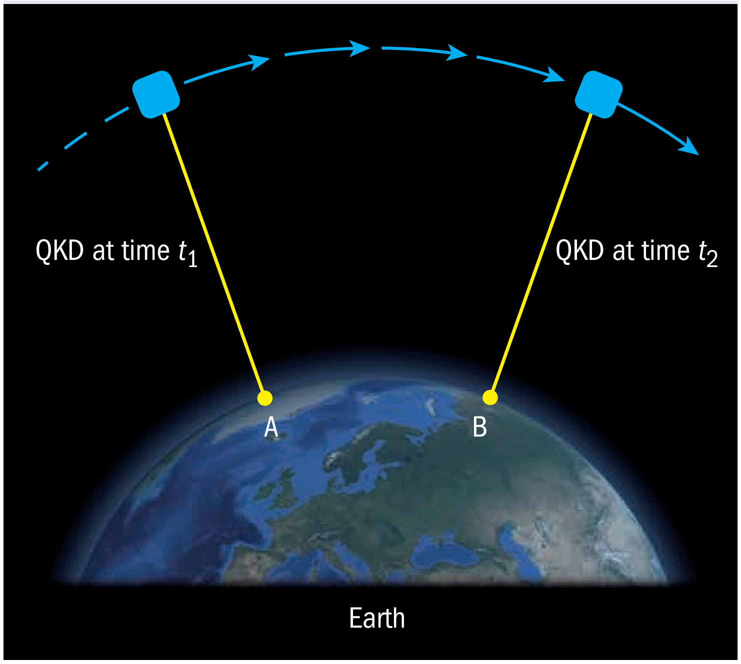


Figure 2.2: Illustartion of satellite-based trusted node configuration. Reprinted from [81]

by sending single photons either by an uplink or by a downlink and establishes a key K1. Then after traveling a distance when the satellite comes on site of the second station, B creates another key K2 by performing a second QKD operation. The satellite knows both keys while the stations only know their key. Then the satellite encrypts key K1 by K2 and sends over the classical channel to the station B. Afterward, B preforms $K2 \oplus (K1 \oplus K2) = K1$, (where $\oplus$ indicates the exclusive-or operation), to gain key K1. This operation facilitates both stations to share a common secret key K1, which the stations will use on the ground in classical channels for secure communication. In this scheme, the satellite must be trusted because it knows the key. If an adversary gets access to the satellite, the security of information will be compromised.

2.2.2 Untrusted node QKD scheme

A different approach, like scheme 3 in Fig. 2.2, where an in-orbit entangled-photon source distributes photon pairs to the ground stations, does not require to be trusted (Space-QUEST mission concept [76] and also implemented by Micius satellite [31]). Since each photon of an entangled pair is sent to the stations A and B separately, only A and B will know their measurement outcome. Both stations will perform Bell tests [83] to verify the quantum correlations of the photon pairs, and will form a common secret key. The Bell

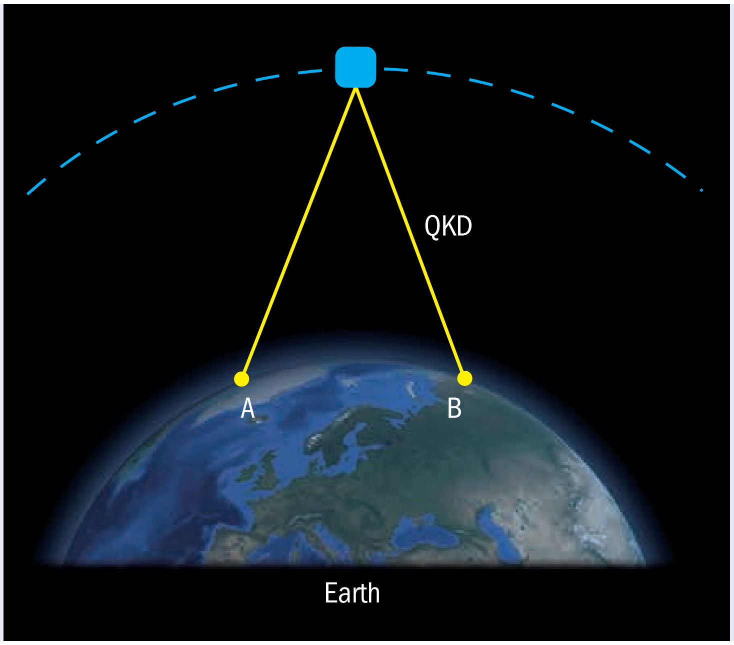


Figure 2.3: Illustartion of satellite-based untrusted node configuration. reprinted from [81]

test ensures that the information of the resultant measurement outcome is not leaked to any third party, including the satellite. Since the satellite has no knowledge of the key, the quantum source can be untrusted. However, in this approach, the two stations must be concurrently within the field-of-view of the satellite, and the probability of arrival of the photon pairs to their ground stations are very low as the pair travels a long high-loss path (∼60dB of loss). Hence, the key generation rate is very low, where the Micius mission was able to acquire only a little more than a single pair per second.

2.2.3 QKD satellite orbits

The features of communication links are highly dependent on the orbital altitude of a satellite [84]. The orbits are classified into three categories depending on their distance from the Earth surface: i) Low Earth Orbit (LEO) – 160 to 2000 km in altitude, ii) Medium Earth Orbit (MEO) – 2000 to <35786 km in altitude, and iii) Geostationary orbit (GEO) – exactly 35786 km of altitude for circular orbits. Although LEO and GEO orbits are most appropriate for satellite QKD applications, current missions are primarily targeting the LEO orbits because of their proximity to the earth. These orbits have a lower link loss (discussed in section 2.3) and also significantly low cost compared to the GEO satellites due to the smaller size of the LEO satellites. However, due to relatively high orbiting speed of the LEO satellites with respect to the earth (i.e., around 7.8 km at 800 km of altitude), it is difficult to maintain an accurate and stable link during signal transmission. On contrary, maintaining a link would be easier with the GEO satellites as they appear to be 'fixed' over an Earth location but at the cost of much higher losses [85]. Telescope optics are used as the transmitter and the receiver to establish the optical links and to transmit quantum signals between the satellite and ground stations.

The number and the time of flyovers, and the duration of being on line-of-sight of an LEO satellite with a ground station depends on orbital inclination and location of the ground station. For example, satellites in a sun-synchronous polar orbit, which are synchronous with the sun, pass over a specific location of the Earth at the same local time. A study showed that a circular sun-synchronous noon/midnight LEO orbit at an altitude of 600 km gives around 713 night time passes over a year at 90° of elevation [36]. The Micius satellite at 500 km sun-synchronous orbit crosses over the Xinglong ground station each night at around 12:50 am local time with total link duration of 5 minutes [32]. On the other hand, the International space station orbit would pass over an Earth location at 40° of inclination giving 150 usable night time passes over a year [71].

2.3 Challenges of quantum communication

Satellite-based quantum communications are extremely challenging in respect of payload (in this context, the quantum source or receiver) design within the limited available resources. The launching cost scales up with the spacecraft dimension, weight, and power [64]. In addition, the quantum payloads need to be robust enough to withstand the launching process and to survive in the space vacuum, radiation, microgravity, and thermal environment [86]. Therefore, before moving on building the infrastructure for the space-QKD, extensive theoretical and experimental feasibility studies have been performed [36, 64, 87–89]. The studies have been done on different aspects of quantum space communication, such as system automation [87], possibility of lightweight payload design, [64], and link loss analysis [36, 88–90]. This section briefly discusses the transmission challenges of quantum signals between the ground and satellite.

Quantum signals degrade as they propagate in the free-space. Several effects are responsible for this degradation, such as beam scattering, absorption, atmospheric turbulence, and pointing error. Of theses effects, scattering and absorption are caused by the molecules in atmosphere, like water, carbon dioxide, and ozone. Depending on the molecular type and concentration, the loss of signals vary through the atmosphere. The signal transmissions are also dependent on their wavelengths. J. P Bourgoin *et al.* performed a comprehensive simulation to find out the low absorption transmission wavelengths [36]. The study reported several low-loss transmission wavelengths– 665 to 685 nm, 775 to 785 nm, 1000 to 1070 nm and 1540 to 1680 nm are the most notable.

Another effect, the atmospheric turbulence leads to beam broadening and wandering, and scintillation [36]. This effect originates from the variation of refractive index due to temperature fluctuations that dominate in the lower 20 km of the atmosphere and depends on the elevation angle and direction of propagation. An uplink is more affected by the turbulence as it appears at the beginning of the signal propagation. However, turbulence does not affect the polarization of quantum signals [91]. A simulation of atmospheric turbulence has shown that location of a ground station plays an important role to have optimal link efficiency [90]. The link loss varies around 10 dB between a location at sea-level to an excellent location. Use of adaptive optics can increase the link efficiency up to 8 dB.

Beam diffraction also causes beam broadening [36]. Consequently, the total beam broadening is a contribution from both the diffraction and turbulence. Diffraction induced losses, which depends on signal wavelength, size of the transmitter telescope, and the link distance, dominates in the downlinks. Beam divergence due to diffraction can be reduced either by using telescopes having larger diameters or by using shorter signal wavelengths. Therefore, a trade-off is required between these two parameters to mitigate diffraction losses, as seen in equation 2.1.

$$sin(\theta) \approx \frac{\lambda}{D_T} \tag{2.1}$$

here, θ is the Beam divergence, D_T is the transmitter aperture size or diameter, and λ is photon wavelength. However, for ground-based transmitters, having telescope diameter larger than a few tens of centimetres has less effect in reducing the overall loss due to the atmospheric turbulence.

In addition, misalignment due to the telescope jitter and error in the tracking system also contributes to the link loss. In-orbit jitter control of the telescopes is challenging, which affects more to the downlinks. Pointing accuracy is an important factor in minimizing the total link loss. The simulation performed by J. P. Bourgoin *et al.* demonstrated that 2 μrad or less error in the pointing would not contribute more than 1–4 dB in the total loss [36].

Overall summary is optimization of the diameter of the transmitter and the receiver telescopes, photon's wavelengths, and the pointing system can minimize total link loss.

2.4 Ground Based Free-space QKD

Since the first complete protocol for quantum cryptography in 1984, the first free-space QKD protocol was demonstrated in lab using photon polarization in 1991 [58], although the link length in the air was only 32 cm. The distance was extended to 205 m in another laboratory demonstration by a research group at Los Alamos National Laboratory (LANL) [26]. In 1996, researchers at the Johns Hopkins University were first able to transmit qubits over a 75 m link under bright daylight condition [92]. This distance was subsequently extended to 950 m over an outdoor free-space link during nighttime in 1998 by the LANL researchers using B92 protocol [25]. With their consistent effort in the outdoor, they successfully demonstrated 500 m point-to-point link at daytime in 1999 [93] and in 2000 they could further extend the link length first ever into kilometer range – 1.6 km using a better QKD system [94]. They also showed the feasibility of achieving secret bit rates of 3 kHz that is protected against the simple beam splitting attack and intercept-resend attack. They further demonstrated the BB84 protocol in free-space over 10 km during daylight condition with the secret key rate of 264 Hz in 2002 [95]. Later in the same year, researchers at the Ludwig-Maximilian University were able to exchange secure keys between two mountains over 23.4 kilometers free-space link [96]. Their raw key rate was 1.5 - 2 kbit/s with a bit error rate of less than 5%. They also exchanged keys up to 27 dB of transmission in the poorer visibility . Most of these successful outdoor tests [25, 92–96] envisioned ground to satellite quantum links as a possible means for future long-distance quantum cryptography.

In the continuous efforts made for extending the range of free-space links, a European research group in 2006 performed QKD over 144 km between two Canary Islands– La Palma and Tenerife. They used both weak coherent laser pulses [62] and entangled photons [56], and this was the first demonstration of entangled-photon distribution across such a long distance. The atmospheric loss within such range is comparable with that between a low-Earth orbit and a ground station, which confirmed the possibility of a quantum satellite. In their BB84 QKD demonstration, the distributed secure key rate was 12.8 bps with a 6.48% quantum bit error rate (QBER) and about 35 dB of transmission loss. Their polarization-entangled photon distribution achieved the violation of Bell inequality by 13 standard deviations, confirming the entanglement. The produced secret key rate was 2.37 bps with 4.8% of QBER. They also performed quantum teleportation between the islands to demonstrate the feasibility of the ground-to-satellite quantum teleportation. [97].

In 2012, a Chinese research group developed an advanced acquiring, pointing, and tracking (APT) system to follow an arbitrary object with high-frequency and high-accuracy.

They demonstrated quantum teleportation and quantum entanglement distribution over a 97 km link across a lake [98]. They were able to send polarization-entangled photon-pairs over the link with 35 to 53 dB of channel loss depending on the weather conditions, and achieved 80.4% of average fidelity for the quantum states. They also performed entanglement distribution over a two-link quantum channel to the receivers separated by 101.8 km with 66 to 85 dB of total channel loss. Their result showed the feasibility of a high-loss uplink or two-downlink channel, quantum teleportation, and entanglement distribution.

On the other hand, a research group at the University of Waterloo (UW) in Canada led by Dr. T. Jennewein is actively developing an uplink scheme for the quantum satellite [54, 66, 99]. Since an uplink experiences very high transmission losses, around 40—60 dB, the scheme requires innovative photon source and advanced timing analysis. The group implemented a 76 MHz photon source at 532 nm wavelength [100], and used that source and commercially available silicon single-photon detectors to analyze satellite uplink losses for a decoy-state QKD protocol [66]. They demonstrated the viability of a satellite uplink up to 57 dB of channel losses in the infinite key limit with a secure key rate of 2 bps. They also implemented a complete post-processing procedure–error correction, privacy amplification on the shifted key– for key extraction at various channel losses up to 56.5 dB [54]. Their achieved secret key rate was 0.5 bps at a total loss of 56.5 dB, showing the feasibility of the uplink scheme. This UW group designed a less complex quantum receiver to achieve a robust system. Their receiver uses a passive polarization analyzer instead of an active analyzer because active components require time synchronization that increases the probability of failure in orbit.

Dr. Jennewein's team later verified the feasibility of QKD between a ground station and a moving object. They performed QKD between a stationary transmitter and a moving receiver carried by a truck [99]. The receiver had an angular speed of 0.75°/s equivalent to the speed of a 600 km low-Earth orbit satellite, and the secret key rate was 40 bps.

2.5 Airborne and Ground-to-satellite QKD Experiments

QKD demonstrations using airborne platforms were the crucial steps for verifications of the readiness of quantum technologies and their compatibility with the classical technologies. A German research team first ever performed a proof-of-principle experiment for quantum key distribution from a moving aircraft to an optical ground station [101]. The aircraft carried a transmitter along with an advanced pointing and tracking system to ensure the steady transmission of single-photons. It traveled on a circular path of radius 20 km around the ground station at a speed of 290 km/h equivalent to 4 mrad/s of angular velocity. On the other hand, the ground station was equipped with a 40 cm Cassegrain telescope together with the receiver system. The very first step of communication is to establish a quantum link between the transmitter and the receiver. To do that, when the aircraft enters the arc path, the transmitter and the receiver adjust their telescopes by knowing their position via a global positioning system. Then the telescopes start tracking each other via a fine pointing assembly which constantly follows the beacon laser illuminated between the transmitter and the receiver. During the experiment, the pointing error of QKD beam was narrowed down to $\approx$ 180 μrad. BB84 polarized photons were used for key generation and a one-way classical channel was used for post-processing. The resultant total link loss was 38 dB, and the average shifted key rate was 145 bps with a 4.8% of QBER. An accurate compensation system was used to deal with the rotation of photon bases to reduce QBER. Although the technology required more up-gradation for full QKD demonstration, the experiment was successful in proving at least the feasibility of QKD between a ground station and a flying object.

Later, Dr. Jennewein's team at UW performed a full QKD in an airborne uplink configuration in 2016 [102]. They equipped the airplane with a path-to-space prototype of QKD receiver. A 400 MHz QKD source and a transmitter telescope were located on the ground station. The plane travelled at 198–259 km/h which emulates the angular velocity of 600 km LEO satellite with respect to the ground station. The aircraft followed two types of paths: circular path at a constant radius around the ground station and straight-line paths. In the straight-line paths, aircraft's motion is closer to the apparent motion of the satellite over a ground station that gives a better test of the pointing system. The test was performed at an altitude of $\approx$ 1.6 km above sea level consisting of 14 passes at the distances of 3 km, 5 km, 7 km, and 10 km, both circular and straight paths. Establishing a quantum link was successful for seven out of the 14 passes where 10 km arc and 7 km straight paths allowed a key exchange for a longer duration. The 10 km arc path gave 70947 secret bit at QBER of 3.39% with mean total loss of 42.6 dB whereas the 7 km straight path exchanged 9566 secret bits at QBER of 3.58% with a mean link loss of 51.1 dB. This successful demonstration proved the technological readiness of an uplink quantum satellite.

A research group in China analyzed several critical issues related to the quantum communication via satellite: i) The rapid angular motion with a ground station, ii) The random motion of a satellite, and iii) atmospheric turbulence at high-loss conditions [103]. Transmitter on a turntable is used to simulate the angular velocity and acceleration for a satellite allowing a key rate of 48 bps with a QBER of $\sim$4% at a total loss of $\sim$40 dB over a distance of 96 km. A different platform, a hot-air balloon at a distance of 20 km, was used to mimic the random motion of a satellite to verify the pointing, acquisition and tracking system's ability to maintain a link under adverse weather conditions. They demonstrated the technologies to address the critical issues of a quantum communication satellite.

Besides the above experiments, the feasibility test for satellite-quantum communication has been performed with in-orbit corner-cube retroreflectors (CCRs) by the research groups in Italy [104] and china [105]. The CCRs was placed on an orbiting satellite at 400 km of altitude as a transmitter while the receiver located on the ground. The photon states were streamed upwards from the ground and were reflected back by the in-orbit CCRs. This experiment, performed by Yin *et al.*, [105] verified the single-photon transmission over a downlink with a total link loss of ≈41 dB. On the other hand, Vallone *et al.* [104] used polarization preserving coatings on the CCRs to verify the preservation of polarization quantum states over a downlink.

2.6 Quantum Communication Space Missions

Several nations are working towards building a quantum satellite. China has made a huge progress by launching their first quantum communication satellite at an altitude of ~ 500 km in August 2016. Jian-Wei Pan's group at the University of Science and Technology of China (USTC) developed the quantum satellite 'Micius'. The mission achieved three basic milestones for a global quantum network: decoy state QKD over ∼1200 km [32], Entanglement distribution to two ground stations separated by ∼1200 km and Bell test [31], and quantum teleportation [33]. Moving towards the long-standing goal of building fully operational constellation of satellites, China has definitely led the start. Now other countries are also rapidly catching up with the quantum communication space technologies. A summary of satellite QKD initiatives is presented in Fig. 2.4.

The research group of Dr. Anton Zeilinger at the University of Vienna in Austria collaborated with USTC team to implement the quantum communication protocols between the LEO satellite and ground station. The group performed an intercontinental secure key exchange between the optical ground stations in Graz (Austria), and in Xinglong and Nanshan(China) using the decoy state protocol where "Micius" acted as a trusted node [82]. Also, the key was used for a first ever quantum cryptographically secured video call between two continents, Vienna and Beijing showing that quantum internet is not a dream any more [106]. The Vienna group also planned and designed the Space QUEST (Space—Quantum Entanglement Space Test) mission with the European Space Agency

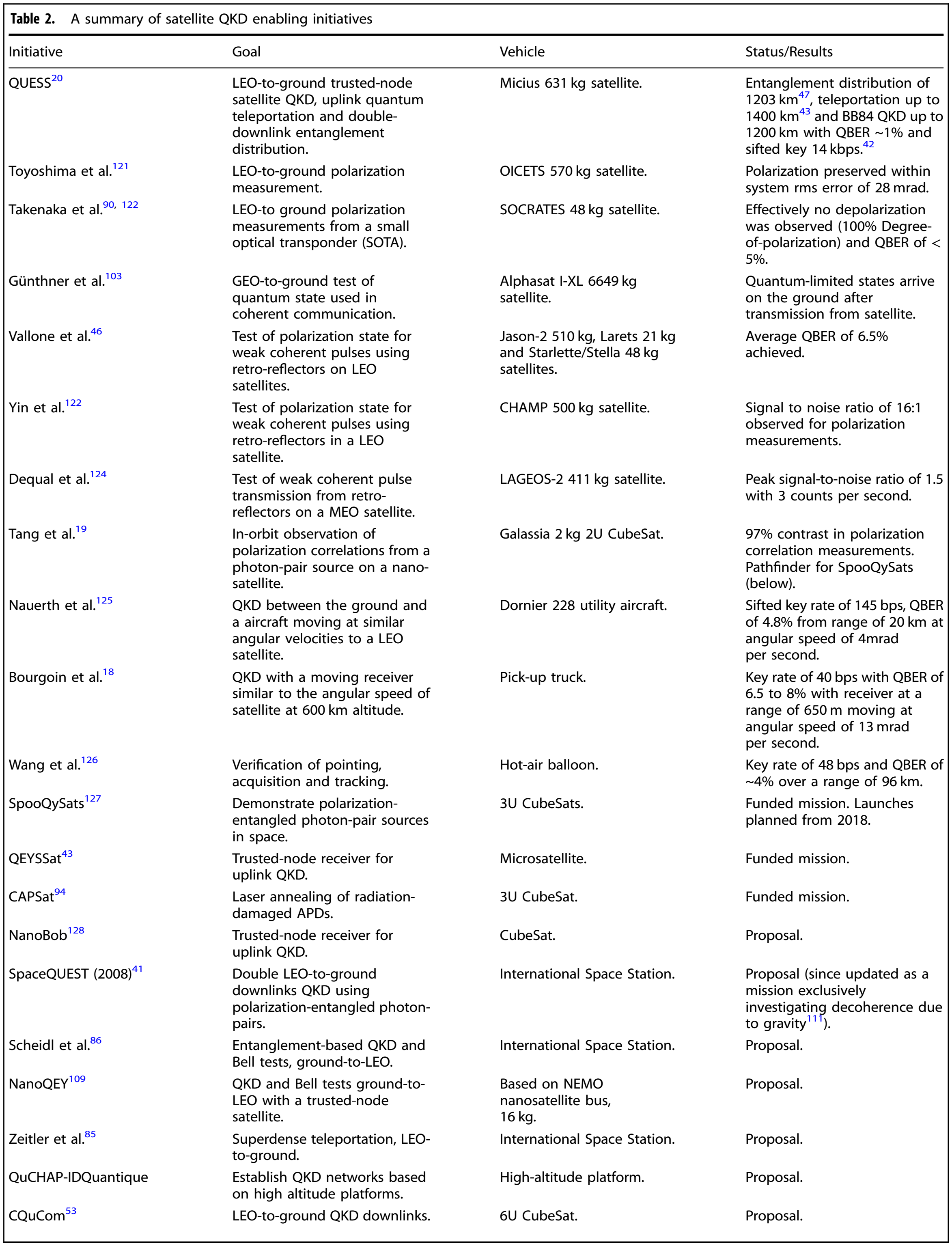


Table 2. A summary of satellite QKD enabling initiatives

Initiative	Goal	Vehicle	Status/Results
QUESS[20]	LEO-to-ground trusted-node satellite QKD, uplink quantum teleportation and double-downlink entanglement distribution.	Micius 631 kg satellite.	Entanglement distribution of 1203 km[47], teleportation up to 1400 km[43] and BB84 QKD up to 1200 km with QBER ~1% and sifted key 14 kbps.[42]
Toyoshima et al.[121]	LEO-to-ground polarization measurement.	OICETS 570 kg satellite.	Polarization preserved within system rms error of 28 mrad.
Takenaka et al.[90, 122]	LEO-to ground polarization measurements from a small optical transponder (SOTA).	SOCRATES 48 kg satellite.	Effectively no depolarization was observed (100% Degree-of-polarization) and QBER of < 5%.
Günthner et al.[103]	GEO-to-ground test of quantum state used in coherent communication.	Alphasat I-XL 6649 kg satellite.	Quantum-limited states arrive on the ground after transmission from satellite.
Vallone et al.[46]	Test of polarization state for weak coherent pulses using retro-reflectors on LEO satellites.	Jason-2 510 kg, Larets 21 kg and Starlette/Stella 48 kg satellites.	Average QBER of 6.5% achieved.
Yin et al.[122]	Test of polarization state for weak coherent pulses using retro-reflectors in a LEO satellite.	CHAMP 500 kg satellite.	Signal to noise ratio of 16:1 observed for polarization measurements.
Dequal et al.[124]	Test of weak coherent pulse transmission from retro-reflectors on a MEO satellite.	LAGEOS-2 411 kg satellite.	Peak signal-to-noise ratio of 1.5 with 3 counts per second.
Tang et al.[19]	In-orbit observation of polarization correlations from a photon-pair source on a nano-satellite.	Galassia 2 kg 2U CubeSat.	97% contrast in polarization correlation measurements. Pathfinder for SpooQySats (below).
Nauerth et al.[125]	QKD between the ground and a aircraft moving at similar angular velocities to a LEO satellite.	Dornier 228 utility aircraft.	Sifted key rate of 145 bps, QBER of 4.8% from range of 20 km at angular speed of 4mrad per second.
Bourgoin et al.[18]	QKD with a moving receiver similar to the angular speed of satellite at 600 km altitude.	Pick-up truck.	Key rate of 40 bps with QBER of 6.5 to 8% with receiver at a range of 650 m moving at angular speed of 13 mrad per second.
Wang et al.[126]	Verification of pointing, acquisition and tracking.	Hot-air balloon.	Key rate of 48 bps and QBER of ~4% over a range of 96 km.
SpooQySats[127]	Demonstrate polarization-entangled photon-pair sources in space.	3U CubeSats.	Funded mission. Launches planned from 2018.
QEYSSat[43]	Trusted-node receiver for uplink QKD.	Microsatellite.	Funded mission.
CAPSat[94]	Laser annealing of radiation-damaged APDs.	3U CubeSat.	Funded mission.
NanoBob[128]	Trusted-node receiver for uplink QKD.	CubeSat.	Proposal.
SpaceQUEST (2008)[41]	Double LEO-to-ground downlinks QKD using polarization-entangled photon-pairs.	International Space Station.	Proposal (since updated as a mission exclusively investigating decoherence due to gravity[111]).
Scheidl et al.[86]	Entanglement-based QKD and Bell tests, ground-to-LEO.	International Space Station.	Proposal.
NanoQEY[109]	QKD and Bell tests ground-to-LEO with a trusted-node satellite.	Based on NEMO nanosatellite bus, 16 kg.	Proposal.
Zeitler et al.[85]	Superdense teleportation, LEO-to-ground.	International Space Station.	Proposal.
QuCHAP-IDQuantique	Establish QKD networks based on high altitude platforms.	High-altitude platform.	Proposal.
CQuCom[53]	LEO-to-ground QKD downlinks.	6U CubeSat.	Proposal.

Figure 2.4: An overview of ongoing and planned satellite QKD missions. Reprinted from [85]

(ESA) to transmit entangled quantum states from the International Space Station [107]. Very recently, ESA made an agreement with the European commission to build a pan-European quantum communication infrastructure [108].

A team at the National Institute of Information and Communication Technology (NICT) in Japan is researching on optical satellite communications for many years [109–111]. Recently, an NICT team led by Dr. Masahide Sasaki and Dr. Morio Toyoshima performed a quantum communication experiment between a SOCRATES (Space Optical Communications Research Advanced Technology Satellite) microsatellite in LEO and a ground station [34]. Through the demonstration, the NICT team validated their QKD technology for a complete satellite-to-ground QKD.

Prof. Gerd Leuchs's team at the Max Planck Institute for the Science of Light in Erlangen, Germany, demonstrated detection of coherent quantum states from a geosynchronous satellite to a ground station [112]. At Los Alamos National Laboratory in the US, Richard Hughes' team has been working on space-QKD for many years [26, 87, 93, 95].

Prof. Alexander Ling's research team at the National University of Singapore (NUS) is developing SpooQySats [70] to demonstrate QKD using CubeSat platform. They are building a technology for a robust, space qualified entanglement-source and aiming to test the space worthiness of the source using CubeSat Platform [71, 113–117]. The team is targeting an entanglement distribution via CQuCoM mission in 2020 [71] and an inter-satellite entanglement distribution using CubeSats [118].

At the Institute for quantum computing (IQC), Thomas Jennewein's group is working closely with the Canadian Space Agency to carry out the QEYSSat (Canadian Quantum Encryption and Science Satellite) mission. They have been working for years in the 'uplink' configuration to send the quantum receiver on satellite. The team is gradually building and shaping the required technologies for the uplink by a thorough performance analysis [36, 66, 90], and outdoor experiments [99, 102].

In short, a number of nations are accelerating their space technologies to demonstrate the on-orbit QKD. The world can envision the desired global scale quantum-secured communications in the 2020s [119].

Chapter 3

CubeSat and its space environment

3.1 Introduction

Quantum experiments in the space environment on traditional spacecraft is technically challenging due to their long development process, and the high costs of launch, operation, and maintenance. These satellites have mass around 1000 Kg or more and are suitable for long-term applications. Therefore quantum communication experiments are taking advantage of the cost-effective satellites, such as CubeSats (cube satellites), to evolve the quantum technologies. CubeSats, which are usually launched to low-Earth orbits (LEO), are nanosatellite standard spacecraft. Their mass is around 1 Kg to 10 kg and can be built using commercial-off-the-shelf (COTS) components [120, 121], which reduces their developing cost and time. Previous chapter (section 2.6) mentioned several upcoming quantum communication missions in the CubeSat platform, for example SpooQySats [70], CubeSat Quantum Communications Mission (CQuCoM) [71], NanoBob [69], and the Cooling, Pointing and Annealing Satellite (CAPSat) [48]. This chapter introduces CubeSats and briefly explains the orbital environment that the CubeSats will experience in the LEO.

3.2 CubeSats

A CubeSat is a cube-shaped miniature satellite having a standard dimensions of 10 cm × 10 cm × 10 cm for a one unit (1U), as illustrated in Fig 3.1. A unit spacecraft has a mass approximately 1.3 kg and limited power capacity (usually less than 1.5 W) [123]. CubeSats can be just one unit or a group of units maximum of 24 depending on the needs of a particular mission [122]. They were originally developed by professor Jordi

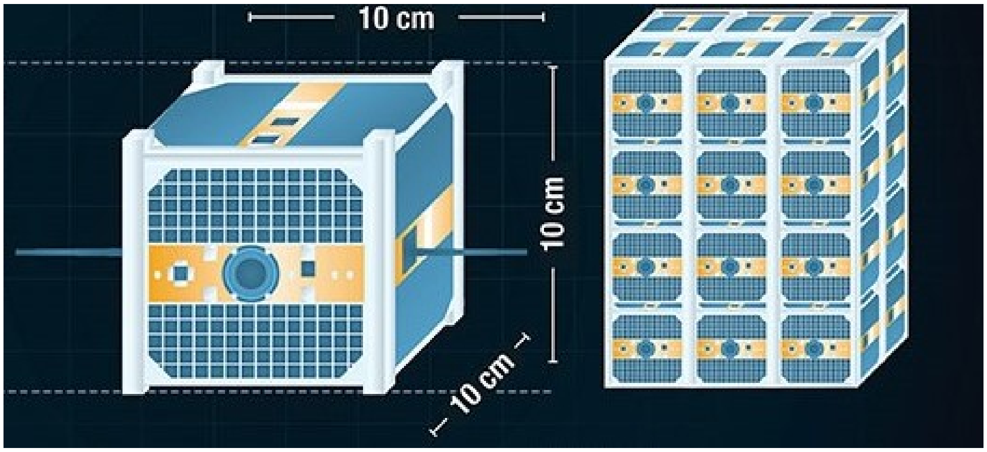


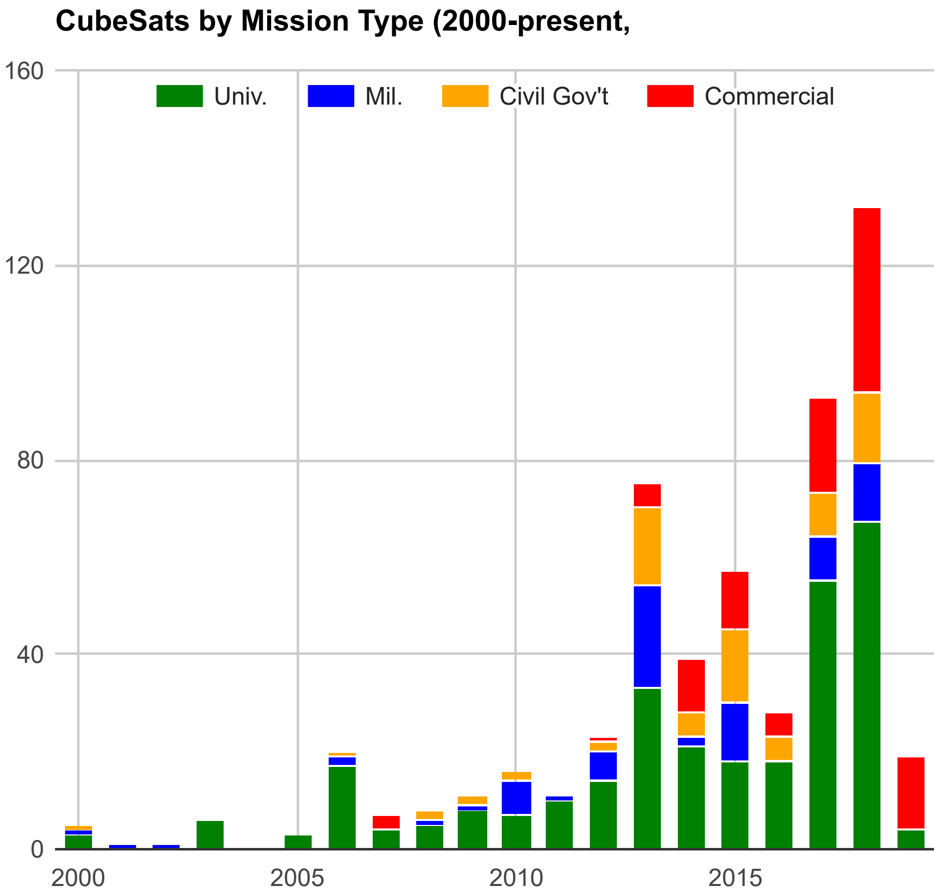
Figure 3.1: CubeSat dimension. Depending on the mission, CubeSats can be just one unit or a stack of multiple units. Picture is taken from [122]

Puig-Suari from California Polytechnic State University and professor Bob Twiggs from Stanford University in 1999 to facilitate inexpensive access to space [124]. Now, these small satellites are very popular amongst academia [125], hobbyist [126], and commercial services [127].

CubeSats are launched as an auxiliary payload carried by the launching vehicles (or rocket) having extra capacity or from the International Space Station. Usually, CubeSats are packed in a dispenser which is a interface between the spacecraft and the launching vehicle (LV). The dispenser provides protection against launching vibration and dispenses the CubeSats into space. At an appropriate time, the LV sends an electrical signal to open the door of the dispenser and deploys the CubeSats into the expected orbits. While launched, they operate autonomously in the orbit.

CubeSats have several common basic elements or subsystems. These are the CubeSat frame structure, solar panels, antenna, communication system (COMM), on-board computer (OBC), attitude determination and control systems (ADCS), electrical power system (EPS), and the mission-specific payload. Due to the standardized dimensions and aspects, many companies are capable of massively producing most of the basic subsystems and offering off-the-shelf components (COTS). Thus it is possible to build a CubeSat by developing the payload only substantially reducing the development time. For the past six years, the number of CubeSat launches has increased significantly for university and commercial applications, as seen in Fig. 3.2.

The major challenges of the CubeSats are their limited budget for power, space, and shielding. Moreover, the COTS components used for the CubeSat development have less radiation tolerance that limits the satellite lifetime to less than one year [42].



[Chart created on Mon May 27 2019 using data from M. Swartwout]

Figure 3.2: The number of CubeSat launches per year.

3.3 Space environment in Low-Earth-Orbit

CubeSats in the LEO orbits, ranging from 200 to 1600 km of altitude, are exposed to extreme space environments that can degrade the spacecraft electronics and materials. These environment includes extreme heat and cold cycle, micrometeoroids, orbital debris, ultra-high vacuum, atomic oxygen, solar ultraviolet radiation, and high-energy charged particle radiation. Consequently, while building payloads for the CubeSats, it is important to choose the components and materials considering the orbital environment and mission lifetime. This section gives a brief explanation of several harsh environmental effects of the LEO orbits.

3.3.1 Thermal stress in LEO

As the spacecraft systems periodically come in and out of sunlight while orbiting around the Earth, they face extreme thermal fluctuations. These periodic thermal variations can oscillate between -150°C and +150°C while orbiting [128]. The degradation of materials due to the thermal extremes caused by several factors, such as thermal properties of materials, areas exposed to sun, duration in shadow and in sunlight, thermal mass, and heat-producing components [129]. To minimize thermal effects on the spacecraft hardware, an active thermal system consisting of a heater or cooler can be used. However, active systems are not practical for CubeSats because of their limited power budget. In this situation, a thin polymeric coating (also called conformal coating) can be used to protect the underlying components. It is also important to select materials and components having higher thermal tolerance for CubeSat payloads to prevent damages.

3.3.2 Vacuum pressure in LEO

LEO orbits experiences ultra-high vacuum with pressure around 5×10^{-10} torr [130]. At the ultra-low pressure at around 10^{-6} to 10^{-9} torr , some materials starts outgassing [131] which is a discharge of gas that was trapped or dissolved into the material. The gas then deposits on nearby surfaces which can affect or degrade the performance of spacecraft, more specifically sensitive optics of the satellites. It is thus crucial to choose materials or components with low outgas properties while preparing the payloads for high-vacuum environment. If the materials chosen have outgas probability, they should be thermal oven backed for about one day at 100°C or more than the expected in-orbit temperature [131].

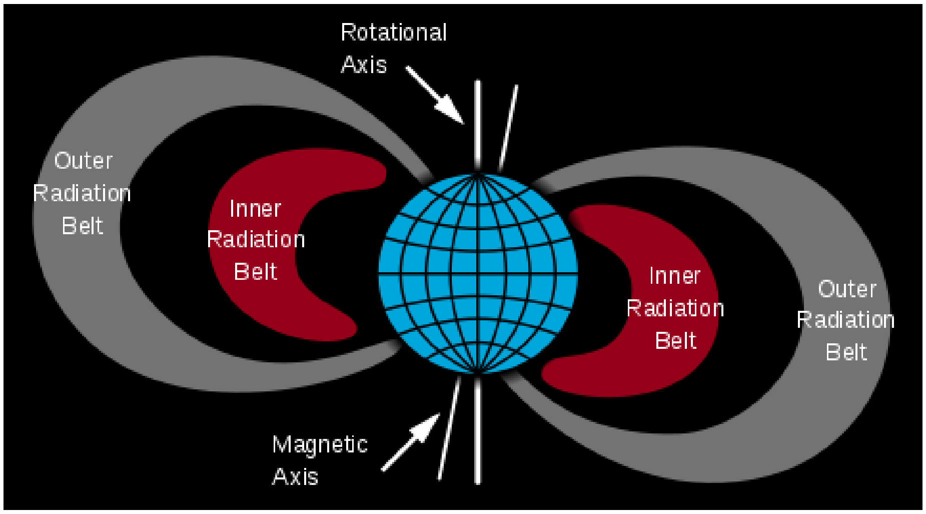


Figure 3.3: Earth's radiation belts. Reprinted from [135]

3.3.3 Space radiation in LEO

Space radiation contains several high energy particles, such as protons, heavy ions, and electrons, which originates from galactic cosmic rays or solar flares, and it cause a huge deterioration to the spacecraft electronics [132]. In the case of LEO, a major source of the radiation particles is the trapped ions from the two donut-shaped radiation belts [41], as illustrated in Fig. 3.3. The belts are also known as Van Allen radiation belts, which trap and store charged particles. Due to the slight difference in the Earth's rotational axis and the magnetic pole, one side of the inner radiation belt is dragged towards Earth's surface to an altitude of 200 − 800 km which is known as South Atlantic Anomaly [133]. Any spacecraft passing through this radiation belt will strongly interact with protons having energies above 10×10^6 eV moving at a density of 3000 $\text{cm}^{-2}\text{s}^{-1}$ [134]. Fig. 3.4 illustrates the radiation flux distribution at an altitude of 800 km, which shows higher radiation occurs at the southern part of Earth. It is important to equip the satellites with proper measures to protect the systems and electronics against radiation.

The radiation severely affects mainly the spacecraft electronics. Usually, two types of damages happen due to the radiation: total ionizing dose (TID) and displacement damage (DD) [136]. In the case of TID, when highly energetic protons and electrons travel through a device substrate, transfer the energy to the atoms of the semiconductor substrate that generates new electron-hole pairs. The excess charges either recombine or are moved away by an electric field leaving behind the holes. This causes a charge accumulation creating permanent damage to the devices. On the other hand, relatively low-energy non-ionizing radiation causes displacement damage. The non-ionizing particles cannot create

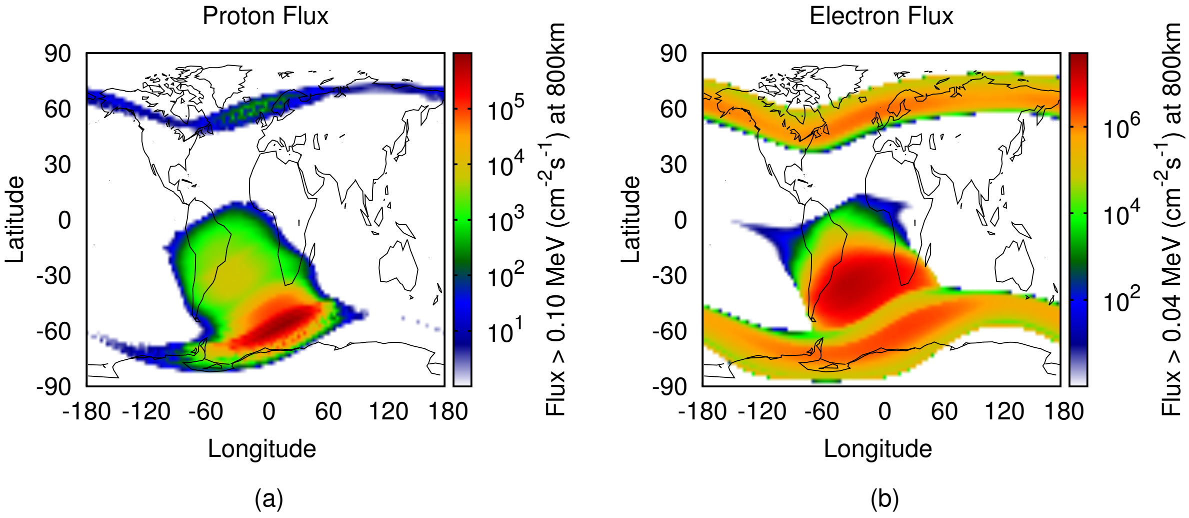


Figure 3.4: Proton and electron radiation flux at 800 km altitude. Southern hemisphere has increased radiation due to the South Atlantic Anomaly. Reprinted from [135]

new carriers, instead dislocates atoms from lattice forming structural damage [132]. DD may change the device's working principle or destroy completely [137].

The satellites in LEO are partially protected against radiation by the Earth's magnetic field despite the South Atlantic Anomaly. However, spacecraft still will be exposed to a radiation dose of about 100 rad/year [139]. To achieve further protection, we can use additional aluminium shielding [138]. Fig. 3.5 demonstrates the protection against radiation doses with respect to the thickness of aluminium shielding. Around 5 mm (197 mils[1]) of aluminium is sufficient for shielding most of the high-energy electrons, while proton radiation still dominates. Although the amount of aluminium thickness depends on the spacecraft mass budget, particularly for CubeSats, the amount is highly limited.

The protection measures thus far explained are considered in the design and development of the detector module for the CAPSat [48] annealing payload. Further details are discussed in Chapter 5.

[1] mil is one thousandth of an inch and 1 mil = 0.0254 mm.

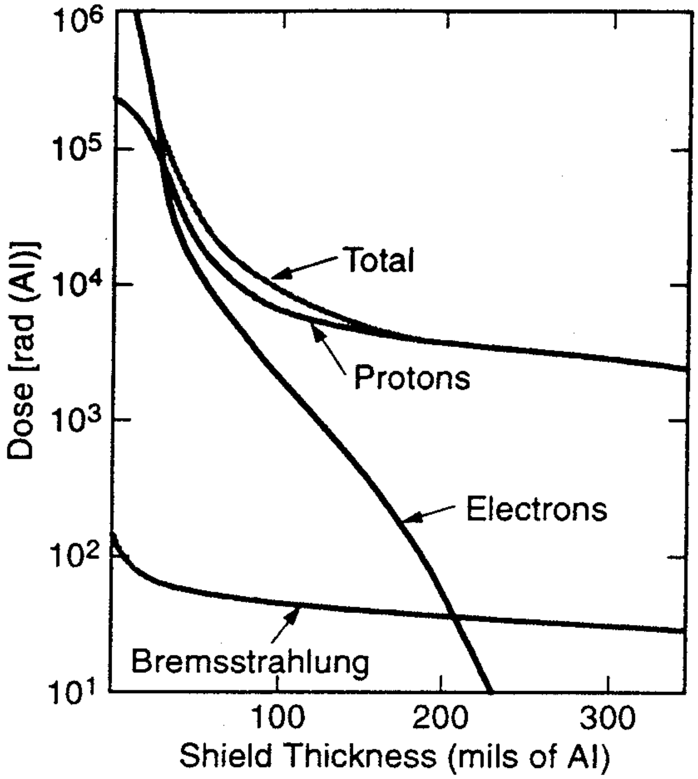


Figure 3.5: Effect of aluminium shielding for protection against radiation doses. Reprinted from [138]. Total dose for a 5-year mission at 705 km polar orbit. Note: 5 mm corresponds to about 197 mils.

Chapter 4

Single-photon detectors for quantum communications

4.1 Introduction

Single-photon detectors (SPDs) have a large internal gain so they can respond to a single photon. SPDs have diverse applications, for example in quantum cryptography [12, 63], basic quantum mechanics [140, 141], quantum computing [142], biomedical imaging [143], eye-safe laser ranging [144], fluorescent decays and luminescence [145, 146], and astronomy [147]. Of these applications, the field of optical quantum communications is rapidly expanding and playing a major role in the advancement of SPDs since the detectors are essential elements for quantum communications (QC). Moreover, SPDs are required to operate within the harsh space environment in the satellite QC implementations. This chapter explains the effects of their exposure to the harsh radiation conditions of space. In addition, the important parameters of SPDs, suitable detectors for the QC applications, SPD readout circuits, and their operation principles are also discussed.

4.2 SPD Characteristic parameters

Various types of SPDs have been used in quantum communication, for instance, photomultiplier tubes (PMTs), single-photon avalanche diodes (SPADs), and superconducting nanowire single-photon detectors (SNSPDs). Selection of SPDs for their applications relies upon several parameters, including their wavelength of operation, quantum efficiency, dark

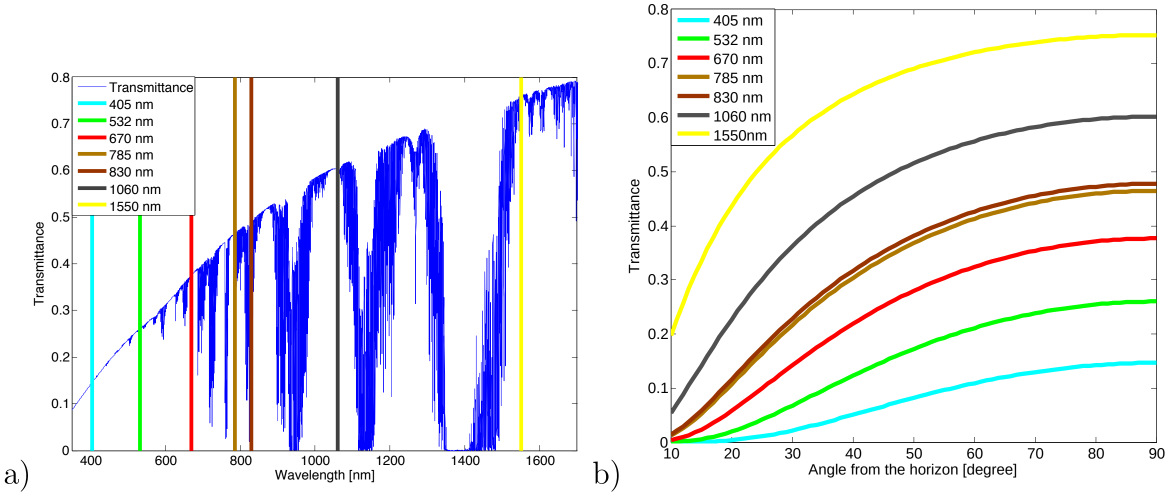


Figure 4.1: Simulation result of optical propagation (a) at zenith and (b) at different elevation angles . Vertical lines corresponds to the wavelengths of commercially available laser sources. Several high-transmittance windows are evident where higher wavelengths tends to have higher transmission. Reprinted from [36]

count rate, maximum count rate, timing jitter, afterpulsing probability, and device active area. This section discusses the details of several parameters.

Wavelength

SPD responds to a single-photon only for a specific range of wavelengths defined by the device materials. For example, silicon single-photon avalanche diodes (Si-SPADs) are sensitive to wavelengths between 400-1000 nm, while InGaAs/InP SPADs are responsive to wavelengths between 950 nm to 1650 nm [61]. Usually, their selection depends on the medium of optical propagation and its transmission windows. For instance, applications that use optical fiber as the propagation medium must adhere to the low loss transmission windows of 1260–1625 nm [148]. On the other hand, the low-loss transmission windows in free-space vary due to the losses induced by atmospheric turbulence, scattering, diffraction, and absorption by the atmospheric molecules. J. P. Bourgoin *et. al.* [36] performed a detailed simulation to find the transmittance of an optical link over a wide range of wavelengths and at various elevation angles. Figure 4.1 presents the simulation results showing possible low-loss transmission windows in free-space. For quantum communications, the possible windows are at 665–685 nm, 775–785 nm, 1000–1070 nm, and 1540–1680 nm. Commercial laser diodes are available at all these wavelengths.

Dark count rate

Dark counts are false counts that occur in the absence of photons, which are considered as noise. The source of these counts can be either the detectors' material, their structure, bias voltages, or the SPDs' sensitivity to outside noise. For instance, dark counts in SPADs arise primarily from the thermal excitation, tunneling effect, and trapped electrons [149]. However, low-temperature operation reduces thermally excited noise, and a lower bias can decrease the tunneling effect. In quantum communication, it is important to choose SPDs with low noise since it affects the overall signal to noise ratio. To date, SNSPDs are reported with the lowest noise, less than 1 cps [150]. Although, low-noise Si [151, 152] and InGaAs [153] detectors are also available.

Detection efficiency

Detection efficiency is the measure of the overall probability of registering a count on the absorption of a single photon by SPD. Generally, SNSPDs have the highest efficiencies; 70–80% at 250–370 nm [154], >90% at 1550 nm [150]. At visible wavelengths, Si-SPADs have been reported with 80% detection efficiency [155]. InGaAs SPADs have maximum efficiency of 25% at 1500 nm [153]. Generally, higher detection efficiency is desirable in most applications, specially in QKD, because better detection efficiency increases the secret bit rate.

Timing jitter

Timing jitter is the fluctuation in the time difference between the photon absorption by a detector and the output electric pulse. The jitter of a photon counting system includes the contribution of the detector itself, and it's quenching circuit. The inherent timing jitter of the device depends on the bias voltages. A Larger bias ensures a quick build-up of an avalanche that reduces the jitter. SNSPDs report the lowest jitter of 14.80 ps full width half maximum (FWHM) [156] while it can vary within 35–400 ps FWHM for SPADs and PMTs [157].

Afterpulsing probability

Afterpulses [158, 159] are also non-photon events like dark counts that contribute to the overall noise. The source of afterpulses are the trapped carriers in energy states in the bandgap. When these carriers are released, they trigger avalanche current. Sometimes, one such avalanche event generates several secondary avalanches. The lifetime of the trapped ions can be a few tens or hundreds of microseconds [160], while their number scales up with the avalanche duration. Afterpulsing probability (P_{AP}) is generally high in SPADs. Although higher temperatures and good quality crystal can reduce the afterpulsing effect [161], it is still a challenging issue for the germanium or InGaAs/InP SPADs. The P_{AP} can be suppressed either by running them in gated mode or by imposing a long dead time after each avalanche in free-running detectors. For example, InGaAs/InP SPADs experience 2.2% P_{AP} for 20 µs of dead time in the free-running mode [162] and 6.5% of P_{AP} at 500 MHz sine-wave gating [163]. In contrast, Si-SPADs suffer comparatively less P_{AP} at around 1% [152].

Maximum count rate

The maximum count rate of an SPD defines how many counts per second the device can register. Generally, an SPD needs a recovery time after an avalanche, within which the detector is not ready for any single-photon detection. The recovery time depends on the types of detectors and their material. For instance, SNSPDs have higher counting rates that range over gigahertz [164, 165]. In contrast, semiconductor detectors suffer relatively long recovery time which is in the range of microseconds for Si-SPADs that limits their maximum count rate to the megahertz range [155, 157, 166]. In InGaAs/InP detectors, the maximum count rate is limited by their gating frequency [161] (upto the gigahertz range [167]) or by the additional dead time [168, 169] that are applied to suppress the afterpulsing.

However, before selecting detectors for a particular application, it is important to understand the above-mentioned detector parameters and their relations. For example, detectors' dark count rate contributes to the QBER in QKD applications as the ratio of dark count (D) to the sifted key rate[1]. Therefore, smaller D is expected, which can be further reduced by gating the detectors for a short period. But, the minimum gating interval is limited by the detectors' timing jitter. Along with that, the jitter of detectors (in most cases detector jitter dominates over source jitter) also limits the maximum clock rate of a photon detection experiment. Hadfield formulated a dimensionless figure of merit to define

[1] the detected quantum states that have the matching bases between the transmitter and the receiver.

detectors performance in the best way [157]. It is given by

$$H = \frac{\eta}{D\Delta t_j} \tag{4.1}$$

here, η is the detection efficiency, D is the dark count rate, and Δt_j is the timing jitter. So, H takes into account detectors' three major parameters including their timing performance. This figure is useful for quantum information applications (e.g., QKD) as well as for Time-Correlated Single-Photon Counting (TCSPC) applications [170]. Usually, higher value of H at a certain wavelength refers to a better detector, such as SNSPD detectors have the best figure of merit at 1550 nm wavelength, in the range of 10^7 [157].

4.3 SPDs for quantum communications

Essentially any single-photon detector, such as PMTs, SPADs, or SNSPDs can be used for quantum communications. For successful quantum applications, ideally, the detectors must have a high quantum detection efficiency over a wider spectrum, low noise or dark counts, good time resolution, and shorter recovery time or dead time [63]. It is difficult to find all these qualities in one detector at the same time. Detectors are generally selected based on their practicality for the specific application.

Generally, available single-photon detectors are broadly divided into two major spectral ranges. Si-SPADs are widely used for visible wavelengths (400– 1000 nm), and InGaAs/InP or germanium (Ge) SPADs are well suitable for the near-infrared wavelengths (950–1650 nm). In contrast, PMTs and SNSPDs can have a much wider spectrum extending from ultra-violet to mid-infrared wavelengths, although, SNSPDs are designed and optimized for particular wavelengths.

Up until now, SNSPDs are highly suitable for a broader range of applications because of their exceptional characteristics such as high system detection efficiencies (SDE), ultra-low dark counts, low time jitter, fast recovery, and GHz maximum count rates [150, 154, 156, 165, 171–173]. Their best performances (more than 90% of SDE) are reported at the near-infrared wavelengths. Therefore, they have potential uses at the telecom wavelength quantum applications, for instance in loophole-free tests of local realism [174], quantum teleportation [175], QKD [176] and quantum memories [177]. On the contrary, they are not suitable for satellite QC missions as they require cryogenic cooling to reach sub-kelvin temperatures for their operation. In addition, they have very small active areas (a few tens of micrometers).

As an alternative, semiconductor SPADs such as InGaAs/InP or Ge SPADs are suitable for long-distance quantum communications at telecom wavelengths. Among them, Ge was developed particularly for long-distance applications and has been implemented successfully in several quantum applications, for instance in quantum cryptography, and violation of Bell inequalities [63]. However, the development of Ge devices became limited because of their low performance in the fiber-based applications and the need for liquid nitrogen temperatures [178]. Currently, Ge devices are replaced by the InGaAs/InP diodes for single-photon detection at the near-infrared wavelengths. These devices can operate at much higher temperatures ranging between 150 K and 220 K, and they have good quantum detection efficiencies (above 30%) [178]. They are good for fiber-based quantum applications, due to their compact size, and low power requirements. However, they are not ready for satellite applications, because of their high noise levels and limited repetition rates [179].

Photomultiplier tubes (PMTs) are a possible alternative to SPADs for satellite receivers. They are a matured technology and have been used in space for several years. PMTs have a long spectral range (115–1700 nm) and a big sensitive area (above 10 mm) [157]. Conversely, their detection efficiencies are relatively low (highest 40% at 500 nm), they require voltages in the kV range for operation, also, suffer high afterpulsing effect. Although better technologies such as hybrid photodetectors [180] and micro-channel photomultiplier tubes [181] are available, both of them suffer from a high level of noise.

On the contrary, Si-SPADs have been used for single-photon detection in the visible wavelengths for years. The technology of these devices is matured now in respect to their design, and fabrication methods. They are commercially available with good characteristic parameters, for example, more than 60% quantum detection efficiency [155], low dark counts (<200 cps), good time resolution (better than 350 *ps*) and a few MHz count rates (typically 10 MHz) [157]. Since cooling improves their performance, some commercial detectors are packaged with a built-in thermo-electric cooler (TEC) [182]. Due to their compact size, high detection efficiency and responsivity, low noise, smaller time jitter, and low power requirements, they are suitable for many quantum applications, especially for satellite missions.

Hereafter, the discussion will focus on the avalanche photodiodes, such as the Si-SPADs for visible wavelengths, and the InGaAs/InP SPADs for infrared wavelengths.

4.3.1 Single-photon avalanche diodes

SPADs are semiconductor devices based on p-n junctions that operate at a reverse bias above the breakdown voltage V_B for single-photon detection. At this bias, the electric field at the p-n junction is so high that a single electron-hole pair generated either by a thermal excitation or by absorption of a photon can trigger an avalanche multiplication of carriers at the depletion layer. SPADs are different from traditional avalanche photodiodes (APDs) since each has distinct operation regime as seen in Fig. 4.2. APDs work below V_B that provides a proportional outcome for incoming optical power. In contrast, SPADs exploits their intrinsic positive feedback to achieve a large gain, which produces macroscopic current pulses due to single-photon absorption. This operation mode is known as *Geiger mode* [149], in which a bias voltage V_A greater than V_B is applied across SPAD. The gain is dependent on the excess bias voltage V_E, which is $V_E = V_A - V_B$. Larger V_E increases the probability of single-photon detection while the amount of V_E can be between ~1 and 50 V depending on the types of SPAD material and structure. Under Geiger mode, the first generated carrier with a sufficient impact ionization coefficient collides with another atom and creates new electron-hole pairs while traversing the depletion region. Each newly generated carrier is then accelerated, and their further collisions with other atoms creates more carriers. This phenomenon quickly (within less than nanosecond [183]) builds-up carriers that leads to a macroscopic current pulse. This self-sustaining current persists until it is quenched. Usually, an external electronic circuit, also referred as *quenching circuit*, is employed to quench the avalanche current by bringing the bias voltage below V_B [183, 184]. Quenching circuits greatly affects the operation of SPADs and thus the overall performance of a detector system.

Silicon SPAD

Si-SPADs are well developed and are now commercially available with excellent characteristic parameters, such as high photon detection efficiencies (PDE) and low dark count rates (DCR). The device is formed by p-n junctions on a silicon wafer with a very small active area diameter that is sensitive to wavelengths 400-1000 nm. Efficient photon detections can be achieved by using an epitaxial growth structure in Si-SPADs [185]. As depicted in Fig. 4.3(a), the device can have two thin epitaxial layers of p-Si over an n-Si substrate. A growth of lightly doped p-layer over a highly doped buried p^+ layer intensifies the electric field. Under Geiger mode, the $\mathrm{n}^+ - p$ junction achieves a high enough electric field that creates an avalanche multiplication in response to photon absorption. Usually,

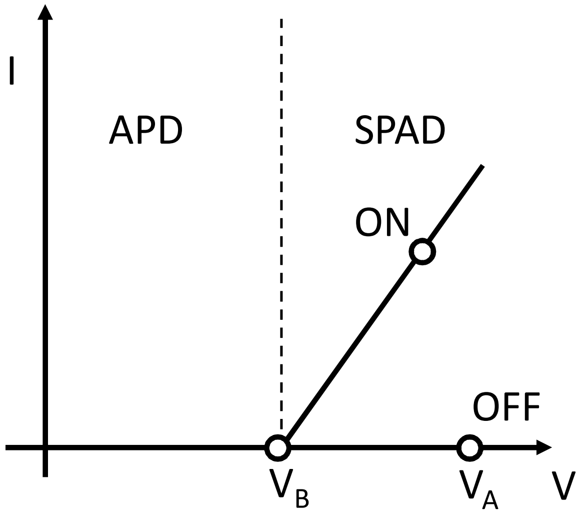


Figure 4.2: Operation regions of APD and SPAD in the reverse I-V curve of a p-n junction. Redrawn from [166].

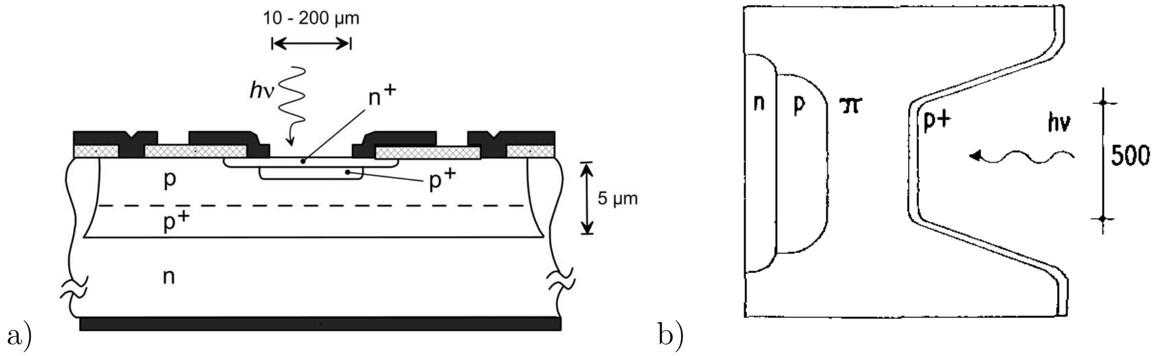


Figure 4.3: Cross-section of Si-SPAD. a) Epitaxial structure of thin junction Si-SPAD, reprinted from [185], and b)thick junction Si-SPAD, reprinted from [186].

these structures have very thin p-n junction width, typically 1 μm, for which they are categorized as thin junction SPADs [183]. These SPADs have a smaller active area diameter (5 – 150 μm), low break down voltage (20 - 50 V), and highest efficiencies at the visible wavelengths (DE of 50% at 550 nm [187]). Their time resolution is smaller than 100 ps FWHM which depends on the size of active area.

Si-SPADs are also available with thick junction geometry, as shown in Fig. 4.3(b). Junction thickness can extend from 20 to 150 μm [188, 189]. The wider thickness of the depletion region supports for a more efficient avalanche current distribution over the whole junction area. These devices allow light illumination on a small area at the center, giving good time resolution, lower than 350 ps. Their photon detection efficiency is greater than 50% over a wide spectral range around 540 – 850 nm, V_B between 200 and 500 V, and a wider active area diameter between 100 and 500 μm. However, they suffer from a non-zero afterpulsing probability that ranges between 1–10% [190].

InGaAs/InP SPAD

InGaAs/InP heterostructure devices are now the mainstream solution for single-photon detection in the near-infrared wavelengths [191, 192]. Various groups are working on designing optimized devices to significantly increase their maximum count rate [193–198]. The design optimization is done considering two intrinsic parameters, detection efficiency and dark count rate. Both of which are not controllable by external quenching electronics [161].

InGaAs/InP SPADs generally have a separate absorption, grading, charge, and multiplication (SAGCM) structure [193] as illustrated in Fig. 4.4. The absorption layer is an InGaAs ($In_{0.53}Ga_{0.47}As$) material having a bandgap energy of 0.75 eV at room temperature that will give photo-sensitivity up to wavelengths of 1670 nm [161]. An InP material works as a multiplication layer. Under a reverse bias, a sufficiently high electric field is ensured in the multiplication region to escalate the avalanche probability. The reduced thickness of this layer allows for a fast transition of the carriers and thus gives a reduced timing jitter. On the other hand, the electric field of the absorption layer is optimized such that this layer induces less avalanche breakdown while maintaining the drift of photogenerated carriers. The grading layer in between the multiplication and absorption layers prevents the build-up of trapped carriers, which helps to reduce the afterpulsing effect and the charge layer adjusts the electric field profile. Both the design and the fabrication process are optimized for improved SPAD performance.

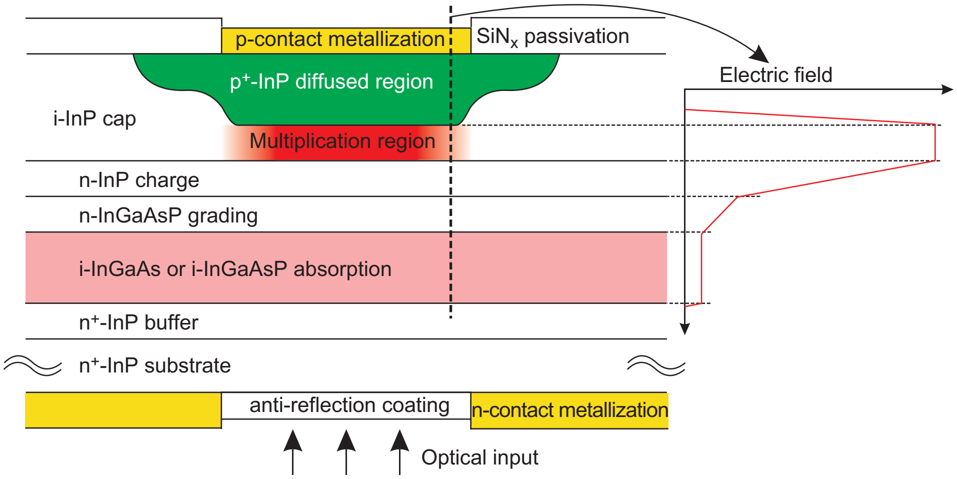


Figure 4.4: Device structure of InGaAs/InP SPAD with separate absorption, grading, charge and multiplication region. Reproduced from [193]

When the SPAD runs in Geiger mode, a photon absorption causes the generation of the electron-hole carriers. Immediately, one carrier drifts to the depletion region of the multiplication layer because of the high reverse bias and triggers a self-sustaining avalanche current by impact ionization process due to the high electric field (around 10^5 V cm^{-1}).

The detection efficiency (DE) of InGaAs/InP SPADs depend on various parameters which can be defined by [161]

$$DE = P_c P_{abs} P_{inj} P_{ava} \tag{4.2}$$

here P_c is the coupling efficiency, P_{abs} is the efficiency of photon absorption at the absorption layer, P_{inj} is the efficiency of the injection of photo-generated carriers from the absorption layer to the multiplication layer, and P_{ava} is the probability of creating an avalanche at the multiplication region. P_c is defined by several factors such as SPAD active area, insertion loss and reflectance. P_{abs} is given by $P_{abs} = 1 - e^{-\alpha d}$, where α is the absorption coefficient and d is the thickness of the absorption layer. Usually, α is $\sim$ 7500cm^{-1} in the In$_{0.53}$Ga$_{0.47}$As layer for 1550 nm photon. The last variable, P_{ava} highly depends on the excess bias $V_{\rm ex}$ above the breakdown voltage and temperature.

Another parameter, the dark count rate (DCR) is also affected by $V_{\rm ex}$ and temperature. Generally, three mechanisms will contribute to the DCR such as carriers generated in the absorption layer due to thermal excitation, direct band-to-band tunneling, and trap assisted tunneling in the multiplication layer. Thermal excitation dominates at high temperatures while low temperatures or large $V_{\rm ex}$ promotes the tunneling effect [193].

The afterpulse probability P_{AP} in InGaAs/InP SPAD devices significantly relies upon the quality of the multiplication layer, such as the amount of defect density [161]. Another approach to lower P_{AP} can be the reduction of charge carrier flow (typically $\approx\ 10^7 - 10^8$ [199]) during an avalanche or shortening the lifetime of the trapped carriers. P_{AP} for a detector system can be modelled as [161]

$$P_{AP}\ \propto\ (C_d + C_p) \times \int_0^{\delta} V_{ex}(t)dt \times e^{-\tau_d/\tau} \tag{4.3}$$

where C_d is the diode capacitance, C_p is the parasitic capacitance that includes both the circuit and the device capacitance, δ is the avalanche duration, τ_d is the hold-off time, and τ is the trapped carrier lifetime. It is seen from the equation that P_{AP} can be reduced either by a) scaling down C_p and δ, b) by lowering V_{ex}, c) by increasing τ_d, or d) by decreasing τ. Each of these approaches has a side effect as well. For instance, smaller C_p and δ will deplete the strength of the avalanche signals causing difficulty in discriminating them from the noise, low V_{ex} will decrease the DE, long τ_d will limit the maximum count rate, and shortened τ (achieved at high temperatures) will increase the DCR. Therefore, the design of InGaAs/InP SPADs might consider their target applications to decide which parameters are of most valuable.

Since InGaAs/InP SPADs experience high afterpulsing effect, their use is mostly limited to gated-mode operation [200–205] with quantum efficiency of 10% – 30% at 1550- nm [201, 206–209]. Although their other operation mode–the free-running mode– also reported with more than 25% of detection efficiency [162], it has limited maximum count rate due to the long hold-off time, typically $\leq$ 10MHz [210]. However, the free-running is essential when photon arrival time is unknown, and low counting rate is not a concern, such as in long distance quantum communication.

4.3.2 Quenching circuits for SPADs

As discussed earlier, when the self-sustaining avalanche current starts to flow in SPADs, it needs to be quenched by bringing their bias voltage below the breakdown voltage V_B. The quenching circuits that are used to quench avalanche currents can be of two types: i) *passive quenching circuit* (PQC) [183, 184], and ii) *active quenching circuit* (AQC) [211–213]. In PQCs, the avalanche current goes down below their threshold current to stop avalanching by itself, that requires a ballast resistor R_L connected in series with the SPAD, as seen in 4.5. The value of R_L can be in kilo-ohm to mega-ohm range, the junction capacitance C_d can be $\sim$ 1 pF, and the stray capacitance C_S (the capacitance of the node at SPAD and

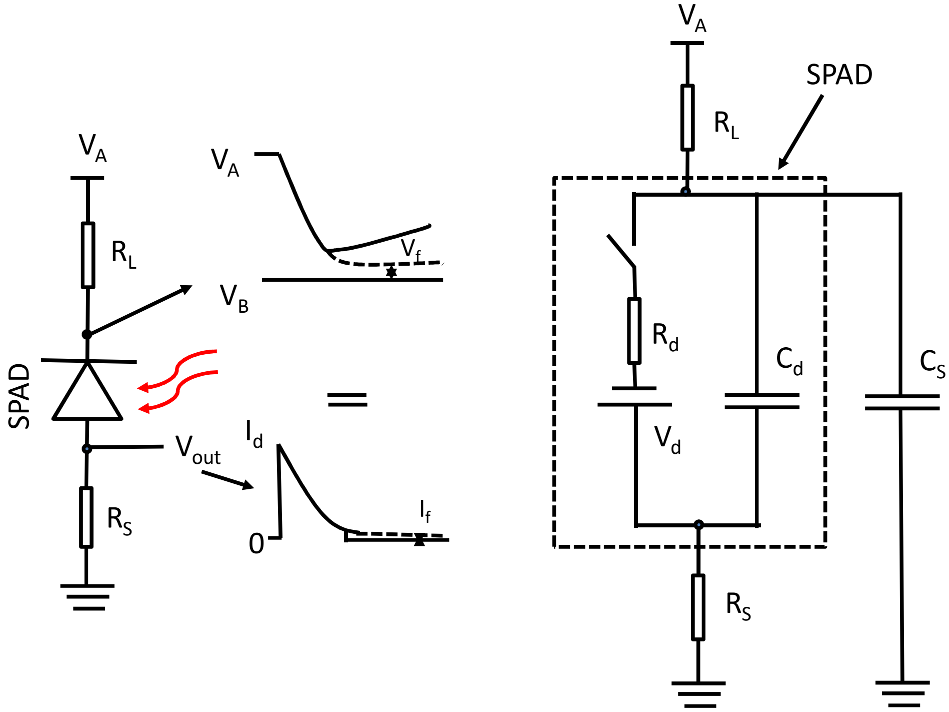


Figure 4.5: Passive quenching circuit for an SPAD. R_L is the large quenching resistor and R_S is a small readout resistor. The right circuit is the equivalent representative of the left circuit. V_d and R_d are the dynamic properties of the SPAD; C_d: junction capacitance; C_S: stray capacitance. Redrawn from [183]

R_L to the ground) can be few pF [183]. R_S is a small resistor (typically 50 Ω) used for avalanche signal readout and R_d is SPAD dynamic resistor which is made up with junction space-charge resistance and resistance of neutral semiconductor.

For photon detection, the SPAD is reverse biased via R_L with a voltage V_A which is V_E voltage above V_B. When relaxed, no current flows through the device, thus there is no voltage drops across R_L, and C_d and C_S charge up by V_A. When an avalanche is triggered (referred as closing switch in the equivalent circuit), a current $i_d(t)$ will flow through the device which is defined by $i_d(t) = (V_d(t) - V_B)/R_d$ and it will cause the discharge of C_d and C_S via R_d and R_L. The current raises the voltage drop across R_L which is $i_d(t)R_L$ that lowers the diode voltage $V_d(t)$ and current $i_d(t)$ exponentially towards their steady-state values of V_f and I_f, respectively [183], where

$$I_f = \frac{V_A \ - \ V_B}{R_d \ + \ R_L} \ \cong \ \frac{V_E}{R_L}, \quad \text{since } R_L \ >> \ R_d \tag{4.4}$$

$$V_f \ = \ V_B \ + R_d I_f \tag{4.5}$$

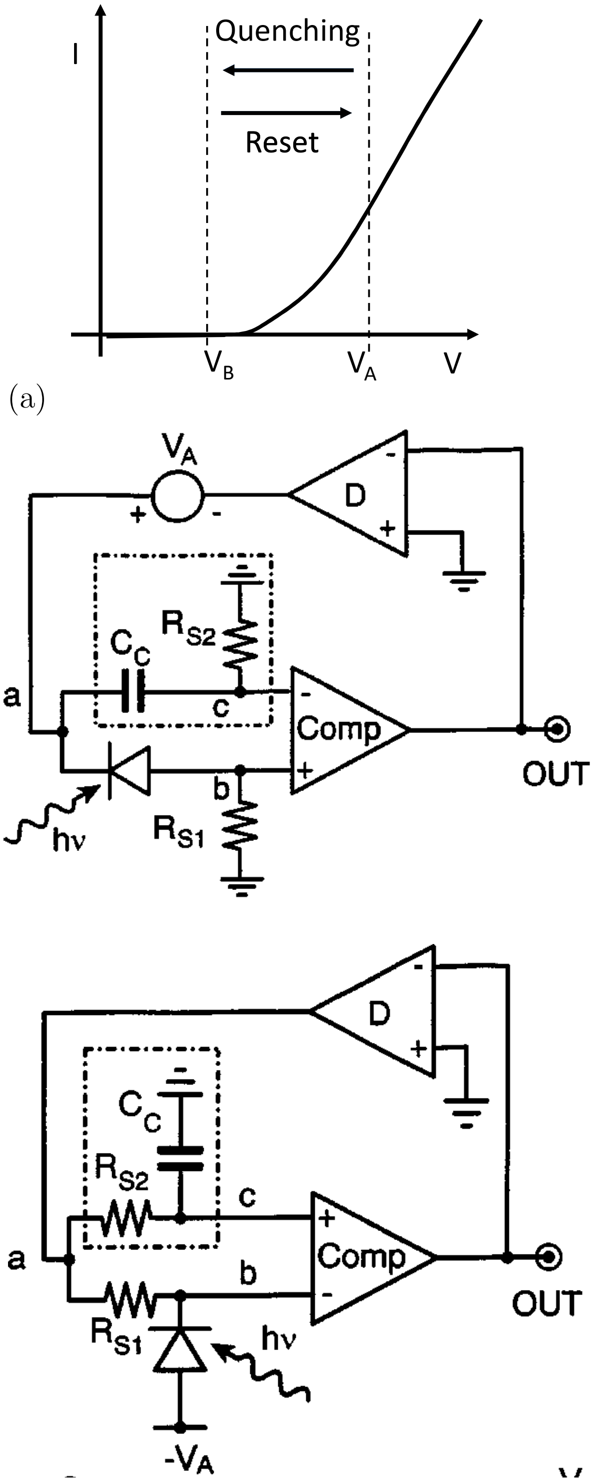
When V_f is close to V_B and I_d is $\leq 100\ \mu A$, the quenching of avalanche current happens with a time constant of $\tau_q \approx (C_d + C_S)(R_d \mid\mid R_L)$ which can be approximated to time constant $\tau_q \approx (C_d + C_S)R_d$ as $R_L >> R_d$. After quenching, the device takes a while to come back to its rest condition which is known as reset time defined by the recharging of C_d and C_S that has a time constant of $\tau_r \approx (C_d + C_S)R_L$.

For an externally connected resistor, the stray capacitance C_S is large, around 10 pF [184]. This causes an increase of the total quenching and reset time, which limits the speed of the device. If a SPAD comes with an integrated resistor, C_S becomes much smaller, ~ 1 pF. Also R_L plays a vital role in defining the speed of the PQCs.

On the other hand, AQCs can resolve the long recovery problem of PQCs. These circuits first sense the trigger time of the avalanche pulses and then force SPADs to quench and reset by a controlled amount of time. As illustrated in Fig. 4.6(a), AQCs have well-defined quenching and reset time, and this switching between the operation states is much faster compared to the PQCs. In AQCs, a fast comparator first senses the rise time of the avalanche pulse, which brings the bias voltage V_A below the V_B for quenching. After a certain hold-off time, the bias comes back to its original bias of V_A.

An AQC has two connections with the SPAD: one for detecting the avalanche pulse and the other one for quenching pulse. These two connections can be at the two terminals of a SPAD (Fig. 4.6(b)) or both connections at the same SPAD terminal (Fig. 4.6(c)). In both configurations, the quiescent level of the sensing terminal is close to the ground voltage, and the elements in the dotted box in Fig. 4.6(b)-(c) compensate the current pulses generated by the quenching pulses due to the SPAD capacitance. The compensation eliminates the possibility that capacitive oscillations are detected by the comparator. The driver D generates the quenching pulses of amplitude higher than V_E to ensure quenching. A hold-off feature can be achieved by employing a monostable circuit that will create the quenching pulses of a certain width synchronously with the leading edge of the avalanche pulses [183]. The hold-off time can effectively control the number of trapped carriers during the avalanche and thus the afterpulsing probability.

Gated-mode operation is another way to operate SPADs for synchronous single-photon detection [214]. This approach is effective for suppressing afterpulses and dark counts. For this operation, a gate pulse of amplitude V_E switches the SPAD to ON state for a short duration, which also limits the charge flow during the avalanches. Usually, the gate OFF time (when $V_A < V_B$) is kept sufficiently long to ensure de-trapping of carriers which helps to reduce the afterpulsing probability. In these circuits, the gate pulses coupled to the SPAD creates derivative signals caused by the capacitive effect of the SPAD. These signals are superimposed with the avalanche signals. Hence, it is challenging for the gated



(a)

(b)

(c)

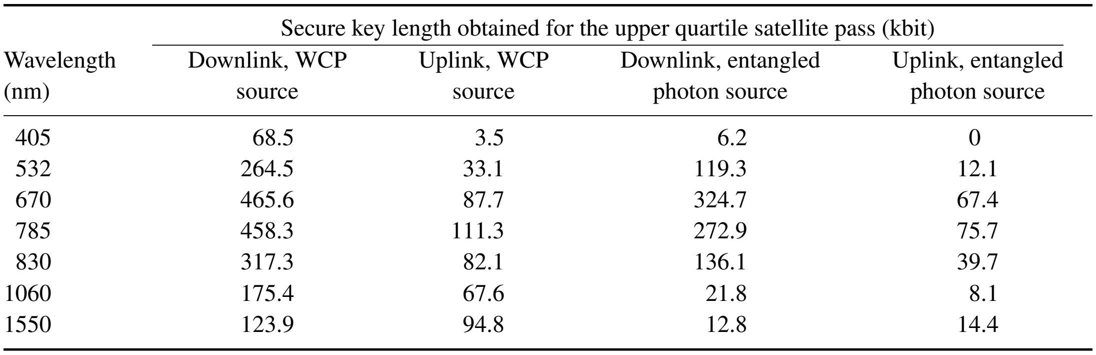
Figure 4.6: Active quenching circuits for SPADs (reproduced from [183]. (a) I-V characteristic curve of the SPAD and switching voltages between quenching and reset. AQC configuration with (b) the different quenching and avalanche sensing terminal of the SPAD and (c) the similar quenching and avalanche sensing terminal of the SPAD.

quenching electronics to extract the avalanche signals from the derivative signals. Another important factor with these circuits is the gating frequency, which is limited by their long gate OFF time for low/no afterpulsing operation.

Generally, the circuits are divided into two categories depending on the gating frequency: i) the low-frequency gating (less than 100 MHz) [214–216], and ii) high-frequency gating (above 100 MHz) [203]. Typically, low frequency gating uses coincidence method [206] or double-SPAD technique [209] for extracting avalanche signals. In contrast, sine wave gating and self-differencing are the two principal schemes used for high-frequency gating [161]. Both techniques give increased frequency rates of up to 2 GHz. High-frequency gating is more widely used in InGaAs/InP SPADs. However, these techniques are also applicable for SPADs with other materials such as Si-SPADs [217].

4.4 SPDs for satellite QKD

In satellite quantum communication, a satellite must carry single-photon detectors either as an integral part of the receiver to detect photons in an uplink or to verify quantum sources in a downlink scheme. The choice of the SPDs depends on the optimal wavelength for a particular scheme considering the secret key lengths and the wavelengths of available quantum sources. J. P. Bourgoin *et. al.* [36] performed a simulation to find the optimal wavelengths for an uplink and a downlink using two types of sources, a weak coherent pulse source, and an entangled photon source [218]. The simulated result is summarized in Fig. 4.7 suggesting that 670 nm and 785 nm wavelengths are suitable for the uplink and downlink, respectively, and entangled photons at $\sim 800\ nm$ are suitable for both schemes. Available PMTs, Si-SPADs and SNSPDs support all these wavelengths. Of these options, SNSPDs are generally not chosen in space applications because of their cryogenic temperature requirement. Conversely, PMTs had been used in space for many years, although they have significantly low quantum efficiencies compared to Si-SPADs at wavelengths above 550 nm (<20% of PMT versus >60% of Si-SPAD). In addition, photocathode degradation has always been a major issue for the use of PMTs in space. Since Si-SPADs are commercially available with high quantum efficiencies over a wider range of wavelengths, they are considered as the prime candidate for satellite implementations [151, 152, 155]. They have already been used in several space missions [35, 219–221], although in those missions the Si-SPADs suffered increased noise levels due to space-radiation. It is thus crucial to analyze the effects of radiation damage of Si-SPADs and find an effective solution to reduce the damages for extending the life time of a mission.



	Secure key length obtained for the upper quartile satellite pass (kbit)			
Wavelength (nm)	Downlink, WCP source	Uplink, WCP source	Downlink, entangled photon source	Uplink, entangled photon source
405	68.5	3.5	6.2	0
532	264.5	33.1	119.3	12.1
670	465.6	87.7	324.7	67.4
785	458.3	111.3	272.9	75.7
830	317.3	82.1	136.1	39.7
1060	175.4	67.6	21.8	8.1
1550	123.9	94.8	12.8	14.4

Figure 4.7: Simulated cryptographic key length at various wavelengths for a WCP and an entangled photon source. The longest key that are produced at 670 nm for a downlink, and at 785 nm for an uplink. The results are for a 600 km orbit. Source rate: 300 MHz for WCP and 100 MHz for entangled photon source; Reprinted from [36]

4.5 Effects of radiation on SPADs

Si-SPADs have been part of several space missions. For instance, Sun *el. al.* in 2004 reported the on-orbit performance of their Si photon-counting system deployed for measuring Earth surface elevation and atmosphere backscattering on their Ice, Cloud, and land Elevation Satellite (ICESat) mission [35]. Their counting module contained the Excelitas reach-through type Si-SPADs. After $\sim$ 380 days of on-orbit operation, almost all the parameters of the detectors were found unaffected by the radiation except the dark count rate, which was increased by $\sim$30 Hz per day. At this incremental rate, the photon detectors would be unusable within a few weeks for QKD applications, since larger DCR contributes more to the QBER and gives smaller key rate. The effect of dark count rates on different quantum communication systems was studied[2] by J.-P. Bourgoin et al. [36]. It was found that the key rate would be 1.2 bps and 0.9 bps for DCR on the order of 100 Hz and 1000 Hz, respectively, using efficient commercial silicon detectors at 785 nm wavelength and 300 MHz weak coherent pulsed (WCP) source. But for the dark counts above 10,000 Hz, it was not possible to perform any form of QKD. Therefore, a target DCR value is defined for successful realization of ground-to-satellite quantum communications, which is $\leq$ 200 Hz per detector [222].

Usually, detector dark counts increases due to the resultant trapped electrons and protons, created from the strong bombardment of the outer space high-energy particles with the detector substrate. The trapped electrons cause ionizing damage, while the trapped

[2] The analysis considered 50 cm transmitter and a 30 cm receiver, 600 km orbit, and rural atmosphere with 5 km visibility at sea level.

protons cause displacement damage [41]. For Si-SPADs, trapped protons cause more damage than the trapped electrons, creating extra energy levels in the bandgap displacing some Si-atoms. It then allows the electrons to transit to the higher energy levels at much lower thermal excitation that causes more dark counts.

However, being a potential candidate for space quantum missions, Si-SPADs have been thoroughly investigated in several ground-based radiation tests [41–46]. A research group in National University of Singapore (NUS) tested Si-SPADs– Perkin Elmer C30902 and Laser Component SAP 500– after irradiating them with γ-rays and proton emission. [42]. They chose a total ionizing dose equivalent to 800 km of altitude, which is 5 krad/year. Then the SPAD samples were irradiated with γ-rays with the doses of $1-5$ krad to analyze ionizing damage. The result showed that the DCR raised by only two times demonstrating the detectors are less sensitivity to the ionizing radiation damage.

They also tested the displacement damage (DD) from proton radiation. DD is measured as a product of the non-ionizing energy loss (NIEL) ($\mathrm{MeV.cm}^{-2}/g$) at each proton energy and the fluence (cm^{-2}). Fig. 4.10 represents the SPENVIS data of a proton energy spectrum at various orbits considering 1.85 mm of Al shielding. Fig. 4.10(a) shows that polar orbits have higher proton fluence than the equatorial orbits, where the dominating proton energies are less than 100 MeV. On the other hand, Fig. 4.10(b) depicts that protons with energies below 100 MeV have much higher NIEL, which causes more damage. Therefore, the DD impact is more substantial in the polar orbits and at longer distances from the Earth. Total displace damage dose is usually calculated by integrating the product of total fluences ϕ_p(E) and the NIEL(E) over the entire energy range (eq. (4.6)). During their experiment, several detector samples were irradiated separately with a particular monochromatic proton energy (ranging between 5 MeV$-$50 MeV) of various proton fluence that ranged from 1.47×10^8 cm^{-2} to 7.48×10^8 cm^{-2}. The total dose of DD damage increased the DCR by one to two orders of magnitude.

$$\text{Dispacement damage dose} = \int_0^\infty \phi_p(E) * NIEL(E)\ dE \tag{4.6}$$

Other ground-based radiation damage experiments on SPADs [41, 43–46] also reported the DCR increase by thousands of counts after irradiation, which is undesirable for successful quantum communication in space.

However, while analyzing the radiation damage, an interesting feature is pointed out by Anisimova *et. al* [37]. They found that irradiation of SPADs when biased develops more DCR than those SPADs at the unbiased condition. Therefore, any quantum mission

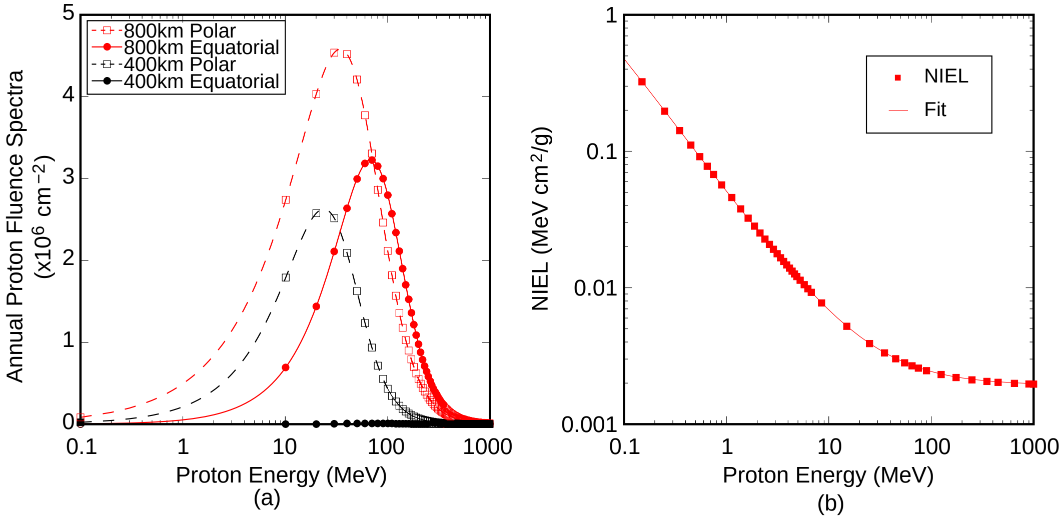


Figure 4.8: a) SPENVIS data for Proton fluence spectra per year at different orbits with 1.85 mm of Al shielding. b) Average Proton Non-Ionizing Energy Loss (NIEL) for silicon. Reprinted from [42]

should consider this during planning of the mission to avoid extra damages from the biased condition.

4.6 Techniques for healing radiation damages in SPADs

The damage experienced by the SPADs due to the in-orbit high energy particles requires to be mitigated to maintain their performance and to enhance their in-orbit lifetime. Since radiation mostly affects the DCR, any potential methods for healing the damages will extend the effective lifetime of the SPADs. To date, several damage healing methods such as *cooling* [37, 42], *thermal annealing* [37, 42, 43, 46] and *laser annealing* [39, 40] are being analysed as promising solutions to mitigate the radiation damage.

4.6.1 Cooling of SPADs

Deep cooling is generally used in non-irradiated SPADs to reduce the rate of thermally generated dark counts [223]. Recently the Singapore group utilized the cooling of -20°C on the irradiated SPADs for improving their DCR [42]. At this temperature, the detectors keep functioning even after the displacement dose of as high as 9×10^6 MeV/g giving a dark counts in the range of 100 kHz. Another study showed that cooling at -20°C on the 24 months equivalent irradiated SLiK detectors exhibits dark counts on the order of 10^5 Hz [37]. All these rates of DCR are too high to perform quantum communication.

Although, the second study demonstrated a reduced DCR of 200 Hz by the irradiated SLiK samples at -86°C. This result proves that the deep cooling is capable of keeping the DCR to the required rate of quantum protocols even after the higher doses. However, deep cooling on the other hand affects the detector's afterpulsing probability, since the lifetime of the trapped carriers increases with the cooling. The analysis by Anisimova *et al.* showed an increased afterpulsing probability after the irradiation, as seen in fig. 4.9 [37], which might influence the quantum communications [223, 224]. Nonetheless, the SLiK detectors will serve better in the quantum communications even after a large radiation doses if enough cooling is provided.

4.6.2 Thermal annealing of SPADs

Thermal annealing is helpful in reducing the DCR of the irradiated devices by resolving defects in the semiconductor structures [42, 43, 46]. It is a process of heating the SPAD substrate at higher temperatures for a certain period that resolves some defects. Recently, this method has been thoroughly analyzed on several SPAD samples (Excelitas C30921SH, Excelitas SLiK, and Laser components SAP500S2) by Elena *et al* [37]. The samples were

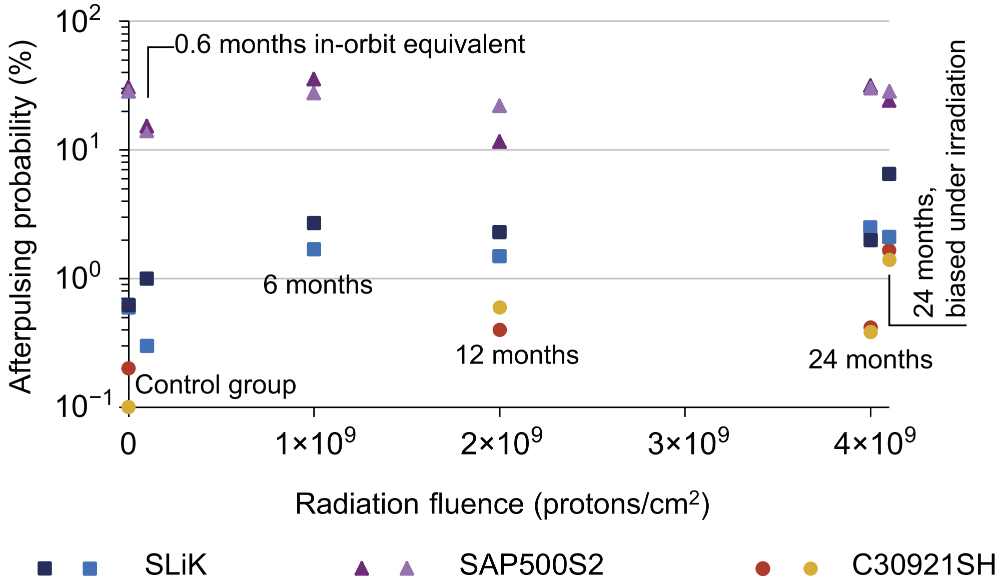


Figure 4.9: Afterpulsing probability P_{AP} at -86°C. The SLiK and C30921SH detectors have increased P_{AP} for the 6 – 12 months of equivalent radiation dose. SAP500S2 showed inconsistent results. Results reprinted from [42]

irradiated with 106 MeV proton fluences of 10^8, 10^9, 2×10^9, and 4×10^9 p/cm^2, equivalent to the radiation dosage that a satellite will experience in an orbit at 600 km of altitude for a duration of 0.6, 6, 12 and 24 months, respectively. The amount of doses was calculated considering 10 mm of Al shielding. After the irradiation, all the samples developed a significantly large DCR, illustrated in Fig. 4.10. In addition, the SLiK and C30902SH detectors experienced higher afterpulsing probabilities, probably due to the newly created defects induced by the radiation. Then they performed thermal annealing on the irradiated samples at room temperature (+20°C) and in a hot-air-flow oven at +50°C, +80°C and +100°C for different amount of time. All the samples were benefited from the high-temperature annealing in healing the damages. However, room temperature annealing was too slow to be useful in any satellite applications.

In contrast, the oven annealing at +80°C for four hours followed by an hour at +100°C resulted in a substantial reduction of the DCR. For instance, the SLiK (C30921SH, and SAP500S2) devices demonstrated a factor of 0.15 (0.3, and 0.28) times the pre-annealed DCR. The study observed a significant reduction of DCR during the first hour of annealing at +80°C, and it continued to improve with additional annealing. They also tested thermal annealing of SLiK SPADs using the built-in thermoelectric cooler (TEC) up to +100°C, which exhibited a consistent improvement of DCR. Thus it suggests that TEC can be a

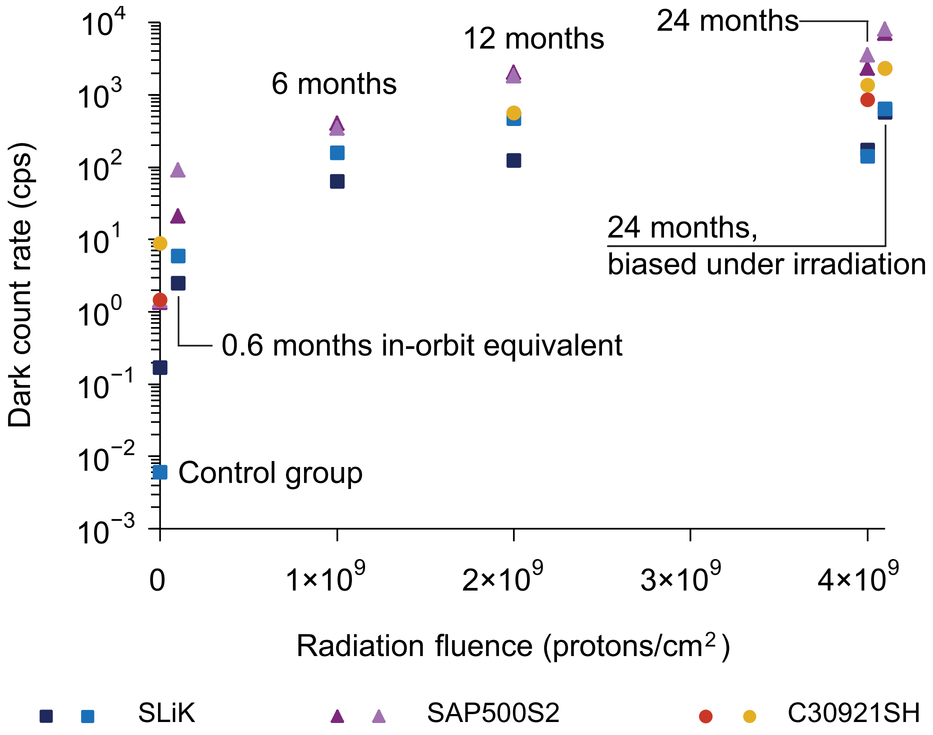


Figure 4.10: DCR of irradiated SPADs measured at -86°C. Control groups detectors were not irradiated. Reprinted from [37]

simplified heating mechanism to be used in the outer space.

The aforementioned thermal annealing technique was performed only once on the irradiated SPAD samples. Ian DSouza in his thesis explained a repeated thermal annealing precess to approximately simulate the annealing in the space environment. They experimented on two detector modules (DM) containing five SPADs each [38]. The DMs were radiated with the two years equivalent doses which is 4 $\times$ 10^9 p/cm^2. DM1 was irradiated with 6.6 $\times$ 10^8 p/cm^2 (4 month equivalent fluence in LEO) incremental doses while DM2 was irradiated with 3.3 $\times$ 10^8 p/cm^2 (2 month equivalent fluence in LEO) incremental doses until the final two years equivalent doses. Seven out of the ten SPADs exceeded 500 Hz of DCR at -80°C after the first proton dose of 6.72 $\times$ 10^8 p/cm^2 and the other three detectors exhibited more than 1 kHz DCR. Thermal annealing of the detectors at +80°C using the in-built TEC for one hour after each irradiation helped to reduce the dark counts. In the experiment, they performed the annealing on the two detector module at two different phases. DM1 was annealed after each radiation phase, while DM2 detectors were annealed only when their dark counts exceeded 2 kHz. Of these two approaches, detectors annealed after the threshold exhibited less dark counts compared to the detectors annealed in regular interval. Moreover, most of the detectors rendered the greatest reduction factor after the first round of annealing showing its effectiveness around first time application. In between the annealing phases, dark count reduction factor varied between 2–5. The study overall showed that annealing was able to keep the DCR below 500 Hz up to 3 years of LEO equivalent fluence (6×10^9 p/cm^2). Thermal annealing therefore can be utilized in the near future satellite quantum communication missions to heal detector damages.

4.6.3 Laser annealing in SPADs

Laser annealing is a highly effective method to resolve the defects in SPAD devices. This process uses a focused laser beam to the active area of detector for the annealing. It was previously manifested that ≈1 W of laser illumination on non-irradiated Si-SPADs improves their dark count rates up to 5.4 times [39] than the pre-annealed DCR. Later, Lim *et al* carried out an experiment of laser annealing on the irradiated Si-SPADs. Their experiment demonstrated an excellent efficiency of this method in healing the radiation damages [40]. They used the same irradiated SPAD samples that were used in [37], and laser-annealed the detectors for a duration of 60 s using a 808 nm continuous-wave (CW) laser. Annealing at $0.8 - 1.6\ W$ of laser power helped to reduce the detector dark counts. The DCR reduction factor for the SLiK detectors were ranging between $1.3 - 10$ times at $-30°$ C and between $5.3 - 41.7$ times at $-80°$ C. The C30902SH detectors exhibited dark count reduction of around 150 times at $-80°$ C. Importantly, this method was able to further reduce the dark counts of the previously thermally annealed detectors.

Their analysis illustrated that most of the detector characteristic parameters stay unaffected by the annealing except the afterpulsing probability, which was increased in each detector after the annealing. This result implies that laser annealing is able to decrease thermally generated dark counts by resolving its primary contributor– the mid bandgap impurities, at the same time it creates new impurities near to the conduction band that contributes to the afterpulses.

To identify the laser annealing effects and its reactions to the detector devices, a different approach is explained in Jin Gyu Lim's thesis [47]. They laser annealed a few samples separately using high-power CW laser for i) 60 s, ii) 180 s, and iii) 50% duty cycle mode at 1.5 kHz for 60 s. In the both 60 s and 180 s duration, detectors' maximum DCR reduction occurred at the same optical power of 800 mW. This result implies that laser annealing seem to be a local heating process. But 180 s annealing showed more dark count reduction at less optical power around $267 - 800$ mW, which suggests that there could be other reason than the local heating. However, in the 50% duty cycle mode, lowest DCR was achieved at 2000 mW which was equivalent to the 60 s method with average power of 1200 mW. This result indicates that electrons possibly play a role in the laser annealing effect as well. To know the actual reasons behind the laser annealing effect need more investigation. Meanwhile, this method will be further studied in space in the CAPSat mission [48]. The details of the in-orbit laser annealing initiative is discussed in chapter 5.

Chapter 5

CAPSat detector module for in-orbit laser annealing

Silicon single-photon avalanche photodiodes (Si-SPADs) are a promising component for detecting single-photons in satellite missions, as discussed in chapter 4. However, space radiation, especially proton radiation, damages these detector devices and increases their dark count rates (explained in section 4.5). When the dark count rates exceed a threshold (around 200 Hz), conducting quantum communication is not possible [36]. So detector damage could affect the goal of space quantum communications and mission lifetime. For mitigating the damages, section 4.6 described several potential methods, such as thermal annealing [37, 38] and laser annealing [39, 40]. Until now these methods have been analyzed in various ground-based experiments on Si-SPADs irradiated with LEO equivalent radiation dose. These analyses showed reduced dark count rates after the annealing that heals the radiation damages. Particularly laser annealing is found more efficient in reducing the detector dark counts. We therefore want to study further this method of laser annealing.

In the previous annealing experiments, the proton radiation dose on the detectors were estimated using SPENVIS software that considers shielding around an object, expected orbiting duration, and orbital altitude. However, this calculation has uncertainty with a factor of 2–3 [225, 226]. Additionally, the high-energy beam radiation produced at a radiation facility is different from the space radiation [227]. The main difference is that a synthetic radiation is delivered only in one direction at monochromatic energy, while naturally occurring proton fluxes are omnidirectional and have a certain energy distribution. Consequently, detector damage induced on the ground will differ from the damage occurring in space. Besides, the previous laser annealing experiments used that detectors which were irradiated with the total calculated dose of proton flux all in a single run [40, 47]. It remains to be known how does the repeated laser annealing work on continuously irradiated SPADs. It is therefore interesting to study the effectiveness of laser annealing in the real space environment and the healing of radiation induced damages of the detectors.

Hence, we are interested in performing an in-orbit laser annealing on the Si-SPADs (similar SPADs used in the other radiation damage experiments). We plan to send a CubeSat in the CAPSat mission [48] incorporating several Si-SPADs with an integrated laser annealing system to an low-Earth orbit (LEO). Through this experiment, we will be able to analyze the in-orbit detector damage and performance of the annealing methods. Since detectors in LEO will be exposed to the radiation during each cycle as it orbits the Earth, particularly the poles and South Atlantic Anomaly, the induced radiation damage will be periodic too. During this mission the degradation of the detectors will be deduced from frequent dark counts measurements. We will activate the in-orbit laser annealing system once detectors' dark counts exceeds a pre-defined threshold. This approach will provide insights into how often the annealing needs to be performed to keep the detector devices useful, and the efficiency of the annealing methods in curing the damages.

Towards this goal, we designed and built a miniaturized and compact detector module (DM) with a CubeSat compatible size, mass and power. The DM is designed to facilitate laser annealing as well as thermal annealing. Since the detector packages used in the module have an integrated thermo-electric cooler that is primarily used to cool the devices, it can also be used to perform thermal annealing by reversing the electrical current. In addition, the module is designed to provide high flexible and software controllable operation. The main challenge of this work has been to accommodate all the circuitry and mechanical structure required for the operation of the detectors within the volume and limited power budget in a CubeSat payload. Additionally, the design had to consider the outer space thermal conditions and the vacuum environment at each step of the DM development.

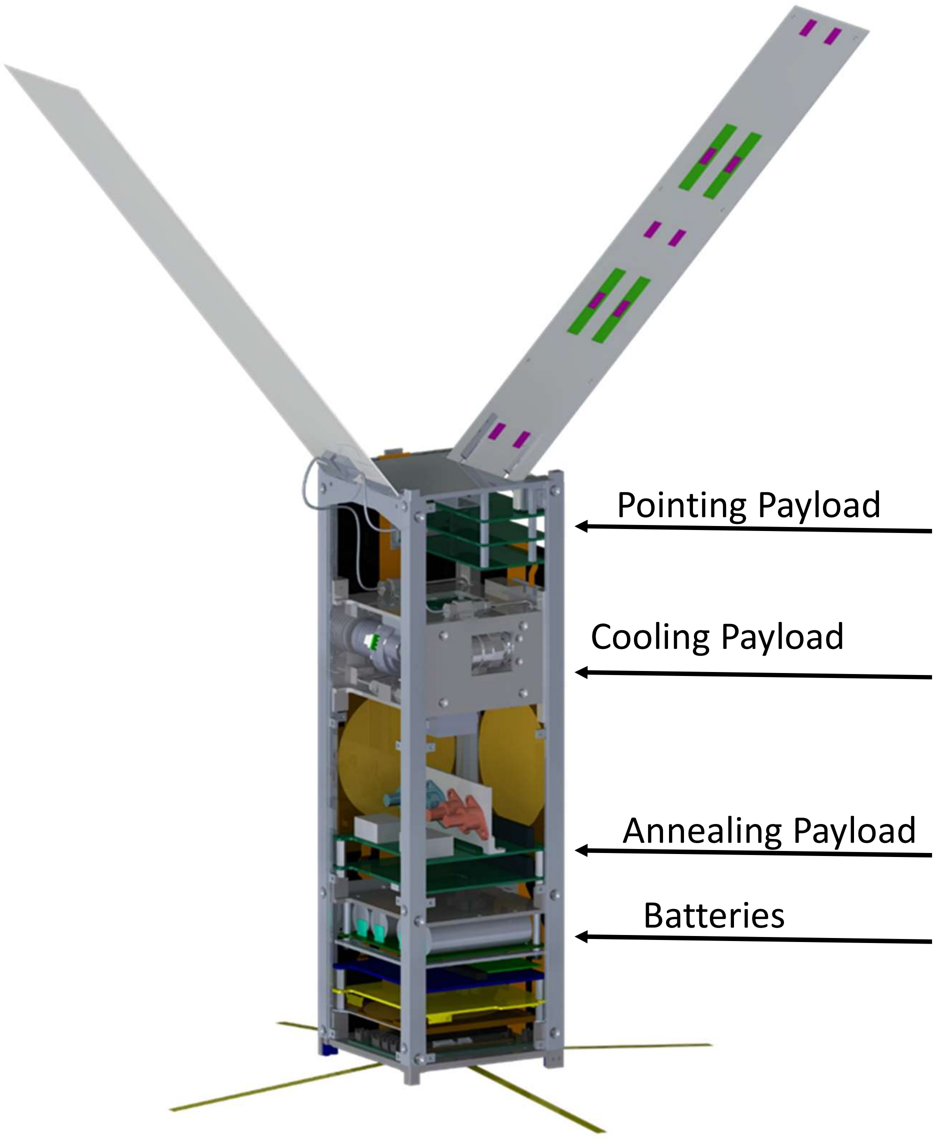


Figure 5.1: 3D model of the CAPSat satellite– IlliniSat 2 bus. Inside view of the satellite shows the loaded payloads. The image is taken from [228]

5.1 CAPSat Mission

The CAPSat mission is being developed as a part of the NASA Science Mission Directorate's Undergraduate Student Instrument Program. The CAPSat will carry three science payloads – Cooling, Annealing and Pointing payloads, which will be housed in a 3U CubeSat bus– IlliniSat-2 [229]. The satellite bus is designed at the University of Illinois at Urbana-Champaign (UIUC). The **annealing payload** (APL) is designed and developed in collaboration with a UIUC team by separating the APL into a detector module (DM) and a controller module.

The APL consists of two printed circuit boards (PCBs) that are stacked together. Fig. 5.1(b) shows the IlliniSat-2 bus loaded with the payloads, including APL. The satellite bus provides power from its power board, supported by a battery. Two power channels are provided to each payload– an unregulated supply directly from the batteries with a maximum voltage ranging around 6 $V \sim 8.4$ V, and a regulated 3.3 V supply. The total instantaneous power limit of the bus is 18 W, and the limit of power consumption by each payload is a maximum of 3 Ah per activation.

The operations of the satellite will be controlled by a Control & Data Handling (C&DH) board of the satellite bus which has a firmware interface to communicate with each payload. The C&DH board is responsible for monitoring the health of the payloads, activation or deactivation of an experiment, and receiving data from the payloads. An RS422 bus is used to interface the payloads with the C&DH board.

The satellite will be transported to the International Space station by a SpaceX Antares spacecraft tentatively in 2020. Afterward, it is anticipated that it will be deployed to a near-sun-synchronous orbit at an altitude of 450 km perigee at 93° inclination. The expected lifetime of the satellite is ten months. If satellite communication has ceased approximately for one week, the spacecraft will be considered to have reached its 'end of life'.

5.2 Annealing payload

The APL is developed with a CubeSat dimension to fit within the CubeSat bus. This payload accommodates all the necessary resources required to operate and characterized several detectors, and for performing thermal as well as laser annealing. Before giving details of the APL, I want to discuss briefly the concept of operation. Fig. 5.2 illustrates the functional arrangement of the payload. An optical-beam from the high power laser diode (LD) is used for annealing of the Si-SPADs, and is focused on the SPAD active area by a fiber optic cable. A photodiode (PD), located close to the fiber, measures the small fraction of the laser beam that leaks from the fiber to monitor optical power towards the SPAD. A light emitting diode (LED) on right of the fiber acts as a reference light source. This LED will send a very faint signal (that inserts into the fiber) to the SPAD when activated to verify the photon detection efficiency of the detectors. The activation and operation of all optical devices will be regulated by a microcontroller.

The APL is implemented into two separate functional units, as shown in Fig. 5.3. The **Control PCB**, developed by the UIUC team, holds two LDs, LED, PD, and a microcontroller (MCU). The **Detector PCB** that we developed contains four Si-SPADs of two types, detector bias and quenching circuits, and a thermo-electric cooler (TEC) controller. The outputs of the two LDs are fiber connected to two SPADs, one from each type. These two detectors will be used for laser annealing. The other two detectors (not connected to LD) will not be annealed. They will act as control detectors to give a measure of cumulative damage due to the high-energy space radiation. Then the LED in the control board working as a reference light source will be used for measuring the SPAD detection efficiency, and the PD will monitor the power sent to the LD and LED.

The detector PCB will be stacked on top of the control PCB to form the complete APL, as shown in figure 5.4. It will draw its driving power from the control PCB. The two boards will communicate via a PC/104 connector and the MCU on the control PCB will regulate the functions of the entire APL devices.

The experiment of the APL will give us two types of data: the DCR and the photon detection efficiency of each detector. This test will collect data at different conditions, such as at various cooling temperatures of the SPADs, before and after annealing, or after several radiation cycles. The C&DH board of the satellite will collect the data and will downlink later to a ground station.

5.2.1 Selection of components

SPADs:

Si-SPADs of two different models are chosen from Excelitas technologies – SLiK and C30902SH [182]. The C30902SH has photosensitive area of 500 µm in diameter, while it is 180 µm for the SLiK devices. The SPADs are hermetically-sealed in a metal housing. A two-stage TEC and a thermistor are also packaged within the SPAD housing. TEC provides precise temperature control of the SPADs between −30°C and 100°C, and the thermistor allows to monitor the SPAD temperature. All the SPADs are coupled with a fiber-connector.

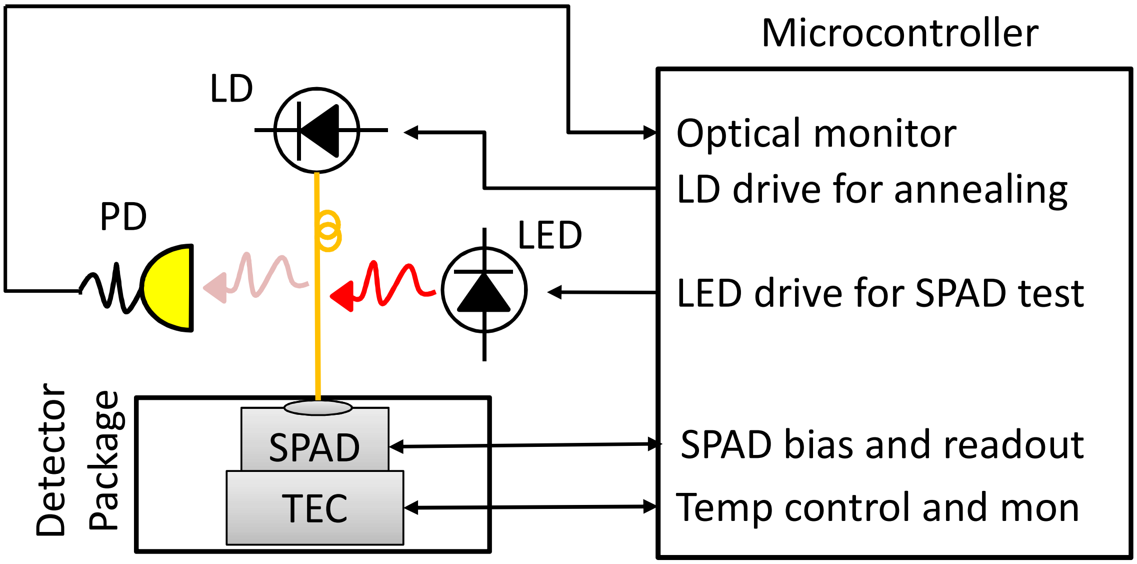


Figure 5.2: Concept of the in-orbit laser annealing. Laser diode (LD) is a high power laser that is used to anneal the single-photon avalanche photodiode (SPAD). LD output is guided to the active area of the SPAD through optical fibre. A light emitting diode (LED) is a reference light-source to test the photon detection efficiency of the SPAD. Photodiode (PD) monitors the power illuminated to the SPAD. TEC is an integrated thermoelectric cooler with the SPAD.

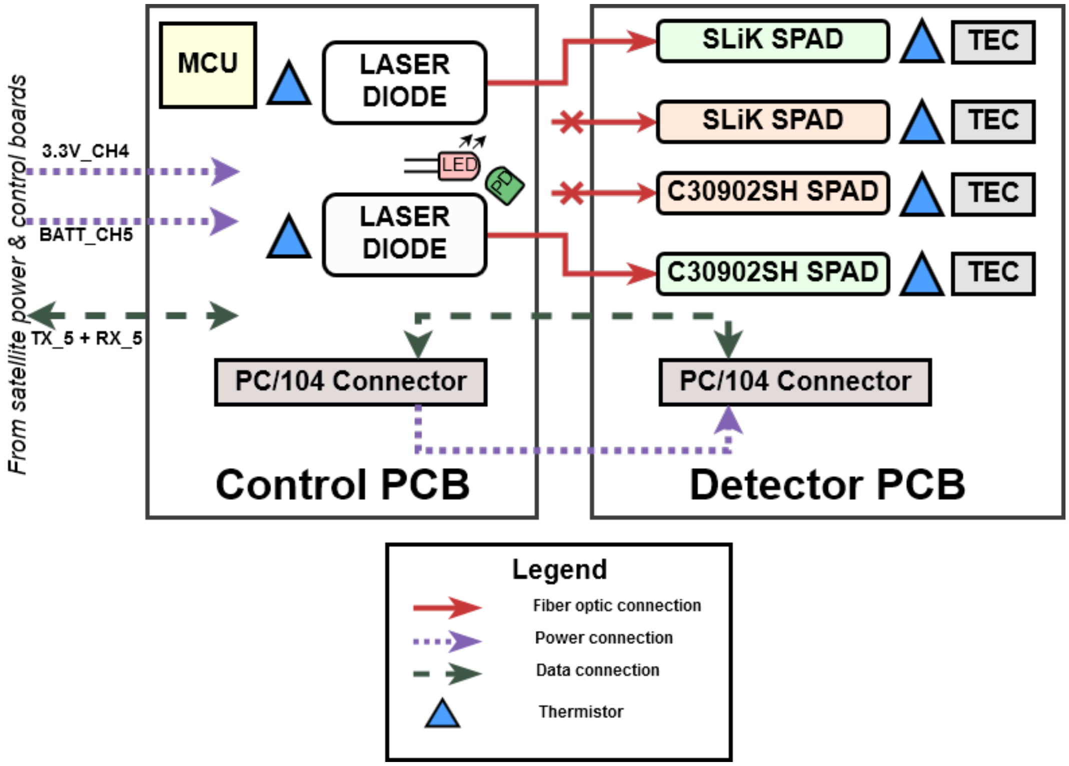


Figure 5.3: Schematic overview of the two PCBs of the annealing payload. Reprinted from [230]

Laser Diodes:

The chosen laser diodes are the two QSP-808-4 diodes from QPhotonics [231]. These diodes that are coupled with multimode fiber can output maximum 4 W of optical power at 808 nm. The diodes come in a hermetically sealed and electrically isolated package and have temperature tolerance between −30°C and 70°C.

Photodiodes and LED:

The PD is chosen from Osram Opto Semiconductors and the model is SFH-203-P [232]. The device has wide spectral sensitivity with a maximum sensitivity at 850 nm. The LED model is MTE2081-OH5 from the manufacturing company Marktech Optoelectronics [233]. The device has maximum emission at the wavelength of 810 nm with a typical output of 20 mW.

Power sources:

The control PCB contains the power system that provides the necessary power and voltages to the APL logic devices. The power system consists of two voltage regulators from Texas Instruments, TPS54427 [234], and TPS54295 [235], that have regulated output of 1.8 V and 5 V, respectively. The inputs of both regulators are connected to the unregulated power channels of the CubeSat batteries. Additionally, a third supply of 3.3 V is also available, which directly comes from the regulated channel of the satellite batteries. Of the three sources, 1.8 V delivers power to the laser diodes, while the other two supplies provide power to the rest of the APL electronics.

Control system:

The platform of the APL is planned around the ultra-low power embedded system Cypress CY8C3666 flash programmable-system-on-chip (PSoC3) [236]. It is an 8-bit 8051 processor that has integrated configurable analog and digital devices, a microcontroller, and a single-chip memory. The configurable peripherals include counters, timers, digital-to-analog converters (DACs), analog-to-digital converters (ADCs), pulse-width-modulators (PWMs), op-amps, and many others devices. The controller also allows flexible routing to any pin. This device is available as a commercial-off-the-shelf (COTS) component and has been used in space-based quantum-optics experiments [237, 238]. In the APL, the PSoC3 is located in the control PCB, and the detector PCB access it via PC/104 connector. The controller sends data to the CubeSat C&DH board via a full-duplex transceiver ADM3488 manufactured by Analog Circuits [239]. This transceiver converts the PSoC signal to the control board protocol RS422.

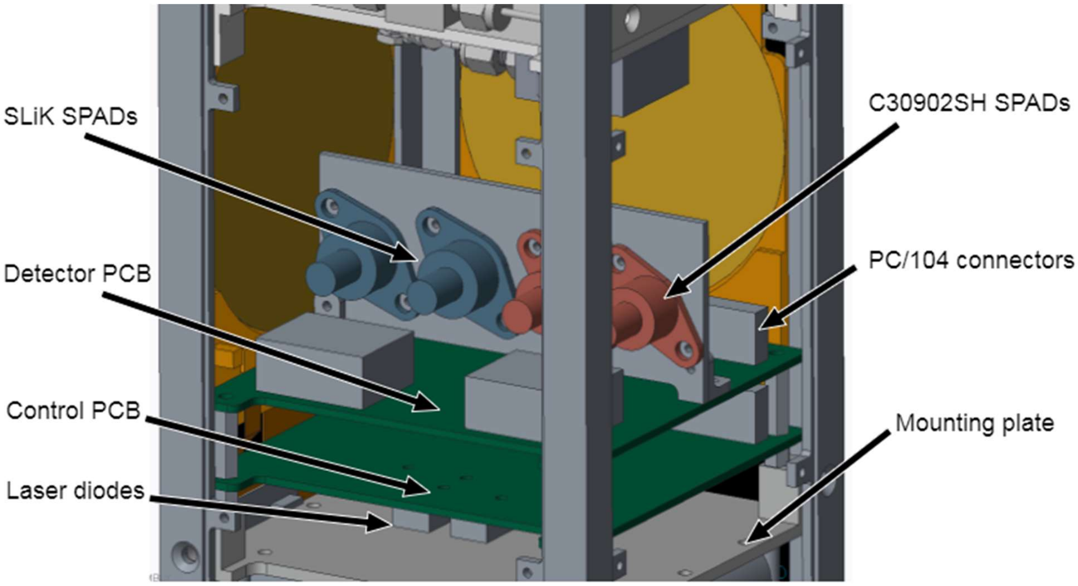


Figure 5.4: 3D model of the annealing payload. Reprinted from [228]

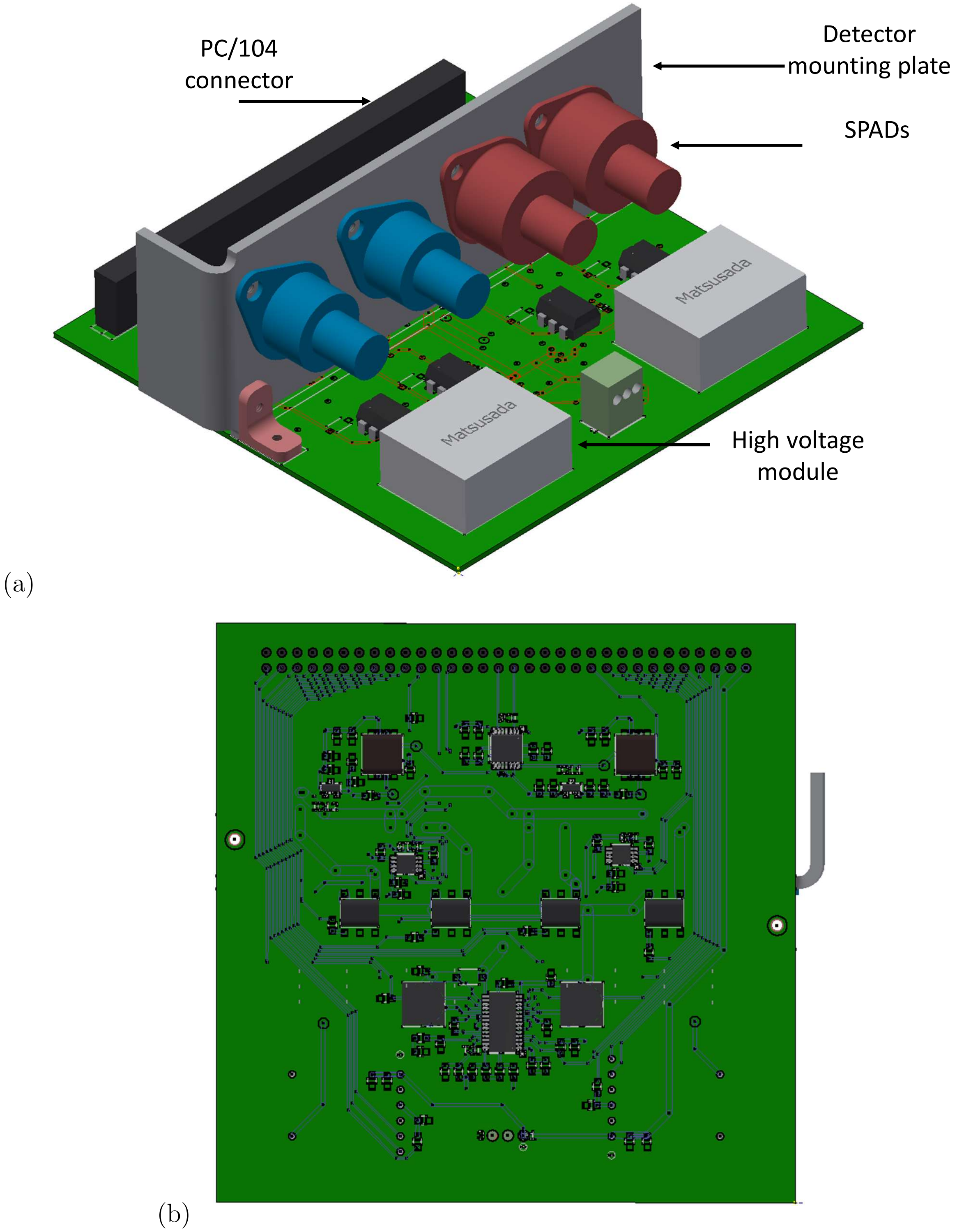
The rest of the discussion focuses on the design, implementation and test of the detector PCB. It is addressed as **'Detector Module'** throughout this chapter.

5.3 Concept of the Detector module

As mentioned in section 5.2, the DM consists of single-photon detectors, their bias, quenching, and readout circuitry, and a TEC driver. The DM is a two sided PCB. Top side holds all the large-sized components, while the bottom side accommodates most of the analog and digital electronics. Fig. 5.5 illustrates the 3D model of the two sides of the DM PCB. The components or parts chosen for the module are not all the way to space-class because the satellites in LEO are mostly exposed to the radiation when they pass the south atlantic anomaly. Therefore, we choose the parts particularly the automotive and military class components which are better than consumer-class.

As seen in Fig. 5.5(a), the PCB contains four detectors of models Excelitas SLiK and Excelitas C30902SH. Two detectors of each model are mounted on an additional piece of aluminium mounting plate, which is attached with the DM PCB. All the detectors are coupled with a fiber connector that facilitates direct fiber connection to the laser diodes.

The DM PCB contains two high-voltage supplies (HVS) to provide the necessary bias voltages to the Si-SPADs. Usually, the SPAD bias voltages vary from 200 V to more than



(a)

(b)

Figure 5.5: 3D model of the Detector module. a) The top-side view, b) The bottom-side view.

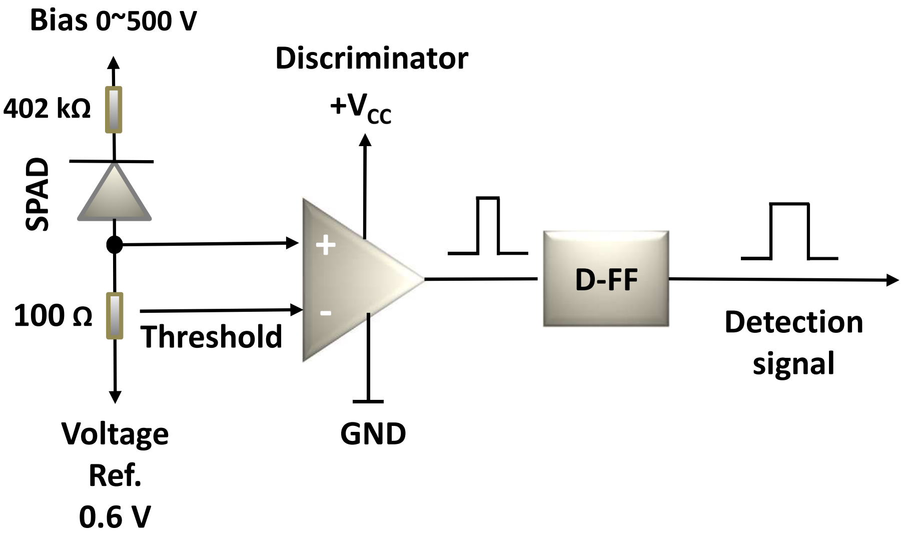


Figure 5.6: The quenching and readout circuits of the SPADs

400 V, depending on the detector samples. So, we choose ultra-compact TZ-0.5Z HVS from Matsusada Precision [240] that can supply output voltages up to 500 V which is achievable only by a maximum of 2.5 V input control voltage. Each HVS provides bias voltages to two SPADs. The high voltages are fed to the SPAD cathodes' via four solid-state relays AQV216SX manufactured by Panasonic [241]. The relays can drive output voltages of 600 V with a peak load current of 40 mA. The DM provides ways to turn ON any SPADs by activating their respective relays, although we will activate one detector at a time to save power.

Figure 5.6 illustrates the quenching and readout circuits for the detectors. This passive quenching circuit (similar to the circuit explained in section 4.3.2) uses a quenching resistance of 402 kΩ. This simple circuit is best suitable for satellite-based quantum-receiver because of its robustness. Moreover, it provides protection against sudden current surge caused by the charged particles, unexpected high voltage spike, or bright light illumination. This circuit can give maximum detection rate of 0.2–0.4 MHz which is sufficient for the QKD missions [36]. In addition, its longer dead-time, around 0.5 µs to more than 1 µs, gives enough time for afterpulse suppression.

For the readout circuit, we choose discriminator RHR801 (from STMicroelectronics [242]) that distinguishes avalanche pulses with typical amplitudes of 400 to less than 1 V from a pre-set threshold. RHR801 is a very high-speed comparator having a sharp rise/fall time of 1.1 ns. Therefore it can reliably discriminate avalanche pulses with typical width of around 5–10 ns. Another reason for choosing RHR801 is its tolerance to radiation.

Its radiation and characterization certification has full compliance with the test standard used for microelectronic devices within Military and Aerospace systems (MIL-STD883 specification).

This discriminator needs dual supplies, $+V_{\mathrm{CC}}$ and $-V_{\mathrm{CC}}$, for its operation with a restriction on its input signals, which must be within $(-V_{\mathrm{CC}}) + 0.5\ V$ and $(+V_{\mathrm{CC}}) - 1.2\ V$. That means, to read signals with the ground base voltage, we need to provide at least $-0.5\ V$ as $-V_{\mathrm{CC}}$. However, the DM PCB has no negative supply available, so we connected the $-V_{\mathrm{CC}}$ pin of RHR801 with the ground to avoid complexity in the design. But it enforced the discriminator input signals to be larger than 500 mV, which was solved by connecting the SPAD anode to a 600 mV voltage reference (ISL21070 IC manufactured by Renesas [243]) instead of the ground. With this approach, the generated avalanche pulses oscillate over 600 mV DC offset and thus solves the issues with the input voltage requirements. After discrimination, RHR801 produces 3 V output pulses that are subsequently fed to a dual-channel D flip-flop (Texas instruments 74AC11074pwr) to extend the pulse widths so the comparatively slow PSoC device can reliably read them. In DM, each SPAD has a separate quenching circuit, and two SPADs share a single readout circuit. Thus the DM PCB has only two readout circuitry to process avalanche signals from four SPADs.

The module also includes a TEC driver circuit to control the temperature of the SPADs via their in-built TECs. This circuit uses a highly compact MAX1968 driver IC from maxim integrated [244]. The driver adjusts the current flow through the TECs to reach a specific temperature. The driver circuit also includes four MOS-FET switches (G3VM-21HR) to select individual TECs and allow current flow only through that particular one. These switches can drive maximum current of 2.5 A in both directions.

5.4 Implementation of the detector module

During the process of design and implementation of the detector module (DM) for the CAPSat mission, we developed three separate DMs. Most of the major components and devices in the DMs are similar except a few changes made in the mechanical structures. Each DM is built to serve individual purposes. The complete implementation and test processes are divided into three different phases. These are:

1. **Phase I: Test prototype DM1**
   Significant amount of work related to the design and the development process has been done in this phase. We built the prototype detector module (DM1) to test and

verify the operation of the detector module, maintaining the CubeSat form factor. The tasks that are performed in this phase are

i. Deciding number of detector channels for the APL of the CAPSat.
ii. Choosing suitable components tolerant to the space environment.
iii. Designing the SPAD bias and quenching circuits, and temperature controller.
iv. Testing the sub-circuits of the DM PCB, and
v. Finally, implementing DM1 integrating all the sub-circuits to verify the proof-of principal operation of the board.

2. **Phase II: CAPSat detector module DM2**
   DM2 is the flight version of the detector module that will be sent in the CAPSat mission. It is developed considering the launching vibration and the space environment (explained in chapter 3). In DM2, a few changes are made in the circuit and also in the PCB dimension from the DM1 to fit it into the satellite bus (Illinisat-2 bus) along with the other payloads. DM2 will provide data from the experiment performed in the orbiting satellite. It is now assembled with the APL control board that is developed by the UIUC team to form the complete annealing payload.

3. **Phase III: Detector module DM3 for test in the high vacuum**
   The third detector module (DM3) is also a flight version module. It is prepared and assembled at IQC in the similar manner that were maintained during the DM2 processing. We built DM3 to continue further ground tests of the module. We will verify the performance of the module in ultra-low pressure using a thermal vacuum chamber (TVAC), which will be performed at the IQC. Prior to launch, this test will allow us to analyse and confirm the behaviour of the module materials and electronics in the vacuum that it will experience in space.

5.4.1 The test prototype DM1

We first breadboarded the individual sub-circuits of the module and verified their operation. It is mentioned earlier that the APL design and its control functions are devised around an embedded system Cypress CY8C3666 PSoC3. However, in the APL the PSoC3 is located on the control PCB, which is not available to us until the two boards are assembled together. Therefore we used a PSoC3 development kit CY8CKIT-030A to test the control functions of the DM1 prototype board. An Integrated Design Environment (IDE) software, *PSOC*

Creator enables configuration of the PSoC3 hardware and firmware concurrently. The control of the DM circuitry is discussed below.

SPAD circuits and their control

PSoC3 control signals to the detectors' bias and readout circuit are illustrated in Fig. 5.7. The DM1 PCB contains two such circuits for driving four SPADs. We see in the figure that a single high-voltage supply (HVS) provides bias voltages to two SPADs via two switches (SW1, SW2). Two signals from the PSoC3 drive HVS's output. First, a digital active Low input (I/O) activates the HVS, and then an analog signal ranging between $0-2.5\ V$ drives HVS's output from $0\ V$ to $500\ V$. A PSoC3 voltage-DAC (VDAC) provides the analog signals to the HVS. Its output voltage is then simultaneously fed to the input of the two SWs, which have good electrical isolation between its input and output. The bias voltages are forwarded to the SPADs when the SWs are activated by the PSoC3. With a sufficient bias voltage, the detectors get ready to generate avalanche pulses. These signals are then compared with a pre-set threshold (THR) in the discriminator (DISC). The THR value is provided by a PSoC3 VDAC which is little larger (around $50-200\ mV$) than $600\ mV$. For each avalanche event, DISC produces $3\ V$ output pulse with a narrower width, $\approx 10\ ns$. These are broadened using a D-FF so that the PSoC3 can properly read the signals. An RC circuit at the D-FF defines the width of the pulses. The values of R and C are chosen such that the pulse width reaches around 100 ns. Finally, the total number of pulses are estimated by a counter configured in the PSoC3. Thus this circuit drives two SPADs and provides their avalanche counts. Since, one SPAD will run at a time, sharing the readout between the SPADs does not cause any problem. We just need to adjust the bias voltages and the DISC thresholds during the operation of each SPAD.

Temperature control

Figure 5.8 illustrates the control of the four in-built detector TECs, and the TEC driver (MAX1968) by the PSoC3. The MAX1968 can drive current in both directions: positive current for the cooling and negative current for the heating of the detector. Four current switches are used to select a particular TEC to which cooling/heating current will flow. Thermistors attached with the SPAD (shown separately in the figure) measure the SPADs' temperature as a voltage. A PSoC3 analog-to-digital converter (ADC) reads these thermistor voltages. Then a piece of C code written in the PSoC creator uses these readings to reach the expected temperatures. The code is known as PID control loop (discussed later).

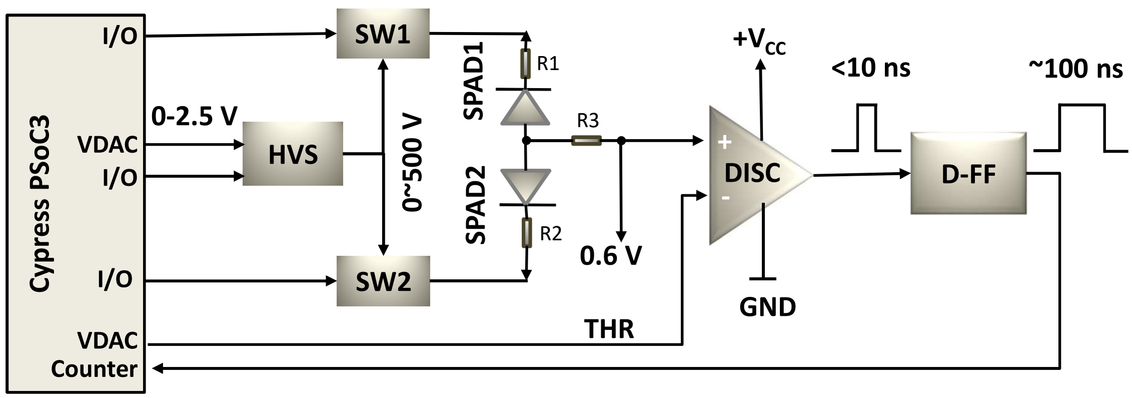


Figure 5.7: Block diagram of the controlling SPAD bias and readout circuit operations by PSoC3. HVS: high voltage supply; SW1, SW2: switches; DISC: discriminator; D-FF: D flip-flop; PSOC3 I/O: general purpose input/output; VDAC: voltage digital to analog converter.

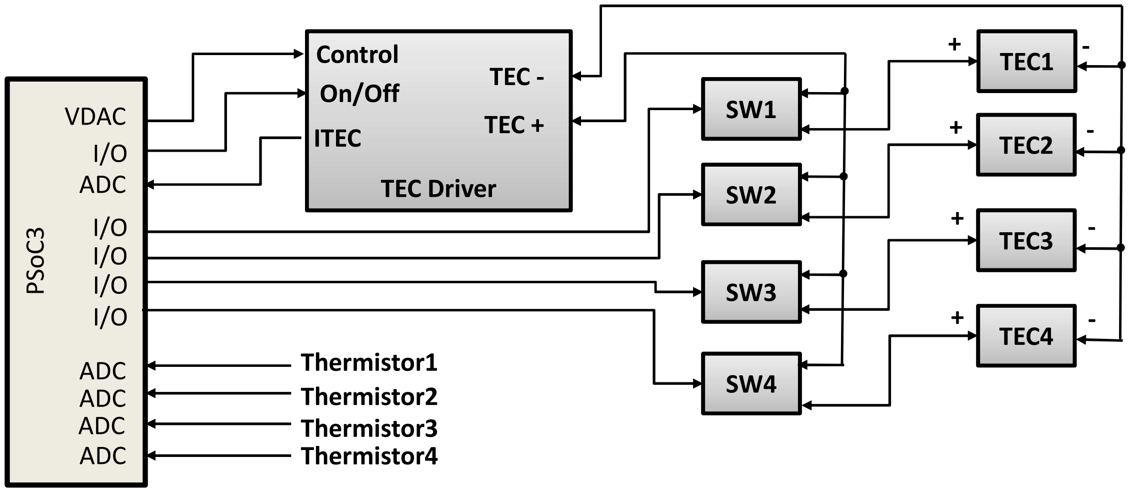


Figure 5.8: Schematic of the signal flow for temperature control. The Opto-coupler switches select the respective TECs when they receive an active high logic input from PSoC3. The active mode of the TEC driver is also chosen by sending an active high signal from the processor. The thermistors measure the temperature of the SPADs. Detail operation is in the text.

It sets a voltage on a VDAC to send appropriate *Control* voltages to the TEC driver based on the thermistor readings and the given expected temperature. Then the *Control* voltage adjusts the TEC current flow that is necessary to reach a particular temperature. The TEC driver also provides a way to measure this current flow via ITEC which can be read by a PSoC3 ADC.

DM1 PCB

We integrated all the aforementioned sub-circuits and built the prototype board DM1, as shown in Fig. 5.9. The size of the DM1 PCB is 95 mm × 95 mm × 40 mm (L × W × H). It is built to test the proof-of-principal operation of the module. The DM includes two fiber coupled SLiK SPADs and two C30902SH detectors that are without fiber connectors. Having fiber connectors with the SPADs were not mandatory for this prototype, since the module is built mostly to test the control functions. The SPADs are mounted on an aluminum (Al) plate so that it can dissipate the produced heat from the detectors. The rear side of the TEC heated up quickly during the cooling of the SPADs via TECs. To radiate this heat, usually, the detectors need to be attached with a material that has good thermal conduction property. Aluminum is chosen because of its good thermal conductivity, which is more than 220 W/mK over a wide range of temperatures [245]. This material has been used previously in other SPAD modules built in our lab to radiate the excess heat [37, 38, 47]. To radiate this heat energy away by the satellite radiator, our primary concept was to attach the Al mounting plate with a wall of the satellite bus. Since DM1 will be operated in lab without the satellite bus, we attached a small heat sink at one side of the mounting plate for heat dissipation, illustrated in Fig. 5.9. The mechanical structure of the mounting plate and the brackets are depicted in Fig. 5.10. Two L-shaped brackets are used to attach the mounting plate with the PCB.

After mounting the detectors on the Al plate, their pins coming through the holes are connected to the PCB using additional vertical wires, as shown in Fig. 5.11. We create an isolation of the pins from the Al plate by inserting wire jackets around each pin that have connections with the PCB. The quenching resistors are also vertically connected with the cathode of the SPADs to keep them as close as possible to the cathode. It is because this approach reduces the parasitic capacitance, which in turn reduces the recharge time of the detectors.

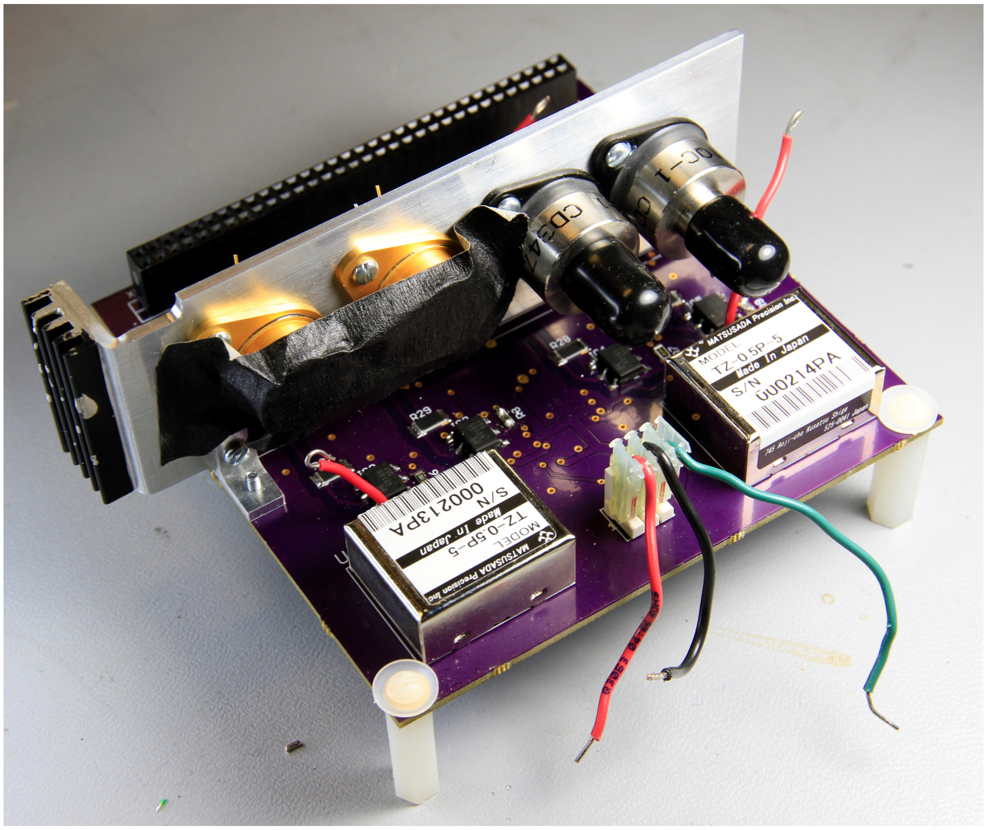


Figure 5.9: Test prototype of the detector module DM1.

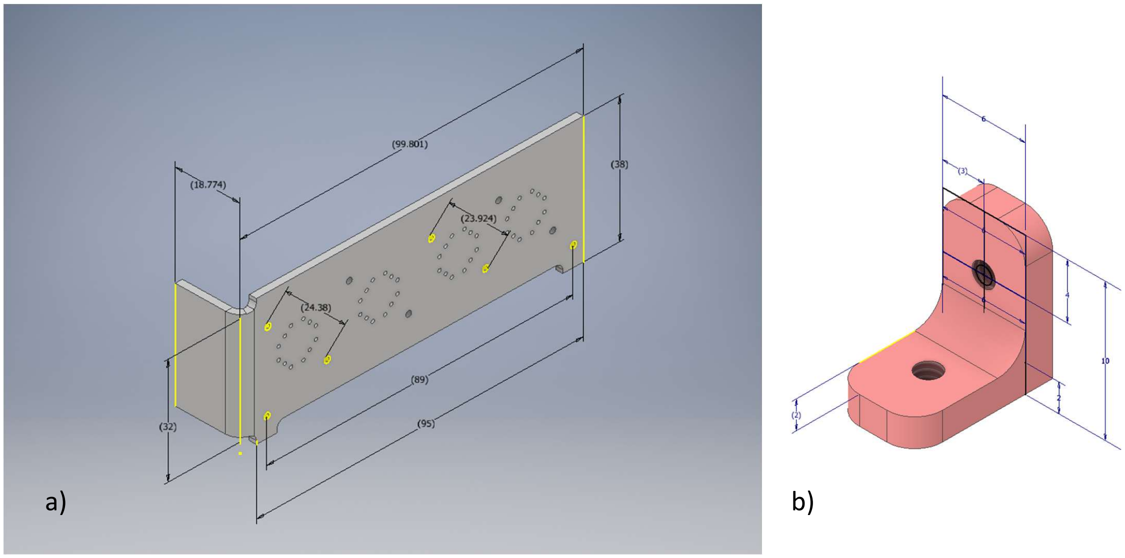


Figure 5.10: DM1 Detector mounting plate. a) mechanical structure of the Al plate, and b) the brackets used to secure the mounting plate with the PCB.

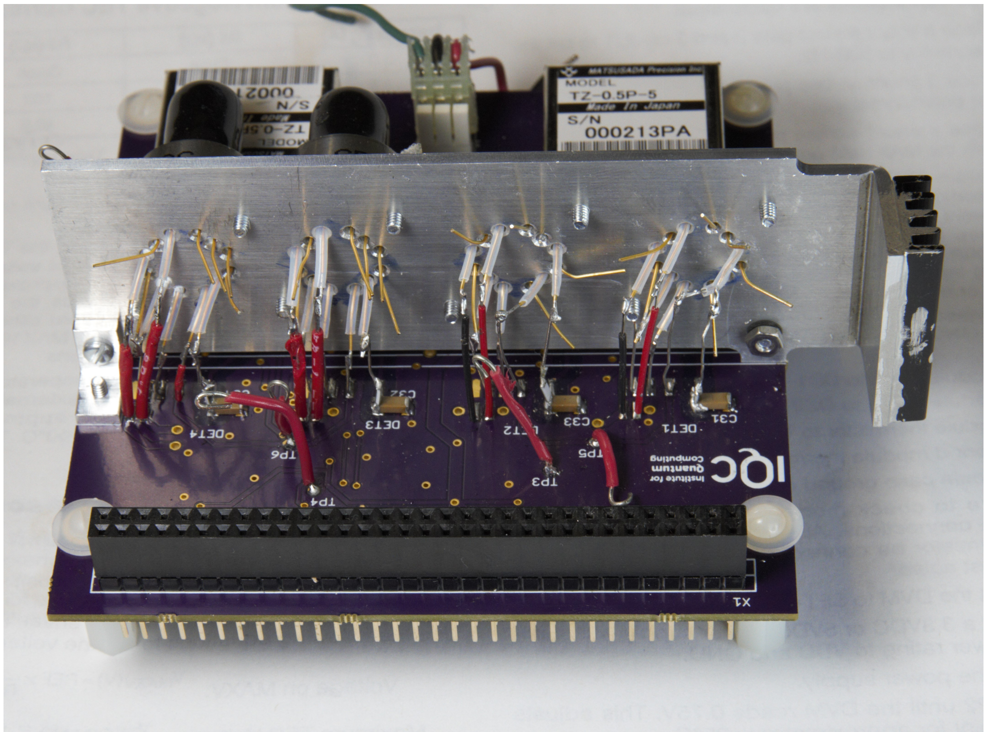


Figure 5.11: Detectors pin connections with the PCB.

Test setup

The operation of the DM1 is tested using a Cypress CY8CKIT-030 PSoC3 development kit. The test arrangement is shown in Fig. A.1. A programming interface is provided with the development board (DB) to program the PSoC3. It interfaces the PSoC3 processor with the PC through a USB port. The same programming USB also supplies power to the development board. PSoC3 component configuration and firmware development are accomplished using an Integrated Design Environment (IDE), PSoC creator software. The very first step is to create a schematic design in the creator workspace adding the required analog or digital components on it. Then the peripheral configuration, routing and pin assignments are also accomplished using the creator. The operation and schedules of the peripherals are defined by a C code that is programmed in the PSoC3 via the programming USB. Before starting any operation, it is important to ensure that the development board and the DM1 PCB both share a common ground. During the test, we provide the power to the DM1 PCB from an external supply.

The creator schematic for the detectors bias and readout circuit is illustrated in Fig. 5.13. It shows the required components for controlling the detector circuits. Two Control Registers function as switch. The register 'SW_HV1' activates the high-voltage supply

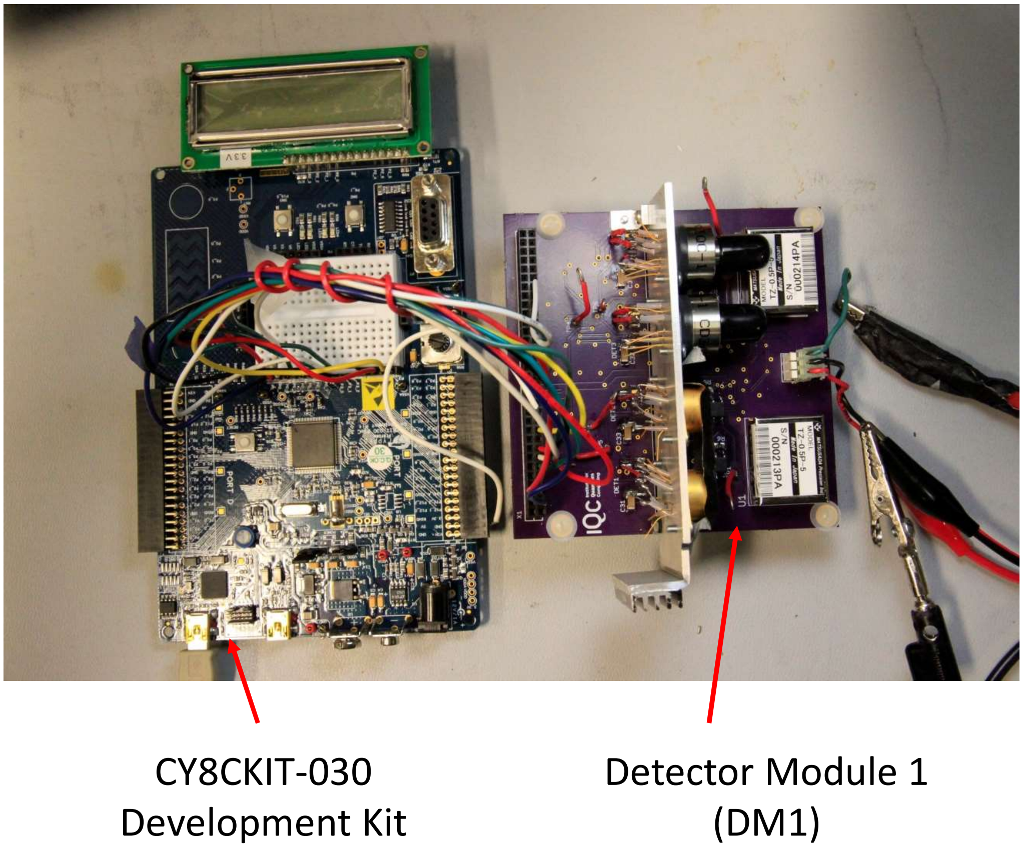


Figure 5.12: PSoC3 development board is connected with the DM1 to test control functions.

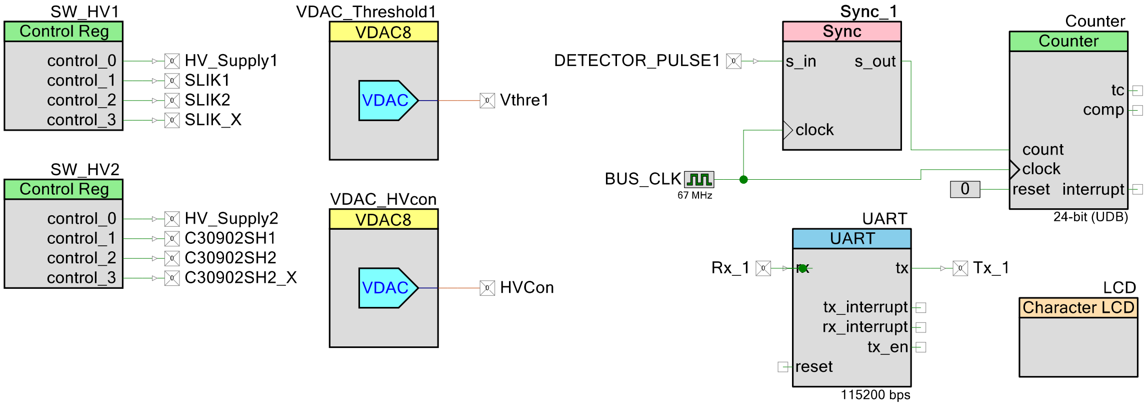


Figure 5.13: Schematic design in the PSoC workspace to control the SPAD bias and readout circuit.

(HVS) that provides bias voltages to the SLiKs, and the corresponding switches of the SLiKs. Similarly, ’SW_HV2’ turns ON the second HVS and the two corresponding switches of the C30902SH detectors. Detector switches need Logic ’1’ for their activation, while the HVS requires logic ’0’ to turn it ON. With this approach, we have a flexibility to turn ON separately any of the detectors, but one detector will be activated at a time to save power consumption. After activating a HVS, the component ’VDAC_HVcon’ sends the analog control voltages to the HVS input to get an expected bias voltage. Then the ’VDAC_Threshold1’ provides the required threshold voltages to the discriminator. We need following sets of code to get high bias voltages from the HVS, and the SPAD avalanche signals.

```
SW_HV1_Write(1001);%/*4 bit: SLIKX,SLIK3,SLIK2,SLIK1,HV_1; 1001 is ...
    the rest condition,*/

SW_HV2_Write(1001);%/*4 bit: C0902SH2,C0902SH1,HV_2;  1001 is the ...
    rest condition,*/

VDAC_HVcon_Start();%/* Sets control voltage of HV1*/
VDAC_HVcon_SetRange(VDAC_HVcon_RANGE_4V);
VDAC_HVcon_SetValue(86);%/*actual value is (setvalue)*16 mV*/


VDAC_Threshold1_Start();%/* Sets threshold value of Discriminator*/
VDAC_Threshold1_SetRange(VDAC_Threshold1_RANGE_4V);
VDAC_Threshold1_SetValue(20);%/*actual value is (setvalue)*16 mV*/
```

In this code, for a VDAC the ’_SetValue’ corresponds to a value = ’_SetValue’ × 16 mV. The HVS output increases by around 3 V for each increment of the ’_ SetValue’. Table 5.1 lists several HVS output voltages at different ’_SetValue’, illustrating a tentative required ’_SetValue’ to reach a certain bias voltage. On the other hand, ’_SetValue’ for the ′VDAC_Threshold1′ is simply found by ′Expected Threshold value/16 mV′. Since the SPAD avalanche signals have DC offset of 600 mV, the discriminator threshold was set around 50 to 200 mV larger than the signals’ DC offset.

After setting a fixed value for the threshold, we increase gradually the HVS control signal (’VDAC_HVcon_SetValue’) to raise the SPAD bias. The SPAD output is monitored in a oscilloscope (OSC). Whenever, the bias reaches to SPAD’s breakdown voltage, small avalanche signals (around 15 mV) start to appear frequently on the OSC display. This process is continued to measure the breakdown voltages for all the SPADs. Table 5.4 summarizes the breakdown voltages and the pulse widths at 20 V excess bias (the voltage

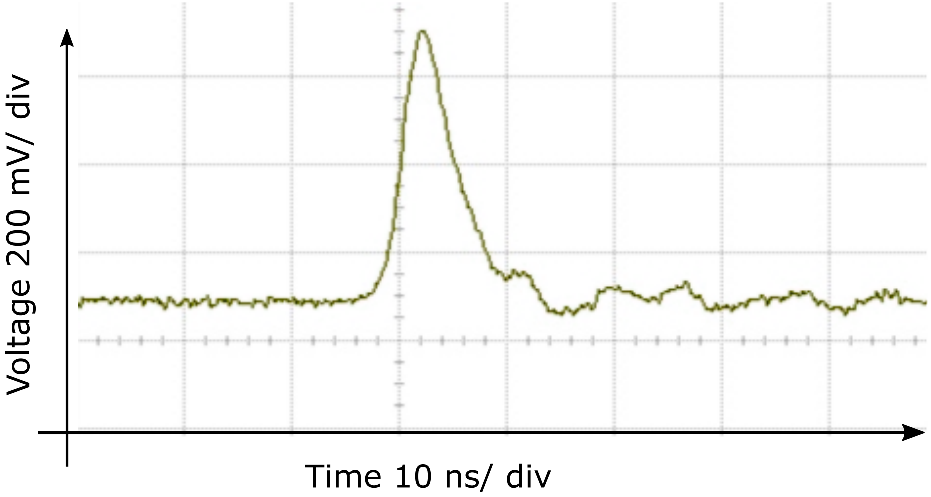


Figure 5.14: The avalanche pulse generated by Excelitas C30902SH at 20 V of excess bias.

above the breakdown) of the DM1 detectors. The amplitude of the signals increases with increased bias voltages. Fig. 5.14 shows an avalanche pulse produced by a Excelitas C30902SH detector at a 20 V excess bias, where the signal is around 600 mV with a width of $\approx$ 5 ns. Then to measure the total number of avalanche events, a 24-bit counter is configured in the PSoC creator. The counter device works together with a Sync device (shown in Fig. 5.13) to properly estimate the number of events. The Sync helps to transfer signals from a different clock domain to the destination clock domain by lining up the signal transition.

Table 5.1: HVS output voltage for different '_ SetValue'

'VDAC_HVcon_SetValue'	**HVS output (V)**
50	150
70	210.8
100	301.8
130	392.4
140	422.7
150	453
160	483.6

Table 5.2: A summary of DM1 SPAD parameters

SPADs	Breakdown Voltage (V)	Pulse width at the discriminator* (ns)
C30902SH_1	259	9.8
C30902SH_2	256	5.9
SLiK_1	314	7.3
SLiK_2	302	7.5

* Pulse width is measured at 20 V excess bias and at 704 mV threshold voltage.

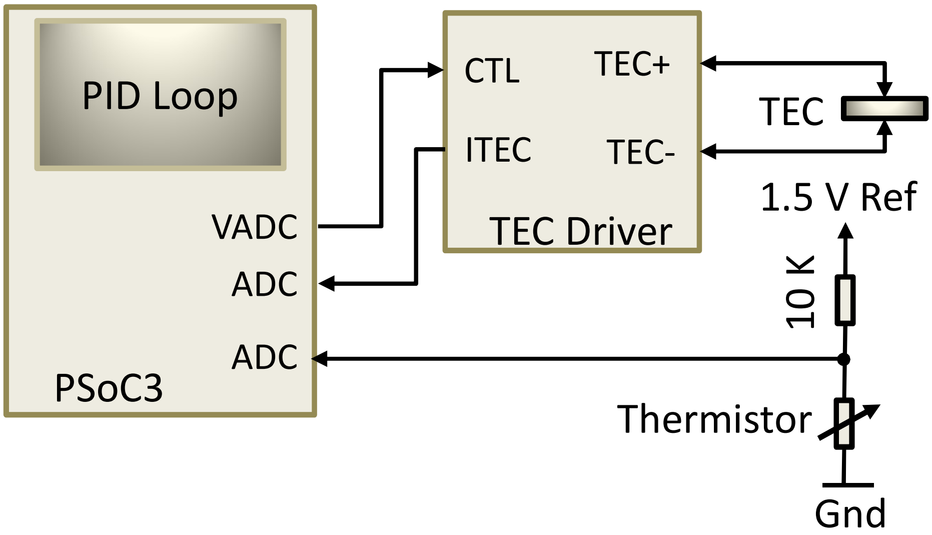


Figure 5.15: TEC temperature Control by PSoC3.

5.4.2 TEC temperature control

The schematic of TEC temperature control is illustrated in Fig. 5.15. The TEC driver adjusts the amount of current through the TEC, depending on the input CTL voltage, to reach a certain temperature. Driver's ITEC pin enables us measuring the TEC current as a voltage which is read by a PSoC3 ADC. An integrated thermistor constantly senses the SPAD temperature, changing its resistance with the variations in temperature. Therefore, the voltage drop across the thermistor (V_{therm}) also varies. A PSoC3 ADC reads the instantaneous V_{therm}, which is converted into temperature in the following way. First, we calculate the thermistor resistance from its measured V_{therm} using eq. (5.1).

$$\begin{aligned} R_{\text{therm}} &= \frac{V_{\text{therm}}}{I_{\text{therm}}} \\ &= \left[V_{\text{therm}} \times \frac{10\ k\Omega}{(V_{\text{Ref}} - V_{\text{therm}})} \right] \Omega \end{aligned} \tag{5.1}$$

where I_{therm} is the current flowing through the thermistor, and V_{Ref} is the reference voltage to which a combination of 10 $k\Omega$ resistance and the thermistor is connected, as seen in Fig. 5.15. Then the resistance is converted into temperature using the following equation.

$$T(K) = \frac{\beta}{ln\left(\frac{R_{\text{therm}}}{r_{\infty}}\right)} \tag{5.2}$$

where β and $r_{\infty} = R_o e^{\frac{-\beta}{T_o}}$ are the thermistor characteristic parameters, which are found from the detector data sheet [151]. The parameters are $\beta = 3200$, and $R_o = 5100\ \Omega$ at $T_o = 298.15$ K, which gives $r_{\infty} \approx 0.1113$.

Once PSoC3 knows the temperature of the SPAD, a control algorithm written in **C** uses that value to reach the expected temperature. This algorithm creates a feedback loop to calibrate the value of the CTL voltage to adjust the amount of the current flow through the TEC. This loop is known as PID control loop, which is discussed later in this section.

Configuring TEC Driver

The TEC driver (MAX1968) in the DM1 is configured first to limit some of its parameters, such as the maximum differential voltage (VMAXV), the maximum TEC positive current (VMAXIP) and the maximum negative TEC current (VMAXIN). This is done by choosing appropriate values for the resistors R10 – R12, and R14 – R16 in the DM1 schematic (Fig. A.1). The limiting parameters depend on the TEC's absolute maximum voltage, maximum cooling, and maximum heating current. TEC parameters are found in the datasheet, for instance, the TECs with the C30902SH detector have the absolute values of maximum current $I_{\text{TEC(MAX)}}$= 1.4 A, and maximum voltage $V_{\text{TEC(MAX)}} = 2$ V. The parameters of the TEC and the TEC driver follow the relationships given in equations 5.3– 5.5

$$V_{\text{TEC(MAX)}}(V) = 4 \times \text{VMAXV} \tag{5.3}$$

$$I_{\text{TECP(MAX)}}(A) = + \frac{\frac{\text{VMAXIP}}{10}}{R_{\text{SENSE}}} \tag{5.4}$$

$$I_{\mathrm{TECN(MAX)}}(A) = -\frac{\frac{\mathrm{VMAXIN}}{10}}{R_{\mathrm{SENSE}}} \tag{5.5}$$

Here, R_{SENSE} is 0.05 Ω. For safe operation, the parameters of the TEC driver are chosen for the TEC voltage $V_{\mathrm{TEC(MAX)}} = 2$ V, TEC cooling current $I_{\mathrm{TECP(MAX)}} = 1$ A, and TEC heating current $I_{\mathrm{TECN(MAX)}} = 0.25$ A. The values of VMAXV, VMAXIP and VMAXIN are then used to calculate the values of the resistors R10 – R12, and R14 – R16 using the equations 5.6 – 5.8. The resistor values are summarized in table 5.3

$$\mathrm{VMAXV}(V) = \mathrm{REF} \times \frac{R14}{(R12 + R14)} \tag{5.6}$$

$$\mathrm{VMAXIP}(V) = \mathrm{REF} \times \frac{R15}{(R11 + R15)} \tag{5.7}$$

$$\mathrm{VMAXIN}(V) = \mathrm{REF} \times \frac{R16}{(R10 + R16)} \tag{5.8}$$

here REF is a fixed voltage of 1.5 V. When no current flows through the TECs, the CTL is similar to the REF voltage. A positive current flows when VCTL > 1.5 V and cooling is required. Conversely, VCTL < 1.5 V during heating and a negative current flows through the TECs. The amount of current is monitored by reading voltages at the ITEC pins of the TEC driver. If no current flows into the TEC, then the ITEC = REF. The amount of TEC current is calculated from the ITEC voltage using eq. (5.9) [244].

$$\mathrm{TEC[current]} = \frac{\mathrm{ITEC[voltage]} - \mathrm{REF}}{8 \times R_{\mathrm{SENSE}}} \tag{5.9}$$

Table 5.3: Values of the TEC driver parameter defining resistors

VMAXV = 0.5 V	R12 = 100 kΩ	R14 = 50 kΩ
VMAXIP = 0.5 V	R11 = 100 kΩ	R15 = 50 kΩ
VMAXIN = 0.125 V	R10 = 100 kΩ	R16 = 769 Ω

PID Control

We implemented a digital PID control loop that continuously adjusts its output within the loop using a feedback mechanism to control a system. Here the term 'PID' stands for

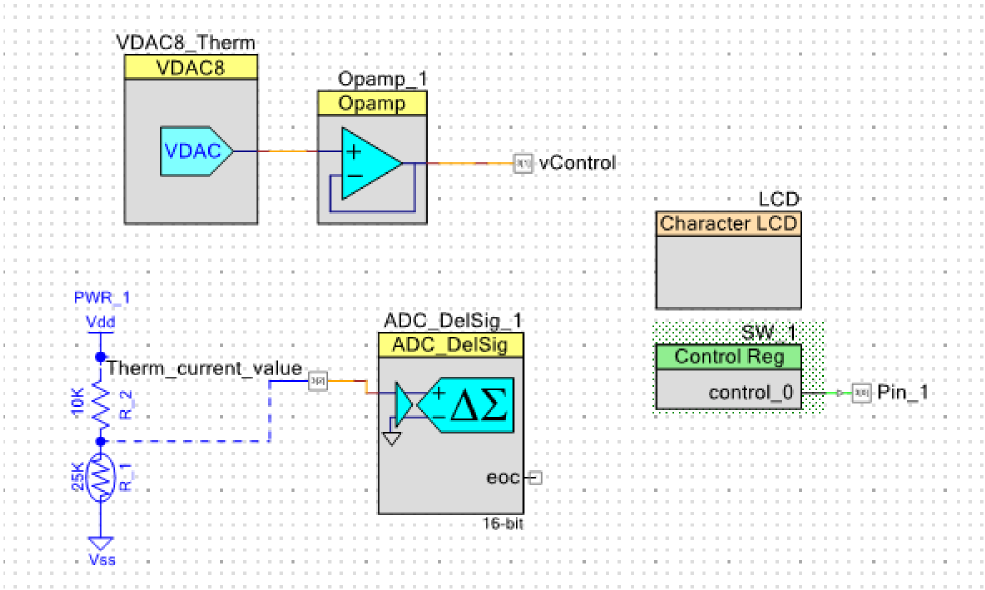


Figure 5.16: PSoC schematic for the temperature control. The components and lines in blue color are not active elements. They are just to show how the PSoC3 active elements are connected to the physical components of the DM1.

Proportional, Integral, and Derivative. We used a parallel form of PID controller [246] to control the temperature. The relation of the control variable u(t) with the PID parameters are given by

$$u(t) = K_p e(t) + K_i \int_0^t e(\pi) d\tau + K_d \frac{d}{dt} e(t) \tag{5.10}$$

where e(t) is the error or difference between the expected and the system output temperature, and K_p, K_i, and K_d are the proportional, integral and differential coefficients, respectively. Here, e(t) is the input to the PID loop, while u(t) is the loop output.

For digital implementation, we need a Z-transform [247] of equation 5.10. It is given by

$$\begin{aligned} U(Z) &= \left[K_p + \frac{K_i}{1-z^{-1}} + K_d(1-z^{-1})\right] E(Z) \\ &= \frac{\left[K_p(1-z^{-1}) + K_i + K_d(1-z^{-1})^2\right]}{1-z^{-1}} E(Z) \\ &= \frac{\left[(K_p + K_i + K_d) + (-K_p - 2K_d)z^{-1} + K_d z^{-2}\right]}{1-z^{-1}} E(Z) \end{aligned} \tag{5.11}$$

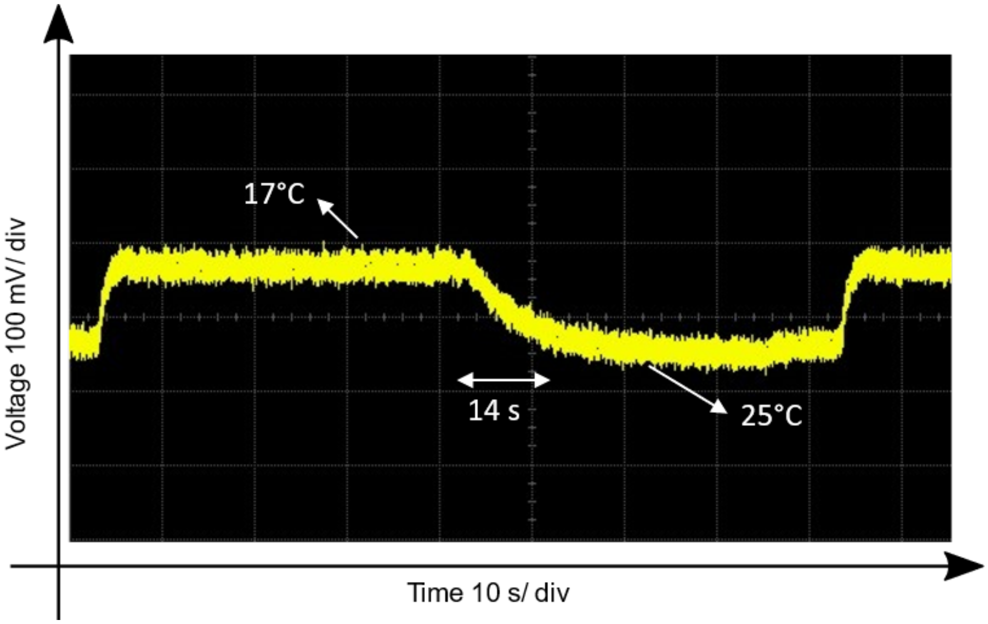


Figure 5.17: Step response of the PID loop for temperature transition between $\sim\ 8°C$. The coefficients were $K_p\ =\ 1.5$, $K_i\ =\ 0.2$, $K_d\ =\ 0.3$.

The coefficients can be defined as,

$$\begin{aligned} K_p + K_i + K_d &= K_1 \\ -K_p - 2K_d &= K_2 \\ K_d &= K_3 \end{aligned}$$

Now, equation 5.11 can be written as

$$U(Z) = z^{-1}U(Z) + \left[K_1 + K_2 z^{-1} + K_3 z^{-2}\right] E(Z) \tag{5.12}$$

Finally, the difference formula of equation 5.12 is

$$u[k] = u[k-1] + K_1 e[k] + K_2 e[k-1] + K_3 e[k-2] \tag{5.13}$$

Equation 5.13 is used to implement the control algorithm in the PSoC creator. The necessary components to run the PID loop are illustrated in the PSoC schematic, shown in Fig. 5.16. The loop reads the instantaneous thermistor voltage utilizing the ADC component and compares it with a given voltage equivalent to an expected temperature

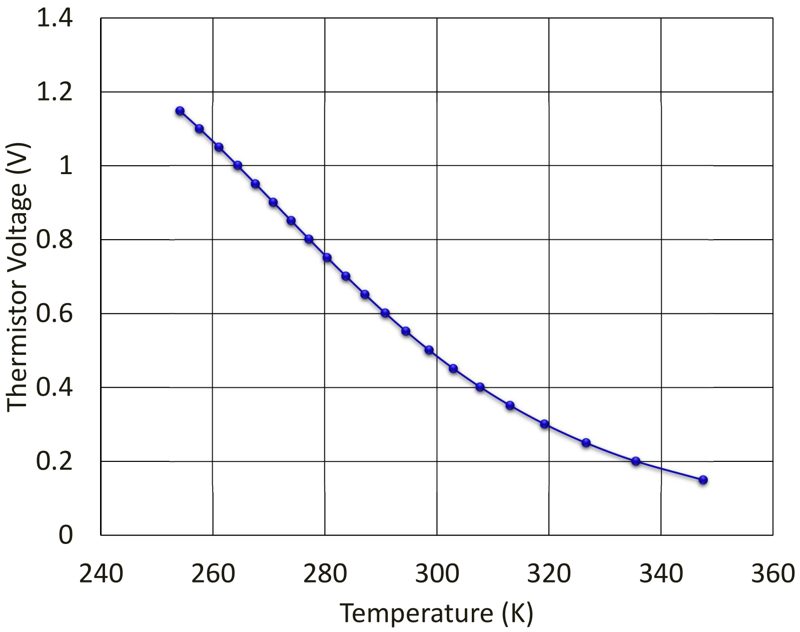


Figure 5.18: Measured thermistor voltages at various temperatures.

in algorithm. Their differences provides the error e(t). The loop keeps record of the errors from previous two iterations. Using those error values, the algorithm calibrates the CTL voltage and changes the TEC current. The loop coefficients K_p, K_i, and K_d were manually tuned to achieve the optimum result. For tuning the PID coefficients, we observed the loops' step function responses at different coefficient values and the overshooting at the instances of reset of the program. First, we tuned only the K_p parameter, keeping the other two parameters zero. With this setting, the PID loop never reaches to its expected value. Then the PI parameters K_p and K_i were tuned, which helped to reach the desired temperature, but the rising and falling time between the two voltages were slow. Tuning K_d parameter along with the other two parameters provided a better loop performance. The optimal performances was found for $K_p = 1.5$, $K_i = 0.2$, and $K_d = 0.3$ for a loop duration of 1000 ms. Fig. 5.17 shows the step response of the loop for temperature changes between $17°C$ and $25°C$. The voltage difference was 100 mV, where the low-to-high steady state transition was around 2 s and the opposite transition took around 14 s. So the PID loop needs longer duration for heating. However, this duration will not affect the performance of the experiment since in the annealing payload the requirement of changing temperature is only as settings before performing any particular operation.

Once the optimum parameters are found, the PID loop together with the hardware arrangements shown in Fig. 5.15 work as a temperature controller. We used this controller to vary the SPAD temperatures utilizing their integrated TECs. The corresponding measured average thermistor voltages and currents are illustrated in Fig. 5.18 and Fig. 5.19, respectively. Thermistor voltages are approximately similar to the given set voltages used in the PID loop, which were incremented at a regular interval of 0.05 V. At the cooling temperatures, the measured temperatures are almost similar to that of the set values. In contrast, these values gradually go off from the set ones as the temperature increases. At the linear region of the thermistor voltages, the temperature drops approximately 3.4 K for each 0.05 V of voltage increment. Over the temperature variations ranging between 347.5 and 254.2 K, TEC current flow varied from (-0.20) to 0.62 A. We restricted the TEC current (both in hardware and in PID loop) to -0.20 A for the heating to avoid overshooting above TEC maximum heating current, which is -2.50 A. So, by using a larger current limit, it is possible to achieve a higher temperature. The estimated thermistor resistance values were extended from 1.1 to 32.6 kΩ over the temperature range of 347.5 to 254.2 K, as shown in Fig. 5.20.

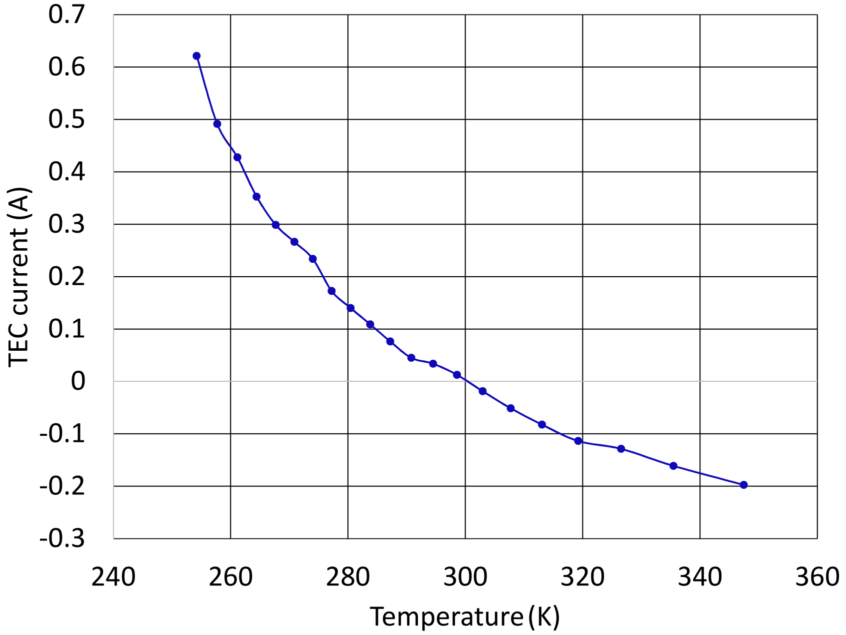


Figure 5.19: TEC current at various temperature

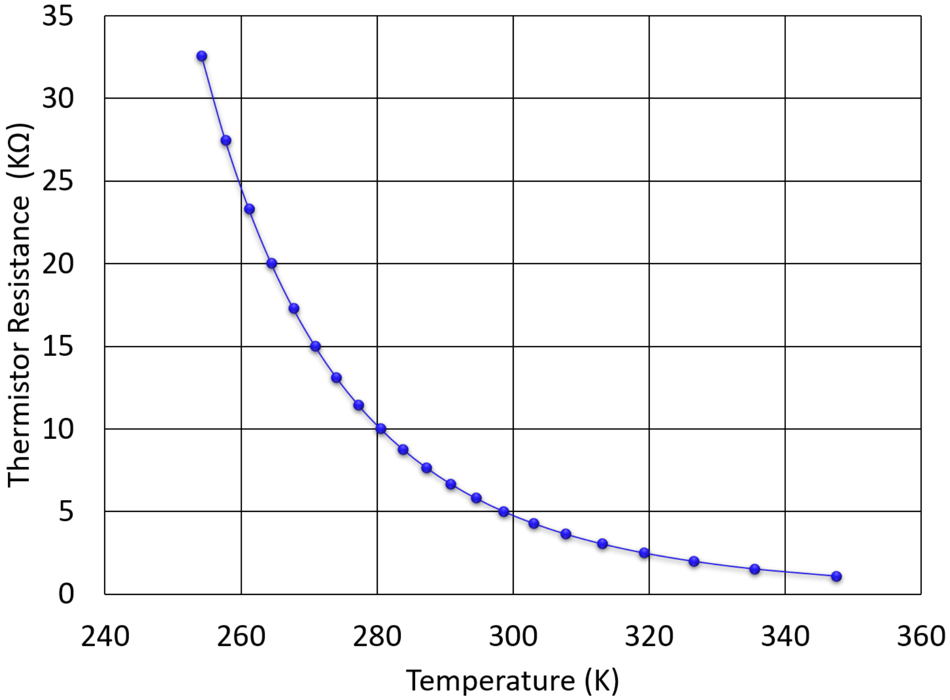


Figure 5.20: Resistance values of the thermistor at various temperatures

Power consumption

Table 5.4 outlines the power consumption by the individual major components of the detector module. It shows that when only a single SPAD device is active, maximum power consumption by the detector PCB was around 2.5 W. This measurement was taken at the high-voltage supply of 485 V and the TEC current flow for $-19°C$. So the power consumption is well below the allocated total power budget of $5-7$ W for the annealing payload.

Table 5.4: Power consumption by major components of the DM1 PCB

Device	Supply Voltage (V)	Current flow (mA)	Power (mW)
High-voltage supply at at V_{out} 200 to 485 V	5	36.7 to 85	183.5 to 225
Discriminator	3.3	8.94	29.5
High-voltage switch	3.3	5	16.5
current switch	3.3	6	20
TEC driver	3.3	659*	2175

* measurement was taken at $-19°C$. Usually, a higher current is required during cooling.

5.5 The CAPSat detector module DM2

DM2 circuits and most of the components are similar to DM1. The main difference of this module is that it is prepared and developed considering the extreme weather conditions in space, such as high-vacuum and high-energy particle radiation. During implementation, we choose carefully each element of DM2, such as the connecting wires, the jackets of the wires, soldering materials, and thermal pasts. The hardware and electronics have gone through several cleaning processes to minimize the contamination. DM2 structures are then assembled in a clean room with filtered airflow at positive pressure to avoid contamination and dust. DM2 will go through several tests and certification procedures to qualify for the actual launch.

The PCB chosen for the DM2 is FR4 PCBs with tight tolerance in trace widths and spacing (4/4 mil) to ensure the quality of the boards. The electrical components are soldered in the PCB using $Sn_{60}Pb_{40}$ leaded solder alloy which is listed in the Electronics Assembly Standard, IPC-J-STD-001D [248] as an acceptable alloy for space applications. Due to their lower melting point, leaded alloy prevents delamination, breaks in the internal paths, and blistering in space. We used Polytetrafluoroethylene (PTEF Teflon) insulated silver-coated 30 AWG copper wires for the connections of the SPAD pins with the PCB. This type of wires has good tolerance to high temperatures, low outgassing properties, and high resistance to moisture [249].

The dimension of the PCB is modified to fit it inside the satellite bus. The PCB dimension is 90 mm × 90 mm × 52 mm (L×W×H) with a 8 mm groove at one side (shown in chapter A). The groove is made to pass the fibers to the detector board from the control board lasers. Once completed populating the PCB with the components, the PCB was cleaned in an ultrasonic bath using isopropyl alcohol 99% (IPA) solution that cleans out oils

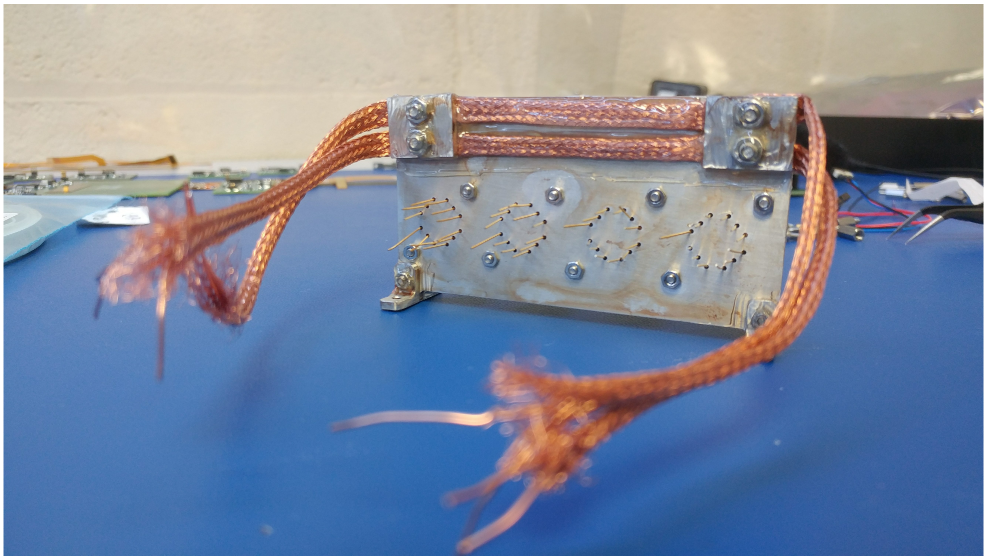


Figure 5.21: Flexible thermal braids pasted with the mounting plate for thermal propagation to the satellite.

and flux from the PCB. Then the mounting plate loaded with the detectors is assembled with DM2 PCB in a cleanroom (ISO 100 standard). Further handling and testing of the module have been performed in the cleanroom. A conformal coating of around 0.5 mm is hand-painted on the PCB to protect electronics from corrosive contamination, mechanical vibration, or shock. We used Arathen 5750 LV as a conformal coating because of their good resistance to heat and humid conditions, as well as their low outgassing properties [250].

Preparation of detector mounting plate

We added a few changes on the Al detector mounting plate. The new dimension is 90 mm × 2 mm × 50 mm (L×W×H), which is shown in fig. A.3. Our initial plan was the Al plate will be attached with the satellite walls so the heat waste generated by the detector propagates to the satellite bus. However, the CAPSat walls are not thermally conductive, only the corner frames (made with Al) of the Illinisat-2 bus are thermally conductive. We therefore devised a new design for transferring the heat away from the mounting plate. We screwed a pair of flexible copper braids at the top of the mounting plate as shown in Fig. 5.21. Also a pair of bare copper wire is inserted in each braid to increase the capacity of thermal propagation. The braids and the screws are then pasted to the plate using thermal epoxy to ensure firm contact of the braids with the plate. The two ends of the braids will be attached with two corner frames of the bus using thermal epoxy, once the payload has loaded into the satellite bus. The flexible braids are chosen so that it can tolerate the launching vibrations without damaging the thermal contact. After preparing the mounting plate, this structure was baked in a vacuum oven at 125°C for 5 hours. Then it was given an ultrasonic cleaning in a solution of Acetone for 15 minutes and subsequently in a IPA solution for another 15 minutes. This process ensures removing any greasy deposits without leaving extra residue. After cleaning, a anodizing coat is applied using a pen (BONDERITE M-CR 1132) on the Al to prevent its oxidization due to space radiation.

Assembling DM2

We load four fiber coupled Excelitas detectors (two C30902SH and two SLiK) in the detector module DM2. The completed detector assembly is now given to the UIUC team to process further tests and verification before its actual launch. Fig. 5.22, shows the flight version of the annealing payload with the two PCBs stacked together. As of this writing, the CAPSat has successfully passed the Orbital Debris Assessment Report performed by NASA and the APL has passed phase 2 of the international space station safety panel. Its anticipated launch is in 2020.

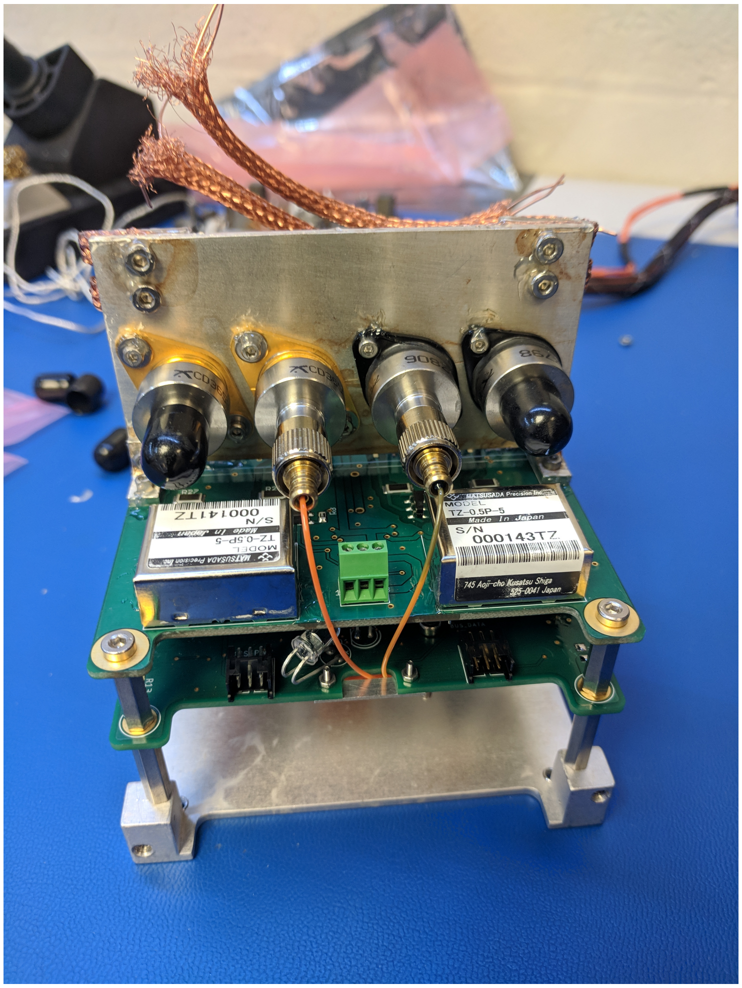


Figure 5.22: Flight version of the CAPSat annealing PCBs stacked together. Courtesy to University of Illinois.

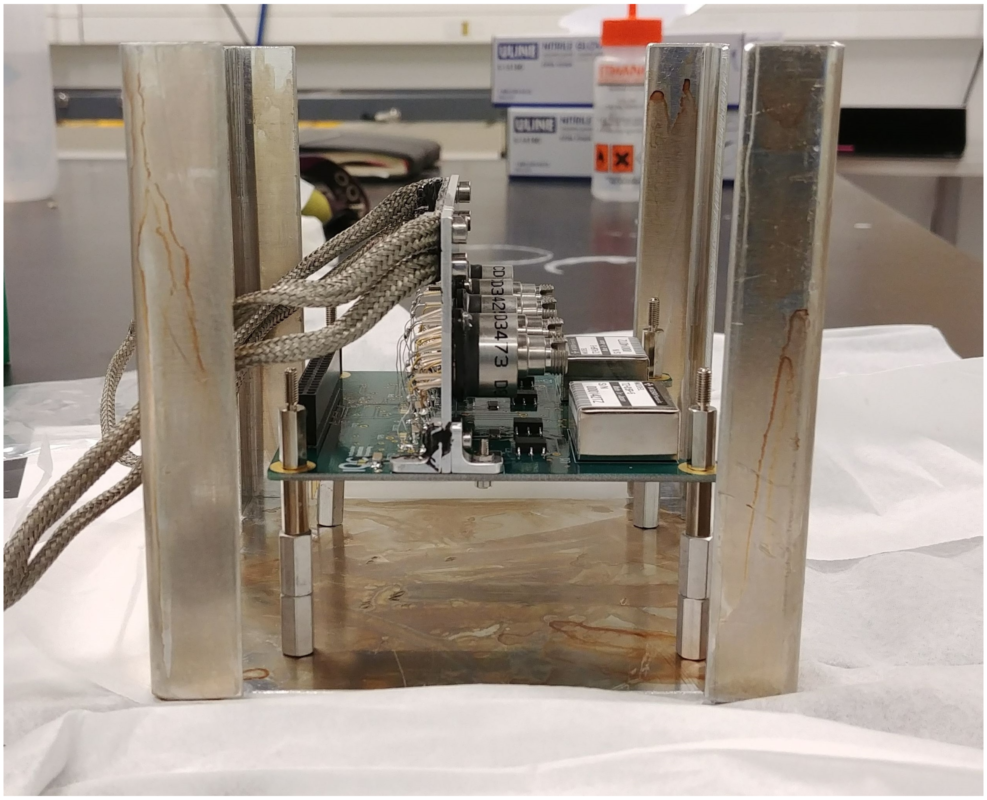


Figure 5.23: The third detector module DM3.

5.6 Detector module DM3

We built a third detector module DM3 to study the performance of the module in high-vacuum that it will experience while in space. It is also a flight compatible module and is built following the similar steps that were maintained during DM2. We mounted four Excelitas SLiK detectors in this module. These detectors were used in the experiment performed by Ian DSouza *et al* [38] and were radiated with a total proton dose of 2×10^{10} protons/cm^2 (equivalent to 10 years fluence in LEO). Figure 5.23 illustrates the assembled DM3. It is mounted on an Al base-frame that imitates a CubeSat bus. This frame also provides a robust structure and protects from accidental breakage during the module handling. It has a dimension of 12 cm^3 and is built from a single-piece Al sheet. The corner frames were cut from the sheet and then bended vertically to give the conner rail structure. The entire structure is cleaned and anodised in the same way as the detector mounting plate was prepared.

DM3 will be tested at low pressures in the range of 10^{-6} torr inside a thermal vacuum chamber (TVAC). We will also conduct laser annealing on the detectors, as well as their characterization in that pressure. Through this experiment, we will study the outgassing properties of the module and performance of the laser annealing in vacuum environment that the module will experience in space. As of this writing, the preparation for the vacuum test in under process.

5.7 Summary

To summarize, this chapter discussed the development of detector modules for the CAPSat annealing payload. This module is one of the two segments of the annealing payload. The details of the module circuits, as well as its preparation and assembling procedures, are also explained. In total, three modules are built, and each one has its own individual purpose. The first module was implemented to verify the functions and control mechanisms. The second and third ones are the flight version of the module. Among these, the second module will be assembled in the satellite bus and will be launched to an LEO orbit to perform the in-orbit laser annealing experiment in 2020. The last one is built to execute a similar experiment in the lab on previously irradiated detectors inside a thermal vacuum chamber. It will provide an insight into the efficiency of the annealing experiments in the space environment.

Chapter 6

A new readout circuit for NFADs and their characterization

The content of this chapter is based on the manuscript in preparation [251].

6.1 Introduction

Free-running [252–254] single-photon detectors (SPDs) [157, 255] at telecom wavelengths are excellent for their diverse applications, such as in optical time-domain reflectometry [256], high resolution depth imaging [257], photon-counting optical communications [258], LIDAR [259], quantum communications [260], and particularly in quantum key distribution (QKD) [13, 261], where photon arrival time is unknown. Types of SPDs for free-running operation include photomultiplier tubes [262], InGaAs/InP single-photon avalanche diodes (SPADs) [263], and superconducting devices like transition edge sensors (TESs) [264] and superconducting nanowire single-photon detectors (SNSPDs) [172]. Of these types, SNSPDs have the best overall performance, including impressive detection efficiencies ($> 90\%$), low dark count rates (< 1 Hz), small timing jitter (< 100 ps), and almost no afterpulses [150]. However, these detectors are polarization sensitive [150], and require cryogenic cooling to reach sub-kelvin operating temperatures. Because of that, they are unsuitable for some applications. Presently, the most practical alternative to SNSPDs are the InGaAs/InP based SPADs because of their close to room temperature operation, compact size, low power consumption, robustness, and low cost.

However, these InGaAs/InP SPADs under free-running mode suffer high afterpulsing probability, which limits their performances. The afterpulses are spontaneous, non-photon avalanche events that occur due to the detrapping of carriers from bandgap energy levels. These carriers were trapped while travelling through the device during avalanche events. One such event also triggers several other secondary avalanches. The probability of these occurrences scales up with the number of carriers involved per avalanche, the avalanche duration, as well as the lifetime of the trapped carriers, which can be a few tens to hundreds of microseconds [160].

One approach to reduce afterpulsing probability of the NFADs is the reduction of charge flow per avalanche by fast quenching of the avalanche current [199]. Usually in conventional SPADs under passive quenching circuits, a large external series resistor is used to quench the avalanche current. But this external resistor adds a large parasitic capacitance to the circuit, preventing fast quenching of the avalanches.

To achieve fast quenching, recently a new InGaAs/InP SPAD device has been developed that is known as negative feedback avalanche diode (NFAD) [49]. In these devices, the detector device is monolithically integrated with a thin-film resistor that provides reduced parasitic capacitance. This approach in NFADs lowers the number of charge flow per avalanche, resulting in a lower afterpulsing probability compared to that of the conventional InGaAs/InP SPADs. Including additional dead time (also called hold-off time) per avalanche further reduces their afterpulsing effect. Previously, several NFAD readout circuits have been reported. In 2012, Yan *et al* [169] demonstrated a readout without any active hold-off feature. In the same year, Lunghi *et al* [168] presented an FPGA based system incorporating an active hold-off function to suppress the afterpulses.

Here, this chapter introduces a new simple design of an NFAD readout module that we implemented adding an active hold-off feature. This module is an upgraded version of the system reported by Yan *et al* [169]. Our readout contains a pulse processing module (PPM) to produce hold-off pulses with tunable width and to process detection pulses. The PPM is designed using traditional low voltage transistor-transistor logic (LVTTL) and emitter-coupled logic (ECL) devices. We also studied the performance of the module and characterized two NFADs from Princeton Lightwave Inc. [210]. This chapter discusses the operation of NFAD devices and our new readout module, as well as NFAD characterization using our new readout.

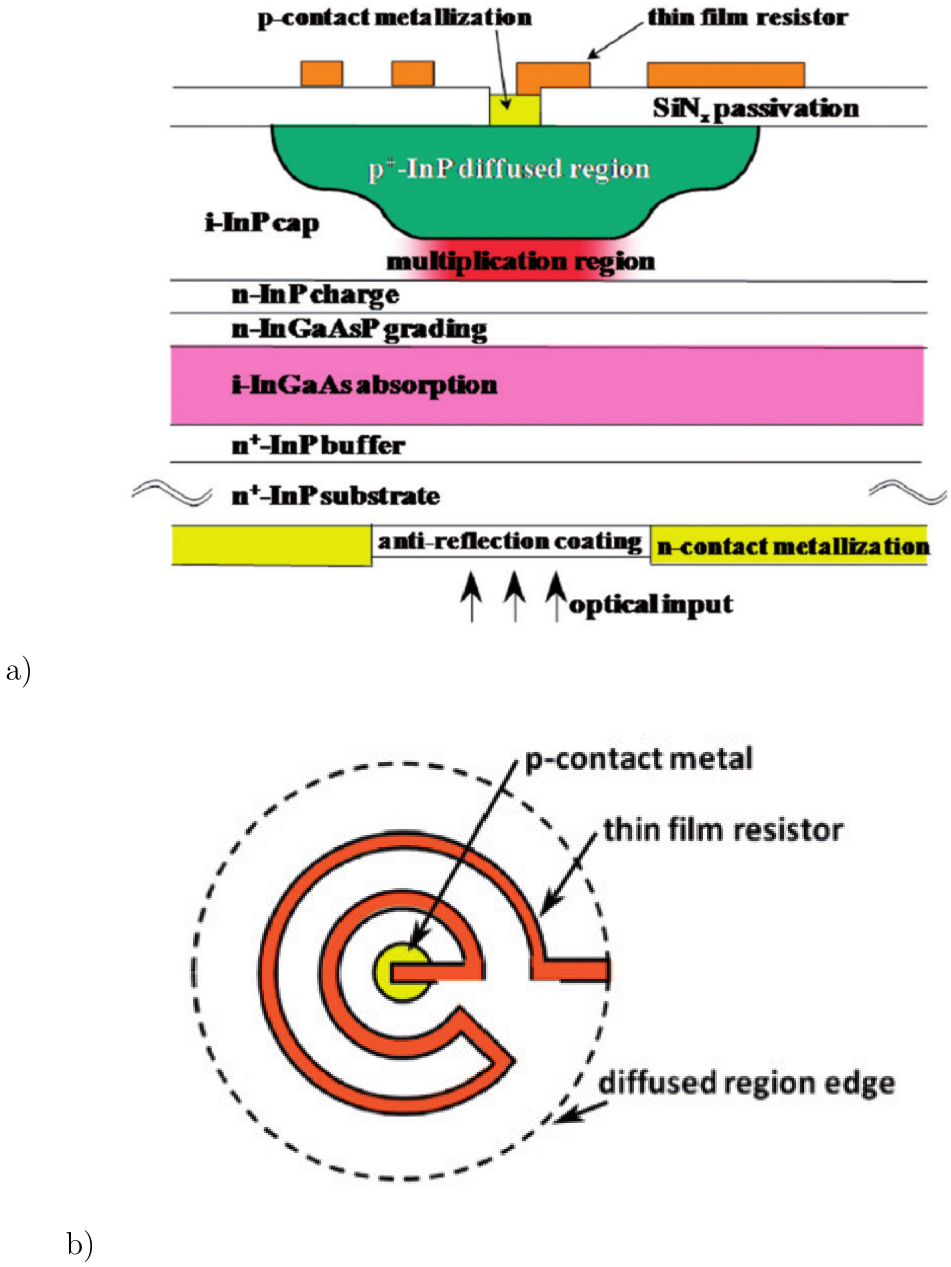


Figure 6.1: NFAD device (reprinted from [168]). a) SPAD growth structure with a thin film resistor integrated on the surface of the device. (b) Top view of an NFAD. The Orange shape is the thin-film resistor and has contact with the p-contact metal of the structure.

6.2 Negative feedback avalanche diodes

NFADs [49] are designed to resolve the drawbacks of conventional SPADs. Figure 6.1 presents the growth structure of NFADs, where a thin film resistor is monolithically integrated with an InGaAs/InP SPAD. This approach minimizes the parasitic capacitance, which in turn achieves fast quenching of avalanche current and also regulates the charge flow per avalanche, around $10^5 - 10^6$ carriers. Therefore, NFADs exhibits less number of trapped charges and significantly low afterpulsing effect compared to the typical InGaAs/InP SPADs. NFADs have been demonstrated with extremely low dark counts (1 Hz at 10% detection efficiency), and afterpulsing probability of 2.2% at a hold-off time of 20 µs [162]. This outcome is comparable with the performance of the SNSPDs, making them suitable for various other applications that were assumed not possible. By now, NFADs have been successfully used in long-distance QKD [57, 162, 169], and singlet-oxygen dosimetry for photodynamic therapy [265].

6.2.1 NFAD device operation

Negative feedback avalanche photodiodes (NFADs) operate in Geiger mode for single-photon detection. They require a fixed DC bias voltage equivalent to the sum of diode's breakdown voltage V_b, and excess bias voltage V_e above breakdown. Under proper bias voltage when avalanche events are triggered, the quenching of avalanche current and generation of output signals both happen independently by the NFAD. Here, the negative feedback approach that utilizes the integrated load resistor is theoretically equivalent to a passive quenching circuit.

Figure 6.2 illustrates the fundamental operational of an NFAD. The detector is considered as the series combination of a SPAD and a negative feedback load resistor. The SPAD itself is modeled as a parallel combination of its dynamic resistance R_d and junction capacitance C_d. The load is represented by a load resistance R_L and a parallel load capacitance C_L. A reverse bias voltage of $V_a = V_b + V_e$ is applied across the NFAD for photon detections.

With a monolithic integration, the parasitic capacitance C_L is negligible [210]. Total charge flow during an avalanche will be determined by the detector capacitance C_d and the excess bias V_e as, $q = C_d \times V_e$. So, smaller q can be achieved through a proper scaling of C_d during manufacture. The operation of NFAD is explained below.

Initially, the NFAD stays in armed stage (the left most circuit in figure 6.2), represented

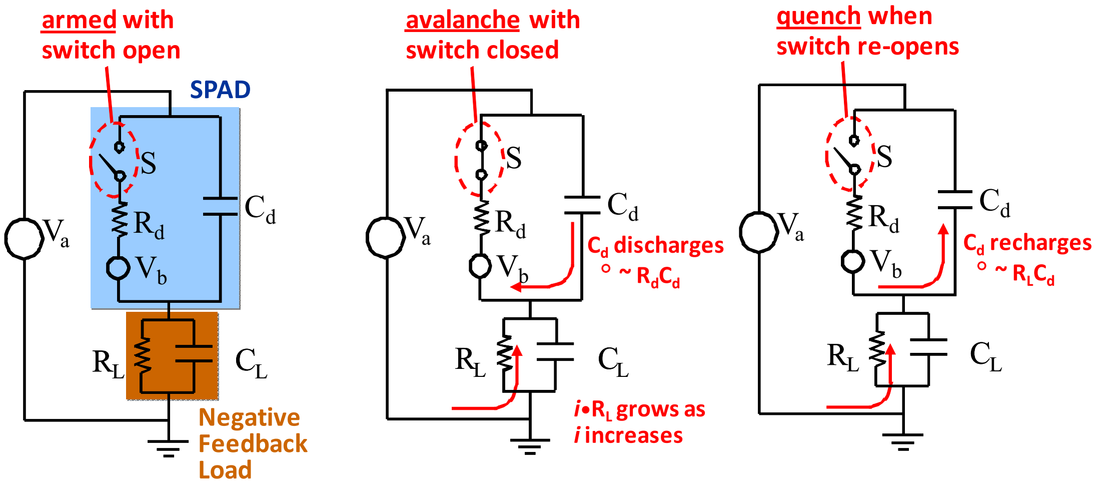

armed with switch open
SPAD
S
C_d
V_a
R_d
V_b
R_L
C_L
Negative Feedback Load
avalanche with switch closed
S
C_d
V_a
R_d
V_b
C_d discharges ◦ ~ R_dC_d
R_L
C_L
i•R_L grows as i increases
quench when switch re-opens
S
C_d
V_a
R_d
V_b
C_d recharges ◦ ~ R_LC_d
R_L
C_L

Figure 6.2: Basic operation of NFADs. The NFAD device is illustrated as a series combination of a SPAD with a negative feedback load R_L. The first circuit is a pre-avalanche condition, represented with the open switch S. An avalanche event is presented with the S closed. After the quenching of avalanche current, NFAD requires a charging time to become ready for next detection, represented by the third circuit. The diagram is reproduced from reference [210]

with the switch S 'open'. At this stage, no avalanche current flows and C_d charges via the voltage V_a. During an avalanche (middle circuit in figure 6.2), with the S 'closed' C_d starts to discharge through R_d with a time constant of $\tau_{discharge} \approx R_dC_d$. This causes a current flow i through R_L that gradually increases, and a voltage $i.R_L$ grows across the load R_L. At the same time, a similar amount of voltage is deducted from the SPAD, reducing its current flow close to the quenching current i_q. Once i_q is reached, avalanche current stops and S goes back to its open state. During this state (third circuit in the figure), the capacitor charges again with a time constant $\tau_{charge} \approx R_LC_d$. Since the charging time and quenching time both depends on the magnitude of R_L, it should be high enough for quick quenching of avalanches, as well as low enough to reduce the charging time. Because a large R_L leads to a long dead time by increasing their charging time and thus reduces the photon counting rates. Therefore, R_L is selected carefully by the manufacturer for NFADs' optimal operation.

6.3 The photon counting module

Figure 6.3 shows the functional diagram of the photon counting module, which consists of two submodules. The detector with its bias circuitry (the left submodule in Fig. 6.3) is inside a Stirling Ultracold freezer (Shuttle ULT:25N-86C) at 192 K. The high voltage bias is provided to the NFAD through the primary coil of a pulse transformer (PE-65968N). The secondary coil transfers the avalanche signals to the right sub-module (Fig. 6.3) via a 50 Ω transmission line. Note that the detection signals are inductively coupled to the amplifiers (located in the right sub-module) via the pulse transformer that allows transfer of avalanche current with improved sensitivity. After processing these avalanche signals by the PPM, generated hold-off pulses are fed back to the NFAD anode by another 50 Ω transmission line.

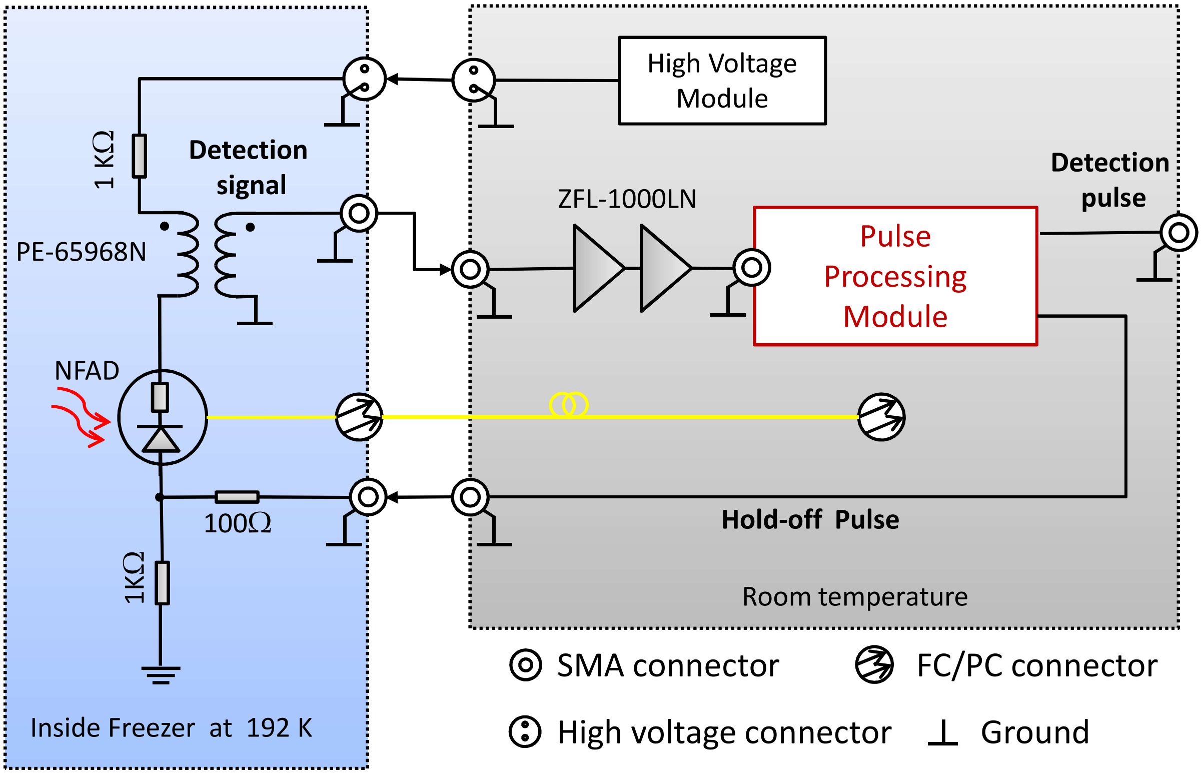


Figure 6.3: Design diagram of our NFAD photon counting module. All components in the gray box are at room temperature, and those in the blue box are in a deep freezer at 192 K temperature. The high voltage module supplies bias voltages to the NFAD. The pulse processing module processes the detection signals and produces hold-off pulses. PE-65968N: pulse transformer; ZFL-1000LN: radio frequency (RF) amplifier; FC/PC: single mode fiber connector; SMA: Coaxial connector.

On the other hand, the right sub-module stays at room temperature that consists of a high voltage module, two wide-band RF amplifiers, and the PPM. The high voltage module (Matsusada, model TP-0.15P) provides the required bias voltages to the NFAD, and the wide-band RF amplifiers (Mini-Circuits, ZFL-1000LN) intensifies the avalanche

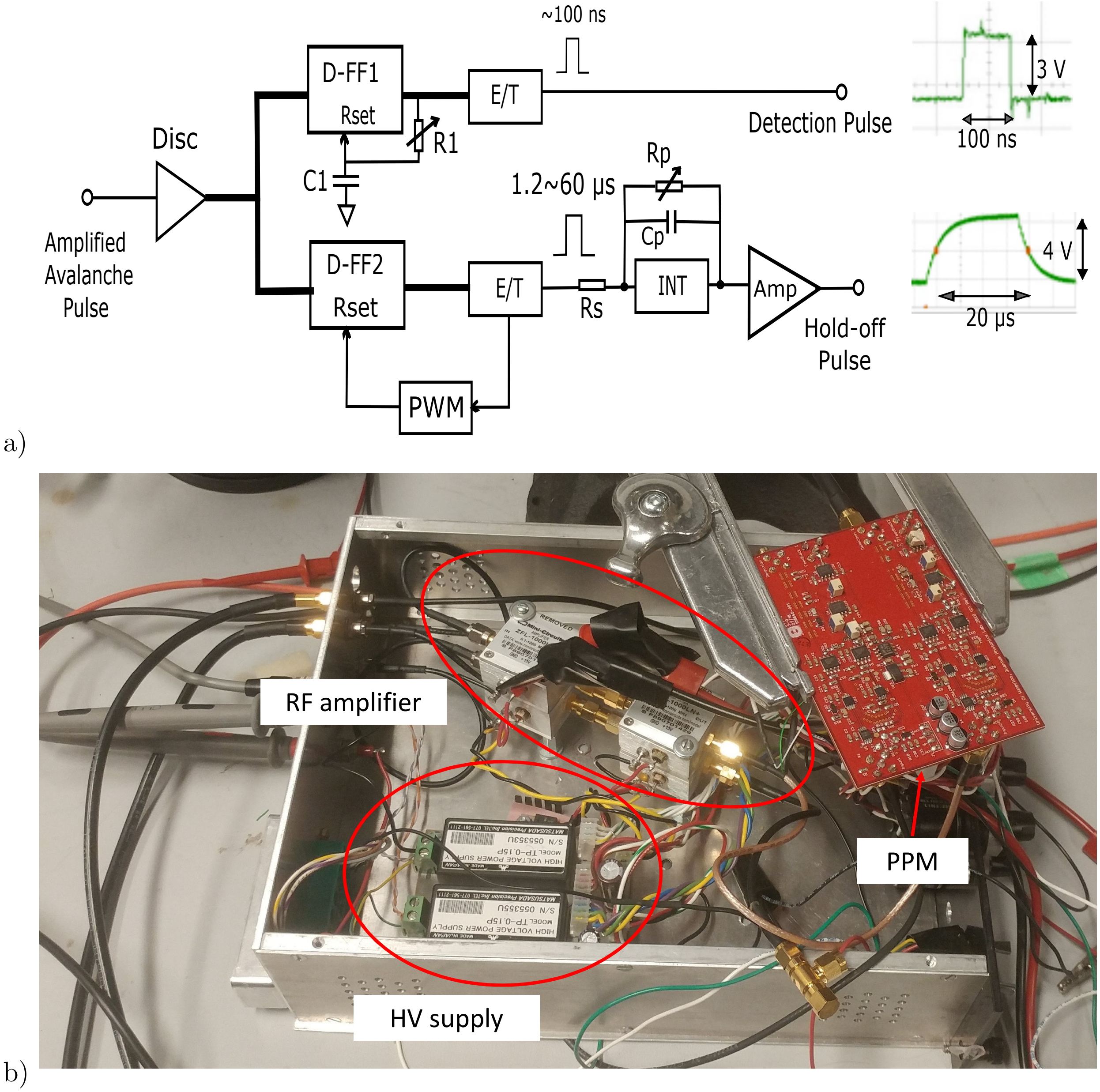


Figure 6.4: a) Electrical schematic of the pulse processing module. The PPM circuit produces a detection pulse and hold-off pulse for each NFAD detection event. Experimental data of a typical detection pulse and hold-off pulse are shown at the two outputs. Bold lines refers to the differential lines. Disc: discriminator (ADCMP553); D-FF: D flip-flop (MC100EP51); PWM: pulse width modulator; E/T: ECL to TTL converter (ICS83021I); INT: Integrator. Functional details are explained in text. b) The readout module that consists of radio frequency amplifiers (RF amplifier), high-voltage supply (HV supply), and the PPM.

signals by +40 dB. The PPM processes the detection pulses as well as simultaneously generates tunable hold-off gate pulses. These gate pulses are LVTTL voltages and reduce NFADs bias below their breakdown voltages to prevent detection for the gate duration.

6.4 Pulse processing module

The pulse processing module (PPM) is designed using LVTTL and high-speed ECL logic devices. The ECL devices have differential input/output, and the difference between the logic levels is only around 0.8 V, allowing their use for fast switching. The block diagram of our PPM is shown in Fig. 6.4.

The PPM has two branches– one path processes the detection pulses, while the other generates hold-off gate pulses. The module operates in the following way: A discriminator (Disc) distinguishes the amplified avalanche signals when their amplitude is larger than a pre-set reference voltage (maximum of 200 mV). The Disc output is fed simultaneously to the non-inverting inputs of two D-FFs in each branch. An avalanche event causes a transition from LOW to HIGH at the output of both D-FFs. Then capacitor C1 at D-FF1 output starts to charge via resistor R1. Once a voltage develops across C1, it resets D-FF1 and generates a pulse with a width defined by the R1C1 time constant of the circuit. We choose a pulse width of 100 ns by tuning R1. Lastly, an ECL to TTL converter (E/T) transforms the differential pulses into LVTTL detection pulses with an amplitude of 3 V.

Similarly, the lower branch of the PPM circuit generates LVTTL hold-off gate pulses after the E/T conversion. In this case, the pulse width is determined by a pulse width modulator (PWM) that resets D-FF2 after a certain duration (between 1.2 and 60 μs). We observed that gate pulses trigger extra detection events at their falling edges due to large voltage change in a short duration at the pulse transformer. Therefore, an integrator (INT) circuit is included following the E/T converter to control the fall time of the hold-off pulses. The INT consists of an operational amplifier (op-amp), and a combination of resistors R_s, R_p and capacitor C_p as shown in Fig. 6.4. We select a value of C_p to give sufficiently long fall time. Then resistor R_p is tuned to increase the fall time until the detection events at the fall edges disappear. Next, an amplifier (Amp) following the INT is used to vary the amplitude of gate pulses by modifying Amp gain.

The resultant gate pulse (shown in Fig. 6.4) has an amplitude of 4 V and a fall time (90% to 10% of full amplitude) of 2 μs. The NFADs are ready for detecting new events within 400 ns from the gate pulse falling edges. The gate pulses (at 10% of full amplitude) lag behind the detection pulses by approximately 80 ns, which is a shorter

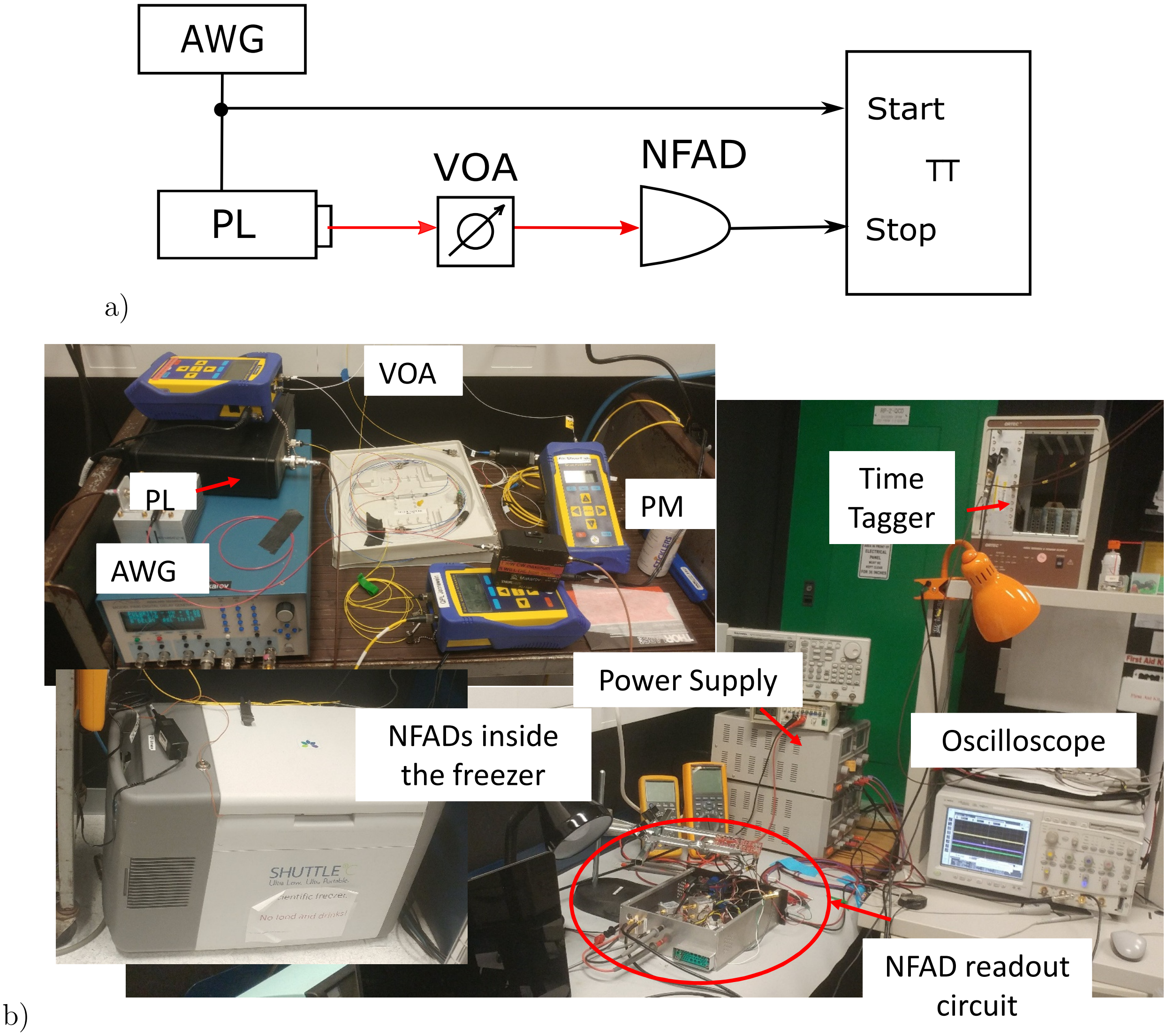


Figure 6.5: Test setup for the NFAD characterization using the time-correlated single-photon counting method (TCSPC) [170]. a) Schematic overview of the setup. The optical pulses from a pulsed laser (PL) are attenuated by a variable optical attenuator (VOA), and then sent to an NFAD. The avalanche events from the NFAD are collected using a time tagger (TT). b) The lab setup and the devices used during the experiment.

duration compared to the microsecond hold-off pulses. Consequently, this delay has a negligible contribution in limiting the count rate of the system. Overall, this simple design of our PPM supports easy operation and troubleshooting of the signal processing, while maintaining an excellent time resolution.

6.5 Characterization of NFAD

We characterized two NFADs using our custom readout electronics. The NFADs used in the system are model E2G6 (NFAD1) and E3G3 (NFAD2) from Princeton Lightwave Inc. [210], with an active area diameter of 22 µm and 32 µm, respectively. Both diodes are single mode fiber coupled and have integrated quenching resistor of 1.1 MΩ. NFAD2 was also characterized using Yan's [169] circuit without the afterpulse suppression feature. Therefore, characterizing NFAD2 using our new readout allows us to compare the performance of the circuits.

A schematic of our characterization experimental setup is illustrated in Fig. 6.5. We used time-correlated single-photon counting method (TCSPC) [170] for the NFAD characterization. The setup used a 1310 nm distributed feedback short-pulse laser source (PL: id Quantique, model # id 300), that is triggered by an arbitrary waveform generator (AWG: Tektronix AFG3502) to generate optical pulses. We attenuate the pulses down to single photon energy levels using a variable optical attenuator (VOA: OZ optics, DA-100-3U-1550). The weak pulses are then transmitted to the NFAD under test. A time-tagger (TT; 16-channel UQDevices) with a resolution of 78.125 ps is used to record the avalanche events with reference to the trigger pulses of the laser. Using this setup we measured the NFADs' characteristic parameters, such as their photon detection efficiency, dark count rate, afterpulsing probability, and timing jitter.

6.5.1 Dark count rate

First, we measured the breakdown voltages (V_B) of the two NFADs at temperature 192 K to be 69.4 V (±0.1 V) and 69.3 V (±0.2 V) for NFAD1 and NFAD2, respectively. Then we measured the dark count rate (DCR), keeping the laser turned OFF and the hold-off time (τ_d) fixed at 20 μs. This DCR includes intrinsic dark counts due to thermal excitation and trap-assisted tunneling, as well as afterpulses originating from intrinsic dark counts.

The DCR of the diodes at various excess bias voltages V_E (the bias voltage above V_B) are shown in Fig. 6.6. We see both diodes respond similarly and have less than 100 counts

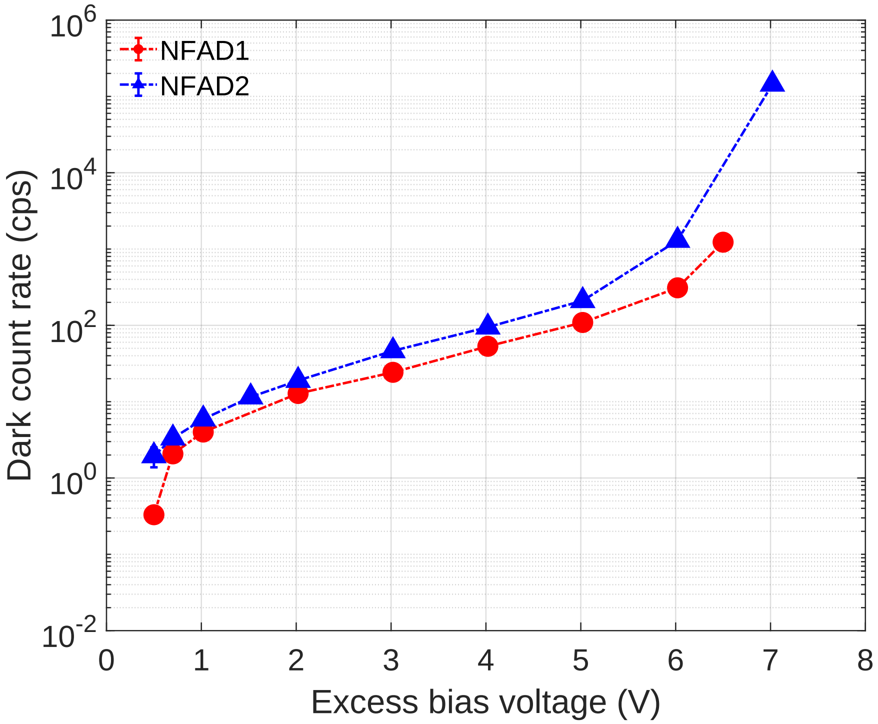


Figure 6.6: Observed dark count rates versus excess bias voltages. The dark count rates for each data point were accumulated in the time-tagger unit for 10 minutes. The hold-off time was 20 μs for both NFADs. The dotted line joining the data points are guidelines. This plot shows the complete operation regime for each NFAD before saturation. The size of the error bars are smaller than the data marker size.

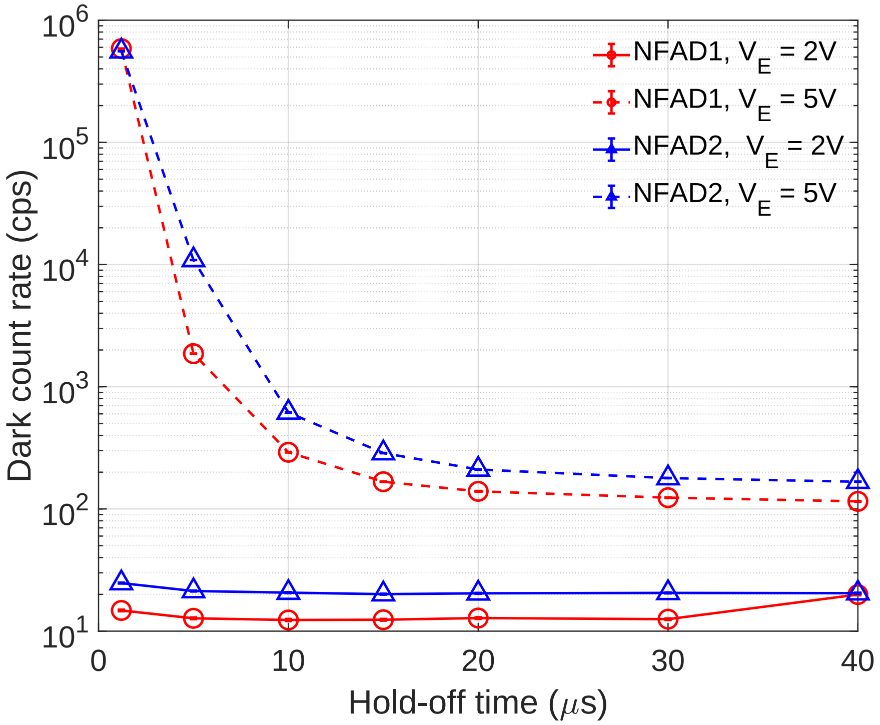


Figure 6.7: Effect of various hold-off times on the dark count rate. Long hold-off time reduces significant number of dark counts, and the afterpulses due to the dark counts. At 2 V excess bias with a 40 μs hold-off time, DCR of NFAD1 increases probably due to a drift in the bias or thermal properties during measurement.

per second (cps) over a wide operation regime, up to around 4 V of V_E. Above 6 V of V_E, the two NFADs suddenly saturate due to a significant increase of afterpulses caused by the large bias voltages. In contrast, under the circuit of Yan *et. al.*, NFAD2 saturated just at 2 V of V_E. This relatively low DCR of the NFADs even at the large bias demonstrates how our new readout circuit can prevent the early saturation by significantly reducing the number of afterpulses. Dark counts can be further suppressed by additional cooling [162].

We then studied the effect of hold-off times on DCR of the NFADs, which is shown in Fig. 6.7. The measurement was performed at two different excess bias voltages, 2 V and 5 V. We see that DCR is almost constant at 2 V of V_E for each diode, around 12 cps (20 cps) for NFAD1 (NFAD2). However, exponential drop of DCR is observed in both NFADs for 5 V of excess bias from τ_d of 1.5 µs to 20 μs. This significant reduction of DCR for a long τ_d refers to substantial suppression of the afterpulses. Note that, DCR is steady above 20 μs of τ_d. For this reason, we kept the hold-off time fixed at 20 μs in most of the other measurements.

6.5.2 Detection Efficiency

We used two methods to measure the detection efficiencies (DE) of the NFADs. A weak coherent pulse (WCP) source was used in the first method, then a spontaneous parametric down-conversion (SPDC) source was used in the second method. The measurement of DE using these methods are discussed below.

WCP method

In this method, we used a WCP source that utilized a 1310 nm pulsed laser (id 300). It generated optical pulses at a rate of 10 kHz, which was much smaller than the system's maximum possible repetition rate of 50 kHz (defined by the τ_d of 20 µs).

Considering the incoming photons have a Poisson distribution, the detection efficiency η_D is given by [169]

$$\eta_D = -\frac{1}{\mu} \ln \left(\frac{1 - \frac{R_{det}}{f_{trig}}}{1 - r_{dc}\tau_0} \right), \tag{6.1}$$

where R_{det} and r_{dc} are the measured count rates with and without the laser illumination respectively, f_{trig} is the trigger frequency of the laser, τ_0 is the coincidence time window on the TT, and μ is the mean photon number. The derivation of eq. (6.1) is given in appendix B.

During experiment, we chose μ to be extremely low, around 0.14 (0.13) for NFAD1 (NFAD2). The process of calibrating μ is explained in appendix B. Detection events from the NFADs were registered in a time tagger, which also recorded the coincident occurrences of the photon detections with the trigger pulses for a time window τ_d of 1 ns. We then estimated the detection efficiencies of the NFADs at various excess bias voltages, which are depicted in Fig. 6.8. We found the maximum detection efficiency of 8.5% and 6% at 5 V of V_E for NFAD1 and NFAD2, respectively.

We also analyzed the evaluation of DE with the photon flux at two different bias voltages, illustrated in the inset of Fig. 6.8. Since detection probability increases with the increased number of photons per pulse, so larger μ gave an expected higher detection efficiency. DE was later verified for various hold-off times and discriminator threshold voltages (summarised in Fig. 6.9 that did not show any noticeable effect on DE.

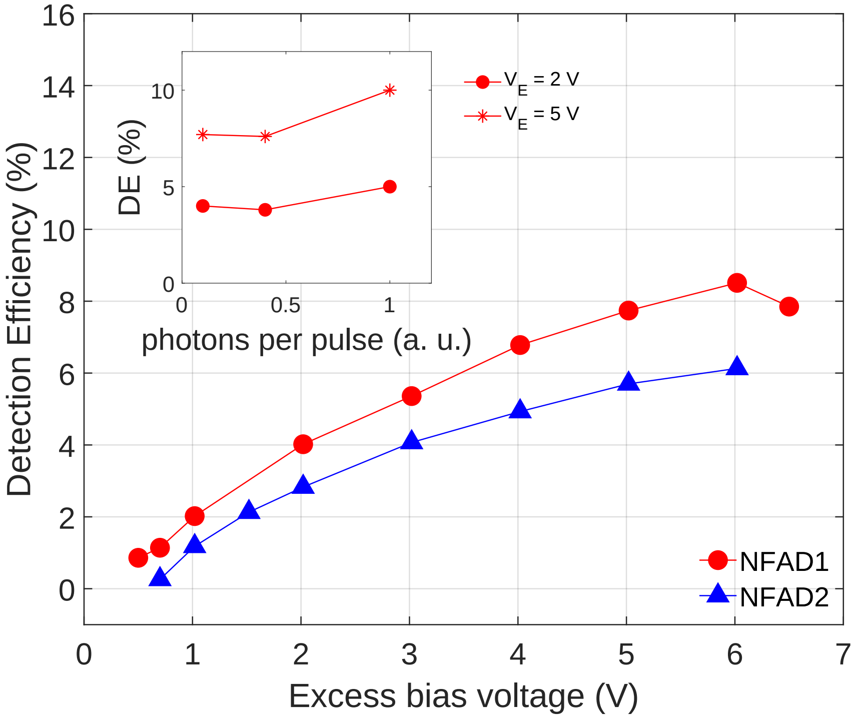


Figure 6.8: Evolution of detection efficiency (DE) of the NFADs with the bias voltages. The lines joining the data points are guidelines. This plot shows the DE for the complete operation regime of the two NFADs. The measurement for each data point is taken for a 20 μs of hold-off time. Inset plot illustrates the evolution of DE of NFAD1 with the photon flux at 2 V and 5 V of V_E.

SPDC method

This method used an SPDC source developed by Dr. Rolf Horn [266]. The source contains a pair of type-0 phase matched PPLN crystal that uses a 776 nm pump laser and produces photon pairs at 1552 nm. Using SPDC source has an advantage because it avoids the uncertainties in the mean photon number calibration. Therefore this method of measurement requires least assumptions in the detection efficiency measurement.

We used two detector arrangements for this test, as shown in Fig. 6.10. In the first arrangement (dotted box (a) in Fig. 6.10), two idQ-201 detectors were used to detect the correlated photon pairs from the SPDC source. Here the idQ-201 SPADs are commercial gated mode InGaAs detectors available with detection probability up to 30% at 1550 nm [267]. The second arrangement consists of one idQ-201 detector and an NFAD pair (dotted box (b) in Fig. 6.10). Later, the output detection events from the two arrangements were

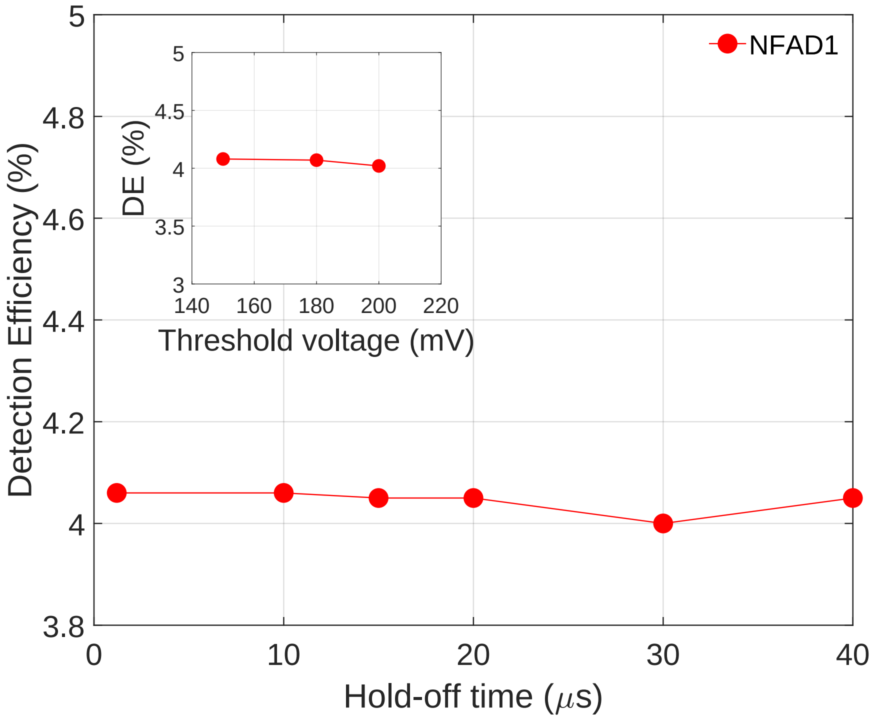


Figure 6.9: Effects of hold-off times and threshold voltages on the detection efficiency. The lines joining the data points are guidelines. The measurement for each data point is taken for a 20 μs of hold-off time and 2 V of V_E.

compared to estimate the efficiencies of the NFADs. For example, when the idQ-201 at the lower arm in box (a) was replaced with an NFAD, we compared the detection events of the NFAD with that idQ-201 detector. Since both of these detectors were connected to the same arm of the SPDC source, the photon coupling loss experienced by that arm would be similar in both measurements. Therefore, we ignored photon coupling loss of the arms during efficiency estimation of the NFADs.

The test procedures are explained here. First, a 50/50 beam splitter (BS) splits the photon pairs from the SPDC source and transmits them to the two idQ-201 detectors (first arrangement). Both of these detectors were triggered by an arbitrary waveform generator (AWG) at 1 MHz. The detector parameters were set to 10% detection efficiency, 10 μs dead time, and 50 ns gate pulse width. Then the individual detection events from the SPADs, and their detection coincidences within a 2 ns window were registered using a time tagger. Afterwards, the setup was changed to second arrangement by replacing IDQ2 with NFAD1. The individual (singles) and coincident counts of the IDQ1-NFAD1 pair were recorded. This process was repeated for the IDQ1-NFAD2, IDQ2-NFAD1, and

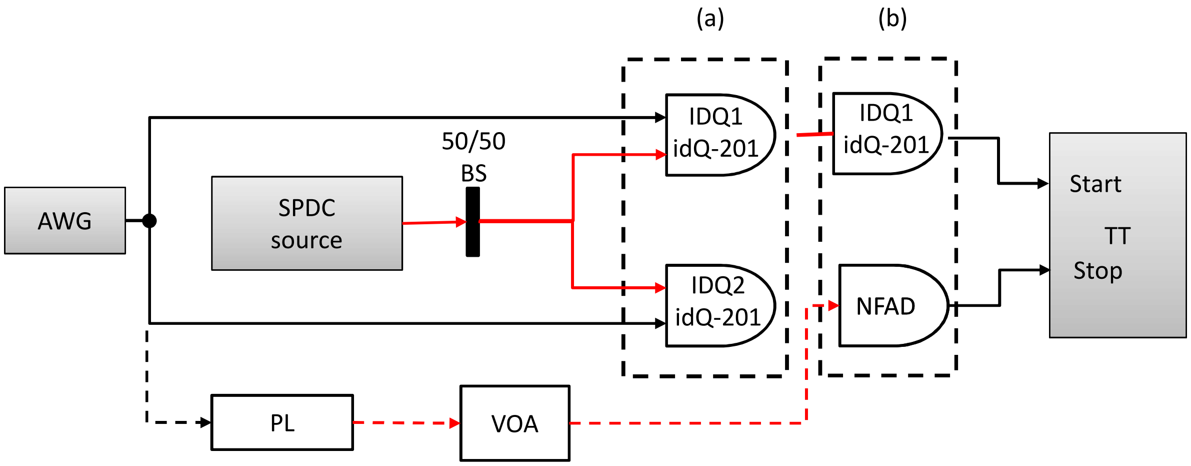


Figure 6.10: Scheme for NFAD's detection efficiency measurement using SPDC source. The photon pairs separated by a 50/50 beam splitter (BS) are transmitted to (a) two IDQ (idQ-201) detectors, and (b) a IDQ-NFAD pair. The avalanche events are registered using a time-tagger (TT). The pulsed laser (PL) source and the variable attenuator (VOA) are used with the arrangement in the dotted box (b).

IDQ2-NFAD2 pairs.

The detection efficiencies of the NFADs were calculated based on the singles and coincidental counts. Let's assume R is the total photon pair generation rate, then the individual detection events of an IDQ-NFAD pair (of an arm of the source) are given by

$$N_{IDQ} = R\ .\ \eta_{IDQ}\ .\ t_{dc} \tag{6.2}$$

$$N_{NFAD} = R\ .\ \eta_{NFAD} \tag{6.3}$$

Here, N_{IDQ} and N_{NFAD} are the singles at the IDQ and NFAD respectively, η_{IDQ} and η_{NFAD} are the detection efficiencies of the IDQ and NFAD SPADs, t_{dc} is the duty cycle of IDQ detectors. The net counts are the total counts minus dark counts in each individual case.

Now the ratio of 6.2 and 6.3 is

$$\frac{N_{NFAD}}{N_{IDQ}} = \frac{\eta_{NFAD}}{\eta_{IDQ}\ .\ t_{dc}}$$

$$\Rightarrow\ \eta_{NFAD} = \frac{N_{NFAD}}{N_{IDQ}}\ .\ \eta_{IDQ}\ .\ t_{dc} \tag{6.4}$$

Table 6.1: Summary of the detection efficiencies for NFAD1 and NFAD2 using SPDC source

Detector	Detector pair	NFAD V_E (V)	Efficiency (%)	
			Coincidence	Singles
NFAD1	NFAD1-IDQ2	2	3.2	4.1
		5	4.9	7.2
	IDQ1-NFAD1	2	4.8	8.0
		5	**8.8**	12.5
NFAD2	NFAD2-IDQ2	2	2.7	2.0
		5	3.6	7.4
	IDQ1-NFAD2	2	2.2	6.7
		5	**4.0**	11.3

Similarly, the detection efficiency of the NFAD based on the coincidental counts is

$$\eta_{NFAD} = \frac{N_{NFAD}^{Coinc}}{N_{IDQ}^{Coinc}} \cdot \eta_{IDQ} \tag{6.5}$$

where N_{NFAD}^{Coinc} and N_{IDQ}^{Coinc} are the coincident events in each pair of detectors. The calculated DE of the NFADs for the different detector arrangements are outlined in table 6.1. It is seen that larger DE is found for the NFADs, when singles are considered. Since the singles also includes the afterpulses, the DE based on the singles is a over estimation of detection efficiency. In contrast, coincidental events are considered for only 2 ns window, where afterpulsing effect is negligible. Therefore, detection efficiencies based on the coincidences are more accurate. This process gives the best DE of 8.8% (4%) for NFAD1 (NFAD2) at the 5 V of V_E. These results closely agree with the efficiencies found in the WCP method.

6.5.3 Afterpulsing Probability

To measure the afterpulsing probability P_{AP}, we used the setup mentioned in Fig. 6.5, where the laser was triggered at a rate of 10 kHz. We accumulated the detection events in the time-tagger for 180 s. It gave a histogram for the successive avalanche events on a 95 µs window. Total P_{AP} was calculated as

$$P_{AP} = \sum_i (\frac{C_i}{C_d} - r_{dc}\tau) \times 100\%, \tag{6.6}$$

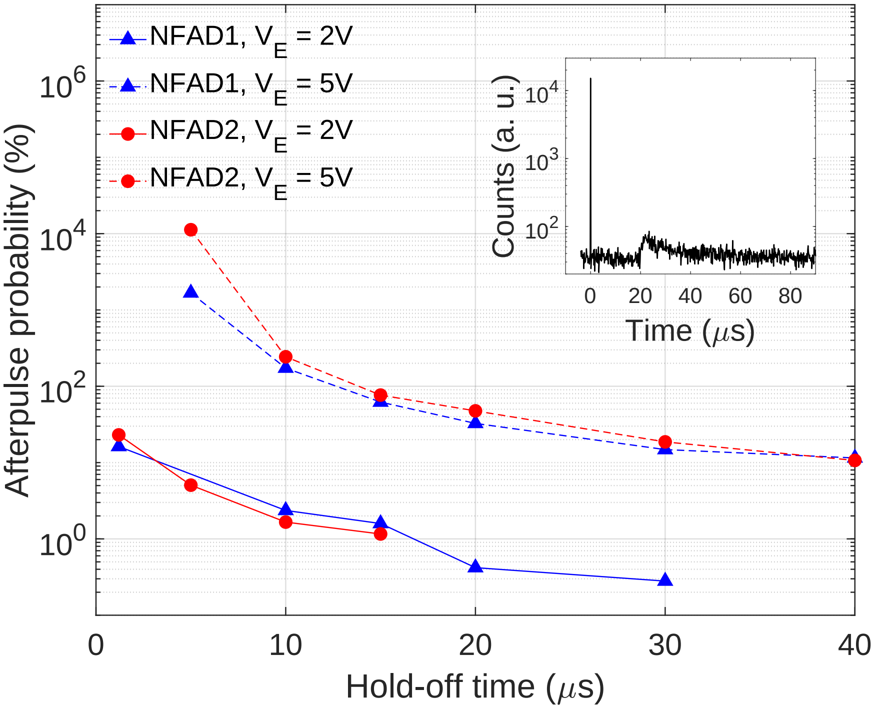


Figure 6.11: Afterpulse probability at various hold-off time (τ_d) for the NFADs. The lines joining the data points are guidelines. The inset plot shows a histogram of the detector counts for NFAD1 with a 20 μs of τ_d. Counts at 0 μs correspond to the photon detection events due to the laser pulses, while the rest of the events result from the afterpulses.

here C_i is the number of events in the remaining time bins that are hold-off time apart from the photon detection bin, and C_d is the number of avalanches that occur due to the laser pulses. r_{dc} is the dark count rate, and τ is the time-bin size, which was 150 ns for our measurement.

Figure 6.11 illustrates the effects of the hold-off times on P_{AP} of the NFADs at 2 V and 5 V of excess bias. We see that afterpulses are significant at the larger bias, and these are substantially reduced for a long hold-off time. For instance, at a τ_d of 20 μs, NFAD1 has P_{AP} of 0.4% and 62.0% at 2 V and 5 V of excess bias, respectively. In the case of NFAD2, 20 μs hold-off time results in a negative afterpulsing probability for 2 V of V_E, inferring to an extremely low P_{AP}, and it is 48% for a 5 V excess bias. In contrast, NFAD2 exhibited more than 200% afterpulsing probability at only 2 V of V_{E} under Yan *et al.* circuit without any hold-off time [169]. This noticeable P_{AP} improvement of NFAD2 under the new readout circuit demonstrates its remarkable afterpulse suppression capability. Notably, this extensive afterpulse reduction is more evident for different hold-off times at 5 V of V_E, at which a considerable amount of afterpulses occur in each NFAD. At this bias, $\mathrm{P_{AP}}$ drops from 1671% to 33% for a τ_d from 10 μs to 30 μs in NFAD1, and drops from 11248% to 48% for a τ_d from 5 μs to 20 μs in NFAD2.

We verified our P_{AP} estimation by computing the intrinsic dark count rate (r^i_{dc}), which should not be affected by the hold-off times. r^i_{dc} was calculated by using the formula (6.7) for various τ_d [168].

$$r^i_{dc} = \frac{r_{dc}}{(1+P_{AP})(1-r_{dc}\tau_d)} \tag{6.7}$$

here r_{dc} is the measured dark counts that includes the intrinsic dark counts r^i_{dc} , caused by the thermally generated carriers or tunnelling effects, and afterpulses caused by the dark counts. This equation considers the hold off time correction and discards the extra counts from afterpulses. Our estimated r^i_{dc} is almost constant with a deviation of ±0.5 (±26) at 2 V (5 V) of V_E that provides a confidence in the resultant P_{AP} in our measurement.

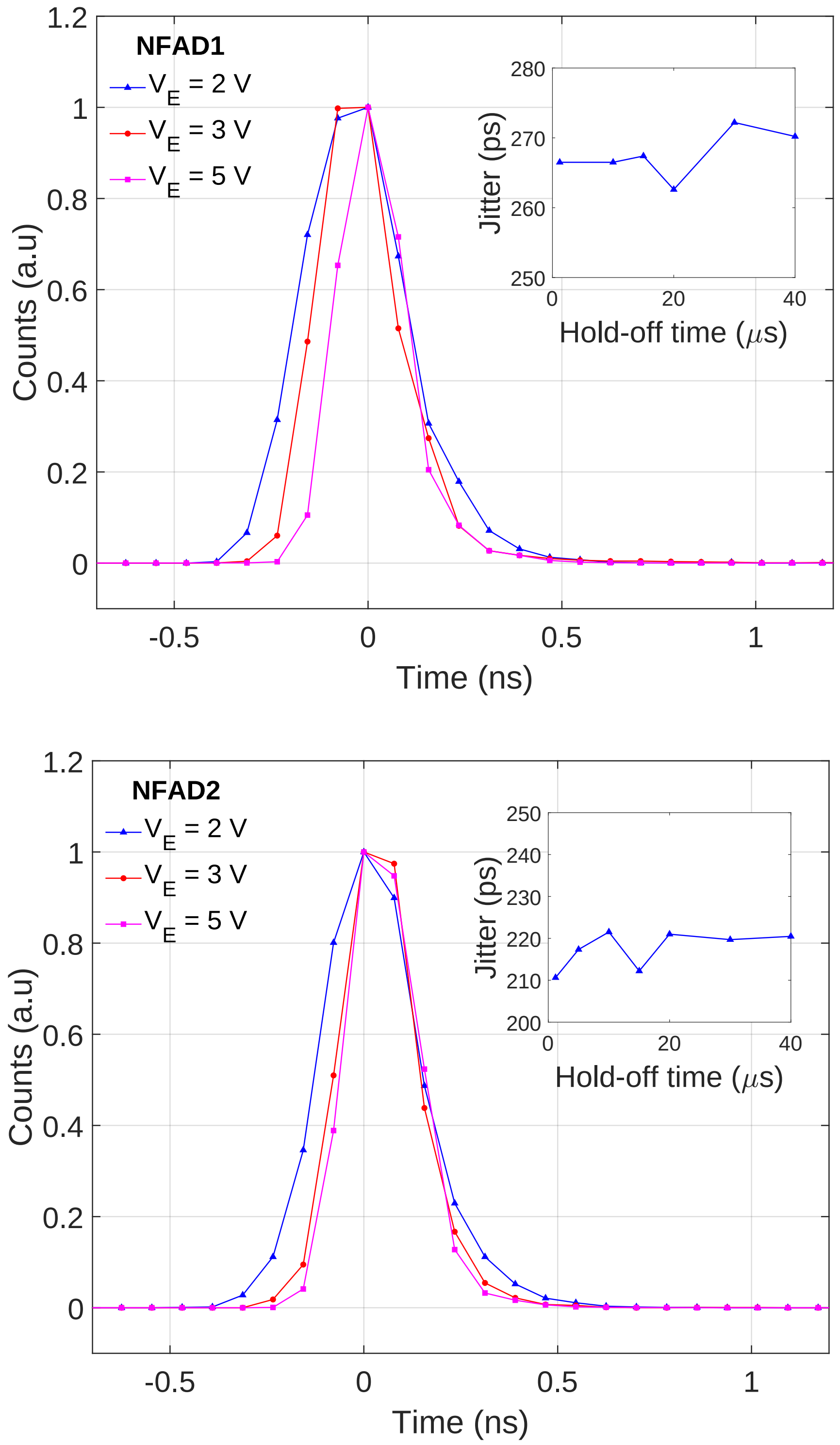
6.5.4 Timing Jitter

Timing jitter ($\Delta t_{\mathrm{jitter}}$) of the NFADs were estimated from the registered counts by the TT unit. $\Delta t_{\mathrm{jitter}}$ includes the jitter contribution from the detector itself and the readout electronics. However, the devices involved in the measurement process, such as the time tagger and the laser diode also contributes to the total measured timing jitter (σ_M). Therefore, TT jitter (σ_{TT}) of 78.125 ps, and the laser pulse width (σ_L) of ~147 ps have been de-convoluted from the σ_M (eq. (6.8)), to calculate the jitter of the readout system.

$$\Delta t_{jitter} = \sqrt{\sigma^2_M - \sigma^2_L - 2\sigma^2_{TT}} \tag{6.8}$$

Figure 6.12 illustrates the σ_M for the NFAD1 and NFAD2 at three bias voltages for a τ_d of 20 µs. It is observed that the detectors respond earlier to the incoming photons as the bias voltage increases. So the late responding curves are shifted to the left, as the plots in Fig. 6.12 are centered at their maximum counts.

We found the resultant Δt_{jitter} for NFAD1 is 74.5 ps full width half maximum (FWHM), while the value is 61.8 ps FWHM for NFAD2 at their maximum efficiencies. These time resolutions of the NFADs are excellent as compared to the findings of ~100 ps jitter by Yan *et al* in [169], and ~ 400 ps jitter at 11% efficiency by Korzh *et al* in [162]. We then verified the time jitter for various hold-off times at 2 V of V_E. The insets of Fig. 6.12(a)-(b)



(a)

(b)

Figure 6.12: Timing jitter (Δt_{jitter}) of the NFAD readout systems at three efficiencies. (a) NFAD1 has Δt_{jitter} of 241.1 ps, 142 ps, and 74.5 ps FWHM, and (b) NFAD2 has Δt_{jitter} of 221 ps, 118.7 ps, and 61.8 ps FWHM at 2 V, 3 V, and 5 V of excess bias, respectively. Insets in (a)-(b) shows the jitter of the NFADs as a function of the hold-off time at 2 V of V_E.

illustrate that Δt_{jitter} deviates only by ±5 ps from the average jitter, showing negligible effect of the hold-off times on timing jitter.

We also estimated the figure of merit of the NFADs using $H = \eta/(DCR\Delta t_{\text{jitter}})$ [157] at their optimum bias condition. NFAD1 gives H = 1.6×10^7 at $\eta = 5.4\%$ and $\Delta t_{\text{jitter}} =$ 142 ps, and NFAD2 has H = $7.4{\times}10^6$ at $\eta = 4.1\%$ and $\Delta t_{\text{jitter}} = 118.7$ ps. These merits are at least one to two order of magnitude higher than the gated InGaAs detectors [255]. Moreover, NFADs with such merits are comparable with many SNSPD detectors.

6.6 Summary and discussions

This chapter discussed a new simple readout circuit for free-running NFADs that incorporates an active afterpulse suppression feature. It explained the functional details of the readout electronics, as well as characterization of two free-running NFADs using this new readout circuit. Detection efficiencies of the NFADs were measured using two methods: using a weak coherent pulsed source and a correlated-photon source. The first method gave the maximum efficiencies of 8.5% and 6% for NFAD1 and NFAD2, respectively, which was verified in the second method using commercial gated mode InGaAs detectors (idQ-201). Detectors with such efficiencies are usable in long-distance quantum communications where the channel loss is generally high. The observed dark count rates of the NFADs were below 100 Hz at 192 K for a 20 μs hold-off time. NFADs with DCR of 100 Hz and detection efficiency of 10% was previously demonstrated in an entanglement-based QKD over 400 km [100]. However, DCR being a dominant factor to the quantum bit error rate, keeping it low is important for QKD applications. DCR can be reduced more by operating them at lower temperatures [162]. Next, we studied the afterpulsing probability P_{AP} at various hold-off times. P_{AP} was significant at 5 V of excess bias and this probability for a 5 μs hold-off time was reduced by a factor of 51 and 236 under 20 μs of hold-off for NFAD1 and NFAD2, respectively. This result demonstrates a noticeable afterpulse reduction capability of our readout circuit. Here limitations in the maximum possible detection rate imposed by the 20 μs hold-off will not affect the long-distance quantum communications because of the lower receiving rate imposed by the high channel loss (e.g., 70 dB loss across 400 km quantum channel [169]). Our readout also showed a good time resolution. The timing jitter of the readout system was 75 ps and 62 ps FWHM for NFAD1 and NFAD2, respectively. So the overall resultant characteristic parameters of the NFADs under our custom readout system ensure their suitability in quantum optics applications, such as quantum cryptography, long-distance quantum communication, and characterizing entangled sources at telecommunication wavelengths.

Chapter 7

Blinding Attack on NFADs

The content of this chapter is a partial contribution to the publication [268].

7.1 Introduction

Any implementation of quantum key distribution (QKD) trusts the detectors that are used for detecting single-photons. However, in practice these detectors are not perfect. Their imperfections introduce loopholes into the systems that leads security threats in QKD. Because by exploiting the imperfections, an eavesdropper Eve can gain partial or complete information on the key using various types of attacks, such as intercept-resend attack [269], photon number splitting (PNS) attack [270, 271], detector efficiency mismatch attack [272], Trojan-horse attack [273–275], time-shift attack [276], or faked state attack [50–53, 277–281]. Of these attacks, utilizing faked state attack Eve can gain the full information on the raw key. In this attack, which is also known as blinding attack, Eve blinds Bob's detectors using a bright illumination and then forces his detection to fully match with her measurement outcome without being caught by Alice and Bob. This attack has already been successfully implemented on the single-photon avalanche photodiodes [282–286], and superconducting nanowire single-photon detectors [287, 288] using commercial off-the-shelf components.

This chapter discusses the blinding attack on NFADs, which are different types of detectors than the above mentioned single-photon detectors, as well as they require a particular kind of readout circuits. It is crucial to verify their vulnerability to blinding attacks so proper countermeasures can be incorporated into the systems to eliminate any threat. To our knowledge, this test on NFADs has not been demonstrated before. We performed this experiment in collaboration with ID Quantique researchers. We used the two NFADs described in Chapter. 6 under our custom readout [251] and ID Quantique used two commercial NFADs, model ID220 [289]. The combined results of these two experiments are in preparation for publication [268]. However, this chapter particularly explains the experiment of blinding attack performed on our two NFADs.

7.2 Working principle of blinding attack

The avalanche photodiodes diodes (APDs) used in most QKD systems work in Geiger mode (biased above breakdown voltage V_{br}) to detect single-photons. When APDs are biased below V_{br}, works in the linear mode where they respond linearly with the optical input, as demonstrated in Fig. 7.1. In this mode, Eve can eavesdrop a QKD system using an intercept-resend attack [51, 277]. First, Eve blinds the detectors with bright illumination to bring them in the linear mode. Then regulated laser pulses are superimposed to the blinding power to force Bob to detect the exactly same outcome as Eve prepared, when measured at the matching bases. Conversely, Bob detects nothing when he measures in the wrong bases.

The control of Bob's detection works as follows: Eve keeps a copy of Bob's state that is sent from Alice and measures in a random basis. She resends the measured outcome to Bob using bright trigger pulses instead of sending single-photon state. The optical power of the trigger pulses are just above the P_{th}, which will produce a 'Click' event at Bob's detector, only if Bob's basis choice agrees with Eve's measurement basis (as illustrated in Fig. 7.2). Conversely, the optical power divides into halves for Bob's wrong basis choice and transmits to both Bob's detectors. In this case, the optical power in the APDs are below P_{th}, and none of the APD generates 'Click'.

This attack results with a loss of half bits, which is not an issue for a QKD system. It is because the transmittance between Alice and Bob is below 1/2, and Bob's APDs do not posses quantum efficiencies always above 50%. However, in the blinding process, trigger pulses always cause a click for the right bases. As Eve listens the open communication between Alice and Bob in the classical channel during the shifting process, she applies the same operation on the bits as Bob does. Finally, Eve ended up having the same key as Bob.

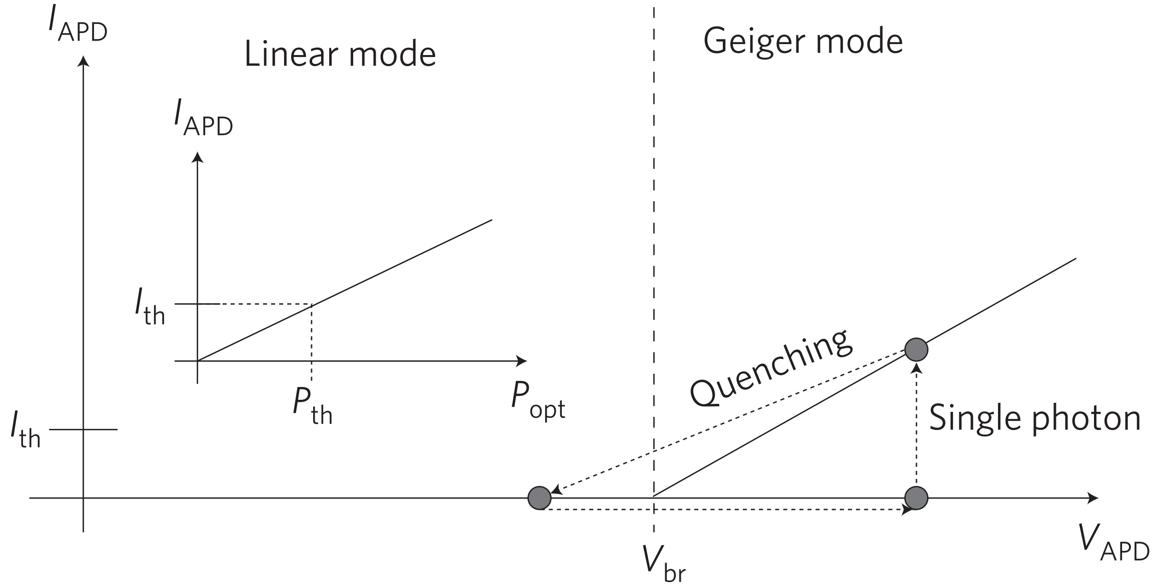


Figure 7.1: Operation mode of APDs (Reprinted from [284]). In Geiger mode, a large current I_{APD} flows through the APD in response to single-photon detection. When the I_{APD} is higher than the threshold current I_{th}, APD can detect the signal. To quench an avalanche, APD bias needs to be below V_{br}. In the linear mode, I_{APD} proportionally scales with the input optical power P_{opt}, which must be above the threshold power P_{th} to be detected.

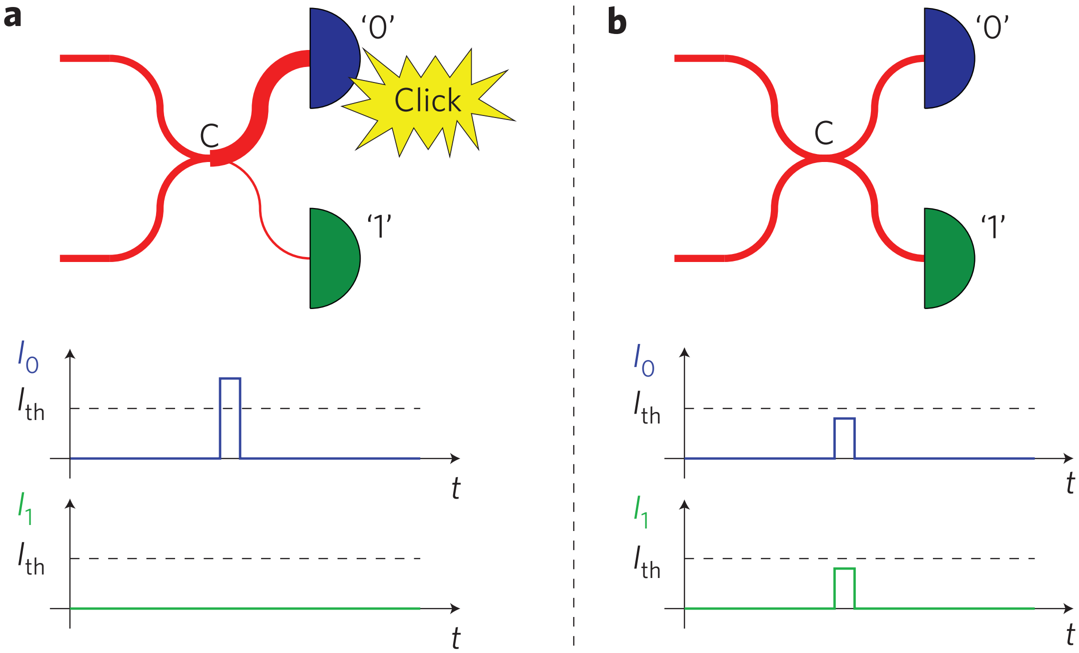


Figure 7.2: Scheme shows how Bob detects Eve's trigger pulses (Reprinted from [284]). APDs '0' and '1' are the two Bob's detectors. a) Eve and Bob measure in similar bases, b) Eve and Bob measure in opposite bases.

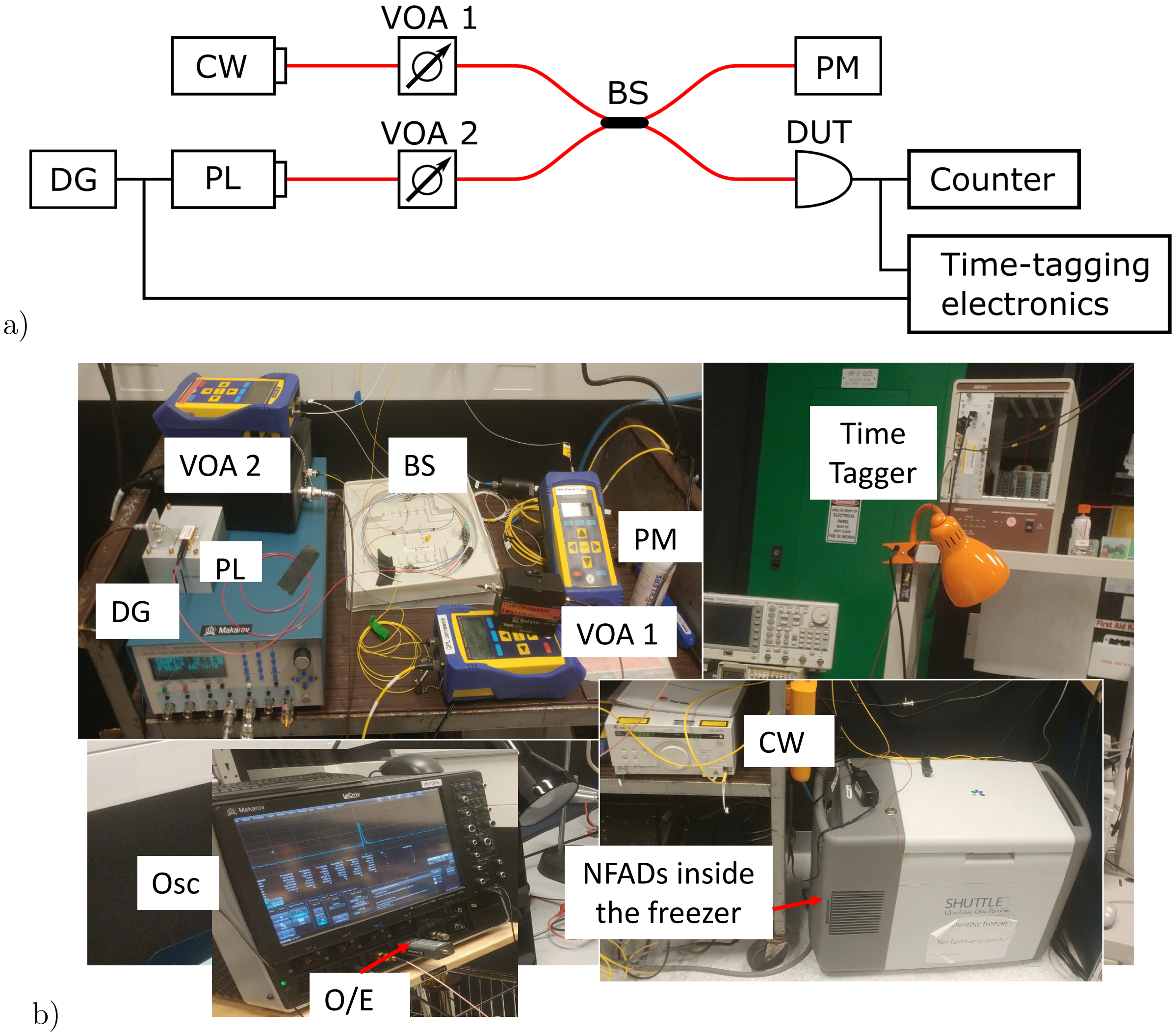


Figure 7.3: Experimental setup used in the blinding control of the NFADs. a) Schematic diagram of the experiment setup (Reprinted from [268]). The optical power of the continuous wave laser (CW) and the pulsed laser are adjusted using variable optical attenuators (VOA). The pulsed laser (PL) is triggered using a delay generator (DG). The two laser outputs are combined into a 50:50 beam splitter (BS), whose divided outputs are then sent to an NFAD (DUT) and to a power meter (PM). A time-tagging electronics is used for logging the detector counts. b) Experiment setup used in the lab indicating each apparatus.

7.3 Experimental setup for blinding attack

The experimental setup for the blinding attack is demonstrated in Fig. 7.3. Two lasers at telecom wavelength are used for this attack. A continuous-wave (CW) laser (Santec TSL-210V) sends optical power to the NFADs (DUT) for blinding and brings them in the linear mode, in which the diodes are no longer sensitive to single-photons. During the experiment, the CW power is kept fixed at 2 mW, and a variable optical attenuator (VOA 1) next to the CW laser is used to adjust its continuous power. The second laser (PL: DFB-1551.72) produces optical pulses of 161 ps full width half maximum (FWHM) to manipulate Bob's detection after the blinding. A delay generator (Highland Technology P400) provides the trigger signals to the pulsed laser, and a second attenuator (VOA 2) regulates its optical pulse energy. PL pulses are then split up by a 50/50 beam splitter (10202A-50-FC-CWD07212909), which is not shown in the schematic. Half of the PL pulse energy is combined with the CW power using another 50/50 beam splitter (BS: 10202A-50-FC-CWD07215053), and the second half is fed to an oscilloscope (Lecroy Wavepro 760Zi) via an optical-to-electrical converter (O/E: OE455) for pulse energy monitoring. On the other hand, the BS transmits the combined optical energy to the NFAD, and a power meter (PM) for monitoring total power sent to the detectors. Finally, a time-tagger unit registers the detection events from the NFADs.

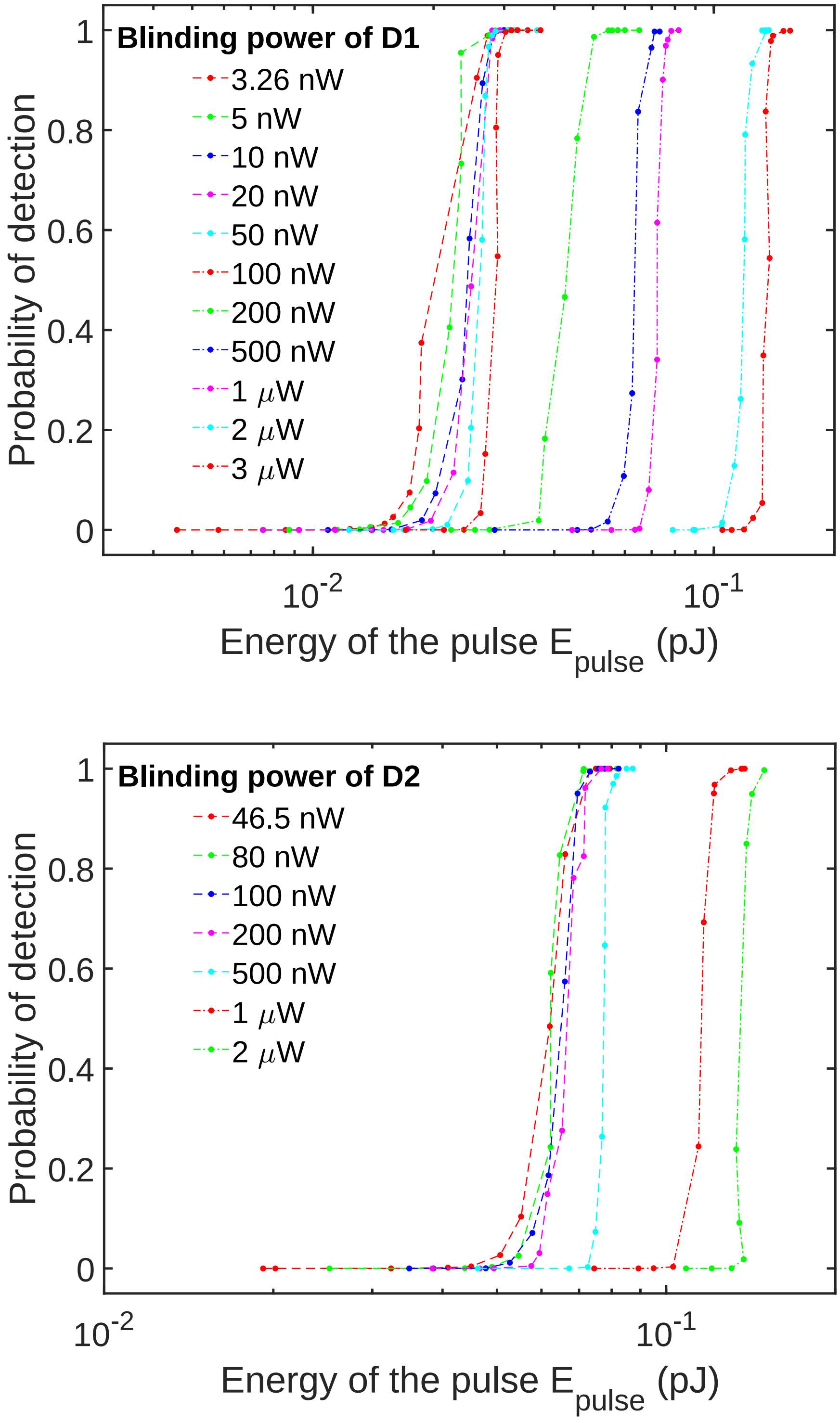
7.4 Detector Control

For controlling Bob's detection, Eve first sends CW laser power to the detector at its biased condition. In the beginning, detector's counts were just the dark counts. With the increased bright illumination, detector's counts drop to zero, which ensures the blinding. Then Eve adds the controlled optical pulses to the detector. Bob's detection outcome depends on these pulse energies because of a comparator in the readout circuit. If the pulse energy is too small, none of Bob's detector creates a click. For an adequate trigger pulse energy E_{pulse}, Eve has a probability p to make the detectors to click. The maximum energy that never causes a click can be defined as E_{never}, and the energy above which there is always a detection defined as E_{always}. Now, to force a detection in QKD systems, E_{never} and E_{always} must fulfill certain conditions that depend on the protocol in use [285]. For example, in the BB84 protocol, when $E_{\text{pulse}} > E_{\text{always}}$, as well as Eve and Bob measure in a matching basis, all energy must hit one detector to generate a click. On the contrary, for the non-matching bases, E_{pulse} will be halved and hit both detectors, which should not give any detections. To ensure this, the trigger pulse energy E_{pulse} must meet the condition,

$E_{\text{pulse}}/2 < E_{\text{never}}$. After combining these two requirements, it becomes $E_{\text{never}} > E_{\text{always}}/2$. Since Bob's detection rate is higher at the shorter distances, Eve must choose E_{pulse} to have higher click probability. Conversely, click probability can be less at the longer distances.

Fig. 7.4 shows the detection probability of NFAD1 (D1) and NFAD2 (D2) for various trigger pulse energies at different blinding power. The dead-time is set to 20 μs that allows maximum detection rate of 50 kHz for the detectors and the trigger pulses are sent at 40 kHz. As demonstrated in Fig. 7.4, above certain blinding power, there is a sharp transition between E_{never} and E_{always}. The width of the transition energy is shorter towards higher blinding power, which is more apparent in Fig. 7.5. Since the transition energy is wider at the lower blinding power, the blinding condition does not meet at this region. Therefore, Eve will not be able to extract the entire key for short distance BB84 protocol using this attack [52]. In such case, Eve either can increase the blinding power to achieve a narrower transition, or get a partial attack on the key without introducing any disturbance in Bob's detection rate [290]. With the high blinding power, NFADs operate in the linear mode where their gain is less due to a low voltage drop across the detector. This mode requires increased trigger energy to get a click. In contrast, with the low blinding power, the detectors operate at linear mode but more close to the breakdown voltage region, where the devices have much higher gain. At this region, even very low trigger energy gives a non zero probability to click, due to which E_{never} is smaller at lower blinding powers. Similarly, when the detectors operate at higher efficiencies, they require more blinding power as the detector's bias voltage is high, as seen in Fig. 7.5. Detector D1 and D2 have similar response except for a difference in their minimal blinding energy requirement, which can be due to sample to sample variation.

We also study the change in trigger pulse energy with the discriminator threshold V_{Th}, where the transition energies are shown in Fig. 7.6. The difference in the transition energies at various V_{Th} are almost similar. We further see that, the changes of the hold-off times does not affect the blinding power and transition energies, as demonstrated in Fig. 7.7.



a)

b)

Figure 7.4: Probability of forced control at various trigger energy for a) D1, and b) D2. The diodes were biased 2 V above breakdown and trigger pulses were sent at rate of 40 KHz.

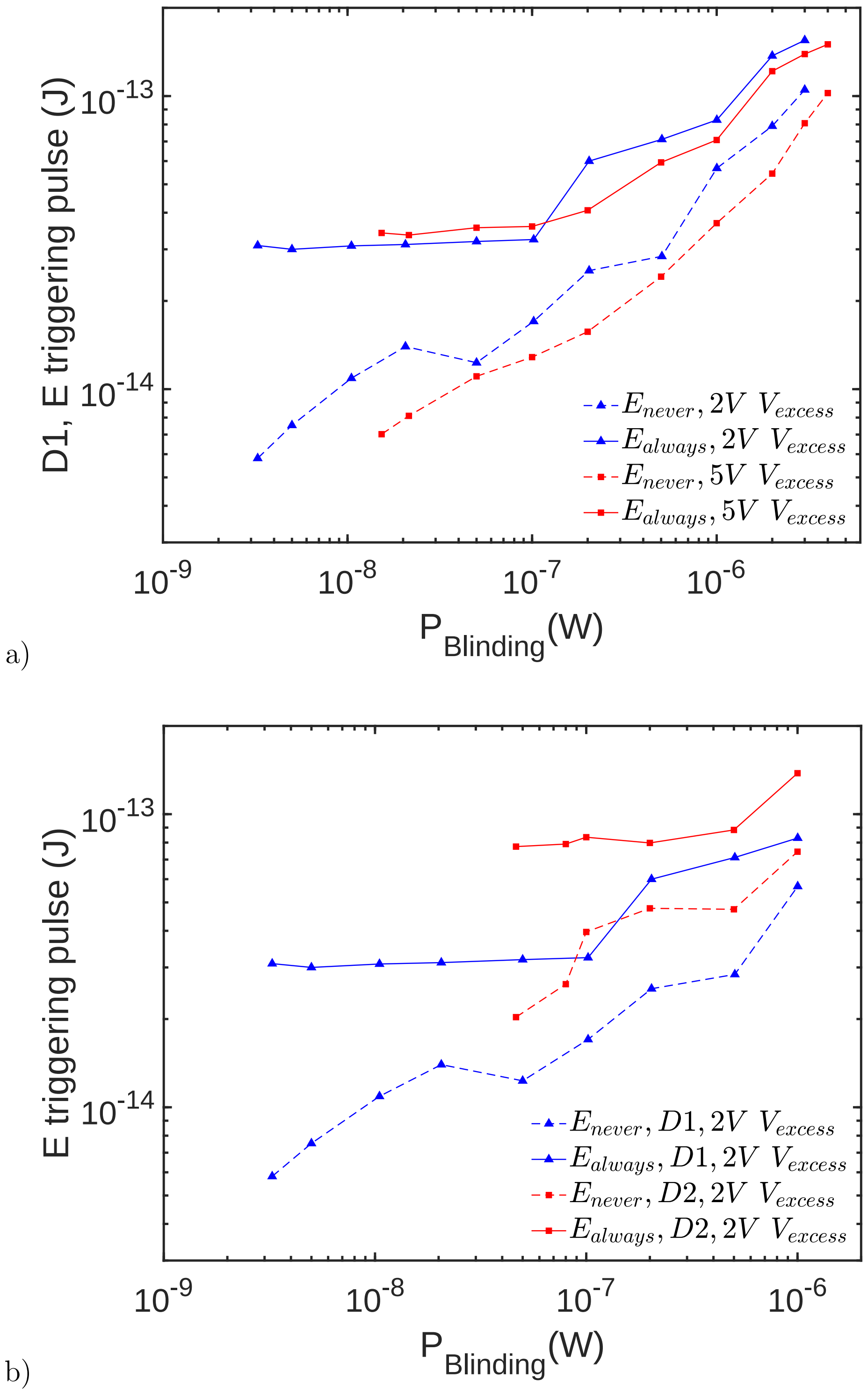


Figure 7.5: Transition energies depending on the blinding power. a) Comparison of trigger energies for diode D1 at two efficiencies, 2 V and 5 V V_{excess}. b) Comparison of energies between D1 and D2 at the same efficiency, 2 V V_{excess}.

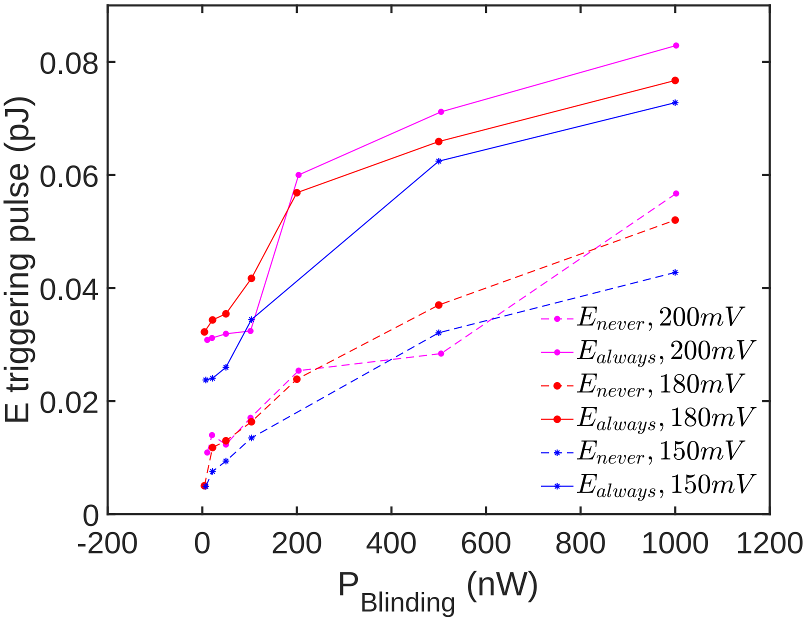


Figure 7.6: Evolution of trigger energy E_{always} and E_{never} at different discriminator threshold voltages for D1. The bias was 2V excess voltage and the hold off time was 20 µs.

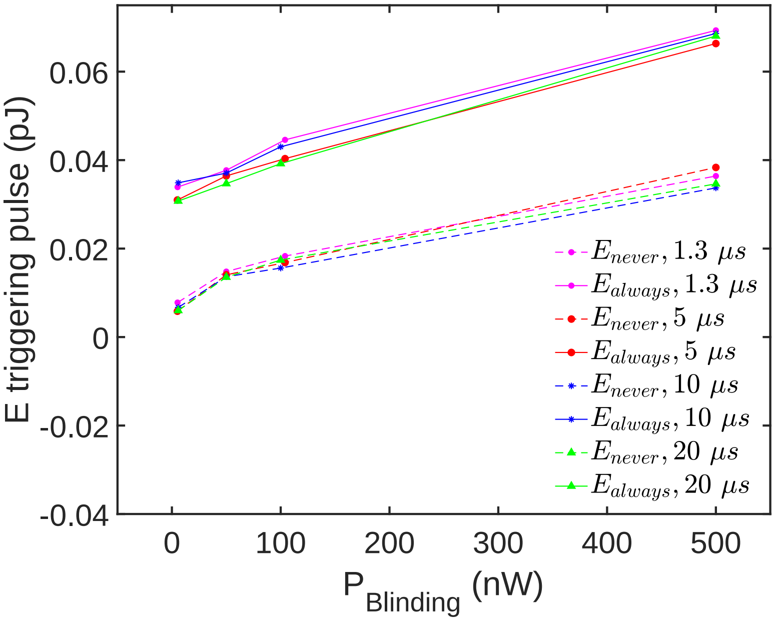


Figure 7.7: Evolution of trigger energy E_{always} and E_{never} with the change of hold off time for D1.

7.5 Timing jitter

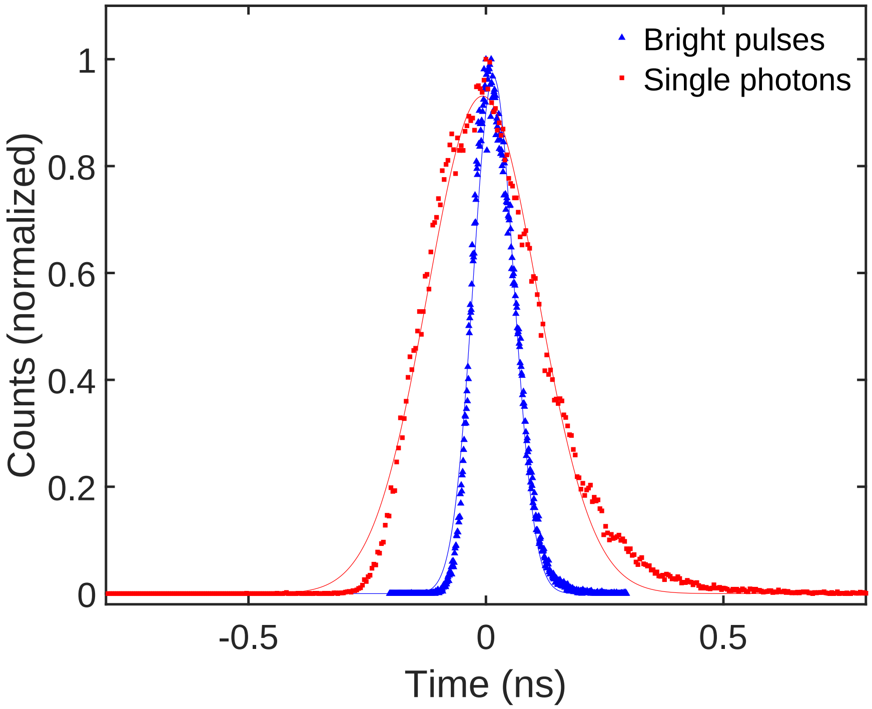


Figure 7.8: Time jitter of single mode D1 for bright pulse and single-photon. Solid line represents the Gaussian approximation of the respective plots. The detection of bright pulse has 100.6 ps FWHM and single photon detection has 271.8 ps FWHM. D1 was biased at 2V V_{excess}, and triggered at 40 kHz

For detector control, another important requirement is that timing jitter for the bright pulses must be smaller than that of single-photons. We used a time-correlated single photon counting (TCSPC) technique (discussed in section B.3) to measurement the jitter for both single-photons and bright pulses. The width of the used bright pulses are 161 ps FWHM and the single-photon pulses are 147 ps FWHM. The resultant timing jitter for the D1 is shown in Fig. 7.8. We see that the control-pulse jitter is much shorter compared to the single-photon jitter. This fact will also enable Eve to control the timing of clicks at the Bob's detector. In addition, Eve can increase artificially the jitter width to imitate the single-photon detection. The results of the jitter measurements for the two diodes are summarized in table 7.1. We observed a reduced jitter at the larger efficiencies and higher mean photon numbers μ, due to the achieved larger click probability of the detectors. It is also seen that D2 jitter is larger compared to D1, probably due to the variations between

Table 7.1: Summary of time jitter for D1 and D2

Detector	V_{excess} (V)	Bright pulse		Single Photon	
		Blinding power (nW)	Jitter FWHM (ps)	Mean photon no. μ	Jitter FWHM (ps)
D1	2	3.26	111.8	0.12	358.86
				0.75	292.30
D1	5	100	63.6	0.09	63.83
				1.0	36.43
D2	2	46.5	120.9	0.11	365.01
				0.71	357.46
D2	5	100	132.7	67.0	56.98
				0.80	83.53

the samples. However, in all cases, single-photon jitter is larger than that of bright pulses, which demonstrate the detectors' vulnerability to the blinding attack.

7.6 Summary and discussions

This chapter showed that the NFAD detectors, running under our custom made readout, are controllable by Eve using bright illumination. However, Gaëtan *et al* explained two countermeasures in [268] to detect this attack. One method is keeping track of the current flow through the NFADs and the other one is high-bandwidth measurement. Since Eve's blinding control will cause the detectors to be always conductive even during the dead time, it will increase the average current flow. Therefore in the earlier method, Bob will be able to catch Eve's attack by monitoring the photocurrent through the NFADs. But Eve could apply a cleaver attack to reduce the mean photocurrent. She can attack the NFADs when they are active and stop blinding at the time of detectors' dead time. This way of attack will reduce the detector's mean photocurrent, which in turn keeps her presence secret to Bob. However, Bob will be able to catch these shortened attacks by utilizing high-bandwidth measurement. He needs to monitor the detector bias voltages using a high-bandwidth device. This would enable him to see the tiny deviations in the bias voltages caused by the detector voltage drop due to the blinding photocurrent. Thus incorporating countermeasures with the NFAD readout will ensure a secure long distance quantum communication.

Chapter 8

High-Speed Single-Photon Source for airborne demonstration of QKD

This chapter is a partial contribution to the publication [102].

8.1 Introduction

In satellite QKD, especially in the uplink configuration, quantum signals experience additional loss caused by the atmospheric turbulence. That leads to low signal compared to the background noise. The quantum sources are therefore required to generate quantum states at a high rate. It will ensure a better signal to noise ratio. Sate-of-the-art quantum sources feature pulse rate in the range of GHz [176, 291–293]. Most QKD implementations use either weak laser pulse (WCP) sources [32, 102, 294–298] or entangled photon-pair sources [31, 88, 299–303]. These quantum sources are expected to emit single photons within the shortest possible time frame to perform QKD over high-lossy channels in the uplink satellite communication schemes[100]. To meet that purpose, Yan *et.al* [100] built a 532 nm WCP source utilizing sum-frequency generation (SFG) of a pulsed Ti:Sapphire (Ti:Sp) 810 nm laser and a continuous laser at 1550 nm. However, this source is not suitable for satellite communications because of a few reasons. First, its repetition rate is low, limited to 76 MHz. Second, 532 nm is not the optimal wavelength for free-space communication. The other reason is, being a complicated and bulky laser, Ti: Sp is difficult to use in outdoor experiments. We therefore build a new source to overcome these limitations. Like Yan *et al*, our source also utilizes SFG of two laser frequencies, but it avoids the complicated lasers to accomplish a compact and movable system. Our source generates photons' polarization states at 785 nm, which was shown optimum for free-space communication [36]. The sum of 1550 nm laser pulses and 1590 nm continuous laser pulses generates the 785 nm output pulses. This approach enabled us to achieve a higher repetition rate up to 500 MHz using a pulsed laser with 300 ps pulse width. This source generates signal and decoy states to implement decoy-state BB84 QKD [304] system. This source was also successfully demonstrated in a QKD demonstration between a ground station and a flying receiver in an aircraft.

Previous source implementations using polarization degree of freedom incorporated different approaches. That includes use of multiple laser diodes combined with a polarization encoder [32, 104, 305–307], or a single laser combined with four semiconductor optical amplifiers [297]. These multiple device approaches need to ensure identical frequency, intensity, and bandwidth at the output quantum states. Otherwise, these will open loopholes, which can be exploited by an eavesdropper. Another approach for source incorporated a phase modulator with a Faraday mirror [308]. In which quantum states will suffer polarization modal dispersion while propagating through polarization-maintaining (PM) fiber, affecting the quality of produced states. A comparatively simple source demonstrated recently that utilizes a polarization modulator inside a Sagnac interferometer provides long-term temporal stability both at 800 nm and 1550 nm [309, 310]. However, this source is reported very recently, and still needs to be verified that how it performs for long distance QKD. Moreover, our source is built long before this newly reported source. This chapter explains our WCP source that ensures better thermal stability and is optimized at uplink wavelength.

8.2 Weak coherent pulse source

A WCP source generates coherent states that are quantized electromagnetic field state. These states are described as

$$|\alpha\rangle = e^{-\dfrac{|\alpha|^2}{2}} \sum \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{8.1}$$

A phase modulation of $\theta \in [0, 2\pi)$ on $|\alpha\rangle$ implements $|\alpha^{i\theta}\rangle$. Ideally, the phase of a coherent state must be randomized to implement a mixed state of Fock states [311] that follows a Poisson distribution with a mean photon number of $|\alpha|^2$. In practice, laser pulses are heavily attenuated to generate coherent states in WCP sources. There is a nonzero probability of generating other than single photons. The probability of finding n photons per pulse is found from the Poissson distribution as,

$$P(n|\mu) = \frac{\mu^n}{n!} e^{-\mu}, \tag{8.2}$$

here, μ is the mean photon number. So, the probability of finding a single-photon per pulse is:

$$P(1|\mu) = \mu e^{-\mu}. \tag{8.3}$$

When μ is close to 0.1–0.01, most of the pulses carry one photon. However, these sources occasionally generate more than one photon per pulse. Eve exploits these occurrences to enforce an attack, known as photon number splitting (PNS) attack [58, 58, 312]. In this attack, Eve could split up the multi-photon pulses, and keep one portion for herself while giving the other portion to Bob. This attack can be accomplished without being noticed Eve's presence by Alice and Bob. This will compromise the security of QKD. To overcome this sophisticated PNS attack, in 2003 W. Y. Hwang first proposed a decoy-state protocol [304].

8.2.1 Decoy state BB84 QKD

In the BB84 protocol using decoy states [304, 313, 314], Alice intentionally generates additional photon pulses (decoy pulses) apart from signal states. The μ is different in the decoy pulses and the signal states. Then Alice sends randomly these states to Bob and keeps a record of photon distribution of each pulse. This protocol use the signal states for key generation and the decoy pulses for identifying the PNS attack. The polarization of the decoy pulses are also randomized to make them indistinguishable from the signal states. The yield and the quantum bit error rate (QBER) for both types of the pulses must be similar. Generally, Eve is unaware about the photon number statistics of the two types of states, she only knows the number of photons per pulse. Her interruption will affect significantly the yield or QBER of signal or decoy states revealing Eve's presence. Thus, decoy state protocol provides a way to recognise PNS attack.

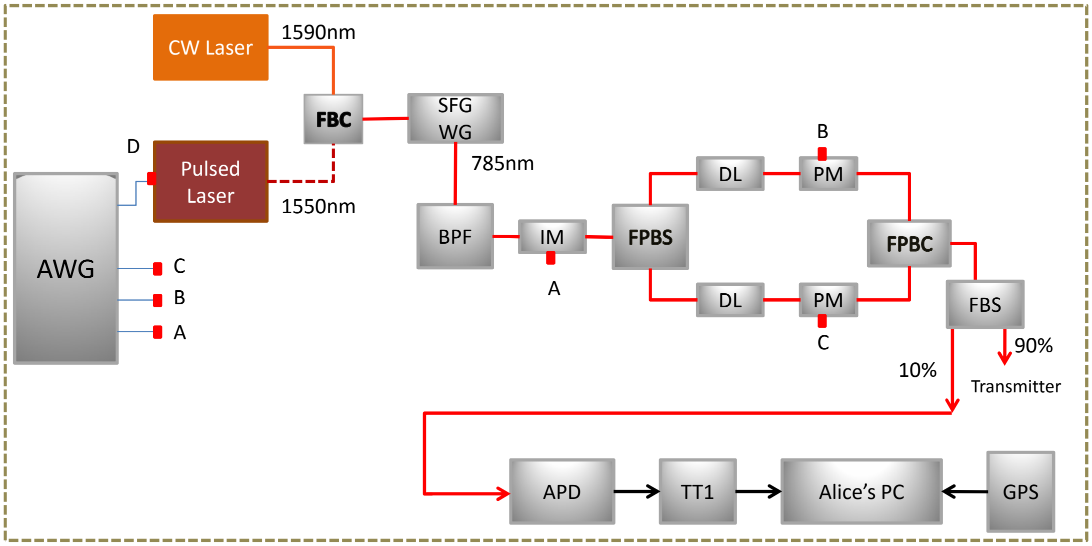


Figure 8.1: Schemetic of the high speed WCP polarized source. 785 nm pulses are generated by the sum frequency generation (SFG) waveguide combining a 1590 nm continuous wave (CW) laser and a pulsed 1550 nm laser. Acronyms are as follows: Arbitrary waveform generator (AWG); fiber beam coupler (FBC); Sum-frequency generation (SFG); Band pass filter (BPF); intensity modulator (IM); phase modulators (PM); fiber polarizing beam splitter (FPBS); delay line (DL), fiber beam splitter (FBS); avalanche photo diode (APD); TT1: time tagger unit; global positioning system (GPS).

8.3 High-speed decoy state WCP source

Figure 8.1 depicts the block diagram of our WCP source that generates polarized photons at 785 nm to implement decoy-state BB84 QKD. The source utilizes the sum-frequency generation (SFG) scheme to generate the 785 nm wavelength. This scheme takes the advantage of the high-speed pulsed lasers at telecom wavelengths, and thus avoids the difficulty of finding a high-speed 785 nm laser. The source uses optical intensity and phase modulators to generate decoy and signal states in a balanced Mach-Zehnder interferometer configuration. The source setup is explained into two sections: The preparation of 785 nm pulses and the modulation system.

Generation of 785 nm Pulses

First, a narrowband 1590 nm continuous (CW) laser was combined with a pulsed 1550 nm laser (id-300, 500 MHz) using a fiber coupled beam combiner (FBC). Then the combined optical beams travelled through a SFG waveguide that is a PPMgO:LN crystal (Periodically poled MgO doped lithium niobate) from HC Photonics [315]. PPMgO:LN is a highly efficient non linear crystal at THz frequencies which produces 785 nm pulses at its output. To ensure maximum optical power at the crystal's output, we characterized crystal's performance at various temperatures, illustrated in Fig. 8.2. For input wavelengths of 1551.72 nm and 1590.52 nm, the maximum output power at 785 nm wavelength was found to be 11.8 nW at 34.7 °C. Along with the desired 785 nm wavelength, the SFG crystal also generates output at 775 nm and 795 nm which are doubles of the crystal's input wavelengths, respectively. Therefore, a band pass filter (BPF) was used to allow only the desired wavelength to pass through discarding any undesired frequencies. In this setup, the trigger signals to the pulsed laser were provided by a 1.25 GHz arbitrary waveform generator (AWG) from Tabor Electronics [316].

Phase randomization

Our source utilizes passive phase randomization technique [317], where the pulsed laser was turned on and off to produce the pulses. The laser current remains completely off between the adjacent pulses and therefore these pulses do not have phase correlation among them. For many quantum information processing protocols especially in QKD, it is crucial to ensure continuous phase randomization between the consecutive pulses. Otherwise, one

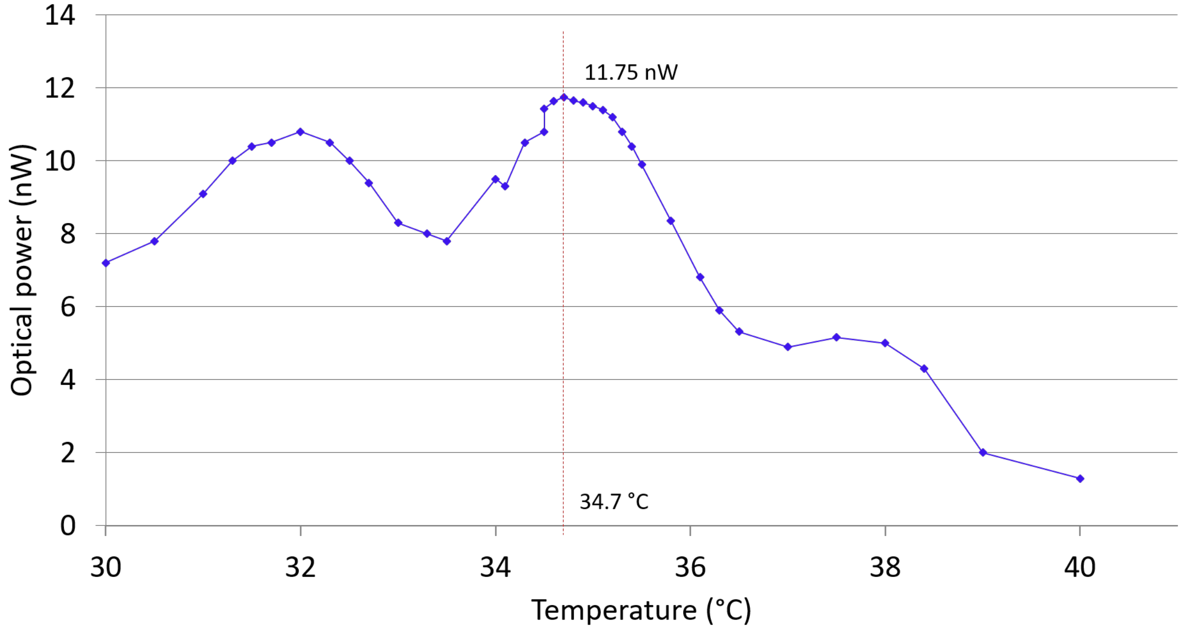


Figure 8.2: 785 nm optical power output of the SFG crystal with the changes of its temperatures. The two input wavelengths were 1551.72 nm and 1590.52 nm.

assumption of security proof will be violated [296, 318]. In addition, QKD systems can be hacked utilizing this phase correlations of the pulses [319, 320]

The Modulation system

To prepare polarized decoy and signal states, the modulator system includes an intensity modulator (IM) and two phase modulators (PMs) in the Mach-Zehnder configuration. The intensity and phase modulators are electro-optic LiNbO$_x$ (lithium niobate) 785 nm crystal from EOSpace. Each of the modulators has a radio frequency (RF) co-axial port to provide the driving voltages. The RF ports has external 50 Ω termination. These modulators features low insertion loss $<$ 3 dB, and requires only a few volts (around 2.2 V) to induce a π phase shift.

The IM works as a variable optical attenuator that controls the intensities of the input signals. The amount of attenuation is determined by the provided driving voltages. In this setup, IM generates vacuum, signal and decoy pulses with μ of 0, 0.5, and 0.1, respectively. The voltages at the IM are chosen carefully to obtain the expected μ values. The pulses then enter the MZI interferometer at diagonal polarization. The first polarizing beam splitter (PBS) at the front end of the MZI separates the orthogonal polarization into two

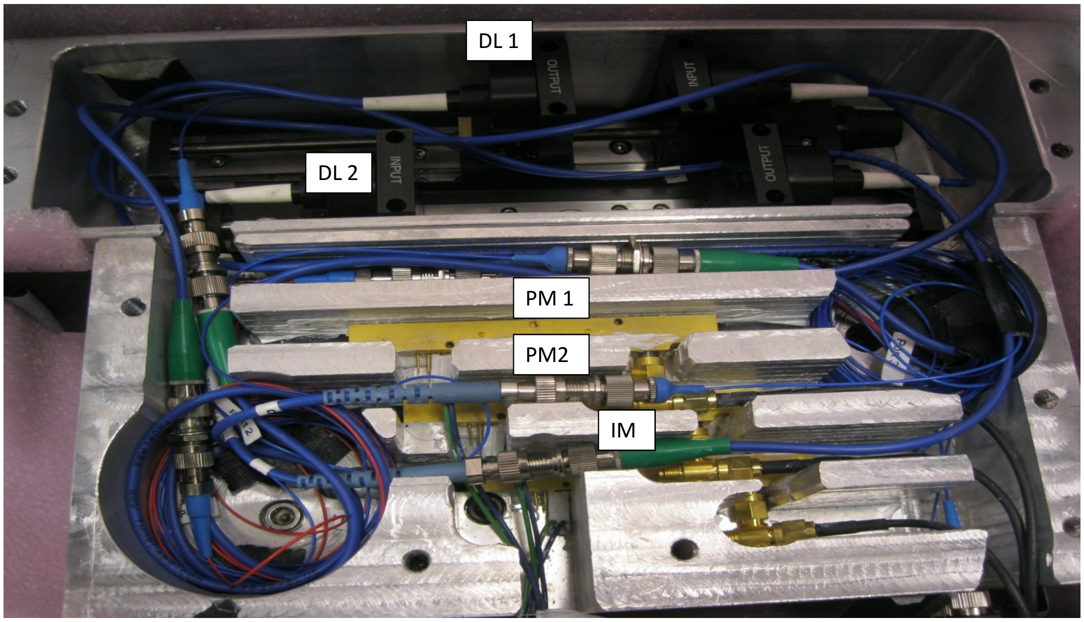


Figure 8.3: The modulator system. An aluminium housing contains the intensity modulator (IM), two phase modulators (PMs), two free space delay lines (DLs)

arms. The diagonal polarization of the input pulses ensures equal beam intensities entering into the two arms of the interferometer. Two free-space delay lines (DL) on the two arms of the MZI are used to balance the path lengths of them. A femtosecond laser giving a 50 fs pulse width is utilised during the delay lines adjustments. Each arm of the MZI also includes a PM that controls the relative phases of the horizontal (H) and vertical (V) polarizations in the two arms. We applied four different voltage combinations to the PMs to obtain four distinct phase differences between the states in the arms. When recombined, the MZI produces diagonal (D), anti-diagonal (A), right-circular (R), and left-circular (L) polarizations. The relative phase differences and the polarised states are explained as follows:

$$\begin{aligned}
\Delta\varphi &= 0; \;\; |H\rangle + |V\rangle = |D\rangle \\
\Delta\varphi &= \pi; \;\; |H\rangle - |V\rangle = |A\rangle \\
\Delta\varphi &= \frac{\pi}{2}; \;\; \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) = |R\rangle \\
\Delta\varphi &= -\frac{\pi}{2}; \;\; \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle) = |L\rangle
\end{aligned}$$

A subsequent rotation of the polarised states results in the four BB84 polarizations: H, V, D, and A. The states are generated randomly by driving the modulators with a random sequence of voltages to the IM and the PMs. The driving voltages are also provided by the AWG. All the modulators and the pulsed laser were triggered simultaneously to eliminate any loophole in the QKD. It was ensured by the AWG (model # WX1284C) we used, because it has four synchronized channels. Each channel is capable of supporting maximum 1.2 G sample per second per channel and has 4M memory capacity. This can be readily upgraded up to 8M per channel using already available highest memory capacity [316]. However, due to the limited AWG memory, we load a limited number of voltage sequences in each channel. Fig. 8.4 represents a random voltage sequence for the modulators and the 1550 pulsed laser. Each channels provide $4V_{P-P}$ into 50 Ω termination.

Fig. 8.3 shows the modulator system that is housed in an aluminium frame. The intensity modulator (IM), two phase modulators (PMs), two free space delay lines (DLs) are contained in an aluminium housing. The housing provides a good isolation from the environment and also acts as a good heat sink. The structure ensures long term thermal stability.

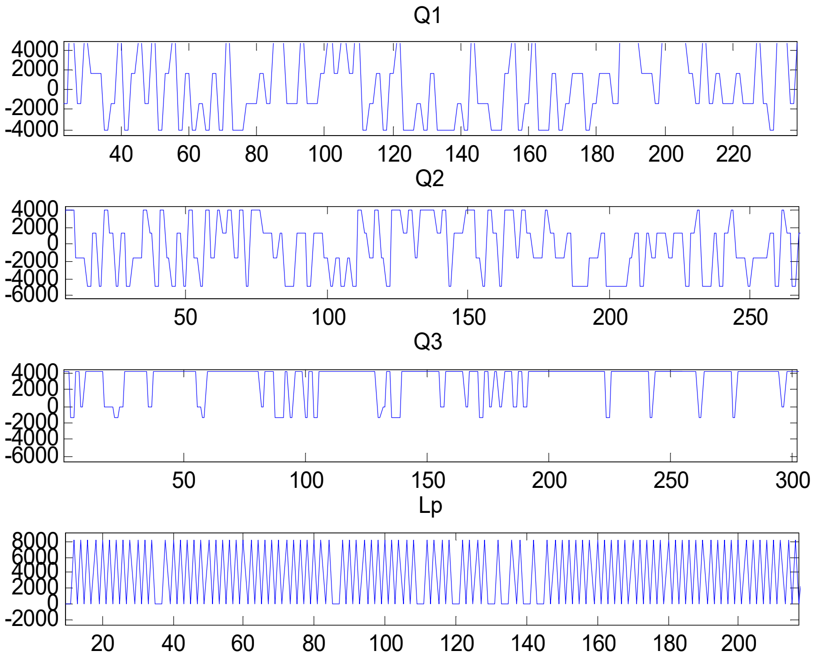
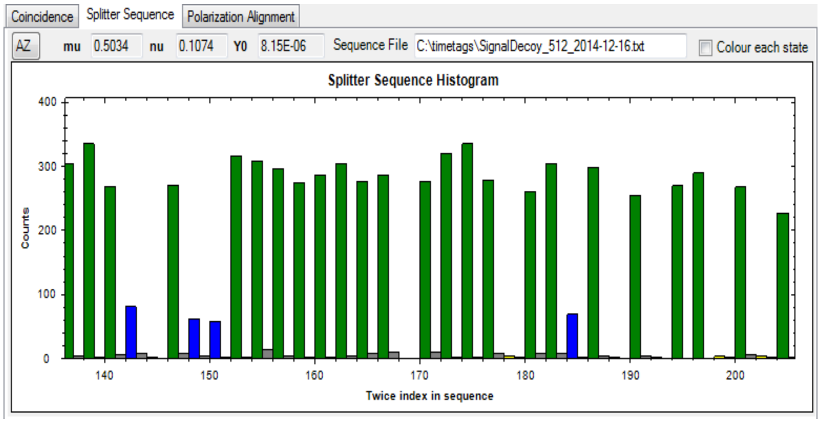


Figure 8.4: A sample of voltage sequences for the EO modulators and the pulsed laser.

Finally, when the polarization states are prepared, a fiber beam splitter (FBS) splits them into 90:10 ratio. 90% of the modulated signals are then transmitted to Bob and the remaining 10% are used for source characterization. Fig. 8.5 illustrates the sequence of polarized states measured by Alice.

To generate the random voltage sequences and then to load those on the AWG, two pieces of MATLAB code were written. One code generates the four voltage sequences for the modulators and the pulsed laser, and then saves those in four different files (see chapter C. Another code, known as VISA (Virtual Instrument standard architecture) program, interfaces the computer with the AWG. The VISA does the following tasks: i) opens up a session, ii) sets the repetition rate of the AWG, ii) loads the pre defined files in respective channels, iv) synchronously turns on the four output channels, and v) when requires closes the session. In each new session, the VISA loads different sequences at the channels, while in a particular session each channel repeats a single sequence. The length of each sequence can be extended by upgrading the AWG memory capacity up to 32 M.

Overall, the major features of our high-rate decoy state WCP source are as follows: 1) It prepares four non-orthogonal, BB84 states since the great advantage of polarization encoding is that earth's atmosphere preserves the polarization, 2) The pulsed laser synchronously operates with the intensity and phase modulators, 3) The balanced MZI configuration with two phase modulators in the two arms of MZI ensures higher visibility in the polarization states, 4) Provides maximum repetition rate of 500 MHz, which is limited by the speed of the pulsed laser. The rate can be scaled up to GHz by using a high repetition rate pulsed telecom laser, and 5) An aluminium enclosure for the modulator system provides more thermal stability,



mu 0.5034 nu 0.1074 Y0 8.15E-06 Sequence File C:\timetags\SignalDecoy_512_2014-12-16.txt

☐ Colour each state

Figure 8.5: A portion of the generated states measured by Alice. Height indicates the intensity, and color indicate types of pulses. Green represent signal states (0.5 photons/pulse), blue are decoy states (0.1 photon per pulse), and grey is the background measured between pulses (not used for QKD). The intensities for signal (mu), decoy (nu), and vacuum (Y0) are shown in the boxes on the top left

8.4 Airborne QKD demonstration

In 2016, our WCP source was used in an airborne QKD demonstration, between a ground station at Montague Airport, Smiths Falls and a Twin Otter research airplane from the National Research Council of Canada (NRC) [102]. During the flight, when the receiver on the aircraft came at the transmitter's line of sight, both tracked each other onward and established an optical link. The polarization states prepared at the ground station source were navigated through a transmitter telescope and then sent up to the receiver. Both the source and receiver kept records of the quantum states' polarization and their arrival times. Later this information was used for checking the correlation and post-processing to extract the secret key.

The experiment consisted of in total 14 night-time passes. The aircraft passes were at an altitude of around 1.6 km with distances of 3 km, 5 km, 7 km, 10 km from the ground station in the straight line paths and arc paths. Fig. 8.6 demonstrates two– 7 km line and arc paths.

During the test, our source generated signal, decoy and vacuum states, with probabilities of 80%, 14%, and 6% respectively. The source rate was 400 MHz. The sequences used for the intensity and phase modulators repeated in every 1000 pulses. Although this is not ideal for QKD systems, it was sufficient for the demonstration. 90% of the weak

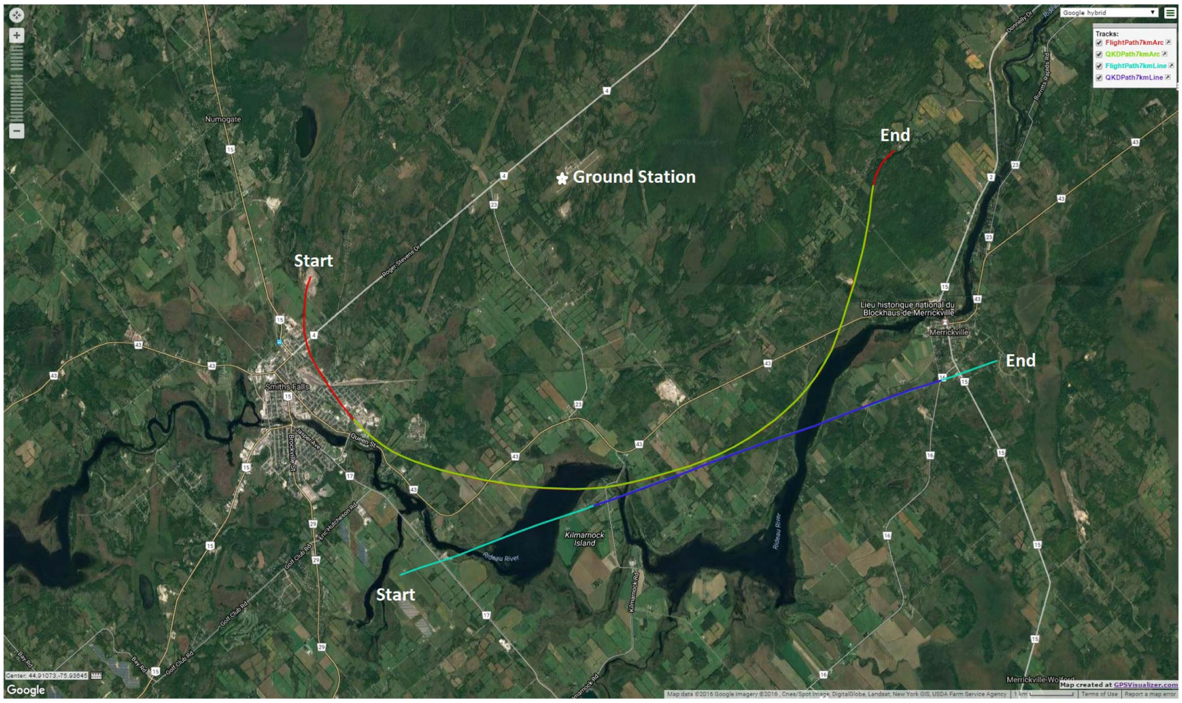


Figure 8.6: Flight paths from left to right. These are 7 km arc and line paths. The ground station located at the middle established a quantum link with the aircraft at the inner portion of each path. Reprinted from [102].

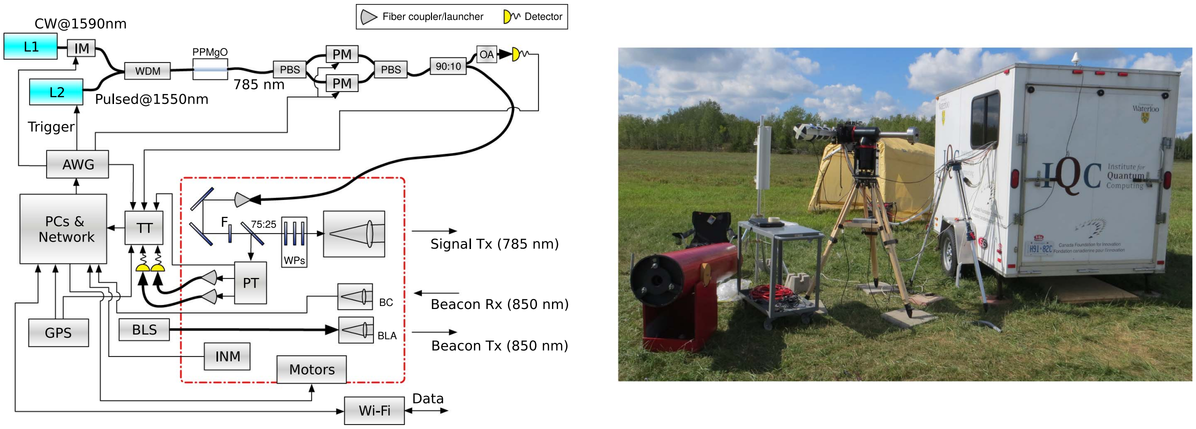


Figure 8.7: Apparatus used in the ground station. Left, the schematic diagram of the source and transmitter. Right, ground station at Smiths Falls–Montague airport. The source is located in the trailer, and the motor mount with attached transmitter telescope, and Wi-Fi antenna are outside. Reprinted from [102].

pulses are then guided to the transmitter and sent to the receiver on the aircraft by a 12 cm diameter refractive telescope. On the ground station, the source optics and electronics were kept inside a trailer to preserve the thermal and humid stability. The big telescope, and the Wi-Fi antenna were located outside just beside the trailer, as shown in Fig.8.7.

On the receiver side, a telescope with a 10 cm aperture facing out from the cabin door collected the incoming signals. An integrated optical assembly (IOA) containing a passive-basis-choice polarization analyser measured the signal into corresponding four BB84 states (H, V, D, and A). Four output fibers of the IOA were fiber coupled to the receiver's detector module that contains four Excelitas SLiK silicon single-photon avalanche diodes. Then, a control and data processing unit (CDPU) accumulated the detector events.

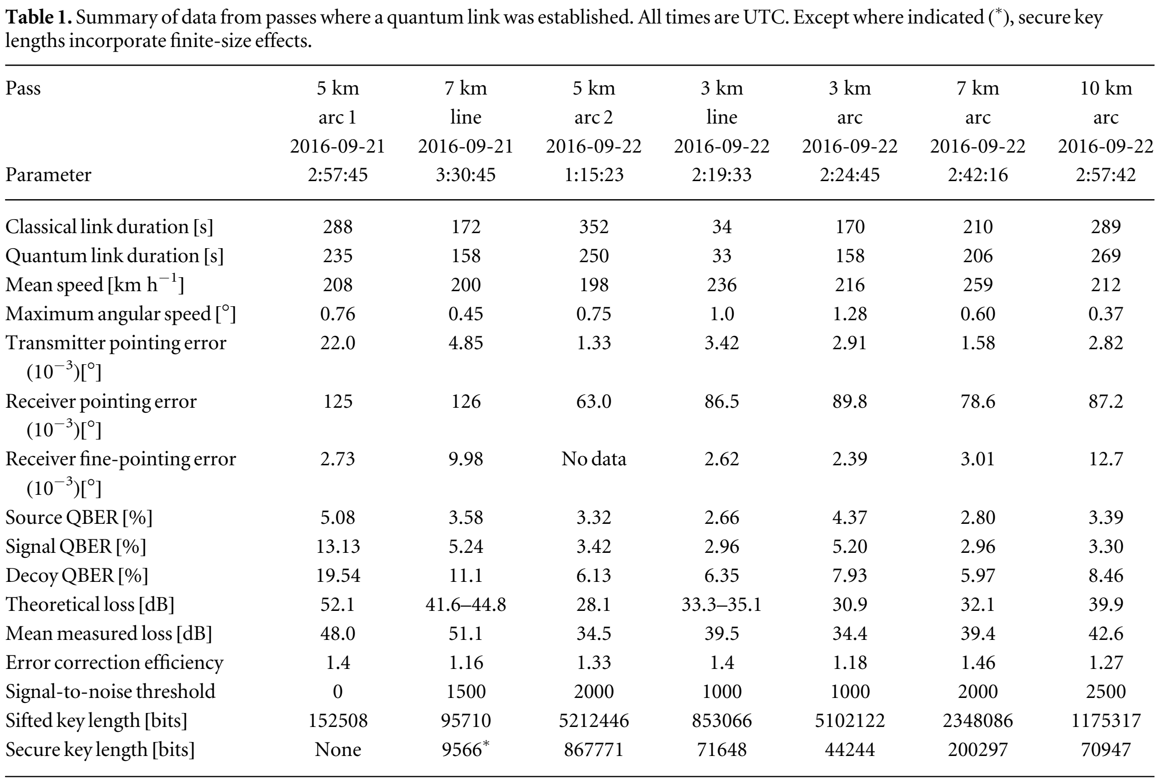


Table 1. Summary of data from passes where a quantum link was established. All times are UTC. Except where indicated (*), secure key lengths incorporate finite-size effects.

Pass Parameter	5 km arc 1 2016-09-21 2:57:45	7 km line 2016-09-21 3:30:45	5 km arc 2 2016-09-22 1:15:23	3 km line 2016-09-22 2:19:33	3 km arc 2016-09-22 2:24:45	7 km arc 2016-09-22 2:42:16	10 km arc 2016-09-22 2:57:42
Classical link duration [s]	288	172	352	34	170	210	289
Quantum link duration [s]	235	158	250	33	158	206	269
Mean speed [km h^{-1}]	208	200	198	236	216	259	212
Maximum angular speed [°]	0.76	0.45	0.75	1.0	1.28	0.60	0.37
Transmitter pointing error (10^{-3})[°]	22.0	4.85	1.33	3.42	2.91	1.58	2.82
Receiver pointing error (10^{-3})[°]	125	126	63.0	86.5	89.8	78.6	87.2
Receiver fine-pointing error (10^{-3})[°]	2.73	9.98	No data	2.62	2.39	3.01	12.7
Source QBER [%]	5.08	3.58	3.32	2.66	4.37	2.80	3.39
Signal QBER [%]	13.13	5.24	3.42	2.96	5.20	2.96	3.30
Decoy QBER [%]	19.54	11.1	6.13	6.35	7.93	5.97	8.46
Theoretical loss [dB]	52.1	41.6–44.8	28.1	33.3–35.1	30.9	32.1	39.9
Mean measured loss [dB]	48.0	51.1	34.5	39.5	34.4	39.4	42.6
Error correction efficiency	1.4	1.16	1.33	1.4	1.18	1.46	1.27
Signal-to-noise threshold	0	1500	2000	1000	1000	2000	2500
Sifted key length [bits]	152508	95710	5212446	853066	5102122	2348086	1175317
Secure key length [bits]	None	9566*	867771	71648	44244	200297	70947

Figure 8.8: Summary of the successful passes during trials. Reprinted from [102].

8.5 Results

Of the 14 aircraft passes, seven could establish quantum links successfully. The results of these passes are summarized in Fig. 8.8. The pass distances and the angular velocity were different. Circular-arc passes could maintain the quantum links for longer duration compared to the line paths, as because the receiver telescope managed to keep a constant position during the flight, which made it easier for the pointing system to establish and maintain the link. Nonetheless, the straight line paths are more similar to the satellite passes as the angular speed changed during the pass over the ground station. The angular speed was maximum when the aircraft was closest to the ground station: the maximum angular speed was measured $1.28°s^{-1}$ at the 3 km arc distance. Such speed is consistent with a LEO spacecraft, for instance, angular speed of the QEYSSat would be $0.72°s^{-1}$ at 600 km altitude, or for the International Space station it is $1.2°s^{-1}$. The total quantum link loss varied between 34.4–51.5 dB. The source QBER varied between 2.66%–5.08% for each pass. Of the successful passes, six could extract the secret key. Through this experiment the viability of an uplink satellite QKD was demonstrated.

Chapter 9

Conclusion and outlook

This thesis presented the results of my four research projects. In chapter 5, I discussed the design and development of a highly compact and miniaturized single-photon detector module (DM) that facilitates thermal and laser annealing, as well as detector characterization. This DM works together with a control board developed by our collaborating team at the University of Illinois Urbana-Champaign (UIUC) and forms the complete annealing payload. The control board contains high power lasers required for the laser annealing, a light source and a photodiode required for detector characterization, and a microcontroller. Our DM consists of four silicon single-photon avalanche photodiodes (SPADs): two Excelitas C30902SH and two Excelitas SLiK. The SPADs mounted on an aluminium plate is attached with the DM PCB, which contains SPAD bias and readout electronics, and an active temperature controller. Module operation is controlled by a Cypress programmable embedded system-on-chip (PSoC). Throughout the development process, we implemented three detector modules. The first module (DM1) was built to test the proof-of-principal operation of the detector PCB, which has a dimension of 95 mm × 95 mm × 40 mm (L × W × H). The second PCB (DM2) is the actual flight version with a proper CubeSat dimension (90 mm × 90 mm × 52 mm), that fits into the CubeSat bus. DM2 implementation considered the launching vibration, as well as the low-Earth orbit (LEO) thermal and vacuum environment. This completed module is now sent to the UIUC team for further test and under preparation for its launch. As of this writing, the UIUC team is continuing functional tests of the annealing payload, which has so far passed the second phase of the international space station safety panel and next will go over other safety tests and certifications. When ready for the actual launch, a 3U CubeSat bus will carry the payload to an LEO orbit in the CAPSat mission. The tentative time of the flight is sometime in 2020.

After the launch of the payload to an LEO, we will be able to conduct the annealing experiments in space. The time of operation of the DM will be controlled from a ground station. This test will provide us an insight about the radiation damage that occurs to in-space detector devices and the annealing methods. We will know the effectiveness of the annealing methods in mitigating the in-orbit damages. The success of this experiment will lead us to assess a few other issues before incorporating the system in the future satellite quantum receivers. One issue is analyzing the statistical fluctuations between the samples. For that, we need to test more samples in the real space environment. The second concern is, the high power laser used for the annealing also degrades over time due to the space radiation and temperature fluctuations. Their lifetime could also affect the mission lifetime. Therefore, a comprehensive study is required to analyze high power lasers' behaviour and their lifespan in space. The other problem is, we still need to find out an effective way for coupling the incoming single-photons from a ground station source and the annealing high power laser with the detectors.

However, in the meantime, prior the actual launch of the annealing payload, we built another detector module (DM3) in a similar manner as maintained during DM2 implementation. As of this writing, we are processing an experiment to perform annealing on the DM3 detectors in a thermal vacuum chamber. This experiment will allow us to analyze the performance of the overall module in vacuum that it will face in the lower Earth orbit.

In chapter 6, I explained a new simple design of an NFAD photon detection module that includes an active afterpulse suppression circuit. We used this module to characterize two NFAD samples. We found the maximum photon detection efficiencies of 8.5% and 6% for NFAD1 and NFAD2, respectively. These efficiencies are acceptable in the long-distance quantum communications where the channel loss is usually high. The study of the hold-off times on the DCR and afterpulsing probability showed that 20 μs of hold-off time is sufficient to achieve DCR below 100 Hz and highly reduced afterpulsing probability P_{AP}. At the 5 V of excess bias, where P_{AP} is generally high, a 20 μs hold-off time reduced the afterpulses significantly. At this hold-off time, the afterpulsing probabilities are 0.02 and 0.004 times of the probabilities at a 5 μs hold-off time for NFAD1 and NFAD2, respectively. This outcome demonstrates a noticeable afterpulse reduction capability of our readout module. Additionally, the maximum possible detection rate imposed by the 20 μs hold-off will not affect the long-distance quantum communications because of the low photon receiving rate at the receiver. Our new readout system also has an excellent timing resolution, which is around 75 ps and 62 ps FWHM for NFAD1 and NFAD2, respectively. The overall resultant characteristic parameters of the NFADs under our new readout system prove the system's as well as the detectors' suitability in the quantum optics applications at telecommunication wavelengths.

Chapter 7 discussed the blinding attack of the NFADs mentioned above using bright illumination. Our experiment demonstrated the detectors' vulnerability to the attack that is utilized by an Eavesdropper to leak quantum information. This attack on the detectors can be prevented by incorporating countermeasures, such as by monitoring detector current, or through measurement using high bandwidth devices [268].

Finally, in chapter 8, I presented the development of a high-speed weak coherent pulsed (WCP) source. Our WCP source modulator uses phase and intensity modulators to generate polarization quantum states at different intensities to implement decoy-state BB84 protocol. Its maximum repetition rate is 500 MHz, which can be upgraded in the range of GHz by replacing the pulsed laser with a GHz speed laser. However, this source running at 400 MHz was used in a ground station to transmit polarized qubits to a receiver located on a flying aircraft. This QKD demonstration established a secure key of length 70947 bits in a 269 s duration at a 10 km distance.

Appendix A

Mechanical and Electrical models of the CAPSat Detector Module

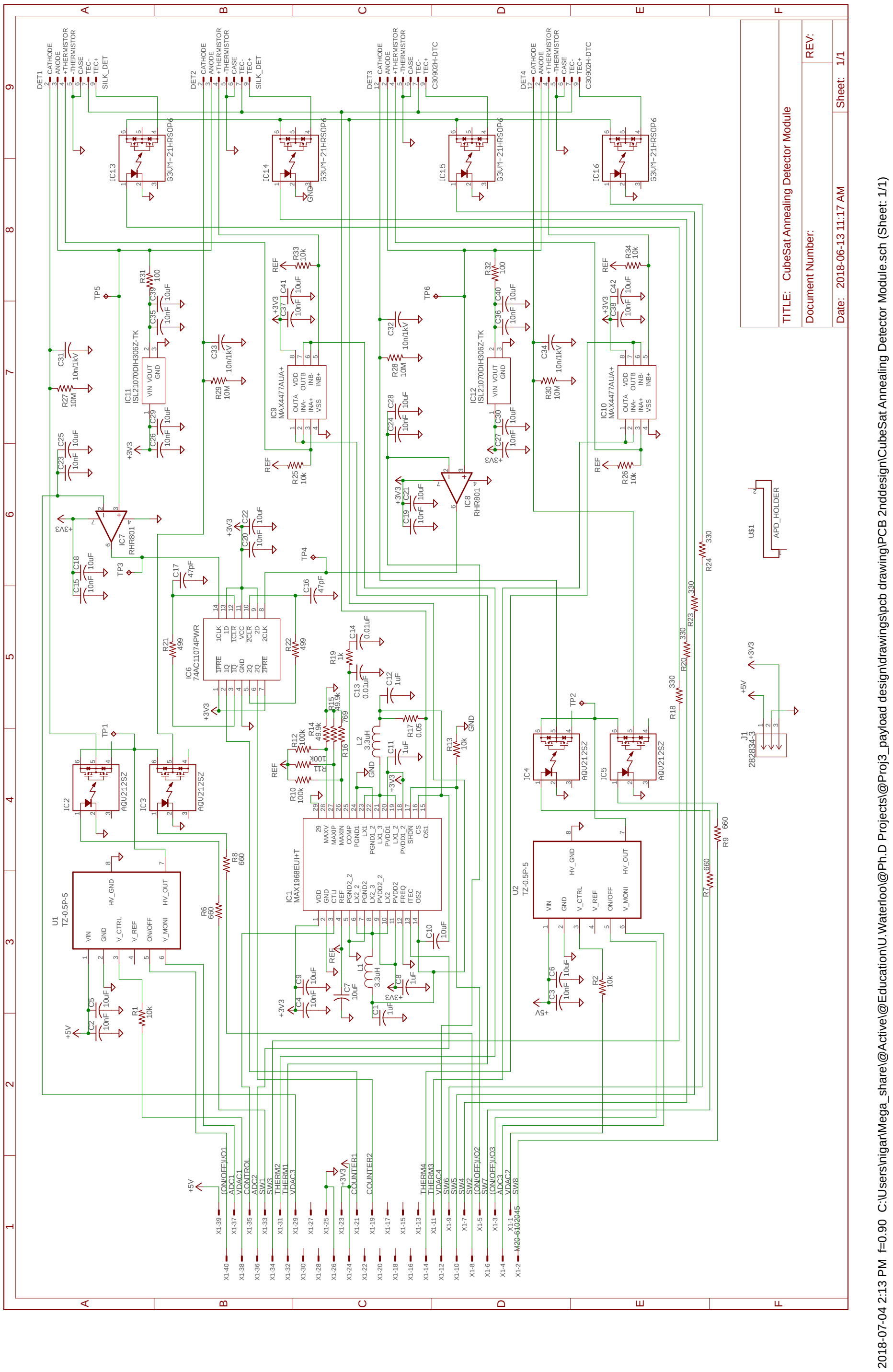


Figure A.1: PCB schematic of the CAPSat detector module.

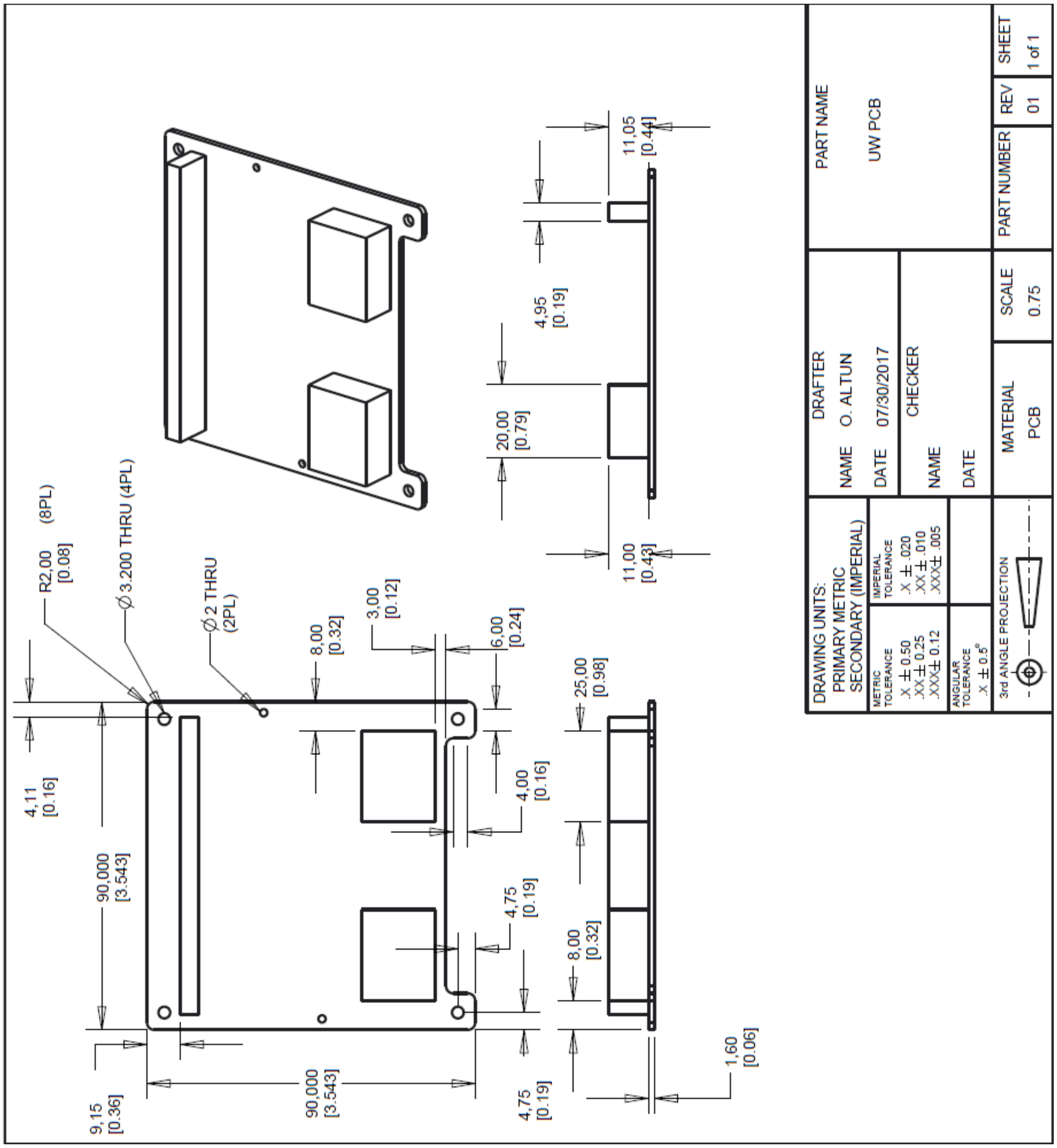


Figure A.2: Engineering drawing of the DM2 and DM3 PCB with the high voltage supply loaded. Courtesy to University of Illinois.

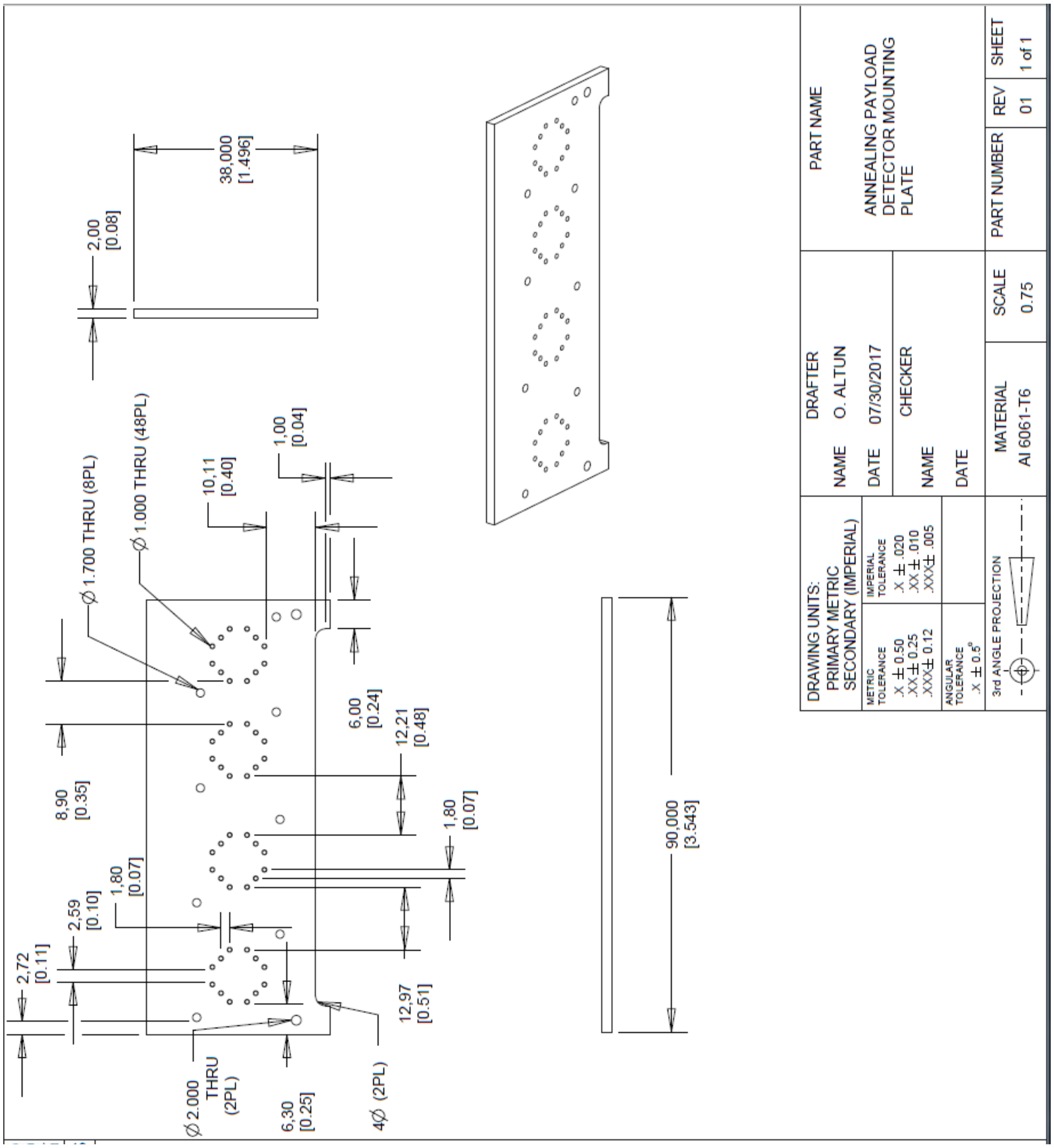


Figure A.3: Engineering drawing of the DM2 and DM3 detector mounting plate.

Appendix B

Supporting details for characterization of negative feedback avalanche diode

B.1 Formula for detection efficiency

Photons from a weak coherent pulsed (WCP) source, usually a highly attenuated laser pulses, follows Poisson distribution [321]. When these photons are detected by a single-photon detector having a quantum efficiency of η_{D}, the probability of detection can be written as

$$P(n) = e^{-\mu\eta_D}\frac{\mu^n}{n!} \tag{B.1}$$

Here, P(n) is the probability of detecting n photons, μ is the mean photon number, and η_D is the detector's efficiency. Detectors should not click for the laser pulses containing no photon. The probability of no photon is

$$P(0) = e^{-\mu\eta_D} \tag{B.2}$$

and if the laser pulses contain one or more photons, detectors will click. The probability of detection due to photon is therefore

$$P(\geq 1) = 1 - e^{-\mu\eta_D} \tag{B.3}$$

However, practical single-photon detectors have some dark count probability d_{c}, which are generally thermally generated carriers. Due to these dark counts, the detectors produce extra click events even at the absence of photons. So, the total click probability of the detectors within a time window τ_o will be

$$\begin{aligned}
P(D) \quad &= \text{Click probability due to photon} + \text{Click probability due to dark counts}\\
\Rightarrow \quad & P(D) = (1 - e^{-\mu\eta_D}) + e^{-\mu\eta_D} d_c\tau_o\\
\Rightarrow \quad & e^{-\mu\eta_D}(1 - d_c\tau_o) = 1 - P(D)\\
\Rightarrow \quad & e^{-\mu\eta_D} = \frac{1 - P(D)}{1 - d_c\tau_o}\\
\Rightarrow \quad & \mu\eta_D = -ln\frac{1 - P(D)}{1 - d_c\tau_o}\\
\Rightarrow \quad & \eta_D = -\frac{1}{\mu}ln\frac{1 - P(D)}{1 - d_c\tau_o} \qquad \text{(B.4)}
\end{aligned}$$

If the laser triggers at a rate of f_{trig} and the detector clicks at a rate of R_{det}, then the detection efficiency η_{D} can be written as

$$\eta_D = -\frac{1}{\mu}ln\frac{1 - \frac{R_{\text{det}}}{f_{\text{trig}}}}{1 - d_c\tau_o} \qquad \text{(B.5)}$$

Equation B.5 gives the detection efficiency of a single photon detector when a WCP source is used.

B.2 Photon number calibration

To do the photon number calibration, we used a high power laser (OPO Ti:Sp) at 1310.44 nm to determine the loss factor of the attenuator. In our setup, the attenuator consisted of a 90:10 beam splitter (BS) followed by a digital variable optical attenuator (VOA: OZ optics: DA-100-3U-1300/1550-9/125-S-50). The optical input was first attenuated by feeding it into the 10% arm of the BS, which was further weakened by the VOA. By measuring the optical power at the input (P_{I}) and output (P_{O}), we calculated the total loss (Eq. B.6) of the attenuator combination. We also considered the losses through the fibers that were contained in the optical path. The cleanliness of the fibers and the FC/PC connectors have a significant contribution to the total loss.

$$\text{Loss} = 10\ Log_{10}\frac{P_{\text{O}}}{P_{\text{I}}} \qquad \text{(B.6)}$$

Once the loss of the attenuator was carefully determined for different loss settings in the VOA (which were used later with the low power pulsed laser), we switched the OPO TI:Sp with the low power pulsed laser id-300. From the measured input power of id-300 and the known attenuation factor, the output optical power P$_O$ that was illuminated on the detector was found using equation B.6. Then the number of photons per pulse was estimated by

$$N_P = \frac{P_O}{f_{tr}.h\nu} \tag{B.7}$$

Where f_{tr} is the laser trigger frequency, and $h\nu$ is the photon energy at wavelength of laser. Thus, this procedure gave us the photon flux for various attenuations.

B.3 Timing jitter measurement using oscilloscope

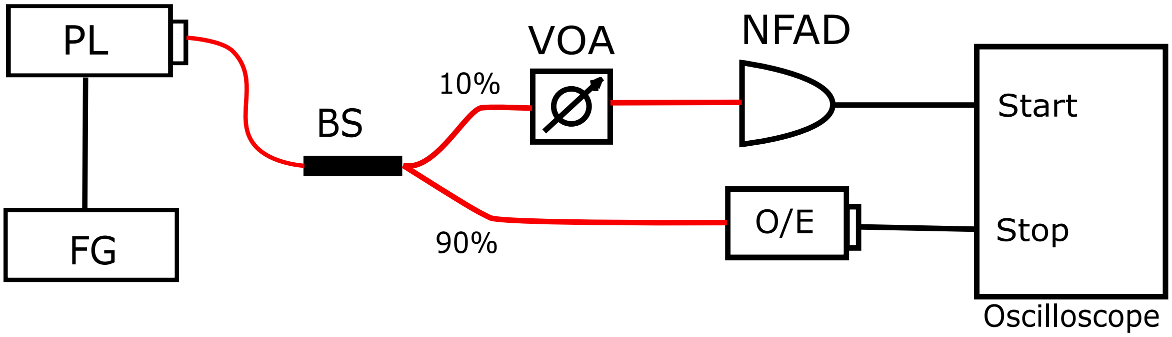
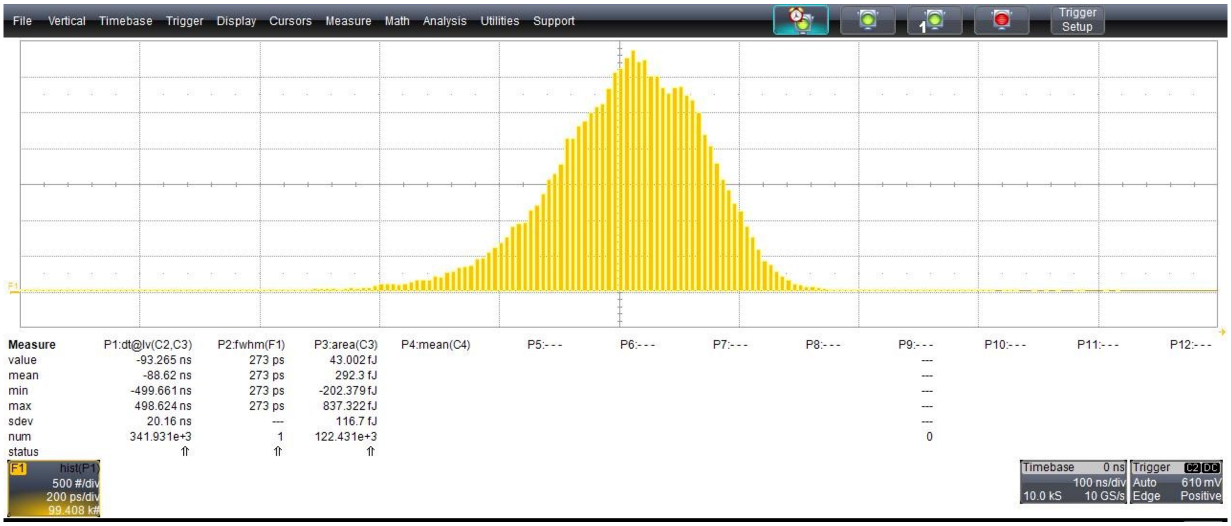


Figure B.1: Timing jitter measurement setup using oscilloscope. The acronym are PL: pulsed laser, FG: function generator, VOA: variable optical attenuator, O/E: optical to electrical converter. The start channel on the oscilloscope refers that the trigger was set on this channel.

We used a 6 GHz Lecroy wavepro 760Zi oscilloscope (OSC) to measure the timing jitter of the NFADs. The scheme is illustrated in B.1. Photons from a pulsed laser (id-300), with a pulse width of 147.2 ps FWHM and triggered at a rate of 40 kHz, were sent to an NFAD (at the 10% arm of BS). Its detection signals were the trigger signals in the OSC. On the other hand, 90% of the pulsed optical output (PL), following an optical to electrical conversion (O/E: LeCroy OE455, DC-3.5 GHz), were also fed to the OSC as stop signals. The time differences between the two signals were calculated as a function P1 within the OSC. The threshold voltages for the two OSC input signals were kept fixed: half of the amplitude for detection signals and one-quarter of full amplitude for the optical signals. A histogram of P1 for ∼100 K counts were generated in OSC to measure the timing jitter of the counting module. Fig. B.2 illustrates a histogram of the time differences between the signals. Then a Gaussian plot was produced from the histogram in Matlab, and the standard deviation (σ) and the full width at half maximum (FWHM) were calculated using equations B.8 and B.9, respectively.



Measure	P1:dt@lv(C2,C3)	P2:fwhm(F1)	P3:area(C3)	P4:mean(C4)	P5:- - -	P6:- - -	P7:- - -	P8:- - -	P9:- - -	P10:- - -	P11:- - -	P12:- - -
value	-93.265 ns	273 ps	43.002 fJ						---			
mean	-88.62 ns	273 ps	292.3 fJ						---			
min	-499.661 ns	273 ps	-202.379 fJ						---			
max	498.624 ns	273 ps	837.322 fJ						---			
sdev	20.16 ns	---	116.7 fJ						---			
num	341.931e+3	1	122.431e+3						0			
status	⇑	⇑	⇑									

F1 hist(P1)
500 #/div
200 ps/div
99.408 k#

Timebase 0 ns
100 ns/div
10.0 kS 10 GS/s

Trigger C2 DC
Auto 610 mV
Edge Positive

Figure B.2: Histogram in oscilloscope for the time differences between the laser input and the detector signals.

$$\sigma = \frac{C}{\sqrt{2}} \tag{B.8}$$

$$J_T \text{ (FWHM)} = 2\sigma\sqrt{2log2} \tag{B.9}$$

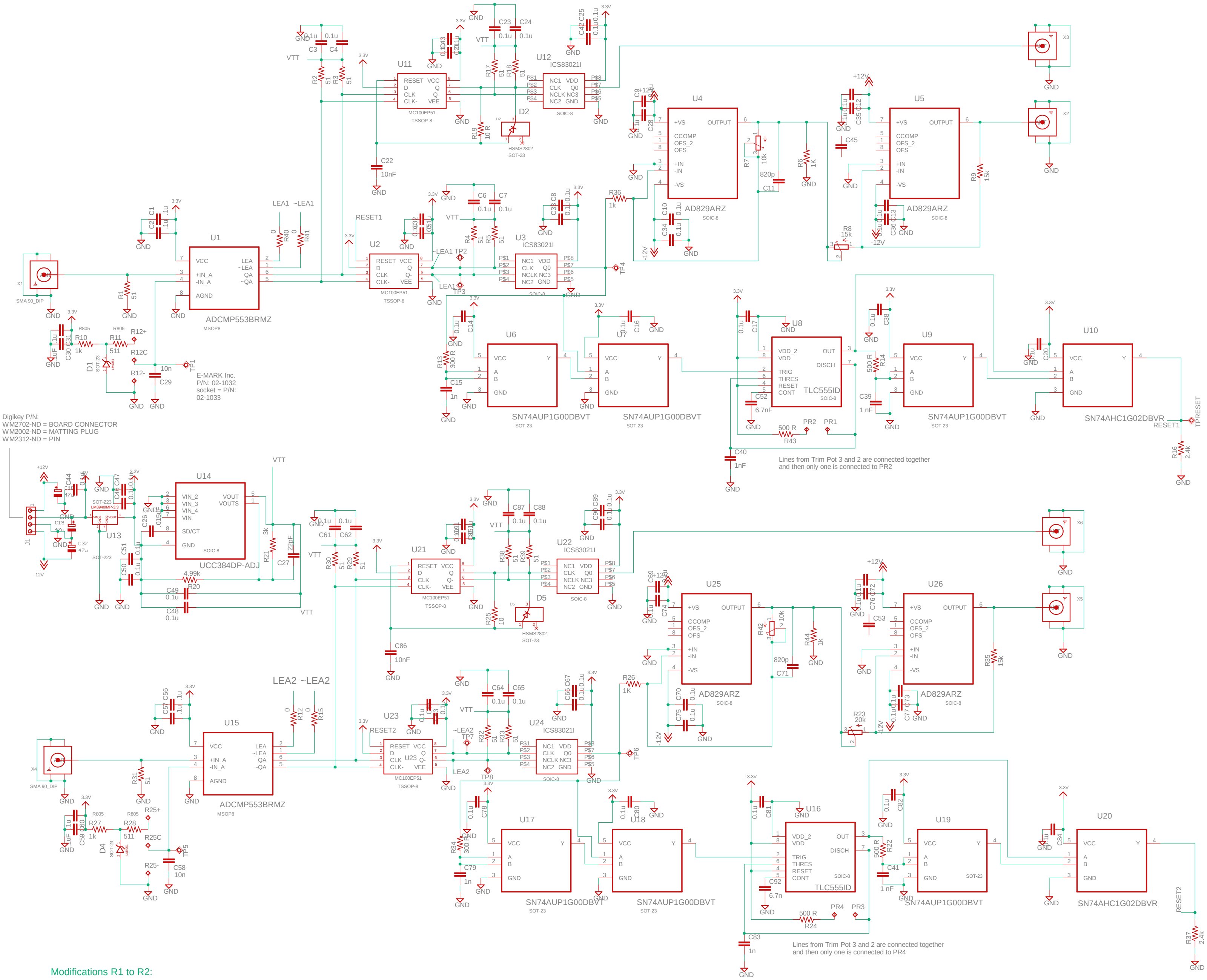
here C is a coefficient found from the Gaussian distribution that defines the width of the distribution.

The timing jitter found following this process includes the jitter contribution from all the devices involved in the setup. We measured the overall jitter by gradually increasing the photon flux. The jitter decreases with the increase of photon flux, as illustrated in Fig. B.3. For sufficiently high photon flux, the jitter asymptotically reaches a minimum value, which was considered as the overall jitter contribution from all connected devices. It was only $\sim$ 40 ps, and we therefore neglected the jitter contribution from the OSC and the O/E. Hence, the timing jitter of the counting module was found using the formula (B.10).

$$\Delta t_{\text{jitter}} = \sqrt{J_T^2 - J_L^2} \tag{B.10}$$

here, J_T is the measured jitter and J_L is the laser pulse width, which was $\sim$ 147 ps FWHM.

B.3.1 Schematic of the pulse processing module (PPM) printed circuit board (PCB)



E-MARK Inc.
P/N: 02-1032
socket = P/N:
02-1033

Digikey P/N:
WM2702-ND = BOARD CONNECTOR
WM2002-ND = MATTING PLUG
WM2312-ND = PIN

Lines from Trim Pot 3 and 2 are connected together
and then only one is connected to PR2

Lines from Trim Pot 3 and 2 are connected together
and then only one is connected to PR4

Modifications R1 to R2:

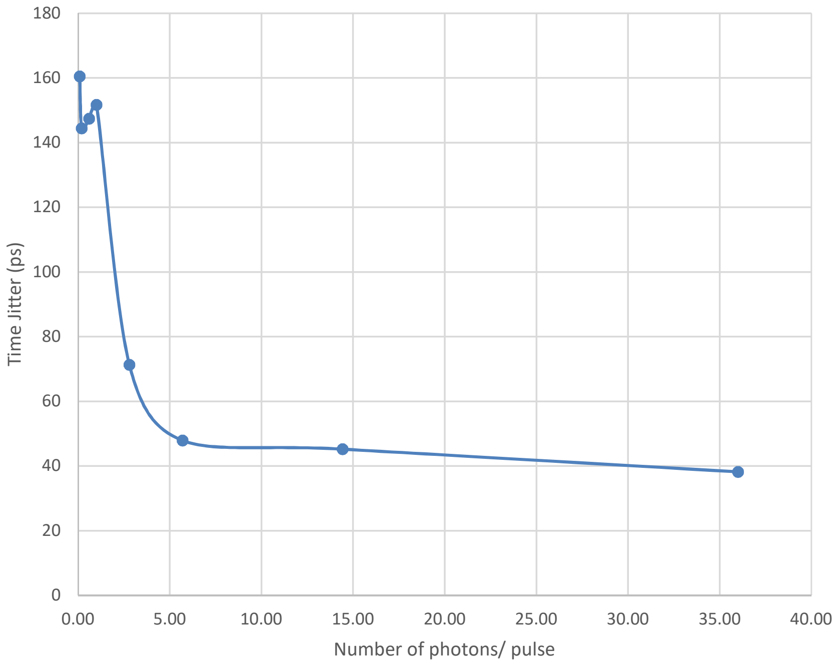


Figure B.3: Measured timing jitter with respect to various number of photons per pulse. Jitter is smaller for larger number of photon flux.

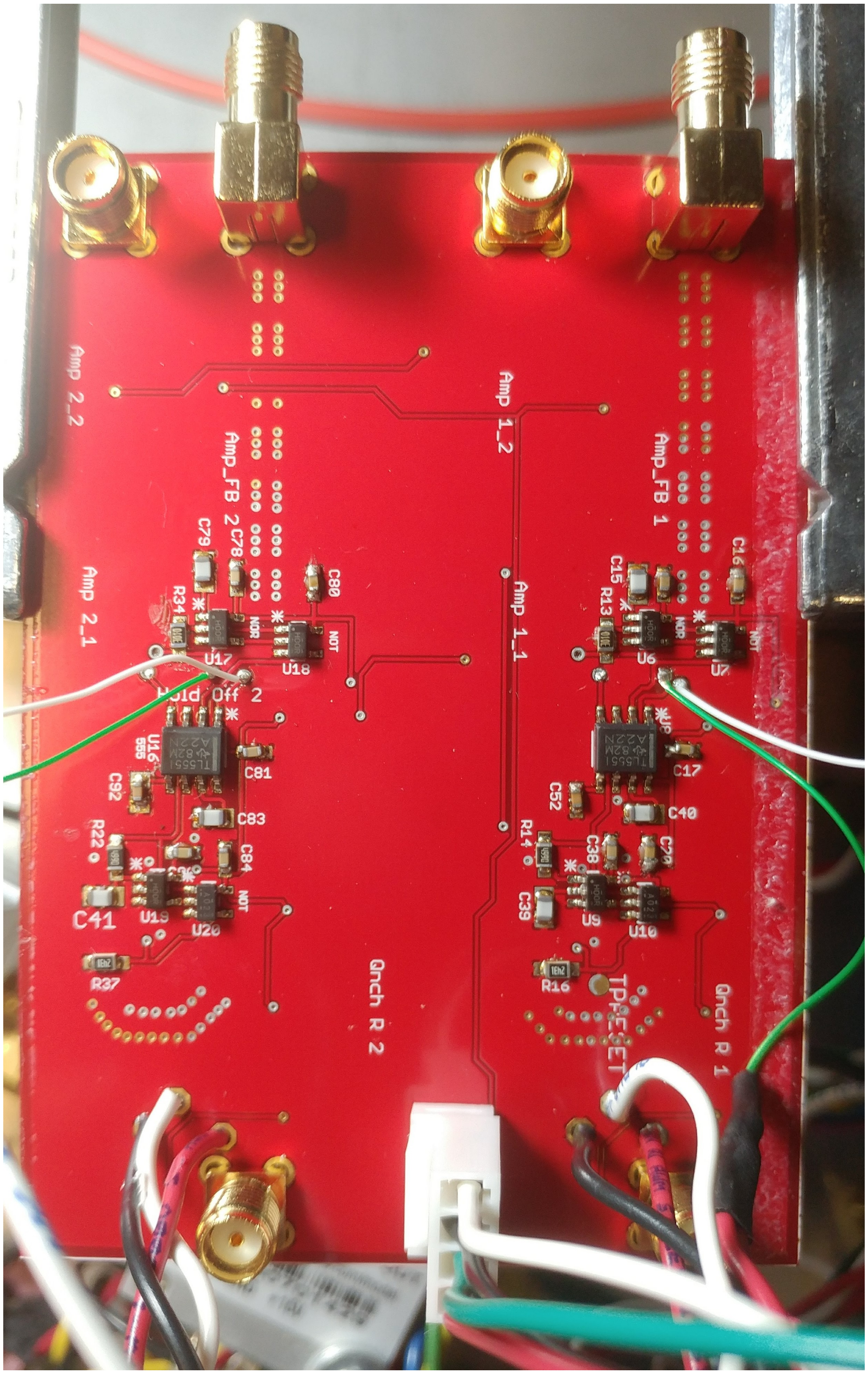


Figure B.4: Top view of the PPM PCB

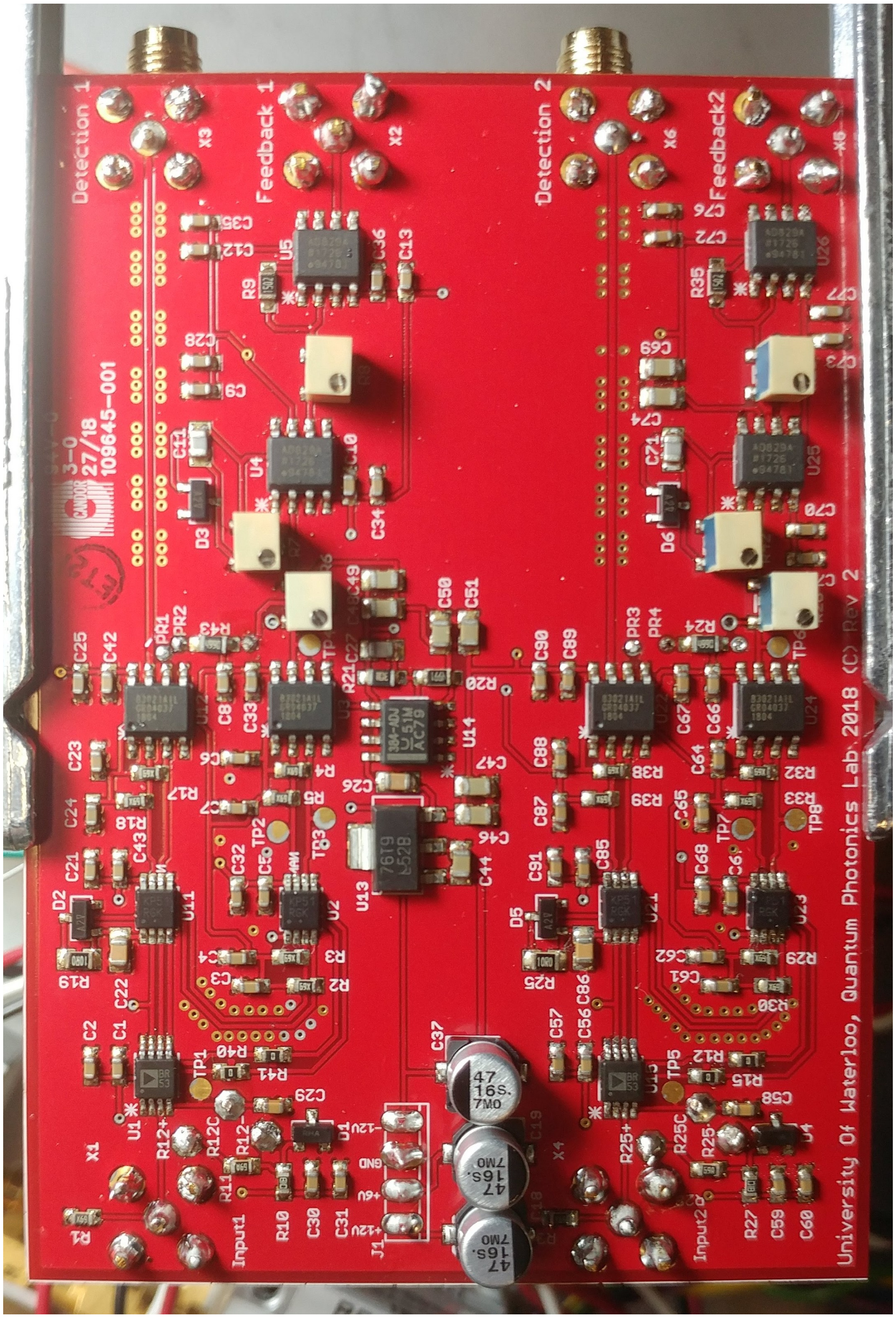


Figure B.5: Bottom view of the PPM PCB

Appendix C

MATLAB code to generate the modulation sequence

```

warn=0;          %will turn to 1 if voltages are not appropriate

DAQ_Q1_max=voltmax;        %max voltage of the DAQ for the ...
    corresponding channel
DAQ_Q2_max=voltmax;        %max voltage of the DAQ for the ...
    corresponding channel
DAQ_Q3_max=voltmax;        %max voltage of the DAQ for the ...
    corresponding channel
DAQ_Lp_max=voltmax;        %max voltage of the DAQ for the ...
    corresponding channel

V_H=Vpi/8+offset_H;
V_V=3*Vpi/8+offset_V;
V_D=Vpi/8+offset_D;
V_A=3*Vpi/8+offset_A;

%Signals begins;

Lp=zeros(seq_no,1);
Q1=zeros(seq_no,1);
Q2=zeros(seq_no,1);
Q3=zeros(seq_no,1);

for j=1:seq_no

```

```
%The IDquantique laser needs pulses to trigger, so we have to make ...
    the signal
%alternate from max to 0. To accomodate this we assign each modulator ...
    points
%two identical values. Therefore, each pulse periods create 2 ...
    identical points
%for each modulators and 1 on and 1 off point for the laser, ...
    resulting in
%2*seq_no number of points for the DAQ. This also means the QKD ...
    system will
%run at half the DAQ frequency (i.e. 1GHz will give 0.5GHz laser and ...
    modulator frequency).

    if (int_vect(j)==0)       %Vacuum pulses, laser does not trigger
        Lp(1+mod(Lp_d+2*j-1,2*seq_no))=0;
        Q1(2*j-1)=0;
        Q1(2*j)=0;
        Q2(2*j-1)=0;
        Q2(2*j)=0;
        Q3(1+mod(Q1_d+2*j-1,2*seq_no))=Vac;
        Q3(1+mod(Q1_d+2*j-2,2*seq_no))=Vac;
    else
        Lp(1+mod(Lp_d+2*j-1,2*seq_no))=2;
    end
        Lp(1+mod(Lp_d+2*j-2,2*seq_no))=0;

    if (int_vect(j)==1)
        Q3(1+mod(Q1_d+2*j-1,2*seq_no))= Sig;
        Q3(1+mod(Q1_d+2*j-2,2*seq_no))= Sig;
    elseif (int_vect(j)==2)
        Q3(1+mod(Q1_d+2*j-1,2*seq_no))=Decoy;
        Q3(1+mod(Q1_d+2*j-2,2*seq_no))=Decoy;
    end

    if (pol_vect(j)==1)
        Q1(2*j-1)=V_H;
        Q1(2*j)=V_H;
        Q2(2*j-1)=-V_H;
        Q2(2*j)=-V_H;
    elseif (pol_vect(j)==2)
        Q1(2*j-1)=-V_V;
        Q1(2*j)=-V_V;
        Q2(2*j-1)=V_V;
        Q2(2*j)=V_V;
    elseif (pol_vect(j)==3)
        Q1(2*j-1)=-V_D;
        Q1(2*j)=-V_D;
        Q2(2*j-1)=V_D;
        Q2(2*j)=V_D;
    elseif (pol_vect(j)==4)
        Q1(2*j-1)=V_A;
        Q1(2*j)=V_A;
        Q2(2*j-1)=-V_A;
        Q2(2*j)=-V_A;
    end;

end

if max(abs(Q1)) > DAQ_Q1_max
    warning('Q1 goes outside bounds!')
    warn=1;
end
if max(abs(Q2)) > DAQ_Q2_max
    warning('Q2 goes outside bounds!')
    warn=1;
end
if max(abs(Q3)) > DAQ_Q3_max
    warning('Q3 goes outside bounds!')
    warn=1;
end
if max(abs(Lp)) > DAQ_Lp_max
    warning('Lp goes outside bounds!')
    warn=1;
end

%converting data into 14 bit format
Q1=int16((2^13-1)*Q1/DAQ_Q1_max);
Q2=int16((2^13-1)*Q2/DAQ_Q2_max);
Q3=int16((2^13-1)*Q3/DAQ_Q3_max);
Lp=int16((2^13-1)*Lp/DAQ_Lp_max);

%writing to the binary file
fid1= fopen('Q1.wav', 'w');
fid2= fopen('Q2.wav', 'w');
fid3= fopen('Q3.wav', 'w');
fid4= fopen('Lp.wav', 'w');
fwrite(fid1,Q1,'int16',0,'l');
fwrite(fid2,Q2,'int16',0,'l');
fwrite(fid3,Q3,'int16',0,'l');
fwrite(fid4,Lp,'int16',0,'l');
fclose(fid1);fclose(fid2);fclose(fid3);fclose(fid4);


%ploting the voltages
subplot(4,1,1);plot(Q1),title('Q1')
subplot(4,1,2);plot(Q2),title('Q2')
subplot(4,1,3);plot(Q3),title('Q3')
subplot(4,1,4);plot(Lp),title('Lp')

%End of the program%
```

References

[1] NIST-FIPS Standard. Announcing the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197(1-51):3–3, 2001.

[2] The National Institute of Standards NIST and Technology. https://csrc.nist.gov/csrc/media/publications/sp/800-67/rev-2/draft/documents/sp800-67r2-draft.pdf, Cited 2019.

[3] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[4] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[5] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[6] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[7] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[8] Lov K Grover. A fast quantum mechanical algorithm for database search. *arXiv preprint quant-ph/9605043*, 1996.

[9] Chad Rigetti. The rigetti 128-qubit chip and what it means for quantum. *Medium*, 2018.

[10] Craig Gidney and Martin Ekerå. How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. *arXiv preprint arXiv:1905.09749*, 2019.

[11] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography.* US Department of Commerce, National Institute of Standards and Technology, 2016.

[12] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[13] A.K. Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[14] Werner Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. In *Original Scientific Papers Wissenschaftliche Originalarbeiten*, pages 478–504. Springer, 1985.

[15] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[16] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[17] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[18] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities. *Physical review letters*, 49(2):91, 1982.

[19] Cerberis QKD system. http://www.qphotonics.com/Multimode-fiber-coupled-laser-diode-4W-808nm.html, cited 2019.

[20] MagiQ Technologies. http://www.magiqtech.com/, ccited 2019.

[21] SeQureNet. https://www.cbinsights.com/company/sequrenet, Cited 2019.

[22] P. D. Townsend, J. G. Rarity, and P. R. Tapster. Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel. *Electronics Letters*, 29(14):1291–1293, 1993.

[23] Jacques Breguet, Antoine Muller, and Nicolas Gisin. Quantum cryptography with polarized photons in optical fibres: Experiment and practical limits. *Journal of Modern Optics*, 41(12):2405–2412, 1994.

[24] J. D. Franson and H. Ilves. Quantum cryptography using polarization feedback. *Journal of Modern Optics*, 41(12):2391–2396, 1994.

[25] 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. *Physical Review Letters*, 81(15):3283, 1998.

[26] W. T. Buttler, R. J. Hughes, P.G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Free-space quantum-key distribution. *Physical Review A*, 57(4):2379, 1998.

[27] Richard J. Hughes, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux, Gabriel G. Luther, George L. Morgan, Jane E. Nordholt, and C. Glen Peterson. Quantum cryptography for secure free-space communications. In *Free-Space Laser Communication Technologies XI*, volume 3615, pages 98–103. International Society for Optics and Photonics, 1999.

[28] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.

[29] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbacha, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Free-space distribution of entanglement and single photons over 144 km. *Nature Physics*, 3:481–486, 2007.

[30] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[31] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[32] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43, 2017.

[33] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70, 2017.

[34] Hideki Takenaka, Alberto Carrasco-Casado, Mikio Fujiwara, Mitsuo Kitamura, Masahide Sasaki, and Morio Toyoshima. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nature photonics*, 11(8):502, 2017.

[35] Xiaoli Sun, Michael A Krainak, James B Abshire, James D Spinhirne, Claude Trottier, Murray Davies, Henri Dautet, Graham R Allan, Alan T Lukemire, and James C Vandiver. Space-qualified silicon avalanche-photodiode single-photon-counting modules. *Journal of Modern Optics*, 51(9-10):1333–1350, 2004.

[36] J. P. Bourgoin, E. Meyer-Scott, Brendon L. Higgins, B. Helou, Chris Erven, Hannes Huebel, B. Kumar, D Hudson, Ian D'Souza, Ralph Girard, et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.

[37] Elena Anisimova, Brendon L. Higgins, Jean-Philippe Bourgoin, Miles Cranmer, Eric Choi, Danya Hudson, Louis P. Piche, Alan Scott, Vadim Makarov, and Thomas Jennewein. Mitigating radiation damage of single photon detectors for space applications. *EPJ Quantum Technology*, 4(1):10, 2017.

[38] Masters thesis of Ian DSouza. Silicon avalnche photodiodes for satellite based quantum communication, 2018.

[39] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov. Laser damage helps the eavesdropper in quantum cryptography. *Physical review letters*, 112(7):070503, 2014.

[40] Jin Gyu Lim, Elena Anisimova, Brendon L. Higgins, Jean-Philippe Bourgoin, Thomas Jennewein, and Vadim Makarov. Laser annealing heals radiation damage in avalanche photodiodes. *EPJ Quantum Technology*, 4(1):11, 2017.

[41] Xiaoli Sun, Daniel Reusser, Henri Dautet, and James B Abshire. Measurement of proton radiation damage to si avalanche photodiodes. *IEEE transactions on Electron Devices*, 44(12):2160–2166, 1997.

[42] Yue Chuan Tan, Rakhitha Chandrasekara, Cliff Cheng, and Alexander Ling. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *Optics express*, 21(14):16946–16954, 2013.

[43] Xiaoli Sun and Henri Dautet. Proton radiation damage of si apd single photon counters. In *2001 IEEE Radiation Effects Data Workshop. NSREC 2001. Workshop Record. Held in conjunction with IEEE Nuclear and Space Radiation Effects Conference (Cat. No. 01TH8588)*, pages 146–150. IEEE, 2001.

[44] Martino Marisaldi, Piera Maccagnani, Francesco Moscatelli, Claudio Labanti, Fabio Fuschino, Michela Prest, Alessandro Berra, Davide Bolognini, Massimo Ghioni, Ivan Rech, et al. Single photon avalanche diodes for space applications. In *2011 IEEE Nuclear Science Symposium Conference Record*, pages 129–134. IEEE, 2011.

[45] Ivan Prochazka, Karel Hamal, and Lucas Král. Single photon counting module for space applications. *Journal of Modern Optics*, 54(2-3):151–161, 2007.

[46] Francesco Moscatelli, Martino Marisaldi, Piera Maccagnani, Claudio Labanti, Fabio Fuschino, Michela Prest, Alessandro Berra, Davide Bolognini, Massimo Ghioni, Ivan Rech, et al. Radiation tests of single photon avalanche diode for space applications. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 711:65–72, 2013.

[47] Jin Gyu Lim. Laser annealing irradiated silicon single-photon avalanche photodiodes for quantum satellite receiver, 2018.

[48] University of Illinois at Urbana-Champaign. Illinois wins nasa awards for three cubesat missions. https://aerospace.illinois.edu/news/illinois-wins-nasa-awards-three-cubesat-missions, 2016.

[49] M.A. Itzler, X. Jiang, B. Nyman, and K. Slomkowski. InP-based negative feedback avalanche diodes. In *SPIE OPTO: Integrated Optoelectronic Devices*, pages 72221K–72221K. International Society for Optics and Photonics, 2009.

[50] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686, 2010.

[51] V Makarov, A Anisimov, and S Sauge. Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by eve. *arXiv preprint arXiv:0809.3408*, pages 1–4, 2009.

[52] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, 11(6):065003, 2009.

[53] Lars Lydersen, Johannes Skaar, and Vadim Makarov. Tailored bright illumination attack on distributed-phase-reference protocols. *Journal of Modern Optics*, 58(8):680–685, 2011.

[54] Jean-Philippe Bourgoin, Nikolay Gigov, Brendon L Higgins, Zhizhong Yan, Evan Meyer-Scott, Amir K Khandani, Norbert Lütkenhaus, and Thomas Jennewein. Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations. *Physical Review A*, 92(5):052339, 2015.

[55] idQuantique. `http://www.idquantique.com/`, cited 2019.

[56] Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7):481, 2007.

[57] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 9(3):163, 2015.

[58] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3, 1992.

[59] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, JF Dynes, et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[60] Masahide Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics express*, 19(11):10387–10409, 2011.

[61] V. Scarani, B.-P. Helle, N.J. Cerf, D. Miloslav, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[62] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[63] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[64] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4(1):82, 2002.

[65] C. Simon, M. Afzelius, J. Appel, A. B. de La Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, et al. Quantum memories. *The European Physical Journal D*, 58(1):1–22, 2010.

[66] Evan Meyer-Scott, Zhizhong Yan, Allison MacDonald, Jean-Philippe Bourgoin, Hannes Hübel, and Thomas Jennewein. How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss. *Physical Review A*, 84(6):062326, 2011.

[67] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, and A. Setharaman. Performance comparison of bb84 and b92 satellite-based free space quantum optical communication systems in the presence of channel effects. *Journal of Optical Communications*, 32(1):37–47, 2011.

[68] Canadian Space agenecy. Quantum encryption and science satellite (qeyssat). http://www.asc-csa.gc.ca/eng/sciences/qeyssat.asp, Cited 2019.

[69] Erik Kerstel, Arnaud Gardelein, Mathieu Barthelemy, Matthias Fink, Siddarth Koduru Joshi, Rupert Ursin, CSUG Team, et al. Nanobob: a cubesat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technology*, 5(1):6, 2018.

[70] James A Grieve, Robert Bedington, Zhongkan Tang, Rakhitha CMRB Chandrasekara, and Alexander Ling. Spooqysats: Cubesats to demonstrate quantum key distribution technologies. *Acta Astronautica*, 151:103–106, 2018.

[71] Daniel KL Oi, Alex Ling, Giuseppe Vallone, Paolo Villoresi, Steve Greenland, Emma Kerr, Malcolm Macdonald, Harald Weinfurter, Hans Kuiper, Edoardo Charbon, et al. Cubesat quantum communications mission. *EPJ Quantum Technology*, 4(1):6, 2017.

[72] J. A. Griev, R. Bedington, Z. Tang, R. C.M.R.B. Chandrasekara, and A. Ling. Spooqysats: Cubesats to demonstrate quantum key distribution technologies. *Acta Astronautica*, 151:103–106, 2018.

[73] Thomas Scheidl, Eric Wille, and Rupert Ursin. Quantum optics experiments using the international space station: a proposal. *New Journal of Physics*, 15(4):043008, 2013.

[74] T. Jennewein, J. P. Bourgoin, B. Higgins, C. Holloway, E. Meyer-Scott, C. Erven, B. Heim, Z. Yan, H. Hübel, G. Weihs, et al. Qeyssat: a mission proposal for a quantum receiver in space. In *Advances in Photonics of Quantum Computing, Memory, and Communication VII*, volume 8997, page 89970A. International Society for Optics and Photonics, 2014.

[75] T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, J. P. Bourgoin, H. Hakima, B. Higgins, and R. Zee. The nanoqey mission: ground to space quantum key and entanglement distribution using a nanosatellite. In *Emerging technologies in security and defence II; and quantum-physics-based information security III*, volume 9254, page 925402. International Society for Optics and Photonics, 2014.

[76] Josep Maria Perdigues Armengol, Bernhard Furch, Clovis Jacinto de Matos, Olivier Minster, Luigi Cacciapuoti, Martin Pfennigbauer, Markus Aspelmeyer, Thomas Jennewein, Rupert Ursin, Tobias Schmitt-Manderbach, et al. Quantum communications at esa: towards a space experiment on the iss. *Acta Astronautica*, 63(1-4):165–178, 2008.

[77] Martin Pfennigbauer, Walter Leeb, Markus Aspelmeyer, Thomas Jennewein, and Anton Zeilinger. *Free-space optical quantum key distribution using intersatellite links.* na, 2003.

[78] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Ground test of satellite constellation based quantum communication. *arXiv preprint arXiv:1611.09982*, 2016.

[79] Jane Qiu. Quantum communications leap out of the lab. *Nature News*, 508(7497):441, 2014.

[80] K. Boone, J. P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon. Entanglement over global distances via quantum repeaters with satellite links. *Physical Review A*, 91(5):052325, 2015.

[81] Thomas Jennewein and Brendon Higgins. The quantum space race. *Physics World*, 26(03):52, 2013.

[82] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, et al. Satellite-relayed intercontinental quantum network. *Physical review letters*, 120(3):030501, 2018.

[83] John S Bell. Speakable and unspeakable in quantum mechanics. *Cambridge University*, 1987.

[84] John G. Rarity, Phil M. Gorman, P. R. Knight, Harald Weinfurter, and Christian Kurtsiefer. Quantum communications in space. In *Quantum Communications and Quantum Imaging*, volume 5161, pages 240–252. International Society for Optics and Photonics, 2004.

[85] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, 2017.

[86] Yue Chuan Tan, Rakhitha Chandrasekara, Cliff Cheng, and Alexander Ling. Radiation tolerance of opto-electronic components proposed for space-based quantum key distribution. *Journal of Modern Optics*, 62(20):1709–1712, 2015.

[87] Jane E Nordholt, Richard J Hughes, George L Morgan, C Glen Peterson, and Christopher C Wipf. Present and future free-space quantum key distribution. In *Free-Space Laser Communication Technologies XIV*, volume 4635, pages 116–127. International Society for Optics and Photonics, 2002.

[88] Markus Aspelmeyer, Thomas Jennewein, Martin Pfennigbauer, Walter R Leeb, and Anton Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6):1541–1551, 2003.

[89] Cristian Bonato, Andrea Tomaello, Vania Da Deppo, Giampiero Naletto, and Paolo Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, 2009.

[90] Christopher J. Pugh, Jean-Francois Lavigne, Jean-Philippe Bourgoin, Brendon L. Higgins, and Thomas Jennewein. Adaptive optics benefit for quantum key distribution uplink from ground to a satellite. *arXiv preprint arXiv:1906.04193*, 2019.

[91] A. A. M. Saleh. 9.4-an investigation of laser wave depolarization due to atmospheric transmission. *IEEE Journal of Quantum Electronics*, 3(11):540–543, 1967.

[92] B. C. Jacobs and J. D. Franson. Quantum cryptography in free space. *Optics Letters*, 21(22):1854–1856, 1996.

[93] Richard J Hughes, William T Buttler, Paul G Kwiat, Steve K Lamoreaux, George L Morgan, Jane E Nordholt, and C Glen Peterson. Free-space quantum key distribution in daylight. *Journal of Modern Optics*, 47(2-3):549–562, 2000.

[94] William T Buttler, Richard J Hughes, Steve K Lamoreaux, George L Morgan, Jane E Nordholt, and C Glen Peterson. Daylight quantum key distribution over 1.6 km. *Physical Review Letters*, 84(24):5652, 2000.

[95] Richard J Hughes, Jane E Nordholt, Derek Derkacs, and Charles G Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New journal of physics*, 4(1):43, 2002.

[96] Christian Kurtsiefer, P. Zarda, Matthus Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419(6906):450, 2002.

[97] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, et al. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269, 2012.

[98] Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185, 2012.

[99] Jean-Philippe Bourgoin, Brendon L. Higgins, Nikolay Gigov, Catherine Holloway, Christopher J. Pugh, Sarah Kaiser, Miles Cranmer, and Thomas Jennewein. Free-space quantum key distribution to a moving receiver. *Optics express*, 23(26):33437–33447, 2015.

[100] Zhizhong Yan, Evan Meyer-Scott, Jean-Philippe Bourgoin, Brendon L Higgins, Nikolay Gigov, Allison MacDonald, Hannes Hübel, and Thomas Jennewein. Novel high-speed polarization source for decoy-state bb84 quantum key distribution over free space and satellite links. *Journal of Lightwave Technology*, 31(9):1399–1408, 2013.

[101] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382, 2013.

[102] Christopher J. Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Jeongwan Jin, Nigar Sultana, Sascha Agne, Elena Anisimova, Vadim Makarov, Eric Choi, Brendon L.

Higgins, et al. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology*, 2(2):024009, 2017.

[103] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, Yan-Lin Tang, et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nature Photonics*, 7(5):387, 2013.

[104] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Physical Review Letters*, 115(4):040502, 2015.

[105] Juan Yin, Yuan Cao, Shu-Bin Liu, Ge-Sheng Pan, Jin-Hong Wang, Tao Yang, Zhong-Ping Zhang, Fu-Min Yang, Yu-Ao Chen, Cheng-Zhi Peng, et al. Experimental quasi-single-photon transmission from satellite to earth. *Optics express*, 21(17):20032–20040, 2013.

[106] Austrian and Chinese Academies of Sciences successfully conducted first inter-continental quantum video call. https://www.oeaw.ac.at/en/austrian-academy-of-sciences/the-oeaw/article/erstes-abhoersicheres-quanten-videotelefonat-zwischen-wien-und-peking-geglueckt-1 [2017].

[107] Siddarth Koduru Joshi, Jacques Pienaar, Timothy C. Ralph, Luigi Cacciapuoti, Will McCutcheon, John Rarity, Dirk Giggenbach, Jin Gyu Lim, Vadim Makarov, Ivette Fuentes, et al. Space quest mission proposal: experimentally testing decoherence due to gravity. *New journal of physics*, 20(6):063016, 2018.

[108] European quantum communications networs takes shape. https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/European_quantum_communications_network_takes_shape, 2019.

[109] Morio Toyoshima. Trends in satellite communications and the role of optical free-space communications. *Journal of Optical Networking*, 4(6):300–311, 2005.

[110] T. Jono and Y. Takayama. N. kura, k. ohinata, y. koyama, k. shiratama, z. sodnik, b. demelenne, a. *Bird and K. Arai, OICETS on-orbit laser communication experiments, Proc. SPIE*, 6105:13–23, 2006.

[111] Morio Toyoshima, Hideki Takenaka, Yozo Shoji, Yoshihisa Takayama, Yoshisada Koyama, and Hiroo Kunimori. Results of kirari optical communication demonstration

experiments with nict optical ground station (koden) aiming for future classical and quantum communications in space. *Acta Astronautica*, 74:40–49, 2012.

[112] Kevin Günthner, Imran Khan, Dominique Elser, Birgit Stiller, Ömer Bayraktar, Christian R Müller, Karen Saucke, Daniel Tröndle, Frank Heine, Stefan Seel, et al. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica*, 4(6):611–616, 2017.

[113] William Morong, Alexander Ling, and Daniel Oi. Quantum optics for space platforms. *Optics and Photonics News*, 23(10):42–49, 2012.

[114] Zhongkan Tang, Rakhitha Chandrasekara, Yau Yong Sean, Cliff Cheng, Christoph Wildfeuer, and Alexander Ling. Near-space flight of a correlated photon system. *Scientific reports*, 4:6366, 2014.

[115] Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Kadir Durak, and Alexander Ling. The photon pair source that survived a rocket explosion. *Scientific reports*, 6:25603, 2016.

[116] Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel KL Oi, and Alexander Ling. Generation and analysis of correlated pairs of photons aboard a nanosatellite. *Physical Review Applied*, 5(5):054022, 2016.

[117] Robert Bedington, Xueliang Bai, Edward Truong-Cao, Yue Chuan Tan, Kadir Durak, Aitor Villar Zafra, James A Grieve, Daniel KL Oi, and Alexander Ling. Nanosatellite experiments to enable future space-based qkd missions. *EPJ Quantum Technology*, 3(1):12, 2016.

[118] Denis P Naughton, Robert Bedington, Simon Barraclough, Tanvirul Islam, Doug Griffin, Brenton Smith, Joe Kurtz, Andrey S Alenin, Israel J Vaughn, Arvind Ramana, et al. Design considerations for an optical link supporting intersatellite quantum key distribution. *Optical Engineering*, 58(1):016106, 2019.

[119] Richard J Hughes and Jane E Nordholt. Free-space communications: Quantum space race heats up. *Nature Photonics*, 11(8):456, 2017.

[120] Pumpkin, Inc. https://www.pumpkinspace.com/, printed in May, 2019.

[121] Innovative Solutions in Space. https://www.isispace.nl/, printed in May, 2019.

[122] Candian space agency. What is a cubesat. http://www.asc-csa.gc.ca/eng/satellites/cubesat/what-is-a-cubesat.asp. [cited 2019].

[123] Achieving science with cubesats: thinking inside the box. committee on achieving science goals with cubesats, space studies board, division on engineering and physical sciences, natioanl academies of sciences, engineering, and medicine, 2016.

[124] J Puig-Suari, R Coelho, R Munakata, and A Chin. The cubesat: The picosatellite standard for research and education. In *AIAA Space 2008 Conference and Exhibition, San Diego*, pages 9–11, 2008.

[125] J Muylaert, R Reinhard, C Asma, J Buchlin, P Rambaud, and M Vetrano. Qb50: An international network of 50 cubesats for multi-point, in-situ measurements in the lower thermosphere and for re-entry research. In *ESA Atmospheric Science Conference, Barcelona, Spain*, pages 7–11, 2009.

[126] Adam Wuerl and Melissa Wuerl. Lessons learned for deploying a microsatellite from the international space station. In *2015 IEEE Aerospace Conference*, pages 1–12. IEEE, 2015.

[127] Cyrus Foster, Henry Hallam, and James Mason. Orbit determination and differential-drag control of planet labs cubesat constellations. *arXiv preprint arXiv:1509.03270*, 2015.

[128] RC Tennyson. Composites in space challenges and opportunities. In *Proceedings of the 10th International Conference on Composite Materials, Whistler, Canada*, 1995.

[129] Joyce Dever, Bruce Banks, Kim de Groh, and Sharon Miller. Degradation of spacecraft materials. In *Handbook of environmental degradation of materials*, pages 465–501. Elsevier, 2005.

[130] Soreq nuclear research center. http://soreq.gov.il/mmg/eng/Pages/Low-Earth-Orbit-(LEO).aspx. [cited Sep 2019].

[131] Space Environmental effects. A researcher's guide to International Spaqce Station. https://www.nasa.gov/sites/default/files/files/NP-2015-03-015-JSC_Space_Environment-ISS-Mini-Book-2015-508.pdf. [cited April 2019].

[132] Joseph R Srour and James M McGarrity. Radiation effects on microelectronics in space. *Proceedings of the IEEE*, 76(11):1443–1469, 1988.

[133] JR Heirtzler. The future of the south atlantic anomaly and implications for radiation damage in space. *Journal of Atmospheric and Solar-Terrestrial Physics*, 64(16):1701–1708, 2002.

[134] What is the South Atlantic Anomaly. https://image.gsfc.nasa.gov/poetry/ask/q525.html. [cited September 2019].

[135] Wikipedia. https://en.wikipedia.org/wiki/Van_Allen_radiation_belt. [cited 2019].

[136] Radiation effects on electronics 101. https://www.nasa.gov/sites/default/files/atoms/files/space_radiation_ebook.pdf. [cited 2019].

[137] Juan Sebastián Triana, Sebastian Bautista, and Freddy Alexander Díaz González. Identification of design considerations for small satellite remote sensing systems in low earth orbit. *Journal of Aerospace Technology and Management*, 7(1):121–134, 2015.

[138] AH Johnston. Radiation damage of electronic and optoelectronic devices in space. 2000.

[139] Mihail P Petkov. The effects of space environments on electronic components. 2003.

[140] J. G. Rarity and P. R. Tapster. Experimental violation of bell's inequality based on phase and momentum. *Physical Review Letters*, 64(21):2495, 1990.

[141] YH Shih and Carroll O Alley. New type of einstein-podolsky-rosen-bohm experiment using pairs of light quanta produced by optical parametric down conversion. *Physical Review Letters*, 61(26):2921, 1988.

[142] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816):46, 2001.

[143] Ilaria Bargigia, Alberto Tosi, Andrea Bahgat Shehata, Adriano Della Frera, Andrea Farina, Andrea Bassi, Paola Taroni, Alberto Dalla Mora, Franco Zappa, Rinaldo Cubeddu, et al. Time-resolved diffuse optical spectroscopy up to 1700 nm by means of a time-gated ingaas/inp single-photon avalanche diode. *Applied spectroscopy*, 66(8):944–950, 2012.

[144] Aongus McCarthy, Robert J Collins, Nils J Krichel, Verónica Fernández, Andrew M Wallace, and Gerald S Buller. Long-range time-of-flight scanning sensor based on

high-speed time-correlated single-photon counting. *Applied optics*, 48(32):6241–6251, 2009.

[145] TE Ingerson, RJ Kearney, and RL Coulter. Photon counting with photodiodes. *Applied optics*, 22(13):2013–2018, 1983.

[146] A Andreoni, Rinaldo Cubeddu, C No Knox, and TG Truscott. Fluorescence lifetimes of angular furocoumarins. *Photochemistry and photobiology*, 46(2):169–173, 1987.

[147] NS Nightingale. A new silicon avalanche photodiode photon counting detector module for astronomy. *Experimental Astronomy*, 1(6):407–422, 1990.

[148] FiberLabs Inc. https://www.fiberlabs.com/glossary/about-optical-communication-band/.

[149] Roland H Haitz. Mechanisms contributing to the noise pulse rate of avalanche diodes. *Journal of Applied Physics*, 36(10):3123–3131, 1965.

[150] F Marsili, Varun B Verma, Jeffrey A Stern, S Harrington, Adriana E Lita, Thomas Gerrits, Igor Vayshenker, Burm Baek, Matthew D Shaw, Richard P Mirin, et al. Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, 7(3):210, 2013.

[151] High-speed solid state detectors for low light level applications Exclitas. http://www.roithner-laser.com/datasheets/accessories/dts_c30902_c30921.pdf. [cited 2019].

[152] ID100 Visible Single-Photon Detector. https://marketing.idquantique.com/acton/attachment/11868/f-0238/1/-/-/-/-/ID120_Brochure.pdf. [cited April 2019].

[153] id Quantique. https://marketing.idquantique.com/acton/attachment/11868/f-0234/1/-/-/-/-/ID230_Brochure.pdf. [cited April 2019].

[154] Emma E Wollman, Varun B Verma, Andrew D Beyer, Ryan M Briggs, B Korzh, Jason P Allmaras, F Marsili, Adriana E Lita, RP Mirin, SW Nam, et al. Uv superconducting nanowire single-photon detectors with high efficiency, low noise, and 4 k operating temperature. *Optics express*, 25(22):26792–26801, 2017.

[155] ID120 Visible Single-Photon Detector. https://marketing.idquantique.com/acton/attachment/11868/f-0238/1/-/-/-/-/ID120_Brochure.pdf. [cited April 2019].

[156] Iman Esmaeil Zadeh, Johannes WN Los, Ronan BM Gourgues, Violette Steinmetz, Gabriele Bulgarini, Sergiy M Dobrovolskiy, Val Zwiller, and Sander N Dorenbos. Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution. *Apl Photonics*, 2(11):111301, 2017.

[157] R.H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature photonics*, 3(12):696–705, 2009.

[158] Sergio Cova, A Lacaita, and Giancarlo Ripamonti. Trapping phenomena in avalanche photodiodes on nanosecond scale. *IEEE Electron device letters*, 12(12):685–687, 1991.

[159] Xudong Jiang, Mark A Itzler, Rafael Ben-Michael, Krystyna Slomkowski, Michael A Krainak, Stewart Wu, and Xiaoli Sun. Afterpulsing effects in free-running ingaasp single-photon avalanche diodes. *IEEE Journal of Quantum Electronics*, 44(1):3–11, 2008.

[160] M.A. Itzler, X. Jiang, M. Entwistle, K. Slomkowski, A. Tosi, F. Acerbi, F. Zappa, and S. Cova. Advances in InGaAsP-based avalanche diode single photon detectors. *Journal of Modern Optics*, 58(3-4):174–200, 2011.

[161] J. Zhang, M.A. Itzler, H. Zbinden, and J.-W. Pan. Advances in ingaas/inp single-photon detector systems for quantum communication. *Light: Science & Applications*, 4(5):e286, 2015.

[162] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden. Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency. *Applied Physics Letters*, 104(8):081108, 2014.

[163] N Namekata, S Sasamori, and Shuichiro Inoue. 800 mhz single-photon detection at 1550-nm using an ingaas/inp avalanche photodiode operated with a sine wave gating. *Optics Express*, 14(21):10043–10049, 2006.

[164] Kristine M Rosfjord, Joel KW Yang, Eric A Dauler, Andrew J Kerman, Vikas Anant, Boris M Voronov, Gregory N Gol'Tsman, and Karl K Berggren. Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. *Optics express*, 14(2):527–534, 2006.

[165] A Pearlman, A Cross, W Slysz, J Zhang, A Verevkin, M Currie, A Korneev, P Kouminov, K Smirnov, B Voronov, et al. Gigahertz counting rates of nbn single-photon detectors for quantum communications. *IEEE transactions on applied superconductivity*, 15(2):579–582, 2005.

[166] Sergio Cova, Massimo Ghioni, Arturo Lotito, Ivan Rech, and Franco Zappa. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *journal of modern optics*, 51(9-10):1267–1288, 2004.

[167] ZL Yuan, AR Dixon, JF Dynes, AW Sharpe, and AJ Shields. Gigahertz quantum key distribution with ingaas avalanche photodiodes. *Applied Physics Letters*, 92(20):201104, 2008.

[168] T. Lunghi, C. Barreiro, O. Guinnard, R. Houlmann, X. Jiang, M. Itzler, and H. Zbinden. Free-running single-photon detection based on a negative feedback ingaas apd. *Journal of Modern Optics*, 59(17):1481–1488, 2012.

[169] Z. Yan, D.R. Hamel, A.K. Heinrichs, X. Jiang, M.A. Itzler, and T. Jennewein. An ultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode. *Review of Scientific Instruments*, 83(7):073105, 2012.

[170] Michael Wahl. Time-correlated single photon counting. https://www.picoquant.com/images/uploads/page/files/7253/technote_tcspc.pdf, Cited 2019.

[171] Photon Spot. http://www.photonspot.com. [cited April 2019].

[172] G.N. Gol'Tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski. Picosecond superconducting single-photon optical detector. *Applied Physics Letters*, 79(6):705–707, 2001.

[173] Adriana E Lita, Aaron J Miller, and Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency. *Optics express*, 16(5):3032–3040, 2008.

[174] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.

[175] Hiroki Takesue, Shellee D Dyer, Martin J Stevens, Varun Verma, Richard P Mirin, and Sae Woo Nam. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. *Optica*, 2(10):832–835, 2015.

[176] Hiroyuki Shibata, Toshimori Honjo, and Kaoru Shimizu. Quantum key distribution over a 72 db channel loss using ultralow dark count superconducting single-photon detectors. *Optics letters*, 39(17):5078–5081, 2014.

[177] Jeongwan Jin, Erhan Saglamyurek, Varun Verma, Francesco Marsili, Sae Woo Nam, Daniel Oblak, Wolfgang Tittel, et al. Telecom-wavelength atomic quantum memory in optical fiber for heralded polarization qubits. *Physical review letters*, 115(14):140501, 2015.

[178] Alberto Tosi, Alberto Dalla Mora, Franco Zappa, and Sergio Cova. Germanium and ingaas/inp spads for single-photon detection in the near-infrared. In *Advanced Photon Counting Techniques II*, volume 6771, page 67710P. International Society for Optics and Photonics, 2007.

[179] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, 92(5):057901, 2004.

[180] A Fukasawa, J Haba, A Kageyama, H Nakazawa, and M Suyama. High speed hpd for photon counting. *IEEE Transactions On Nuclear Science*, 55(2):758–762, 2008.

[181] Ho Kume, Ko Koyama, K Nakatsugawa, So Suzuki, and David Fatlowitz. Ultrafast microchannel plate photomultipliers. *Applied optics*, 27(6):1170–1178, 1988.

[182] Excelitas. http://www.excelitas.com. [cited April 2019].

[183] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Applied optics*, 35(12):1956–1976, 1996.

[184] Andrea Gallivanoni, Ivan Rech, and Massimo Ghioni. Progress in quenching circuits for single photon avalanche diodes. *IEEE Transactions on nuclear science*, 57(6):3815–3826, 2010.

[185] Massimo Ghioni, Angelo Gulinatti, Ivan Rech, Franco Zappa, and Sergio Cova. Progress in silicon single-photon avalanche diodes. *IEEE Journal of selected topics in quantum electronics*, 13(4):852–862, 2007.

[186] A Lacaita, M Ghioni, Franco Zappa, Giancarlo Ripamonti, and Sergio Cova. Recent advances in the detection of optical photons with silicon photodiodes. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 326(1-2):290–294, 1993.

[187] Micro Photon Devices. http://www.micro-photon-devices.com. [cited April 2019].

[188] M Ghioni and Giancarlo Ripamonti. Improving the performance of commercially available geiger-mode avalanche photodiodes. *Review of scientific instruments*, 62(1):163–167, 1991.

[189] Robert G. W. Brown, Kevin D. Ridley, and John G. Rarity. Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching. *Applied Optics*, 25(22):4122–4126, 1986.

[190] Mario Stipčević. Commercially available geiger mode single-photon avalanche photodiode with a very low afterpulsing probability. *arXiv preprint arXiv:1505.04407*, 2015.

[191] Joe C Campbell, Stephane Demiguel, Feng Ma, Ariane Beck, Xiangyi Guo, Shuling Wang, Xiaoguang Zheng, Xiaowei Li, Jeffrey D Beck, Michael A Kinch, et al. Recent advances in avalanche photodiodes. *IEEE Journal of selected topics in quantum electronics*, 10(4):777–787, 2004.

[192] Joe C Campbell. Recent advances in telecommunications avalanche photodiodes. *Journal of Lightwave Technology*, 25(1):109–121, 2007.

[193] Mark A Itzler, R Ben-Michael, C-F Hsu, Krystyna Slomkowski, Alberto Tosi, Sergio Cova, Franco Zappa, and Radu Ispasoiu. Single photon avalanche diodes (spads) for 1.5 μ m photon counting applications. *Journal of Modern Optics*, 54(2-3):283–304, 2007.

[194] Philip A Hiskett, Gerald S Buller, Alison Y Loudon, Jason M Smith, Ivair Gontijo, Andrew C Walker, Paul D Townsend, and Michael J Robertson. Performance and design of ingaas/inp photodiodes for single-photon counting at 1.55 μm. *Applied Optics*, 39(36):6818–6829, 2000.

[195] Sara Pellegrini, Ryan E Warburton, Lionel JJ Tan, Jo Shien Ng, Andrey B Krysa, Kristian Groom, John PR David, Sergio Cova, Michael J Robertson, and Gerald S Buller. Design and performance of an ingaas-inp single-photon avalanche diode detector. *IEEE journal of quantum electronics*, 42(4):397–403, 2006.

[196] Joseph P Donnelly, Erik K Duerr, K Alex McIntosh, Eric A Dauler, Douglas C Oakley, Steven H Groves, Christopher J Vineis, Leonard J Mahoney, Karen M Molvar, Pablo I Hopman, et al. Design considerations for 1.06-mu m ingaasp–inp geiger-mode avalanche photodiodes. *IEEE Journal of Quantum Electronics*, 42(8):797–809, 2006.

[197] Fabio Acerbi, Michele Anti, Alberto Tosi, and Franco Zappa. Design criteria for ingaas/inp single-photon avalanche diode. *IEEE Photonics Journal*, 5(2):6800209–6800209, 2013.

[198] Xiao Meng, Chee Hing Tan, Simon Dimler, John PR David, and Jo Shien Ng. 1550 nm ingaas/inalas single photon avalanche diode at room temperature. *Optics express*, 22(19):22608–22615, 2014.

[199] X. Jiang, M.A. Itzler, K. O'Donnell, M. Entwistle, and K. Slomkowski. InGaAs/InP negative feedback avalanche diodes (NFADs). In *SPIE Defense, Security, and Sensing*, pages 80330–80330. International Society for Optics and Photonics, 2011.

[200] Alessandro Restelli, Joshua C Bienfang, and Alan L Migdall. Time-domain measurements of afterpulsing in ingaas/inp spad gated with sub-nanosecond pulses. *Journal of Modern Optics*, 59(17):1465–1471, 2012.

[201] Naoto Namekata, Shunsuke Adachi, and Shuichiro Inoue. Ultra-low-noise sinusoidally gated avalanche photodiode for high-speed single-photon detection at telecommunication wavelengths. *IEEE Photonics Technology Letters*, 22(8):529–531, 2010.

[202] KA Patel, JF Dynes, AW Sharpe, ZL Yuan, RV Penty, and AJ Shields. Gigacount/second photon detection with ingaas avalanche photodiodes. *Electronics letters*, 48(2):111–113, 2012.

[203] Jun Zhang, Patrick Eraerds, Nino Walenta, Claudio Barreiro, Rob Thew, and Hugo Zbinden. 2.23 ghz gating ingaas/inp single-photon avalanche diode for quantum key distribution. In *Advanced Photon Counting Techniques IV*, volume 7681, page 76810Z. International Society for Optics and Photonics, 2010.

[204] Nino Walenta, Tommaso Lunghi, Olivier Guinnard, Raphael Houlmann, Hugo Zbinden, and Nicolas Gisin. Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature. *Journal of Applied Physics*, 112(6):063106, 2012.

[205] Alberto Tosi, Carmelo Scarcella, Gianluca Boso, and Fabio Acerbi. Gate-free ingaas/inp single-photon detector working at up to 100 mcount/s. *IEEE Photonics Journal*, 5(4):6801308–6801308, 2013.

[206] Grégoire Ribordy, Nicolas Gisin, Olivier Guinnard, Damien Stuck, Mark Wegmuller, and Hugo Zbinden. Photon counting at telecom wavelengths with commercial in-

gaas/inp avalanche photodiodes: current performance. *Journal of Modern Optics*, 51(9-10):1381–1398, 2004.

[207] Akio Yoshizawa, Ryosaku Kaji, and Hidemi Tsuchida. Gated-mode single-photon detection at 1550 nm by discharge pulse counting. *Applied physics letters*, 84(18):3606–3608, 2004.

[208] Donald S Bethune, William P Risk, and Gary W Pabst. A high-performance integrated single-photon detector for telecom wavelengths. *Journal of modern optics*, 51(9-10):1359–1368, 2004.

[209] Akihisa Tomita and Kazuo Nakamura. Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm. *Optics letters*, 27(20):1827–1829, 2002.

[210] M.A. Itzler, X. Jiang, B.M. Onat, and K. Slomkowski. Progress in self-quenching InP-based single photon detectors. In *OPTO*, pages 760829–760829. International Society for Optics and Photonics, 2010.

[211] P Antognetti, Sergio Cova, and A Longoni. A study of the operation and performances of an avalanche diode as a single-photon detector. Technical report, 1975.

[212] Sergio Cova, A Longoni, and Giancarlo Ripamonti. Active-quenching and gating circuits for single-photon avalanche diodes (spads). *IEEE Transactions on nuclear science*, 29(1):599–601, 1982.

[213] Philip A Ekstrom. Triggered-avalanche detection of optical photons. *Journal of Applied Physics*, 52(11):6974–6979, 1981.

[214] Gregoire Ribordy, Jean-Daniel Gautier, Hugo Zbinden, and Nicolas Gisin. Performance of ingaas/inp avalanche photodiodes as gated-mode photon counters. *Applied Optics*, 37(12):2272–2277, 1998.

[215] A Spinelli, LM Davis, and H Dautet. Actively quenched single-photon avalanche diode for high repetition rate time-gated photon counting. *Review of scientific instruments*, 67(1):55–61, 1996.

[216] Seok-Beom Cho and Sae-Kyoung Kang. Weak avalanche discrimination for gated-mode single-photon avalanche photodiodes. *Optics express*, 19(19):18510–18515, 2011.

[217] Shingo Suzuki, Naoto Namekata, Kenji Tsujino, and Shuichiro Inoue. Highly enhanced avalanche probability using sinusoidally-gated silicon avalanche photodiode. *Applied Physics Letters*, 104(4):041105, 2014.

[218] Fabian Steinlechner, Pavel Trojek, Marc Jofre, Henning Weier, Daniel Perez, Thomas Jennewein, Rupert Ursin, John Rarity, Morgan W. Mitchell, Juan P. Torres, et al. A high-brightness source of polarization-entangled photons optimized for applications in free space. *Optics express*, 20(9):9640–9649, 2012.

[219] J Kataoka, T Toizumi, T Nakamori, Y Yatsu, Y Tsubuku, Y Kuramoto, T Enomoto, R Usui, N Kawai, H Ashida, et al. In-orbit performance of avalanche photodiode as radiation detector on board the picosatellite cute-1.7+ apd ii. *Journal of Geophysical Research: Space Physics*, 115(A5), 2010.

[220] Michael A Krainak, W Yu Anthony, Guangning Yang, Steven X Li, and Xiaoli Sun. Photon-counting detectors for space-based laser receivers. In *Quantum Sensing and Nanophotonic Devices VII*, volume 7608, page 760827. International Society for Optics and Photonics, 2010.

[221] Ivan Prochazka and Fumin Yang. Photon counting module for laser time transfer via earth orbiting satellite. *Journal of Modern Optics*, 56(2-3):253–260, 2009.

[222] Missions Enabling Technologies. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-MTB-450-12304?order=title_en&sort=asc, cited 2019.

[223] Yong-Su Kim, Youn-Chang Jeong, Sebastien Sauge, Vadim Makarov, and Yoon-Ho Kim. Ultra-low noise single-photon detector based on si avalanche photodiode. *Review of scientific instruments*, 82(9):093110, 2011.

[224] Elena Anisimova, Dmitri Nikulov, Simeng Simone Hu, Mark Bourgon, Rupert Ursin, Thomas Jennewein, and Vadim Makarov. Low-noise single-photon detector for long-distance free-space quantum communication. *preparation; preliminary results presented at QCrypt*, 2015.

[225] SPENVIS tutorial: Radiation models in SPENVIS and their accuracy.

[226] AP8MIN and AP8MAX Trapped Proton Models. https://creme.isde.vanderbilt.edu/CREME-MC/help/ap8min-and-ap8max-trapped-proton-models.

[227] TRIUMF. https://www.triumf.ca/sites/default/files/nsrec_abs.pdf, Cited 2019.

[228] Critical Design review by the Engineering student of the University of Illinois at Urbana-Champaign, 2018.

[229] Wang, Zipeng. Thesis: Design of a scalable nano university satellite bus (illinisat-2 bus) command and data handling system and power system. http://hdl.handle.net/2142/101623, 2018.

[230] Stahl, Joe. Thesis: Mitigation of radiation damage in single-photon detectors via optical annealing, 2018.

[231] QPhotonics. https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/, cited 2019.

[232] Osram Opto Semiconductors. https://www.osram.com/ecat/Radial%20T1%203-4%20SFH%20203%20P/com/en/class_pim_web_catalog_103489/global/prd_pim_device_2219552/, cited 2019.

[233] Marktech Optoelectronics. https://www.digikey.ca/product-detail/en/marktech-optoelectronics/MTE2081-OH5/1125-1158-ND/3973506, cited 2019.

[234] TPS54427, Texus Instruments. http://www.ti.com/lit/ds/symlink/tps54427.pdf, cited 2019.

[235] TPS54295, Texus Instruments. http://www.ti.com/lit/ds/symlink/tps54295.pdf, cited 2019.

[236] Cypress. https://www.cypress.com/documentation/datasheets/psocr3-cy8c36-family-datasheet-programmable-system-chip-psocr, Cited in 2019.

[237] Cliff Cheng, Rakhitha Chandrasekara, Yue Chuan Tan, and Alexander Ling. Space-qualified nanosatellite electronics platform for photon pair experiments. *Journal of Lightwave Technology*, 33(23):4799–4804, 2015.

[238] R Chandrasekara, ZK Tang, YC Tan, C Cheng, C Wildfeuer, and A Ling. Single photon counting for space based quantum experiments. In *Advanced Photon Counting Techniques IX*, volume 9492, page 949209. International Society for Optics and Photonics, 2015.

[239] Analog devices. https://www.analog.com/media/en/technical-documentation/data-sheets/ADM3483_3485_3488_3490_3491.pdf, Cited in 2019.

[240] Matsusada Precision. https://www.matsusada.com/. [cited May 2019].

[241] Panasonic. https://www.mouser.com/datasheet/2/315/semi_eng_gu1a_aqv21_s-850760-1197088.pdf, cited 2019.

[242] STMicroelectronics. https://www.st.com/resource/en/datasheet/rhr801.pdf. [cited May 2019].

[243] Renesus. https://www.renesas.com/jp/ja/www/doc/datasheet/isl21070.pdf, cited 2019.

[244] Maxim Integrated. https://datasheets.maximintegrated.com/en/ds/MAX1968-MAX1969.pdf, cited 2019.

[245] The engineering toolbox. https://www.engineeringtoolbox.com/thermal-conductivity-metals-d_858.html, cited 2019.

[246] PID control. http://www.acsysteme.com/en/serial-or-parallel-pid. [cited 2019].

[247] The Z Transform. https://lpsa.swarthmore.edu/ZXform/FwdZXform/FwdZXform.html, cited 2019.

[248] Association Connecting Electronics Industries (IPC). Requirements for soldered electrical and electronic assemblies - ipc j-std-001d. 2008.

[249] Wire Insulation Selection Guidelines. https://nepp.nasa.gov/npsl/Wire/insulation_guide.htm. [cited 2019].

[250] Atomic Oxygen and Space Environment Effects on Aerospace Materials Flown with EOIM-III Experiment. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19970010450.pdf, 1996.

[251] Sultana, Nigar and Bourgoin, Jean-philippe and Kuntz, Katanya and Jennewein, Thomas. A simple photon counting module for free-running negative-feedback avalanche diodes with active suppression of afterpulses, Manuscript in preperation.

[252] R.H. Thew, D. Stucki, J.D. Gautier, H. Zbinden, and A. Rochas. Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths. *Applied Physics Letters*, 91(20):201114, 2007.

[253] R.E. Warburton, M. Itzler, and G.S. Buller. Free-running, room temperature operation of an InGaAs/InP single-photon avalanche diode. *Applied Physics Letters*, 94(7):071116, 2009.

[254] J. Cheng, S. You, S. Rahman, and Y.-H. Lo. Self-quenching InGaAs/InP single photon avalanche detector utilizing zinc diffusion rings. *Optics express*, 19(16):15149–15154, 2011.

[255] M.D. Eisaman, J. Fan, A. Migdall, and S.V. Polyakov. Invited review article: Single-photon sources and detectors. *Review of scientific instruments*, 82(7):071101, 2011.

[256] Patrick Eraerds, Matthieu Legré, Jun Zhang, Hugo Zbinden, and Nicolas Gisin. Photon counting otdr: advantages and limitations. *Journal of Lightwave Technology*, 28(6):952–964, 2010.

[257] Aongus McCarthy, Nils J Krichel, Nathan R Gemmell, Ximing Ren, Michael G Tanner, Sander N Dorenbos, Val Zwiller, Robert H Hadfield, and Gerald S Buller. Kilometer-range, high resolution depth imaging via 1560 nm wavelength single-photon detection. *Optics express*, 21(7):8904–8915, 2013.

[258] Bryan S Robinson, Andrew J Kerman, Eric A Dauler, Richard J Barron, David O Caplan, Mark L Stevens, John J Carney, Scott A Hamilton, Joel K Yang, and Karl K Berggren. 781 mbit/s photon-counting optical communications using a superconducting nanowire detector. *Optics letters*, 31(4):444–446, 2006.

[259] C. Yu, M. Shangguan, H. Xia, J. Zhang, X. Dou, and J.-W. Pan. Fully integrated free-running ingaas/inp single-photon detector for accurate lidar applications. *Optics express*, 25(13):14611–14620, 2017.

[260] N. Gisin and R. Thew. Quantum communication. *Nature photonics*, 1(3):165–171, 2007.

[261] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE international conference on computers, systems, and signal processing*, pages 175–9, 1984.

[262] C.J. Horsfield, M.S. Rubery, J.M. Mack, C.S. Young, H.W. Herrmann, S.E. Caldwell, S.C. Evans, T.J. Sedilleo, Y.H. Kim, A. McEvoy, et al. Development and characterization of sub-100 ps photomultiplier tubes a. *Review of Scientific Instruments*, 81(10):10D318, 2010.

[263] M.A. Itzler, X. Jiang, R. Ben-Michael, K. Slomkowski, M.A. Krainak, S. Wu, and X. Sun. InGaAsP avalanche photodetectors for non-gated 1.06 μm photon-counting receivers. In *Proc. of SPIE Vol*, volume 6572, pages 65720G–1, 2007.

[264] A.J. Miller, A. Lita, D. Rosenberg, S. Gruber, and S.W. Nam. Superconducting photon number resolving detectors: Performance and promise. In *Proc. 8th Int. Conf. Quantum Communication, Measurement and Computing (QCMC'06)*, pages 445–450, 2007.

[265] Gianluca Boso, Boris Korzh, Tommaso Lunghi, and Hugo Zbinden. Low noise ingaas/inp single-photon negative feedback avalanche diodes: characterization and applications. In *Advanced Photon Counting Techniques IX*, volume 9492, page 94920Q. International Society for Optics and Photonics, 2015.

[266] Rolf Horn and Thomas Jennewein. Auto-balancing and robust interferometer designs for polarization entangled photon sources. *Optics Express*, 27(12):17369–17376, 2019.

[267] ID Quantique. https://www.idquantique.com/resource-library/single-photon-systems/. cited August 2019.

[268] Gaëtan Gras, Nigar Sultana, Anqi Huang, Thomas Jennewein, Félix Bussières, Vadim Makarov, and Hugo Zbinden. Optical control of single-photon negative-feedback avalanche diode detector. *arXiv preprint arXiv:1911.12742*, 2019.

[269] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[270] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *PRA*, 51(3):1863, 1995.

[271] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *PRA*, 61(5):052304, 2000.

[272] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006.

[273] Artem Vakhitov, Vadim Makarov, and Dag R Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *journal of modern optics*, 48(13):2023–2038, 2001.

[274] Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, 2006.

[275] Marco Lucamarini, Iris Choi, Martin B Ward, James F Dynes, ZL Yuan, and Andrew J Shields. Practical security bounds against the trojan-horse attack in quantum key distribution. *Physical Review X*, 5(3):031030, 2015.

[276] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Info. Comput.*, 7(1):73–82, 2007.

[277] Vadim Makarov* and Dag R Hjelme. Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 52(5):691–705, 2005.

[278] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature communications*, 2:349, 2011.

[279] Lars Lydersen, Mohsen K Akhlaghi, A Hamed Majedi, Johannes Skaar, and Vadim Makarov. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New Journal of Physics*, 13(11):113042, 2011.

[280] Shihan Sajeed, Anqi Huang, Shihai Sun, Feihu Xu, Vadim Makarov, and Marcos Curty. Insecurity of detector-device-independent quantum key distribution. *Physical review letters*, 117(25):250505, 2016.

[281] Shihan Sajeed, Poompong Chaiwongkhot, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Physical Review A*, 91(6):062301, 2015.

[282] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19:23590–23600, 2011.

[283] V. Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11(6):065003, 2009.

[284] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics*, 4:686–689, 2010.

[285] L. Lydersen, J. Skaar, and V. Makarov. Tailored bright illumination attack on distributed-phase-reference protocols. *J. Mod. Opt.*, 58(8):680–685, 2011.

[286] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.*, 2:349, 2011.

[287] Mikio Fujiwara, Toshimori Honjo, Kaoru Shimizu, Kiyoshi Tamaki, and Masahide Sasaki. Characteristics of superconducting single photon detector in dps-qkd system under bright illumination blinding attack. *Opt. Express*, 21:6304–6312, 2013.

[288] Michael G Tanner, Vadim Makarov, and Robert H Hadfield. Optimised quantum hacking of superconducting nanowire single-photon detectors. *Opt. Express*, 22:6734–6748, 2014.

[289] id220datasheet. https://marketing.idquantique.com/acton/attachment/11868/f-023d/1/-/-/-/-/ID220_Brochure.pdf, cited 2019.

[290] Lars Lydersen, Nitin Jain, Christoffer Wittmann, Øystein Marøy, Johannes Skaar, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs. Superlinear threshold detectors in quantum cryptography. *Physical Review A*, 84(3):032320, 2011.

[291] Hiroki Takesue, Sae Woo Nam, Qiang Zhang, Robert H Hadfield, Toshimori Honjo, Kiyoshi Tamaki, and Yoshihisa Yamamoto. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nature photonics*, 1(6):343, 2007.

[292] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2 ghz clock quantum key distribution over 260 km of standard telecom fiber. *Optics letters*, 37(6):1008–1010, 2012.

[293] Alberto Boaron, Boris Korzh, Raphael Houlmann, Gianluca Boso, Davide Rusca, Stuart Gray, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Simple 2.5 ghz time-bin quantum key distribution. *Applied Physics Letters*, 112(17):171108, 2018.

[294] AR Dixon, ZL Yuan, JF Dynes, AW Sharpe, and AJ Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Optics express*, 16(23):18790–18797, 2008.

[295] Alexander R Dixon, ZL Yuan, JF Dynes, AW Sharpe, and AJ Shields. Continuous operation of high bit rate quantum key distribution. *Applied Physics Letters*, 96(16):161102, 2010.

[296] M Jofre, A Gardelein, G Anzolin, G Molina-Terriza, JP Torres, MW Mitchell, and V Pruneri. 100 mhz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm. *Journal of Lightwave Technology*, 28(17):2572–2578, 2010.

[297] M Jofre, A Gardelein, G Anzolin, W Amaya, J Capmany, R Ursin, L Penate, D Lopez, JL San Juan, JA Carrasco, et al. Fast optical source for quantum key distribution based on semiconductor optical amplifiers. *Optics express*, 19(5):3825–3834, 2011.

[298] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S Gray, CR Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003, 2009.

[299] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters*, 84(20):4729, 2000.

[300] S Tanzilli, W Tittel, H De Riedmatten, H Zbinden, P Baldi, M DeMicheli, Da B Ostrowsky, and N Gisin. Ppln waveguide for quantum communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 18(2):155–160, 2002.

[301] Evan Meyer-Scott, Hannes Hübel, Alessandro Fedrizzi, Christopher Erven, Gregor Weihs, and Thomas Jennewein. Quantum entanglement distribution with 810 nm photons through telecom fibers. *Applied Physics Letters*, 97(3):031117, 2010.

[302] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Physical Review A*, 76(1):012307, 2007.

[303] Chris Erven, Xiongfeng Ma, Raymond Laflamme, and Gregor Weihs. Entangled quantum key distribution with a biased basis choice. *New Journal of Physics*, 11(4):045025, 2009.

[304] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[305] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509, 2017.

[306] Gwenaelle Vest, Markus Rau, Lukas Fuchs, Giacomo Corrielli, Henning Weier, Sebastian Nauerth, Andrea Crespi, Roberto Osellame, and Harald Weinfurter. Design and evaluation of a handheld quantum key distribution sender module. *IEEE journal of selected topics in quantum electronics*, 21(3):131–137, 2014.

[307] Yang Liu, Teng-Yun Chen, Jian Wang, Wen-Qi Cai, Xu Wan, Luo-Kan Chen, Jin-Hong Wang, Shu-Bin Liu, Hao Liang, Lin Yang, et al. Decoy-state quantum key distribution with polarized photons over 200 km. *Optics express*, 18(8):8587–8594, 2010.

[308] I Lucio-Martinez, Philip Chan, Xiaofan Mo, Steve Hosier, and W Tittel. Proof-of-concept of real-world quantum key distribution with quantum frames. *New Journal of Physics*, 11(9):095001, 2009.

[309] Costantino Agnesi, Marco Avesani, Andrea Stanco, Paolo Villoresi, and Giuseppe Vallone. All-fiber self-compensating polarization encoder for quantum key distribution. *Optics letters*, 44(10):2398–2401, 2019.

[310] Costantino Agnesi, Marco Avesani, Luca Calderaro, Andrea Stanco, Giulio Foletto, Mujtaba Zahidy, Alessia Scriminich, Francesco Vedovato, Giuseppe Vallone, and Paolo Villoresi. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. *arXiv preprint arXiv:1909.12703*, 2019.

[311] Fock state. https://en.wikipedia.org/wiki/Fock_state, cited 2019.

[312] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44, 2002.

[313] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[314] Xiang-Bin Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Physical Review A*, 72(1):012322, 2005.

[315] HC Photonics corp. https://www.hcphotonics.com/, Cited 2019.

[316] Tabor Electronics. https://www.taborelec.com/, Cited 2019.

[317] Zhu Cao, Zhen Zhang, Hoi-Kwong Lo, and Xiongfeng Ma. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New Journal of Physics*, 17(5):053014, 2015.

[318] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.

[319] Shi-Hai Sun, Ming Gao, Mu-Sheng Jiang, Chun-Yan Li, and Lin-Mei Liang. Partially random phase attack to the practical two-way quantum-key-distribution system. *Physical Review A*, 85(3):032304, 2012.

[320] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang Fred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Source attack of decoy-state quantum key distribution using phase information. *Physical Review A*, 88(2):022308, 2013.

[321] The Poisson Distribution and Poisson Process Explained. https://towardsdatascience.com/the-poisson-distribution-and-poisson-process-explained-4e2 cited 2019.