Single-photon detectors for long distance quantum communications

by

Elena Anisimova

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2018

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	Alexander Lvovsky
	Title	Professor
Supervisor	Name	Thomas Jennewein
	Title	Associate Professor
Internal member	Name	Jonathan Baugh
	Title	Associate Professor
Internal member	Name	James Martin
	Title	Associate Professor
Internal member	Name	Norbert Lütkenhaus
	Title	Professor

I hereby declare that I am the sole author of this 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.

Abstract

Quantum communications and quantum cryptography are developing rapidly during the last decades caused partly by a fast progress in quantum computing. Quantum cryptography provides an unconditionally secure way of communicating whereas traditional classical cryptographic protocols are likely to be broken by super powerful quantum computers. In the past few years distances covered by quantum communications have increased by an order of magnitude. To provide a global coverage for the quantum networks, a satellite based quantum communications is the most promising solution.

As an emerging field, QKD systems are still under evolution process. Despite outstanding security proven theoretically, it has loopholes caused by their implementations. To test QKD, find the possible loopholes and suggest ways to fix them, is a job of many scientific groups. In this thesis I start with presenting my work for a securing test of a commercial QKD system Clavis2. A Trojan-horse attack on Bob's apparatus was prepared by testing reflections and transmissions of all optical components in Bob's scheme. The attack was implemented and found to be unsuccessful at the tested wavelengths due to afterpulsing effect in Bob's single-photon detectors reacting to the bright light attack pulses.

Three chapters of the thesis are dedicated to custom built single-photon detectors (SPDs) based on commercial Silicon avalanche photodiodes (APDs). Those detectors demonstrate parameters that altogether are not possible to find in commercially available SPDs, especially if combined with a very compact size. One of the in-lab-built SPDs was implemented in 143 km teleportation experiment, where a low dark count rate was crucial for the success of the experiment. The next generation SPD is already built, characterized and ready to be implemented.

Another 4-channel SPD was built as a prototype for a quantum satellite SPD. It has light weight, low electrical power consumption, low dark count rate and decent other parameters. It was used in the airborne demonstration of QKD receiver payload experiment, when a secret key was successfully generated between a moving aircraft and a ground station.

SPDs installed on a satellite have to be able to work in the harsh space environment during a mission life time. Space radiation dramatically increases dark count rate of APDs.

The last project presented in the thesis committed to a radiation test of three types of APDs and one type of photo multiplier tube. The experiment included characterization of all SPDs before and after irradiation by four levels of proton radiation, equivalent to 3 months – 2 years duration in a 600 km low Earth orbit. Three methods for mitigating radiation damage were tested and found to be successful with perspective to use some of them on a quantum satellite to extent life time of SPDs.

To summarize, this work makes a contribution to the development of SPDs for global quantum communications.

Outline

The thesis is structured as follows. In chapter 1 a brief introduction to quantum communications is presented. In chapter 2, the overview of SPDs suitable for long-distance quantum communications is provided. In chapter 3, an experimental Trojan-horse attack on a commercial QKD is described. In chapter 4 a quantum teleportation over 143 km experiment, used custom built SPDs, is described. In chapter 5, an improved afterpulsing analysis for ultra low noise SPDs is demonstrated. In chapter 6, a low temperature super low-noise in-lab built SPD is presented. In chapter 7, an in-lab built detector prototype for Airborne demonstration of QKD is presented. In chapter 8, a radiation test of SPDs is described. Chapter 9 provides conclusive remarks and outlook on the work.

Acknowledgments

I would like to thank my supervisor Thomas Jennewein for his advices and guidance during my PhD. It was such an enriching experience to work together with him. I would also like to thank my Advisory Committee members: Jonathan Baugh, James Martin, Michele Mosca for their guidance and recommendations. Also I would like to thank my external examiner Alexander Lvovsky.

I would also like to thank all my co-authors and the Quantum Photonic Laboratory group members for their help, support and priceless experience of the collaborative work that made the time of my PhD an unforgettable experience in my life. Also, I am very thankful to many other students, postdocs, faculty and staff of IQC with whom I shared my office, chatted and laughed during break times or discussed problems and searched for support.

I am also very grateful to Prof. Oleg Kotov from SPbSTU, who helped with fruitful discussions and office space for my thesis writing in Saint-Petersburg.

I am very thankful for the financial support allotted to Physics students by the University of Waterloo that in my case included: Graduate Research Scholarship, International Doctoral Student Award, Provost Doctoral Entrance Award for Women, Science Graduate Experience Award, Marie Curie Graduate Student Award and UW Maternity Bursary. A special thank you to Cryptoworks21 program for the scholarship and travel support.

Finally, a huge gratitude to my family and friends who always supported me during this not easy journey of obtaining my doctoral degree.

Dedication

To my husband Vadim M. who continuously encouraged me during this work, my mother Nataliya A. who tremendously helped me with my other duties during the thesis writing, and my dear daughter Daria M. who always was a source of positive emotions for me.

Table of Contents

List of Tables

List of Figures

List of publications

1. E. Anisimova, D. Nikulov, S. S. Hu, M. Bourgon, R. Ursin, T. Jennewein, and V. Makarov, Low-noise single-photon detectors for long-distance free-space quantum communication, (manuscript in preparation),

2. E. Anisimova, B. L. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein, Mitigating radiation damage of single photon detectors for space applications, EPJ Quantum Technol. 4, 10 (2017),

3. J. G. Lim, E. Anisimova, B. L. Higgins, J.-P. Bourgoin, T. Jennewein, and V. Makarov, Laser annealing heals radiation damage in avalanche photodiodes, EPJ Quantum Technol. 4, 11 (2017),

4. C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, Airborne demonstration of a quantum key distribution receiver payload, Quantum Sci. Technol. 2, 024009 (2017),

5. N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New J. Phys. 16, 123030 (2014),

6. X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, Quantum teleportation over 143 kilometres using active feed-forward, Nature 489, 269 (2012).

List of conference presentations

1. **E. Anisimova**, B. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein, Demonstration of suitability of avalanche photodiodes for quantum communications in the low-Earth-orbit radiation environment (poster), presented at QCrypt 2015, Tokyo, Japan, September 28 October 2, 2015,

2. **E. Anisimova**, D. Nikulov, S. S. Hu, M. Bourgon, R. Ursin, T. Jennewein, and V. Makarov, Low-noise single-photon detector for long-distance free-space quantum communication (poster), presented at QCrypt 2015, Tokyo, Japan, September 28 October 2, 2015,

3. **E. Anisimova**, B. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein, Testing the suitability of avalanche photodiodes for quantum communications in the low-Earth-orbit radiation environment (contributed talk), presented at Single Photon Workshop 2015, Geneva, Switzerland, July 1317, 2015,

4. **E. Anisimova**, D. Nikulov, S. S. Hu, M. Bourgon, R. Ursin, T. Jennewein, and V. Makarov, Low-noise single-photon detector for long-distance free-space quantum communication (poster), presented at Single Photon Workshop 2015, Geneva, Switzerland, July 1317, 2015,

5. **N. Jain**, E. Anisimova, C. Wittmann, C. Marquardt, V. Makarov, and G. Leuchs, Investigating the feasibility of a practical Trojan-horse attack on a commercial quantum cryptosystem (poster), presented at DPG-AMOP, Stuttgart, March 12, 2012,

6. **N. Jain**, E. Anisimova, C. Wittmann, Ch. Marquardt, V. Makarov, and G. Leuchs, Investigating the feasibility of a practical Trojan-horse attack on a commercial quantum key distribution system (poster), presented at QCMC 2012, Vienna, Austria, July 30 August 3, 2012.

My contribution to projects

- **Chapters 1 and 2.**
  Introduction to quantum cryptography and quantum communication.
  Contribution: field overviews written by Elena Anisimova.
- **Chapter 3.**
  Trojan-horse attack on commercial QKD.
  Contribution: preparation measurements on commercial QKD system Clavis-2 using optical time domain reflectometry that resulted in a reflection map at three wavelengths; also attenuation of all optical components were measured.
- **Chapter 4.**
  Quantum teleportation over 143 km.
  Contribution: building two detectors for the experiment following an existing example, dark count rate measurements.
- **Chapter 5.**
  Improved SPD afterpulsing analysis method.
  Contribution: main lead of the project, elaboration of the algorithm of the analysis, supervising coding done by undergraduate students.
- **Chapter 6.**
  Super low noise in-lab built SPD.
  Contribution: main lead of the project, mechanical and thermal design of the detector, assembly, characterization tests.
- **Chapter 7.**
  Detector prototype for space QKD.
  Contribution: mechanical and thermal design of the detectors, with their assembly and following characterization tests. Electronics was done by other student and UW technician.
- **Chapter 8.**
  Radiation test and mitigating radiation damage.

Contribution: main lead of the project (except laser annealing part), mechanical design and assembly of the setup, characterization measurements. Laser annealing experiment was led by Jin Gyu Lim, my contribution to the project was discussions, planning, help with the experiment and afterpulsing analysis.

Chapter 1

Introduction to quantum cryptography and quantum communications

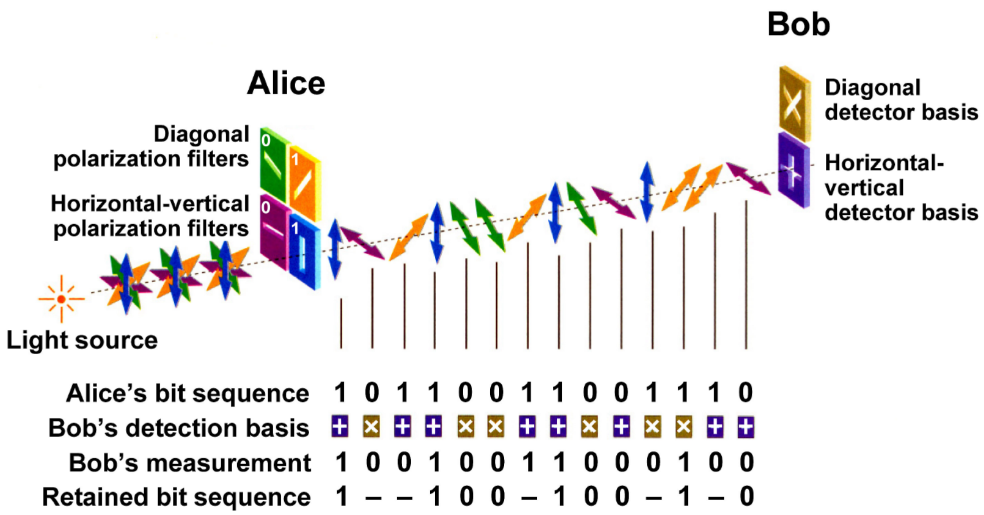
Secure communication was always in interest in all human societies. The oldest known cryptographic example of non-standard hieroglyphs carved into the wall of a tomb is dated around 1900 BCE, was found in Egypt. Also, clay tablets from Mesopotamia dated around 1500 BCE were found, containing encrypted commercially valuable information. Over the following centuries, cryptographic techniques transitioned from simple substitution and transposition cyphers to a "one-time pad" – the only unbreakable classical cypher, that was described first by Frank Miller in 1882 [1], then patented by Gilbert S. Vernam with use of XOR operation for one-time pad in 1919 [2], and proven to be secure by Shannon in 1949 [3]. In this protocol, every symbol in a message is paired with a random secret key, that must be pre-shared between the communicating parties. Every secret key should be used only once, thus, the whole secret key should be of the size of the plain text. Then the main problem of cryptography is in secure distribution of the secret key.

Prior to World War II, mathematical cryptanalysis was developed, leading to invention of mechanical and electromechanical cypher machines. The famous rotor cypher machine Enigma was implemented by German army, and first version was successfully hacked by Polish Cipher Bureau, and British cryptographers hacked the following version, which made a tremendous breakthrough in the cryptography history.

All cryptographic techniques used before 1983 can be classified as "classic" cryptography. The quantum cryptography started in 1983 when Stephen Wiesner published his paper "Conjugate Coding" [4], that first represented a conjugate coding used two principals of quantum mechanics. The first one is Heisenberg uncertainty principle, dated 1927 [5], saying that as much the position of an electron is determined precisely, the less precisely its momentum can be determined, and vice versa. That leads to the fact that it is impossible to measure quantum property of a particle without changing its other parameters. The second principle is the "No-cloning theorem" [6] saying, that it is impossible to create a copy of an arbitrary unknown quantum state without disturbing it. This gives an opportunity to send quantum states between two communicating parties (commonly named Alice and Bob in cryptography) without a possibility for a malicious party (named Eve) to learn the quantum bits secretly. Based on the Wiesner paper, in 1984 Charles H. Bennett and Gilles Brassard proposed a quantum cryptographic protocol for secure communication [7], later referred as BB84 protocol.

1.1 BB84

Suggested by Charles H. Bennett and Gilles Brassard quantum key distribution (QKD) protocol [7] can be implemented to different degrees of freedom of quantum particles. In the paper it was described for a polarization degree of freedom of photons.


Bob
Alice
Diagonal polarization filters
Horizontal-vertical polarization filters
0
1
0
1
Diagonal detector basis
Horizontal-vertical detector basis
Light source

Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Figure 1.1: Principle of the BB84 protocol

(*Re-printed from* [8].)

Alice initiates the protocol by generating a photon in one out of four polarizations. She uses two non-orthogonal bases: one is a horizontal/ vertical (HV) basis and another one is a diagonal/ anti-diagonal (DA) basis. Each basis is used to encode 0 and 1 bits, H and D are for 0, V and A are for 1. Then, she sends the photon to Bob.

Bob randomly chooses a basis for the measurement of the arriving photon's polarization. It results 50% of photons measured in correct basis, and the measurement result is the same as Alice's setting for those photons. When the basis choice is incorrect, it results in random results of 0, 1 with 50% probability each.

After a certain number of photons transmitted and measured, the second part of the protocol starts. Over an authenticated public channel (e.g., internet) Bob reveals to Alice, which measurement basis he used for each photon. Alice communicates to Bob when the basis choice was correct and when not. If an eavesdropper listens to the open channel, it will not provide him any information about the bit values sent. Proper authentication must guarantee that Eve is not participating in this conversation, pretending to be Alice or Bob. Then, Alice and Bob keep only those bits when their bases were the same. It is called a sifted key.

After Alice and Bob got sifted key, they use a portion of it to check errors level: they reveal bits values over the public authenticated channel and compare. There is always some fraction of errors due to equipment imperfection. An important parameter used for description of quantum cryptography protocols – quantum bit error ratio (QBER), determined as

$$QBER = \frac{N_i}{N_i + N_c}, \tag{1.1}$$

where N_i is number of incorrect detected bits, and N_c is number of correct bits. N_i and N_c are determined by direct comparing of measured bits.

A straight-forward attack would be the so called 'intercept and resend' attack, in which an eavesdropper (Eve) tries to measure photons in the quantum channel between Alice and Bob, thereby implementing the same protocol as Bob. Eve resends the results to Bob. Because in 50% of the cases, Even will measure in the incorrect basis, she will inevitably introduce a random bit values in the signals passed to Bob. Therefore, once Bob's measurements are completed, the number of incorrect bits between Alice and Bob will increase to 25%. Thus, Eve's attempt to steal information introduce additional errors.

The next stage of the protocol is the error correction. Alice and Bob implement classical error correction protocol [9] to get identical bit sets. During this step Eve obtains some additional information listening public channel, which needs to be estimated and corrected by the next step.

To finally obtain a secure key, Alice and Bob perform privacy amplification procedure [9], when their obtained bit strings mapped to a smaller secure bits set, called secret key.

The protocol BB84 is theoretically proven to be secure when QBER is less than 11% [10].

1.2 Weak coherent source

True single photon sources are more complicated and can be difficult to implement in practice. More often a heavily attenuated laser pulse is used for QKD, which is called weak coherent pulse (WCP). Then the photon number distribution is described by a Poisson distribution:

$$P(n|\mu) = \frac{(\mu)^n}{n!} exp(-\mu), where$$

P(n—μ) is the probability that the laser emits n photons in a pulse given the mean photon number per pulse is μ. When laser pulses are attenuated that μ is low enough (0.1-0.01), most pulses will contain only one photon, and small portion of pulses will carry two photons or more.

Other QKD protocols were proposed shortly afterwards, specifically, in 1991 Artur Ekert suggested a scheme using entangled pairs of photons (protocol E91) [11], in 1992 Charles Bennett proposed a protocol utilizing only two non-orthogonal polarizations instead of four in BB84 (protocol B92) [9].

For practical implementations of QKD BB84 is the most widely implemented. In practice, QKD systems often use weak coherent laser pulses instead of true single photon sources because these are much easier to implement. A drawback of this solution is that the system gets vulnerable to a photon-number splitting attack (PNS) [9, 12, 13]. This attack exploits the fact that the photon distribution for weak coherent pulses are described by Poisson statistics, and some pulses contain more than one photons. An eavesdropper could split a photon from those multi-photons pulses, and do the measurement, without being noticed. This leads to a security loophole. The mean photon number μ is small (much less than 1) for BB84 prototcol, then a probability for a multi-photon pulse is approximately $\mu^2/2$. Fortunately, adaptations of the protocol implementations were discovered which make implementations robust against the PNS-attack. In 2003 W. Y. Hwang proposed a decoy state protocol [14]. Also, in 2004 V. Scarani, A. Acin, G. Ribordy and N. Gisin published a new protocol [15], robust against PNS attack (SARG04).

1.3 Decoy state protocol

In the BB84 protocol with decoy states [14, 16, 17], in addition to signal pulses carrying encoded bits for the BB84 protocol, Alice generates and sends to Bob decoy pulses with different μ. The decoy pulses are not used for the secret key generation, but serve only for detecting attacks. Alice keeps records which pulses belongs to which distribution and at the sifting stage announces intensity for the each pulse. For an eavesdropper it is impossible to recognize the observed channel transmission, a pulse statistics when multiple intensity levels implemented, but for a successful PNS attack Eve needs to know the photon number statistics. Checking QBER separately for each intensity level, Alice and Bob can therefore discover a possible PNS attack. With the decoy states PNS attack can still be done, but not as effective.

1.4 SARG04 protocol

The SARG protocol [15] can be realized on the same hardware as BB84, as it uses also four non-orthogonal states. Alice randomly sends to Bob one of states ($|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$). Bob measures the state in a randomly chosen basis (**HV** or **DA**). After a string of quantum states sent, Alice and Bob do a sifting procedure over a public authenticated channel, which is different from the BB84 protocol. Alice reveals over public channel a pair to which the sent photon belongs: $(|V\rangle, |D\rangle)$, $(|V\rangle, |A\rangle)$, $(|H\rangle, |D\rangle)$, $(|V\rangle, |A\rangle)$. Within each set the photons are non-orthogonal.

Suppose, Alice sent the $|H\rangle$ state and announced the $(|H\rangle, |A\rangle)$ pair. First, suppose, Bob used **HV** basis for the measurement, which happens with probability 50%. Then he certainly observed **H** as a result. But this result is possible for both states in the announced pair, so Bob has to discard the result. Now suppose, Bob used **DA** basis for the measurement, and got **A** in result, then he also cannot discriminate what state was sent. But if Bob measures in **DA** basis and got **D** in the result, he will know with 100% probability that the sent state was $|H\rangle$. Finally Bob will obtain a raw key that is 1/4 of the sent bits, which is half of that comparing to BB84.

But for the SARG04 protocol Eve will not benefit from PNS attack on two-photon pulses. As Bob's measurement basis is never revealed, she cannot know what state he obtained. Eve could benefit from three-photon pulses, but of the μ is kept low, they are very rare. Thus, the SARG04 protocol is more secure against PNS attack than BB84.

1.5 Polarization and phase encoding

In the considered QKD protocols polarization encoding were implemented. For free-space quantum channels polarization coding suits very well. However, if a standard telecommunication optical fibers are chosen as a quantum channel, photon polarization can rotate due to the birefringence effect. Then the phase encoding [9, 18–20] or time-bin encoding [21, 22] serves better.

For the phase encoding a relative phase between two close pulses is used. A pair of identically unbalanced March-Zehnder interferometers with phase modulators in one arm are used for Alice and Bob. To encode a bit and choose the basis Alice chooses one of four the phase modulator setting $(\pm\pi/4, \pm 3\pi/4)$. Then Bob randomly applies a phase shift of $\pm\pi/4$ to choose the measurement basis.

The QKD protocol for the phase coding is very similar to the polarization coding. It was shown in [18] that the phase and polarization encoding are formally isomorphic to each other and each parameter in the phase coding has its analog in the polarization protocol.

1.6 Plug-n-play system

Both polarization and phase encoding implemented for a fiber based systems require active compensations for possible fluctuations over the quantum channel. A straightforward solution is to send additional more intense pulses and check their properties, then, apply accordingly a compensation (phase drift of polarization) for the quantum states pulses. However for effective work of such scheme, the adjustment pulses should be send quite often, that will slow down the protocol and decrease the secret key rate.

An elegant solution for this problem was suggested by Martinelli in 1992 [23], that allows passively compensate fluctuations in optical fiber, using Faraday mirror. A pulse travels front and back in the system through the same optical conditions. After a pulse starts at Bob's side, it gets reflected at Alice's end by the Faraday mirror, it returns to Bob orthogonal to its original state with all birefringence effects compensated [18].

To implement the phase encoding QKD, the method was combined with time multiplexing in long-path interferometer [24, 25]. In the Fig. 3.1 the scheme of the self-aligned plug-n-play system shown.

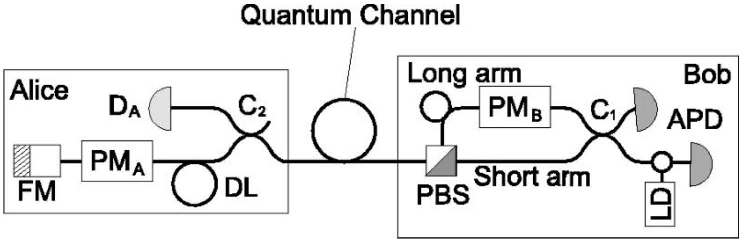


Figure 1.2: Scheme of plug-n-play system

Self-aligned plug-n-play system: LD, laser diode; APD, avalanche diode; C_1, C_2, fiber couplers; PM_A, PM_B, phase modulators; PBS, polarizing beamsplitter; DL, optical delay line; FM, Faraday mirror; D_A, classical detector. (*Re-printed from* [18].)

A laser located at Bob's end emits pulses, which travel by one of two ways: through the long or short arm of Bob's interferometer. Then, the pulses travel through the Quantum Channel (optical fiber) channel, and are reflected by the Faraday mirror at Alice's location, and their phase is modulated according to a phase encoding protocol. Faraday mirror reflects light rotating its polarization by 90 degree. After they arrive to Bob's side again, because of the PBS the pulses travel another arm of the interferometer than they did initially, Bob applies a phase shift on his phase modulator choosing the measurement basis, and finally the pulses got combined at the fiber coupler C_1 and interfere. Single-photon detector register the output port of the photon, providing his quantum state.

1.7 Bell state measurement

Bell states are the simplest two-qubit maximally entangled quantum states named after John S. Bell who used them to violate his Bell inequality [26]. The states are:

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_A \left|0\right\rangle_B + \left|1\right\rangle_A \left|1\right\rangle_B\right), \tag{1.2}$$

$$\left|\Phi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_A \left|0\right\rangle_B - \left|1\right\rangle_A \left|1\right\rangle_B\right), \tag{1.3}$$

$$\left|\Psi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_A \left|1\right\rangle_B + \left|1\right\rangle_A \left|0\right\rangle_B\right), \tag{1.4}$$

$$\left|\Psi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle_A \left|1\right\rangle_B - \left|1\right\rangle_A \left|1\right\rangle_B\right). \tag{1.5}$$

The Bell state measurement (BSM) is a core operation for the quantum teleportation protocol. For a two-qubit state the BSM results in a projection of the states onto a Bell state, indicating correlation between the qubits. The Bell-states form a basis, and any two qubit state can be represented as a superposition of the Bell states:

$$|S\rangle = \alpha_+ \left|\Phi^+\right\rangle + \alpha_- \left|\Phi^-\right\rangle + \beta_+ \left|\Psi^+\right\rangle + \beta_- \left|\Psi^-\right\rangle . \tag{1.6}$$

Then in the result of the BSM, e.g., a probability $|\alpha_+|^2$ to find the state $|S\rangle$ in the Bell state $|\Phi^+\rangle$ can be obtained.

If two qubits before the Bell measurement were not entangled, they will be projected onto one of four Bell states and emerge entangled after this protocol.

1.8 Quantum teleportation protocol

The quantum teleportation transfers quantum information (a state of a quantum particle) over some distance, using classical communication channel and pre-shared quantum entangled particles between two communicating parties.

The quantum teleportation idea was first introduced by Charles Bennett at al. in 1993 in Ref. [27].

Alice and Bob initially share an entangled Bell state:

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right), \tag{1.7}$$

and Alice posses a quantum state $|\psi\rangle_C = \alpha |0\rangle_C + \beta |1\rangle_C$, which she wants to transfer to Bob. Then, the state of the total system is :

$$\left|\Phi^+\right\rangle_{AB} \otimes |\psi\rangle_C = \left(\frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)\right) \otimes \left(\alpha |0\rangle_C + \beta |1\rangle_C\right). \tag{1.8}$$

Representing the Alice's two qubits in the Bell states basis, using the following identities:

$$|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}} \left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right) \tag{1.9}$$

$$|1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}} \left(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle\right) \tag{1.10}$$

$$|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}} \left(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle\right) \tag{1.11}$$

$$|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}} \left(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle \right), \tag{1.12}$$

the total system state can be written:

$$\begin{aligned} &\left|\Phi^+\right\rangle_{AB} \otimes |\psi\rangle_C \\ &\qquad\qquad = \frac{1}{2}\{\left|\Phi^+\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \\ &\qquad\qquad + \left|\Phi^-\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B - \beta\,|1\rangle_B) \\ &\qquad\qquad + \left|\Psi^+\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \\ &\qquad\qquad + \left|\Psi^-\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B - \beta\,|1\rangle_B)\}. \end{aligned} \tag{1.13}$$

Now Alice performs the measurement in the Bell states basis ($|\Phi^+\rangle_{AC}$, $|\Phi^-\rangle_{AC}$, $|\Psi^+\rangle_{AC}$, $|\Psi^-\rangle_{AC}$) leaving the system in one of four states:

$$\left|\Phi^+\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \tag{1.14}$$

$$\left|\Phi^-\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B - \beta\,|1\rangle_B) \tag{1.15}$$

$$\left|\Psi^+\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \tag{1.16}$$

$$\left|\Psi^-\right\rangle_{AC} \otimes (\alpha\,|0\rangle_B - \beta\,|1\rangle_B). \tag{1.17}$$

The measurement changed the state of the system, the Alice's two particles are entangled now, and the originally entangled particles are not entangled anymore. Alice sends to Bob information about results of her measurement through a classical channel. According to that information Bob applies a unitary operation to his qubit to obtain the teleported state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

If Alice informs Bob that she obtained $|\Phi^+\rangle$, Bob knows his qubit is already in the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

If Alice informs Bob that she obtained $|\Phi^-\rangle$, Bob has to implement the Pauli's matrix

$$\sigma_z = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

to obtain the desired result.

If Alice informs Bob that she obtained $|\Psi^{+}\rangle$, Bob has to implement

$$\sigma_x = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

If Alice informs Bob that she obtained $|\Psi^{-}\rangle$, Bob has to implement

$$i\sigma_y = i\sigma_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

1.9 Quantum communications development

Quantum communications including QKD are actively developing during the last decades [7, 9, 15, 27–39]. Not the last reason for that is the fast progress in quantum computing field [27, 40–49]. Skyrocketing computation power of quantum computers will create a threat for security of existing classical cryptographic protocols widely used for secure communications in modern society, because security of many of the classical cryptographic protocols for key establishment based on assumption of a limited computation power of a potential eavesdropper [40, 50, 51]. Although there is a large research on post-quantum cryptography [51] seeking to develop algorithms resistant to powerful attacks from quantum computers, quantum cryptography suggests itself as an excellent solution for a secure communication due to its "un-breakable" nature based on quantum physics.

Because of that reason, QKD presently is the most commercialized area of quantum communications. In particular, a Swiss company ID Quantique commercializes QKD systems, including quantum key generation, distribution and quantum safe network encryption. Their main customers are from governments, banking, industry and academy. Also, China started implementing quantum communications widely. Several research groups are building a biggest quantum network in the world that connects Beijing, Shanghai, Hefei and Jinan with its total length of about 2000 km [36, 52] and utilizing 32 trusted nods. In purpose to extend the quantum network to global scale, a quantum satellite can be used. Distances for quantum communications on the ground are limited by some hundreds kilometers due to losses either in optical fiber or in atmosphere [19, 33, 53–55] and losses scale with distance exponentially. In the space environment there is no absorption and scattering losses, only diffraction losses which scale with distance quadratically. For the ground to satellite link, main losses will occur in the atmosphere part of the light path. Therefore, losses for the ground-to-satellite link will be lower than losses over the longest feasible distance in free-space channel on the ground [56].

In 2016 China launched a quantum satellite [57] and already has tested entanglement distribution [39], quantum teleportation [37] and QKD [38] over the 1200–1400 km long quantum channel between the Earth ground station and the low-Earth orbit satellite. It is a very important step in globalization of quantum communications, as Earth-to-satellite quantum links straightforwardly lead to the global QKD network. A satellite orbiting around the Earth establishes quantum links with two or more locations on the ground and then those locations can share a secret key through a trusted nod on the satellite [35, 56].

In 2017, the European Commission announced 1 billion euro project dedicated to quantum technologies [58], which also includes developments for quantum communication and QKD.

1.10 Quantum communication with satellites

In April, 2017 the Canadian prime minister announced a start of Canadian quantum satellite mission. Financing of about $80 million over five years was provided to Canadian Space Agency (CSA) to develop emerging technologies. Part of this budget is intended for development of quantum technologies in space involving Institute for Quantum Computing in Waterloo. Tentatively, Canadian quantum satellite can be launched in about 5 years.

Ground-to-satellite quantum communication can be realized in two directions: up-link, when a quantum source is located on the ground and SPDs are on the satellite; and down-link, when the source is on the satellite. Both variants have their benefits and drawbacks, considered in details in the Ref. [56]. The up-link is more beneficial for the scientific or technology demonstration mission, as it provides a freedom to test different protocols, implement different sources, interchanging them on the ground. Taking into account the lifetime of a satellite (usually 5-10 years) and a possibility of inventing new better sources of quantum states, it looks very reasonable to place the receiver on a satellite. The choice of potential candidates SPDs for the quantum satellites is considered in the next chapter. The harsh space environment requires SPDs able to withstand and work successful as quantum receivers. That leads to necessity of special tests for potential candidates SPDs, and building of custom detectors.

The projects presented in this thesis are dedicated mostly to work on long distance quantum communications, towards developing Earth-to-satellite quantum communications, and particularly, QKD. Also, one project was about testing a commercial QKD system security.

My contribution to the projects mainly consisted of a work on single-photon detectors (SPDs) for quantum communications.

Chapter 2

Single-photon detectors for long distance quantum communications

In this chapter requirements to SPDs for quantum communications and an overview of available SPDs will be provided.

2.1 Requirements to SPDs for quantum communications

In this section we discuss SPD's parameters important for quantum communications and limiting our choice of detectors.

2.1.1 Wavelength

Wavelength choice for free space quantum communications is determined by an optimal wavelength for transmission through the ground-to-satellite optical channel and by available quantum source wavelengths. Consideration of an optimal wavelength through the atmosphere takes into account atmospheric transmittance windows, angle of an optical link, diffraction, scattering, turbulence and absorption losses. The detailed analysis was done by J.-P. Bourgoin [56], the results of numerical simulation is shown in the Fig. 2.1.

Diffraction losses are smaller for shorter wavelengths, whereas atmospheric transmittance and turbulence losses are smaller for longer wavelengths.

Considered sources are either laser source of WCP, or entangled photon source.

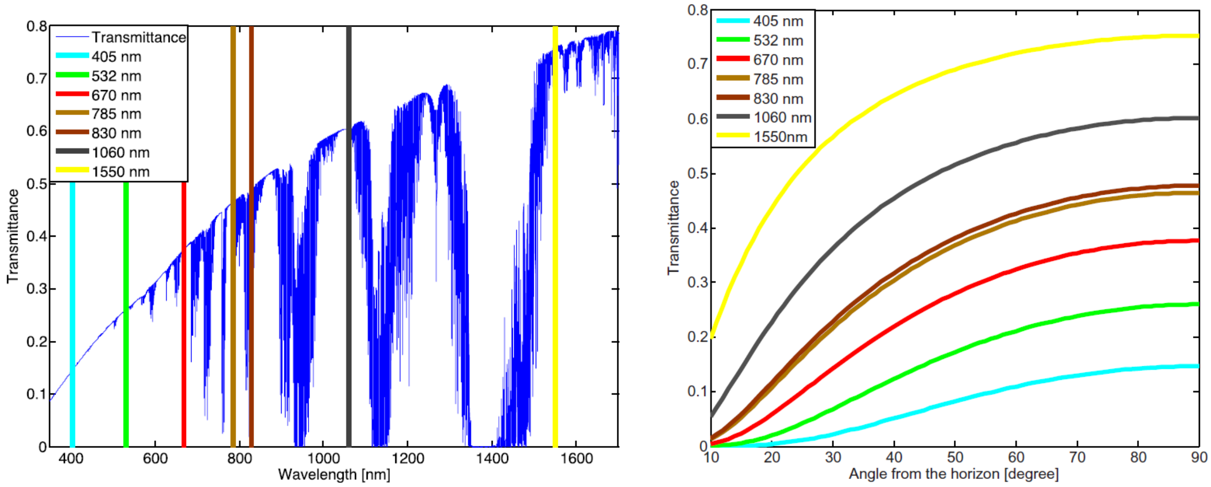


Figure 2.1: Simulated atmospheric transmittance.

Simulated atmospheric transmittance at a typical rural location, for propagation at zenith (left) and for different elevation angles (right). Colored lines represent wavelengths of commercially available laser systems. Several transmission windows are evident, within which optical transmission would experience low loss. Generally, the transmission tends to be better at higher wavelengths, but other factors (e.g. diffraction, sources and detectors) must be taken into account to properly determine the best wavelength choice. (*Re-printed from* [56].)

2.1.2 Important parameters of SPDs

Choosing SPDs for quantum communications we consider many parameters: dark count rate, quantum detection efficiency, timing jitter, afterpulsing, maximum detection rate, size of the sensitive area. A table presenting characteristics for most of the available SPDs is shown in the Fig. 2.2.

- **Dark count rate** is false counts or noise of SPDs. They arise through different mechanisms depending on the SPD's structure and materials. E.g., in APDs most of dark counts are caused by thermal excitation and depend on temperature of APDs; in PMTs dark count pulses originate from thermal emission of electrons from the photocathode and dynodes; in superconducting nanowire SPDs (SNSPDs) dark counts caused by intrinsic processes are extremely low, can be less than 10^{-4} cps [60].

  Dark counts in SPDs of receivers introduce errors for quantum communications. For QKD dark counts are increasing QBER. For the teleportation experiment it was calculated (as shown later in the thesis) how DCR affects data collection time.

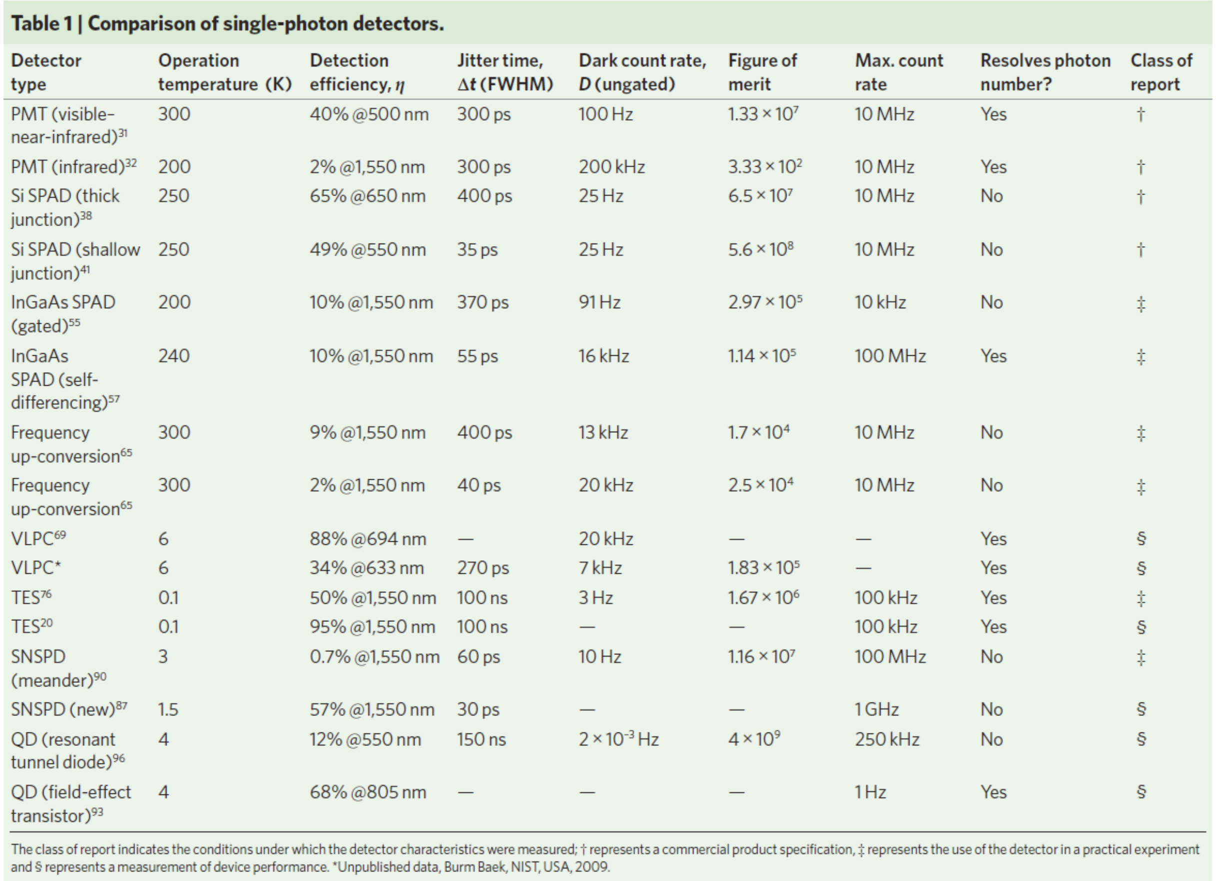


Table 1 | Comparison of single-photon detectors.

Detector type	Operation temperature (K)	Detection efficiency, η	Jitter time, Δt (FWHM)	Dark count rate, D (ungated)	Figure of merit	Max. count rate	Resolves photon number?	Class of report
PMT (visible-near-infrared)[31]	300	40% @500 nm	300 ps	100 Hz	1.33×10^7	10 MHz	Yes	†
PMT (infrared)[32]	200	2% @1,550 nm	300 ps	200 kHz	3.33×10^2	10 MHz	Yes	†
Si SPAD (thick junction)[38]	250	65% @650 nm	400 ps	25 Hz	6.5×10^7	10 MHz	No	†
Si SPAD (shallow junction)[41]	250	49% @550 nm	35 ps	25 Hz	5.6×10^8	10 MHz	No	†
InGaAs SPAD (gated)[55]	200	10% @1,550 nm	370 ps	91 Hz	2.97×10^5	10 kHz	No	‡
InGaAs SPAD (self-differencing)[57]	240	10% @1,550 nm	55 ps	16 kHz	1.14×10^5	100 MHz	Yes	‡
Frequency up-conversion[65]	300	9% @1,550 nm	400 ps	13 kHz	1.7×10^4	10 MHz	No	‡
Frequency up-conversion[65]	300	2% @1,550 nm	40 ps	20 kHz	2.5×10^4	10 MHz	No	‡
VLPC[69]	6	88% @694 nm	—	20 kHz	—	—	Yes	§
VLPC*	6	34% @633 nm	270 ps	7 kHz	1.83×10^5	—	Yes	§
TES[76]	0.1	50% @1,550 nm	100 ns	3 Hz	1.67×10^6	100 kHz	Yes	‡
TES[20]	0.1	95% @1,550 nm	100 ns	—	—	100 kHz	Yes	§
SNSPD (meander)[90]	3	0.7% @1,550 nm	60 ps	10 Hz	1.16×10^7	100 MHz	No	‡
SNSPD (new)[87]	1.5	57% @1,550 nm	30 ps	—	—	1 GHz	No	§
QD (resonant tunnel diode)[96]	4	12% @550 nm	150 ns	2×10^{-3} Hz	4×10^9	250 kHz	No	§
QD (field-effect transistor)[93]	4	68% @805 nm	—	—	—	1 Hz	Yes	§

The class of report indicates the conditions under which the detector characteristics were measured; † represents a commercial product specification, ‡ represents the use of the detector in a practical experiment and § represents a measurement of device performance. *Unpublished data, Burm Baek, NIST, USA, 2009.

Figure 2.2: Comparison of single-photon detectors.

(*Re-printed from* [59].)

- **Detection efficiency** is a probability of creating an output when a photon hits a sensitive area of the detector. The highest detection efficiency over 90% at 1542 nm was reported for SNSPDs [61]. For the visible wavelengths Si-APD provide more than 50% efficiency [59]. In the UV range SNSPDs also demonstrated the highest efficiency of 70–80% at 250–370 nm [60].

  The higher detection efficiency of SPDs used for a QKD protocol increases secret bit rate, making the system more efficient.

- **Timing jitter** describes a fluctuation of time intervals between absorption of a photon by an SPD and output pulse, is usually measured as full-width half-maximum (FWHM). It varies from 15 ps (for SNSPD [62]) to 300–400 ps (for APDs and PMTs [59]). The timing jitter is limiting resolution of SPDs.

- **Afterpulses** are noise counts appeared after a registered count and caused by intrinsic processes in some types of SPDs. In APDs afterpulses are caused by carriers trapped during an avalanche and spontaneously released after a short time called traps life time, and induced a new avalanche. Si-APDs have relatively low afterpulsing probability, 1% [63]; Ge- or InGaAs/InP have higher afterpulsing probability, e.g., 5% with 5 μs dead time [64]. Afterpulsing effect was observed in SNSPDs as well [65], though it could be caused by the design used.

Afterpulsing in SPDs implemented for quantum communications can be suppressed by a properly chosen gate regime, or discarded during post-processing.

- **Maximum count rate** determines the maximum number of photons per second that an SPD is able to count. APDs have a dead time (recovery time) after each avalanche during that they are unable to register photons. The highest count rate of 16.7 GHz was reported for SNSPDs working in 250–340 nm range [60].
- **Diameter of sensitive area** is a very important parameter for quantum communication systems. Depending on an optical scheme implemented a bigger sensitive area of SPDs allows to minimize losses, e.g., in the teleportation experiment [33] our APD detectors with 500 μm were implemented decreasing losses due to turbulence caused beam moving.

2.2 SPDs suitable for quantum communications

The choice of SPDs for quantum communications is determined by the chosen wavelength and other SPD's parameters. Available SPDs can be divided by their response spectral range: ultraviolet ($\leq$ 400 nm), visible (400–1000 nm) and infrared (950–1650 nm).

Infrared range is served by InGaAs or Ge APDs, and SNSPDs. The APDs have low detection efficiency, high DCR and high afterpulsing probability. Whereas SNSPDs made a significant progress and reached extremely good parameters in the last years [60–62, 65–68] demonstrated very high detection efficiency, extremely low DCR, almost no afterpulsing and high resolution. They would be an excellent candidate for ground-to-satellite quantum communications, but they require cryogenic cooling and have very small sensitive area (few–tens μm), that make them not suitable for the receiver on a small satellite.

Silicon based APD detectors work in the range 400–950 nm, providing photon detection efficiency 50-65%, low DCR of 1–200 cps depending on bias voltage and temperature, and maximum count rate of about 10 MHz. Si-APDs are well established technology, detectors do not require cryogenic cooling, usually thermo-electrical coolers (TECs) are sufficient for operation. Also, the APD SPDs have a compact size and do not have high demand for electrical power. All those considerations make them a good candidate for a satellite mission.

For two types of APD detectors J.-P. Bourgoin made a simulation for QKD, showing performance depending on wavelength in the range 450–1550 nm [56]. Also, simulation of several quantum protocols as a function of SPD's DCR was made. As a result of the last, performance of QKD will be significantly limited at DCR of SPDs higher than 250 cps per detector.

Another possible candidate for quantum satellite receiver can be PMTs. They were first used for photon counting in 1949 [69], work in a wide spectral range (115–1700 nm) and have been used in space for a long time. Also, they have big sensitive area more than 10 mm. However, their detection efficiency is significantly lower (the highest is 40% at 500 nm), they require high voltage (few kV) for operation and have high afterpulsing rate comparing to APDs. Though microchannel plate PMTs show the low timing jitter (about 20 ps) [70], PMTs are not our first option for the quantum satellite receiver.

2.2.1 Si-APD

APDs are able to register light due to the photoelectric effect that converts light to electricity. Their design provides in-built gain stage through avalanche multiplication process. To be used for the single photon counting a reverse bias voltage applied to the APD is set above APD's breakdown voltage [71–74]. Then the APD is either in a quiescent state with negligible current or in a state with self-sustaining avalanche breakdown. The avalanche process can be triggered by a single carrier, thermally exited, or resulted from ionization by a photon. To provide quenching for this current, a high load resistor (more than $100\,\mathrm{k\Omega}$) can be connected between the APD and the bias voltage source [71, 72]. This is called passive quenching method. After the avalanche quenched, the APD restored in its zero-current state, and the voltage across diode starts recovering up to its initially set value. The period after an avalanche stopped and until an APD is able to produce the next avalanche is called dead-time. To minimize the dead-time and operate the device at faster rate, an active quenching circuit can be implemented [72, 75, 76]. The quenching transition is forced a few nanosecond after an avalanche is triggered, and the APD can be held off for a controlled time of about few nanosecond.

DCR of APDs is mostly caused by thermally exited carriers which trigger avalanches in the absence of any light. Cooling an APD decreases thermal energy of carriers, and thus DCR of APDs decreases with temperature [74, 77].

Chapter 3

Trojan-horse attack on commercial QKD system

3.1 Trojan-horse attack experiment motivation

Though security of QKD based on laws of quantum mechanics and supposed to be unbreakable, physical implementations of the QKD systems are not perfect and create opportunities for hackers [78–84].

To improve the security of QKD systems, they need to be tested for possible loopholes and side channels. One known potential vulnerability is called a Trojan-horse attack. An eavesdropper tries to steal a secret information passing between Alice and Bob, sending bright light pulses into the optical quantum channel and analyzing back reflected photons properties [85, 86].

If a QKD system is working on BB84 protocol, phase or polarization encoding happens inside Alice's system. Thus, an adversary can send a bright light pulses to Alice side and analyze the information contained in back reflected signals, with the goal of extracting information about Alice's polarizer and phase modulator settings. Because Bob's modulators are classical devices which are operated in a linear optical regime, they will not distinguish between Alice's carefully powered pulse or a brighter pulse from Eve. Following the classical information shared by Alice and Bob through open channel during the post processing, Eve will obtain information about the raw key. One method to prevent this, is installing a detector capable of monitoring the incoming light intensity at Alice apparatus entrance.

When a QKD system employs SARG protocol [15, 87], the secret bits are given by

Bob's basis choice applied to the phase modulator. Eve implementing the Trojan-horse attack could learn about Bob's phase modulator settings, thus obtain information about the raw key [88]. Then, listening open channel and following next steps (sifting, error correction and privacy amplification) Eve would obtain the secret key not leaving any foot prints.

Bob cannot prevent this attack by the same method as Alice. Inserting a monitoring device will attenuate already quite weak light pulses, that will lead to a reduction of the secret key rate. Neither can an optical isolator be implemented in the two-way plug-n-play system, as Clavis2, because by the very principle of operation the two-way transmission of signals is required.

We were able to demonstrate an experimental Trojan-horse attack on a running commercial QKD system Clavis2. We sent bright pulses to the Bob's apparatus and analyzed the reflected photons passing through twice Bob's phase modulator using homodyne detection to learn the phase of the photons imprinted by Bob's phase modulator. Thus, the information about the raw key bits was revealed and the security of the system is compromised.

3.2 Preparation for the Trojan horse attack experiment

The Fig. 3.1, b shows the optical scheme of the considered QKD system Clavis2, manufactured by ID Quantique.

The QKD system is a plug-n-play two-way scheme [90], able to run BB84 and SARG04 protocols. Our attack was intended for the Clavis2 running SARG04. Accordingly to a common assumption, Eve has access to the optical quantum channel, and she inserts her apparatus in the line as shown in the Fig. 3.1, a. As required by the implemented SARG04 protocol, Bob sends bright laser pulse pairs to Alice, she attenuates pulses, prepares quantum states randomly applying a phase shift $\phi_A = 0, \pi/2, \pi, 3\pi/2$ and sends them back to Bob. Bob randomly applies a phase shift $\phi_B = 0, \pi/2$ corresponding to the secret bits 0_B or 1_B, and measures quantum states. The pulses are send in "frames", and the length of the trains of pulses from Alice is limited by the length of Alice's delay line, that serves to separate incoming and out coming pulses. The length of frames in the Clavis2 system under the experiment was set to be of 215 μs.

Eve needs to send her Trojan-pulses to Bob's apparatus before or after a frame in a time, that the Eve's pulse (or its back-reflection from any optical component inside

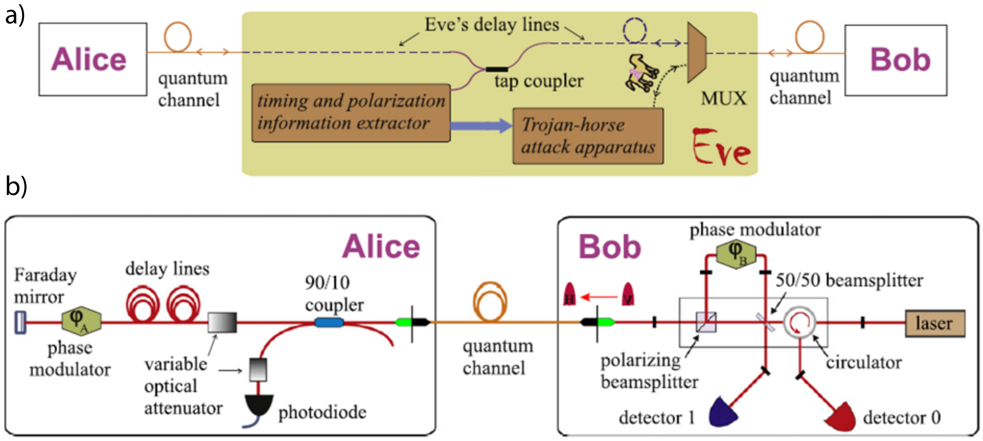


Figure 3.1: Optical schemes of Alice's and Bob's QKD system, and the scheme how Eve's apparatus could be inserted

a) Inserting Eve's apparatus in the quantum channel between Alice and Bob

b) Alice and Bob optical schemes (*Re-printed from* [89])

Bob) will travel through Bob's phase modulator (PM) while it is active. Then Eve's photons will have their phase modulated and Eve can get information about the PM setting.

To prepare the Trojan-horse attack on Clavis2, we had to solve several question, like timing of launched and reflected Eve's light pulses, their wavelength and the best way of back-reflected pulses analysis. I measured levels of reflection from Bob's different optical components at wavelengths of 806, 1310, 1550 nm using optical time domain reflectometry (OTDR) system and results are represented as a temporal distribution of the back-reflection levels – "reflection-map". Also insertion losses for all Bob's components were measured. An OTDR system was connected to the Bob's setup input, and reflections from all components were measured. The polarization of the probe light was set to maximize reflection from the fiber connector right behind the PM. The results for the 806 and 1550 nm wavelengths are shown in the Fig. 3.2, as the OTDR traces for 1310 and 1550 nm were found to be quite similar. The level of back reflection ratio was around -57 dB. Thus, when Eve sends her Trojan-horse pulses with a mean photon number of 2×10^6, she will get back about 4 photons on average. As can be seen from the Fig. 3.2, attenuation and reflectance of optical interfaces and also components depend on the wavelength. To investigate a possibility of an attack at a other wavelengths, it would be necessary to do OTDR measurements over the wide spectral range. Some additional spectral measurements [89] did not reveal reflection peaks besides at 1550 nm.

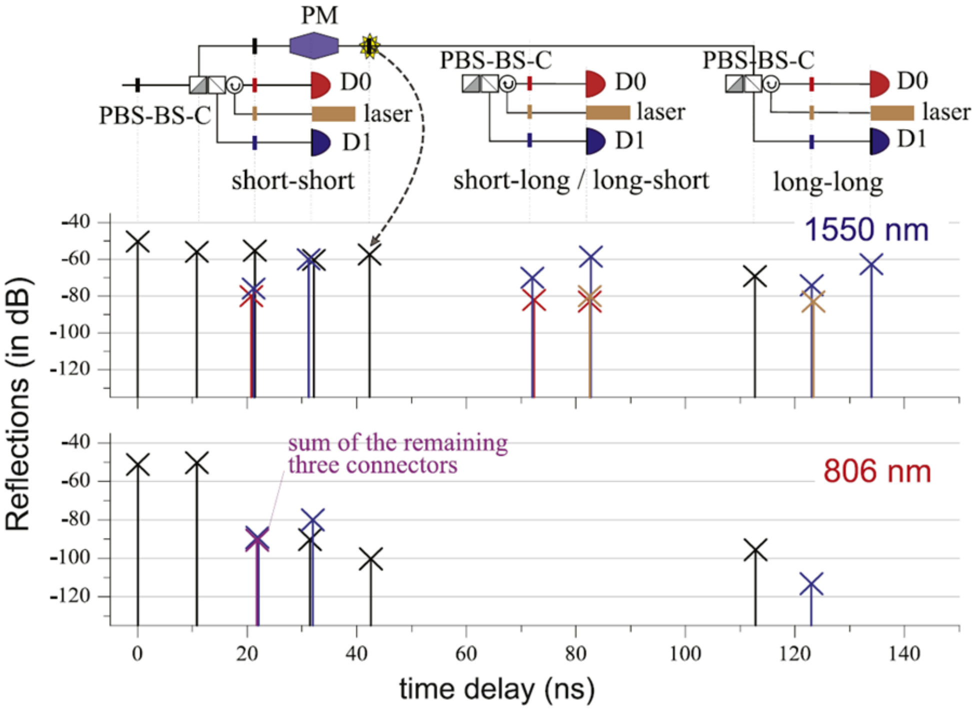


Figure 3.2: Reflections map

Reflections from all components in Clavis2 optical scheme were mapped at 806 and 1550 nm. Reflections from several components close in time are color-coded. OTDR sensitivity was about -83 dB at 1550 nm, and -96 dB at 806 nm. Some important reflections were obtained by combining several measurements on part of Bob. Small filled rectangular blocks represent FC/PC connectors with curved polished surface; PM, phase modulator; D0 and D1, single-photon avalanche diodes; PBS-BS-C, optical assembly of polarizing BS, 50/50 BS and circulator. OTDR model used: opto-electronics modular picosecond fiber-optic system.

(*Re-printed from* [89])

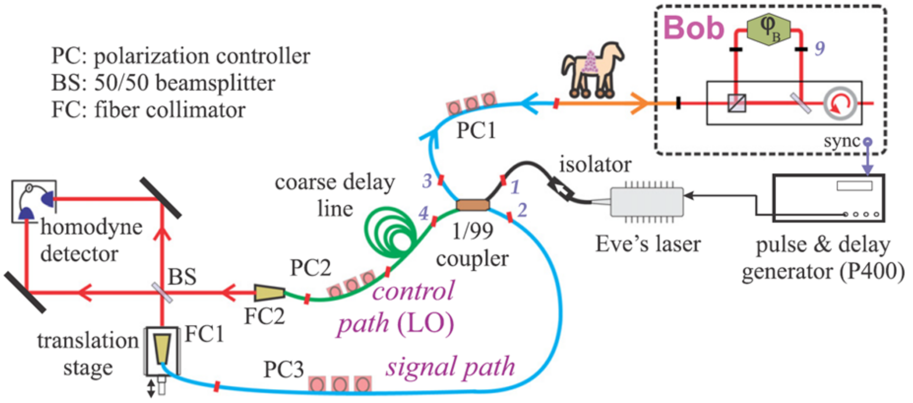


Figure 3.3: Eavesdropper apparatus schematic.
(*Re-printed from* [89])

Eve's apparatus, that we built to experimentally demonstrate Bob's phase read-out, is shown in the Fig. 3.3. Eve's laser generated pulses with frequency of 5 MHz, synchronized with Bob's clock through a pulse delay generator (P400). The pulses were launched to Bob's apparatus through a fiber coupler and passed a polarization controller for power optimization. Other arms of the fiber coupler lead to the homodyne detector. One arm, control path (local oscillator (LO)), from port 4 connected to a delay line, and the other arm is a signal path. Then, the control and the signal pulses mix at the beam splitter (BS) of the homodyne detector. The power of the laser was adjusted so that the mean photon number for LO was more 10^8 and for Eve's pulses to Bob was less than 1.5×10^6 (about 3 back-reflected photons). The output voltage of the homodyne detector was measured with an oscilloscope.

3.3 Results

The obtained results of homodyne detection measurement of the phase of Eve's back-reflected photons are shown in the Fig. 3.4. The upper trace in (a) shows Bob's PM voltage over 5 slots, and the lower trace shows output of the homodyne detector. In (b) the results after integration over the time windows (shown in green) are presented, here they are obviously more distinguishable. The summary of determined PM voltage settings over a QKD frame can be seen in the Fig. 3.5. In average, Eve is able to determine correctly the settings of the PM in about 95% of slots.

Unfortunately for Eve, her bright pulses cause some side effects that could lead to an increased QBER and an aborted protocol, thus Eve was not able to get any secret

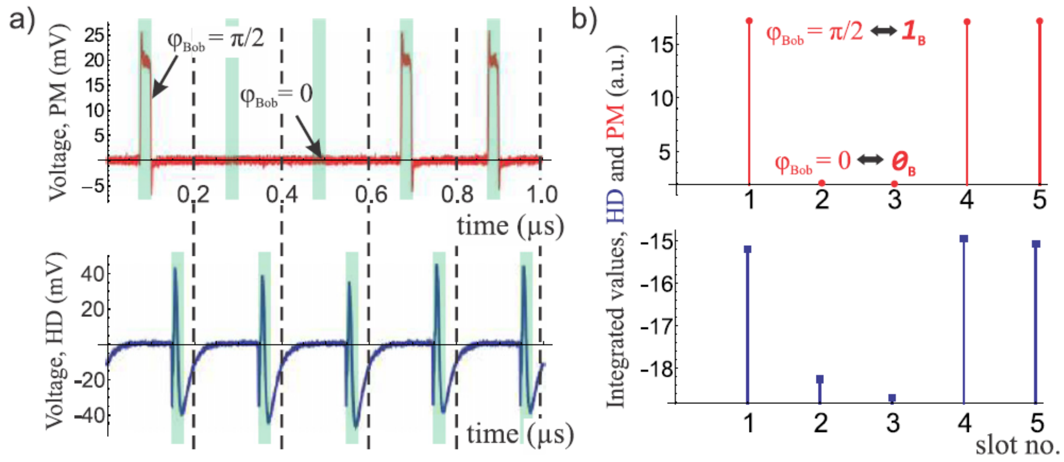
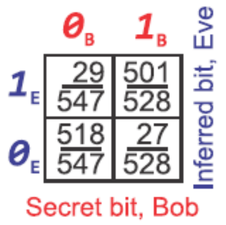


Figure 3.4: Output for Bob's phase modulator and Eve's homodyne detector.
(a) Upper traces present Bob'd phase modulator voltage for 5 consecutive slots and lower traces are from Eve's homodyne detector. Integrating over a time window (green) makes the difference between Eve's output pulses more evident (b). (*Re-printed from* [89])



	0_B	1_B
1_E	$\frac{29}{547}$	$\frac{501}{528}$
0_E	$\frac{518}{547}$	$\frac{27}{528}$

Secret bit, Bob

Inferred bit, Eve

Figure 3.5: Bob's and Eve's resulting bits.
The table shows portion of bits determined by Eve as 0_E (or 1_E) while Bob measured 0_B (or 1_B). (*Re-printed from* [89])

bits. Bob's single photon detectors work in a gated mode, and despite Eve is sending her pulses when Bob's detectors are inactive, the detectors demonstrate increased DCR level during many gates after Eve sent her interrogating pulse. We believe that the bright pulses populate carrier traps in SPADs semiconductor [81, 91] which cause the noise detection level to increase. During the next gate the trapped carriers get released and cause avalanches - afterpulses. This increased level of DCR of SPADs, and thus, increased QBER. When QBER increased above a certain threshold (around 8% in Clavis2), the QKD protocol will be aborted. The level of these afterpulses depends on the brightness of Eve's pulses.

Also, when Eve's pulse arrives a few ns after a gate, it still can cause a click [81] in the same slot. To avoid this, Eve should not use pulses with mean photon number higher than 2×10^6 for Clavis2. In order to keep afterpulsing level low, Eve should use the dimmest-possible pulses. As she already receives only 3-4 photons per pulse, to decrease afterpulses Eve can not attack every slot, but only some of them, thus decreasing the average photon number. This will decrease the amount of information she gains, but it still would compromise the security, because Eve could have some secret bits after the privacy amplification.

To construct a working Trojan-horse attack, Eve could implement some additional tricks. She can change the channel between Alice and Bob to a low noise channel to minimize losses and increase a chance of detecting a photon in a given slot; or she can block the channel completely to decrease a chance of Bob's detection. Also Eve can make use of a dead time after a successful detection event in Bob. Furthermore, she can send her pulses in consecutive sets to maximize a probability of testing on a non-zero slot, as with the low mean photon number in the protocol, most slots are carrying zero photons; then, she would have to make a pause. To mask afterpulses from her attack, Eve can use a substitution sequence, when she sends a sequence of slots on the low noise channel. More detailed description of Eve strategies evaluation can be found in [89].

In our results, with the best optimized crafted strategy, Eve's knowledge of secret bits never exceeded the estimate for it made by Alice and Bob. That means that Eve's attack failed. The main reason for the failure is that Bob's SPADs have quite high level of DCR and afterpulses, that contributed to QBER. Especially one of the detectors had a high DCR. If both SPADs had same DCR as the better of the two, Eve would have been able to gain some secret information. We modeled an optimized attack on a system with better detector parameters (lower DCR, lower afterpulsing), and that attack would succeed. The parameters we used for the modeling are realistic, and next generation of SPADs used for QKD systems can match the conditions.

3.4 Conclusion

We prepared and experimentally demonstrated a Trojan-horse attack on a commercial Clavis2 QKD system running SARG04 protocol [89]. We successfully demonstrated Bob's PM phase readout on the running system by a possible hacker. Also, we determined limitations for launching the full Trojan-horse attack. The attack failed mainly due to high level of afterpulses in Bob's detectors after the bright Eve's pulses.

We analyzed possible Eve's strategies to model a successful attack, and determined conditions for it. We note, Eve can combine the Trojan-horse attack with other known attacks (e.g., after-gate attack [81]) for the better performance.

For one-way systems the best countermeasures against the Trojan-horse attack are isolators and wavelength filters. For two-way system, like the one we tested, it would be useful to decrease reflections from surfaces on the way of incoming pulses. Here some technical recommendation we suggest:

- installing an additional detector at the entrance of Bob, randomly monitoring incoming light level;
- reducing the time during which the PM is active;
- monitoring Bob's SPADs output in real time, not just statistics.

Also, a possible Trojan-horse attack could be incorporated into theoretical security proof, and a proper level of privacy amplification for neutralization the attack could be determined.

In conclusion, the presented work led to another project investigating Trojan attack on QKD systems at another wavelength of 1924 nm, at which Bob's SPADs do not respond so strongly to Eve's bright pulses [84].

Chapter 4

Quantum teleportation over 143 km

On the way of development of long-distance free-space quantum communication, there were many essential steps demonstrating implementation of different quantum protocols including quantum teleportation, Bell state measurement and entanglement based quantum communication through longer and longer distances, see [9, 26, 27, 55, 92–95].

Our new detector demonstrates an extremely low DCR without a decreased performance in other important parameters (detection timing jitter, detection efficiency, afterpulsing). Implementation of such SPDs can be very beneficial for quantum communications over high loss channels. Our previous generation in-lab built Si SPDs were implemented in an experiment demonstrating successful quantum teleportation over 143 km that was performed between two Canary Islands - La Palma and Tenerife [33].

4.1 Challenges of the quantum teleportation field experiment

Quantum teleportation utilize a quantum channel and a classical channel between two communicating parties, usually named Alice and Bob. Alice was located in La Palma, and Bob in Tenerife. They share a auxiliary quantum state via the quantum channel

$$\left|\Psi^-\right\rangle_{23} = \frac{1}{\sqrt{2}}\left(|H\rangle_2 |V\rangle_3 - |V\rangle_2 |H\rangle_3\right), \tag{4.1}$$

where $|H\rangle$ and $|V\rangle$ are horizontal and vertical polarization states, and photon 2 is at Alice's location and photon 3 is at Bob's location. Charlie is a third member of communication, he prepares photon 1 in state $|\phi\rangle_1$, using a heralded single-photon

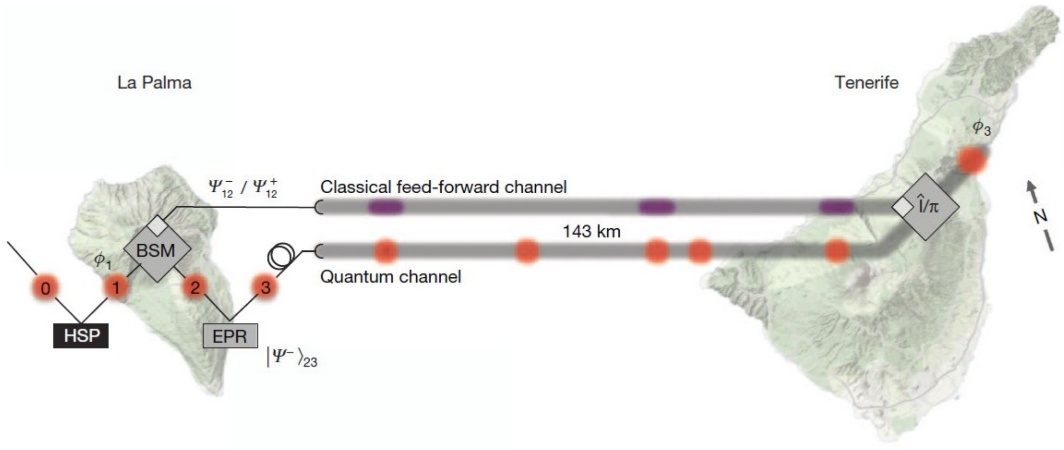


Figure 4.1: Experimental scheme of quantum teleportation.

Experimental scheme of quantum teleportation between the Canary Islands La Palma and Tenerife over both quantum and classical 143-km free-space channels. (*Re-printed from* [33].)

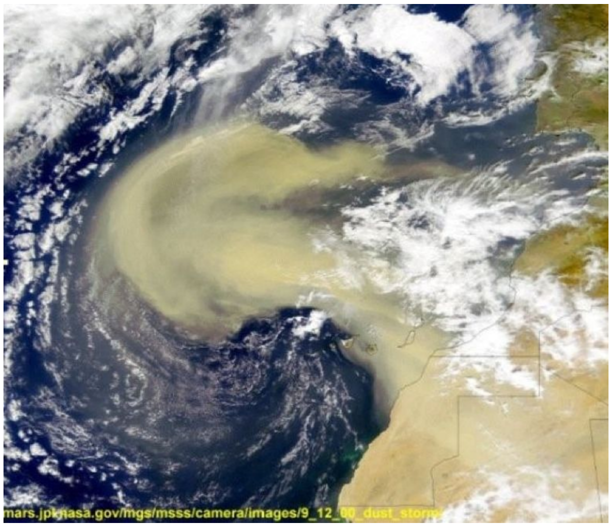


Figure 4.2: Satellite photo of the sand wind from Sahara desert over Canary Islands

(Re-printed from NASA website.)

(HSP) source with a trigger photon 0 (in Fig. 4.1 photons are indicated by black numbers on red circles). An EinsteinPodolskyRosen (EPR) source generates an entangled pair of photons 2 and 3 in the state $|\Psi^-\rangle_{23}$. Alice then performs a Bell-state measurement (BSM) on photons 1 and 2 projecting them onto two of the four Bell states ($|\Psi^-\rangle_{12}/|\Psi^+\rangle_{12}$) each with the same probability 25%. Then she sends the result via the classical channel to Bob. Photon 3 is sent via the free-space quantum channel to Bob, who applies a unitary transformation (identity operation or π phase shift) on photon 3 depending on the BSM result and thus turns its state $|\phi\rangle_3$ into a

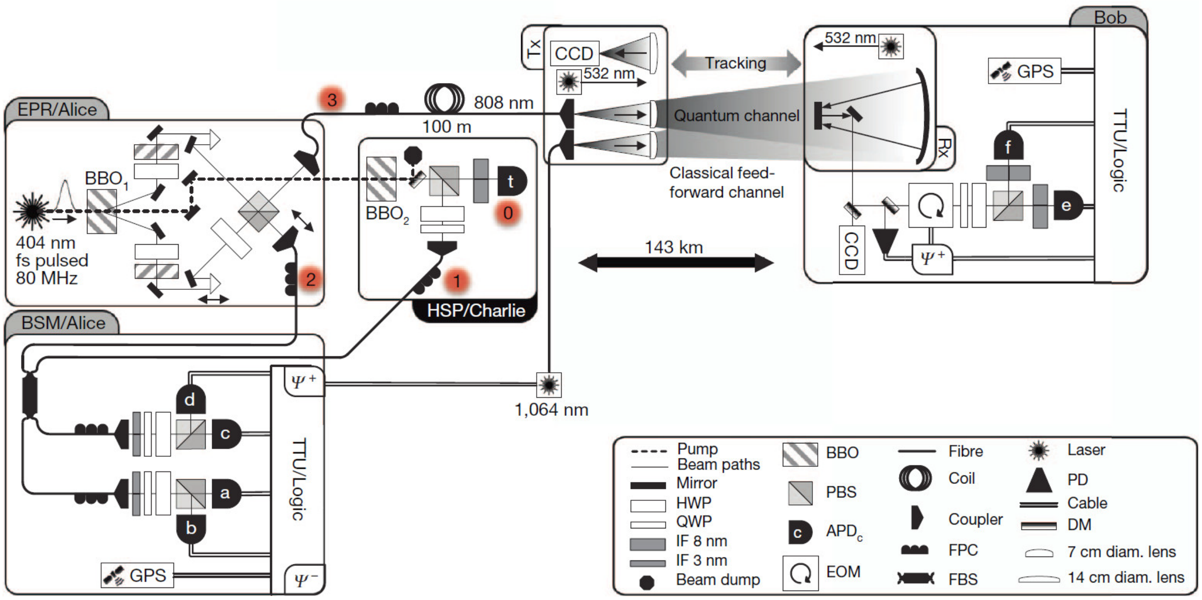


Figure 4.3: Detailed scheme of the teleportation setup

(*Re-printed from* [33].)

copy of the initial quantum state $|\phi\rangle_1$.

The experimental setup is shown in Fig. 4.3. A 808-nm laser located at Alice's location on La Palma iceland at the Jacobus Kapteyn Telescope of the Isaac Newton Group, was emitting femtosecond pulses with frequency of 80 MHz. Then, those pulses were up-converted to 404-nm pulses used for spontaneous parametric down conversion (SPDC) to generate two pairs of entangled photon in two nonlinear BBO crystals. One crystal was producing photons 2 and 3 in the state $|\Psi^-\rangle_{23}$. The second SPDC source was producing photons 0 and 1. Photon 0 was registered by an APD and served as a trigger, and the photon 1 for teleportation by Charlie, who randomly chooses polarization for it using half- and quarter-wave plates. For BSM, photons 1 and 2 were overlapped in a fiber beam splitter (FBS) and then their polarization was analyzed. Our BSM setup was able to identify two out of four Bell states, because of the linear optics only implemented [96]. While the BSM was performed on photons 1 and 2, the photon 3 was being sent to Bob over 143 km free space quantum channel.

Bob's apparatus were located on Tenerife island at the Optical Ground Station of the European Space Agency. Our experiment had two stages. At the first stage, only the cases of the state $|\Psi^-\rangle_{12}$ were considered. In these cases, the photon 3 sent to Bob, was already in the same state as photon 3, so identity operator had to be applied at Bob's location. To check the successful teleportation, a polarization analyzer was used. It consisted of a quarter and half-wave plates, polarization beam splitter and two Si-APDs.

At the second stage of the experiment, a real-time feed-forward operation was implemented. After Alice performed the BSM, she sent the result via classical channel to Bob. Then Bob applied a π phase shift or identity operator to photon 3 and obtains an initial state $|\phi\rangle_1$.

During the experiment, the quantum channel losses varied from 28.1 dB to 39.0 dB, that was mainly caused by fast temperature changes and strong wind. It resulted in significant challenges for the teleportation experiment. First, it was an extremely low signal-to-noise ratio. Second, long data collection time, also because of very low signal level. To overcome those problems several advanced techniques were used: a frequency-uncorrelated polarization-entangled photon pairs source [97–99], entanglement-assisted clock synchronization [93, 100, 101] and ultra-low-noise SPDs with large active area at Bob's side [77].

4.2 Numerical simulation of the teleportation experiment depending on DCR of SPDs

To estimate quantitatively the importance of ultra-low-noise SPDs on Bob's side in the teleportation experiment, Xiasong Ma from Vienna team performed a numerical simulation based on an analytical model shown in the Ref. [102].

The probability of successful teleportation is given as the product of a successful Bell state measurement in Alice, p_{BSM}, and the link efficiency from Alice to Bob η [102]. The corresponding probability to record an error due to noise at Alice location is $p_{\mathrm{BSM}} \cdot D \cdot \tau$, where D is DCR of Alice SPDs, and τ is the coincidence time window. Thus the signal-to-noise ratio (SNR) is given by

$$\mathrm{SNR} = \eta/(D\tau). \tag{4.2}$$

From this follows that reducing D can increase SNR. This is essential for Bob's measurement apparatus because of the low quantum signal after the optical free-space link. In Fig. 4.4 we show the teleportation visibility depending on the link attenuation for two different DCR of Bob's detectors. These simulations are based on following parameters of spontaneous parametric down conversion (SPDC) source: count rate of entangled photon source 90000 cps, count rate of non-entangled photon

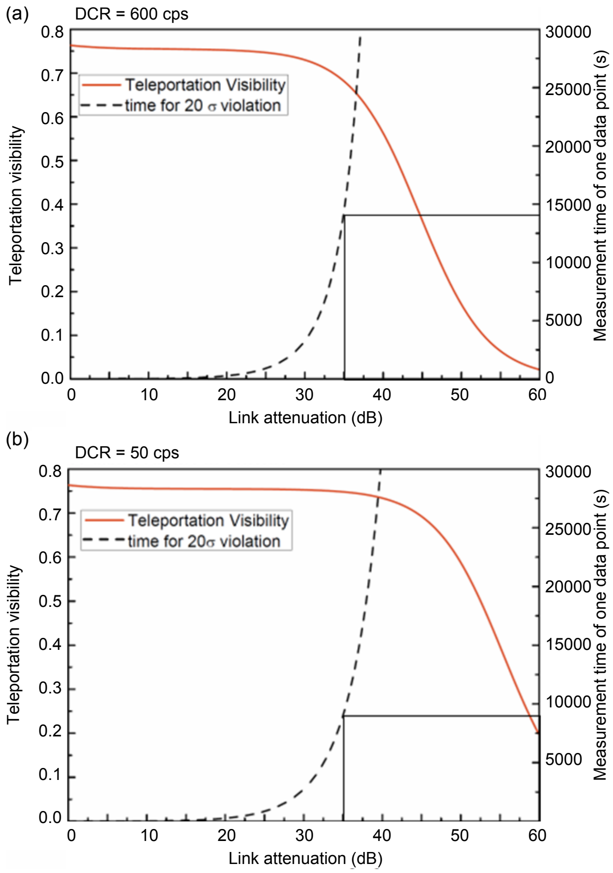


Figure 4.4: Simulation results for the experiment performance

a) with DCR of 600 cps previously, and b) DCR of 50 cps with our detector system. (*Re-printed from private communication with X. Ma*)

source 110000 cps, expected 4-fold count rate at 30 dB attenuation 0.07 cps, local entanglement visibility 91%, coincidence window 1 ns.

Figure 4.4 (a) shows expected visibility and data collection time with SPD with DCR of 600 cps. The teleportation seems feasible up to a link attenuation of around 35 dB with a measurement time of approximately 4 h per data point. Figure 4.4 (b) is for SPDs with DCR of 50 cps: the visibility clearly makes a difference at attenuation higher that 30 dB, which results in almost halved data collection time. In the simulation in Fig. 4.4, the detection rate stays the same for the illustrated point (35 dB). Note that the lower DCR reduces the measurement time, because the observable visibility will be higher.

4.3 Detectors for the experiment

Our SPDs used in the experiment had a low DCR of about 15–20 cps, and the big sensitive area of 0.5 mm [33, 77]. That allowed to reach a decent detection rate in the experiment, and therefore a manageable measurement time. A good weather condition on the day of the experiment (actual date) provided a clear atmosphere. However for an experiment planned and facilities booked months in advance, a weather conditions could prevent the experiment run. Frequent winds from Sahara desert over Atlantic carry sand and dust, and severely decrease transparency of atmosphere in the area of the experiment. Thus, the photon detection rate would drop and measurement time would increase enormously. See picture with an example of Sahara sand wind in the Fig. 4.2. Initially, the quantum teleportation experiment was planned on the summer 2011 and the facilities were booked. But because of a severe pollution the sand wind from Sahara desert the visibility of the free-space optical channel was so low that the whole experiment had to be postponed.

SPDs used in the experiment were replicas of in-lab-built SPDs described in the paper [77]. It was Si-APD based SPDs cooled down with 3 stage TEC (Fig. 4.5), with passive quenching circuit. For the experiment we built 3 SPDs, Fig. 4.5, two were used in the experiment, and one was a spare one. We conducted first DCR measurements. Complete characterization of SPDs was done in-situ at Tenerife.

Their parameters during the experiment were the following:

- DCR of 15 cps for each unit (one SPD was set at −65.5 °C and second one at −64.9 °C),
- efficiency of 50% (at 8 V above threshold, it was a trade of between higher efficiency at higher bias voltage and lower DCR at lower bias voltage),
- afterpulsing probability of 0.15%,
- saturation count rate of 400 kHz

Water chiller was running at +18 °C, comparator threshold was set at 85 mV for both SPDs.

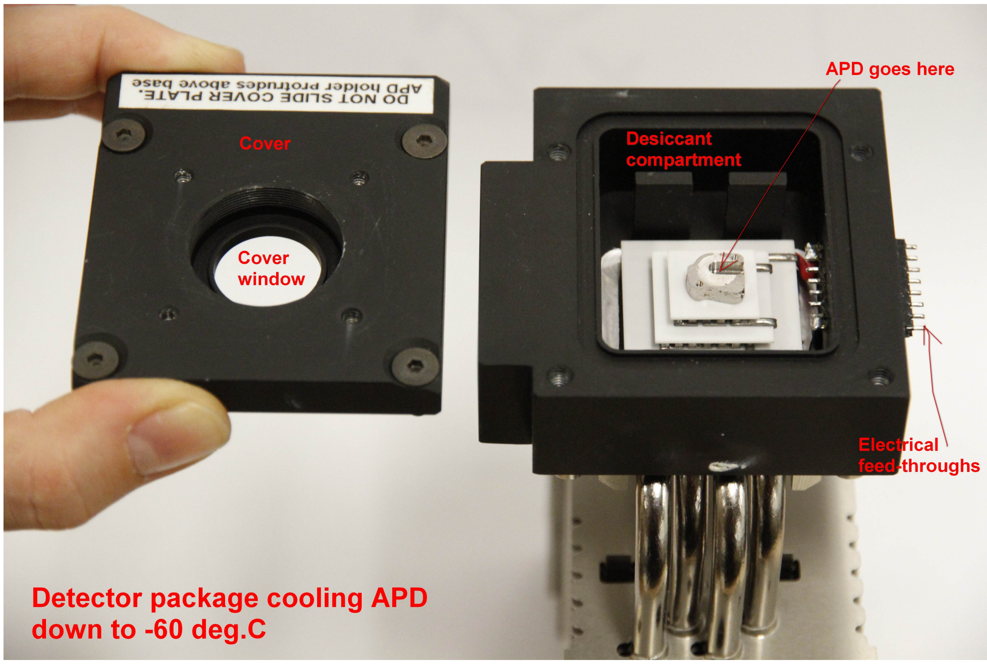

DO NOT SLIDE COVER PLATE.
APD holder protrudes above base
Cover
Cover window
APD goes here
Desiccant compartment
Electrical feed-throughs
Detector package cooling APD down to -60 deg.C

Figure 4.5: SPD, open view.

(photo © Vadim Makarov)

4.4 Results and conclusion

The detailed results of the experiment can be seen in [33].

For the first stage of the experiment tomographic measurements were performed during three nights, in total accumulating data during 6.5 h. The fidelity of the teleported states is defined as $f = \langle\phi_{ideal}|\,\rho\,|\phi_{ideal}\rangle$, where $\phi_{ideal} \in \{|H\rangle\,, |V\rangle\,, (|H\rangle + |V\rangle)/\sqrt{2}, (|H\rangle - i\,|V\rangle)/\sqrt{2}$, and $|\phi\rangle_1$ was approximately one of the four ideal states. The average fidelity was measured $f = 0.863 \pm 0.038$, that exceed the classical limit of $2/3$.

At the second stage of the experiment we implemented the feed-forward of the BSM results from Alice to Bob in real time over 143 km free-space channel. The input states were $|P\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|R\rangle = (|H\rangle + i\,|V\rangle)/\sqrt{2}$. Those states are chosen from different mutually unbiased bases to confirm the generality of the procedure. On Bob's side the arrived photon 3 state was analyzed in the eigenbasis of the input state ($|P\rangle\,/\,|M\rangle$ or $|R\rangle\,/\,|L\rangle$ for the input state $|P\rangle$ or $|R\rangle$), where $|M\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ and $|L\rangle = (|H\rangle - i\,|V\rangle)/\sqrt{2}$. The resulting fidelities for states $|P\rangle$ or $|R\rangle$ were 0.760 ± 0.050 and 0.800 ± 0.037, higher than classical limit of $2/3$.

The presented experiment clearly proves the feasibility of quantum teleportation through a long-distance free-space channel. As the experiment successfully demonstrated teleportation through a high loss channel, it points to a feasibility of a ground - low-Earth-orbit (LEO) satellite teleportation. The attenuation of the used optical link is higher than an attenuation of the ground-to-LEO satellite link, because the path in Earth atmosphere that presents most losses, is shorter than distance between La Palma and Tenerife.

Chapter 5

Improved SPDs afterpulsing analysis method

For afterpulses analysis we developed a new calculation method, adapted especially for long-time afterpulses, which appear in APDs at low temperatures and feature high probabilities and longer lifetimes of traps. In contradiction to previously described methods [103–106], we analyze time intervals of APD's outcoming pulses not only between two subsequent pulses, but all mutual time intervals during 1 s (a chosen time, much longer then the longest afterpulse lifetime). Our way of calculation allows to determine afterpulses with lifetimes longer than time between neighboring pulses. Furthermore, it reveals a 'true' dark count level excluding afterpulses. Our method of afterpulse analysis can be implemented for other APDs as well.

A common way to calculate afterpulsing probability is to analyze time intervals between neighboring counts [103–106]. Then the statistical distribution of time intervals is being computed and histogrammed. This method works reasonable well for short afterpulsing times and large quantities of detection data. However the method fails, when these conditions are not met. We give an example of this afterpulsing analysis from our Si APD at −100 °C. Due to very low DCR at this low temperature the data acquisition took 5.5 days of continuous recording. Fig. 5.1 illustrates the method of analysis and Fig. 5.2 presents two resulting histograms (a, b), obtained by distribution of the analyzed time intervals on equally sized bins. The first histogram was built using smaller bins of 228 ns and provides sufficient temporal resolution for the peak of the histogram representing afterpulses to appear. However, small bins does not filter out statistical fluctuations in the tail of the histogram on the right representing dark counts. The second histogram in the Fig. 5.2 was built using larger

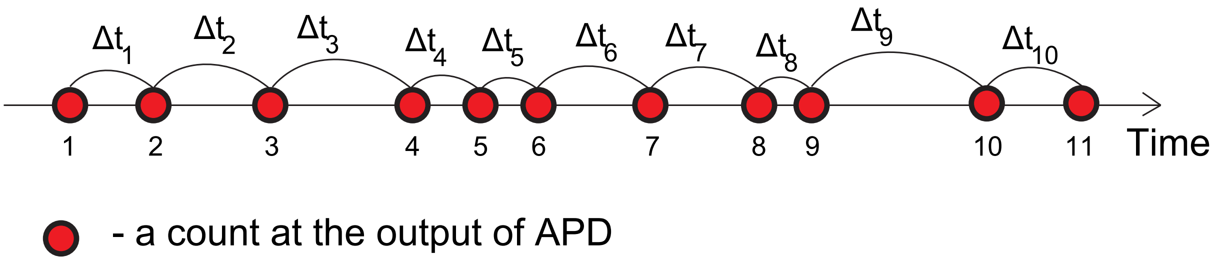


Figure 5.1: Scheme for common afterpulsing analysis
The method considers only time intervals between adjacent counts.

bins of 0.03 s, and the tail of the histogram is now represented well, demonstrating exponential decay caused by Poisson distribution of dark counts. However, 0.03 s is larger than the afterpulsing time, and the peak of the histogram is no longer clearly visible. From both these histograms the detector dead-time can be determined to be about 0.5 µs.

We developed an improved afterpulsing processing with a dramatic advantage, that allows to calculate correctly long-time afterpulses. The main features of our analysis are including in analysis all time intervals between counts during a certain time longer than the longest trap life time, and use of histogram with exponentially increasing bin size.

To calculate afterpulsing we analyze time intervals between a detection count (#1 in Fig. 5.3(a)) and the all subsequent counts (##2..7) during a certain time, up to l =1 s in the presented example. The processing length l should be chosen to exceed the longest possible afterpulsing time. The resulting time intervals $\Delta t_{1-1}..\Delta t_{1-6}$ are histogrammed. The procedure is then repeated starting from the next count #2 (with resulting time differences $\Delta t_{2-1}..\Delta t_{2-7}$), and then starting from the next count #3 and so on until the end of the data is reached.

The resulting histogram shown in Fig. 5.3 (b) is built on 128 bins, exponentially increasing by a factor of 1.2, starting from 78.125 ps. This allows to have higher resolution of the the histogram for short times, and lower resolution for long times. For this histogram time intervals during 10 second after each count were analyzed. This histogram features an almost noiseless tail towards long time scales and quite smooth curve of the peak for short time scales close to zero. From the histogram we can estimate the DCR, afterpulsing probability, APD's dead time and recharge time. The dead time starts after an avalanche (at time=0), and lasts until the next counts appear (about 0.5 µs). The recharge time is determined as a time after the avalanche quenched that is necessary for restoring voltage across the diode. It starts

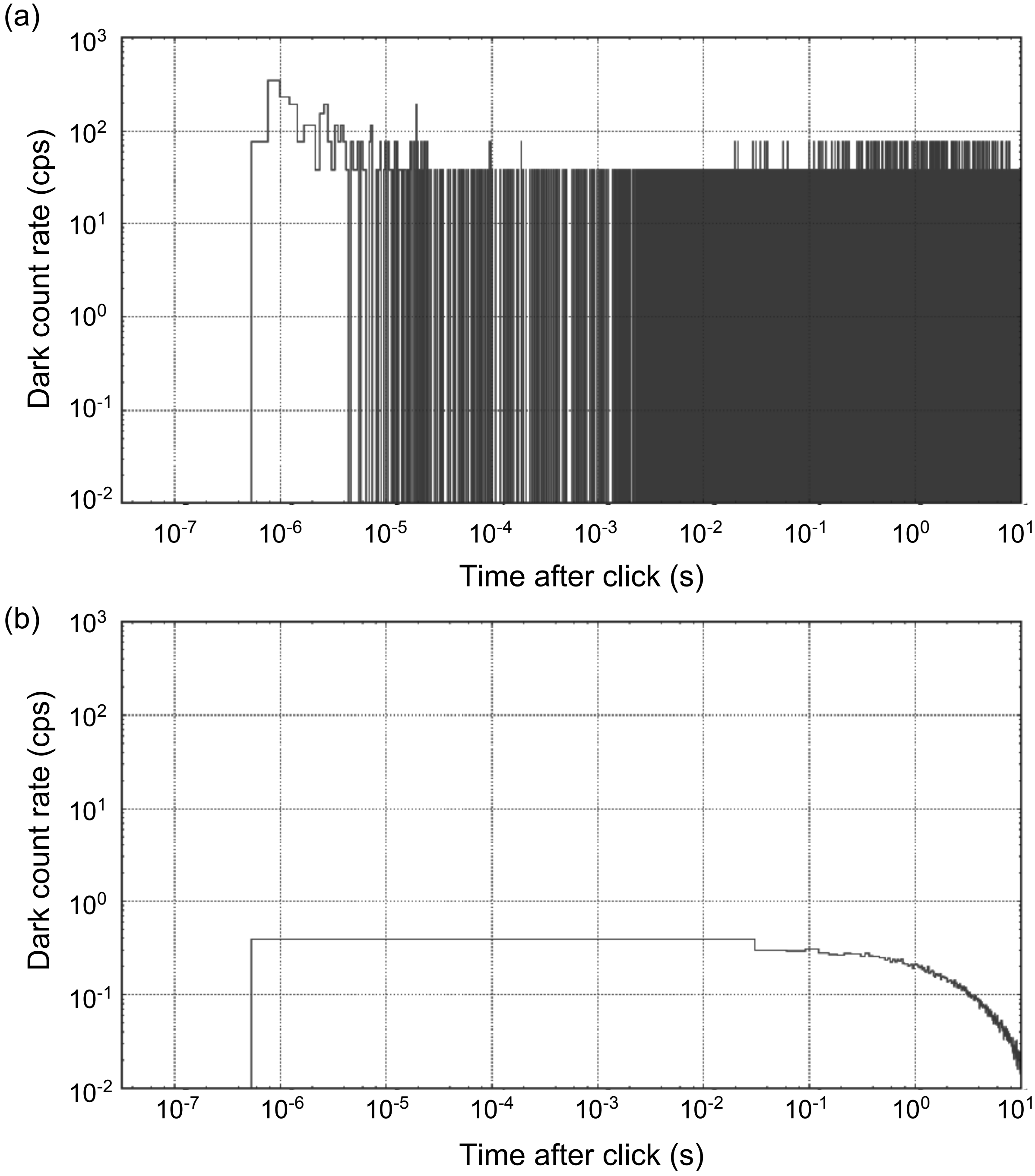


Figure 5.2: Resulting histograms for common way of afterpulsing analysis Histograms built with 228 ns bins (a) and 0.03 s bins (b). The histogram (a) has a higher resolution which makes afterpulsing peak visible, but also makes the "tail" of the histogram noisy. Histogram (b) has a lower resolution, that does not show the afterpulsing peak, but shows the declining "tail" resulting from the Poisson distribution of dark counts. Data size is 114109 counts. The dark counts were obtained from C30902SH APD at −100 °C, at 14 V over breakdown.

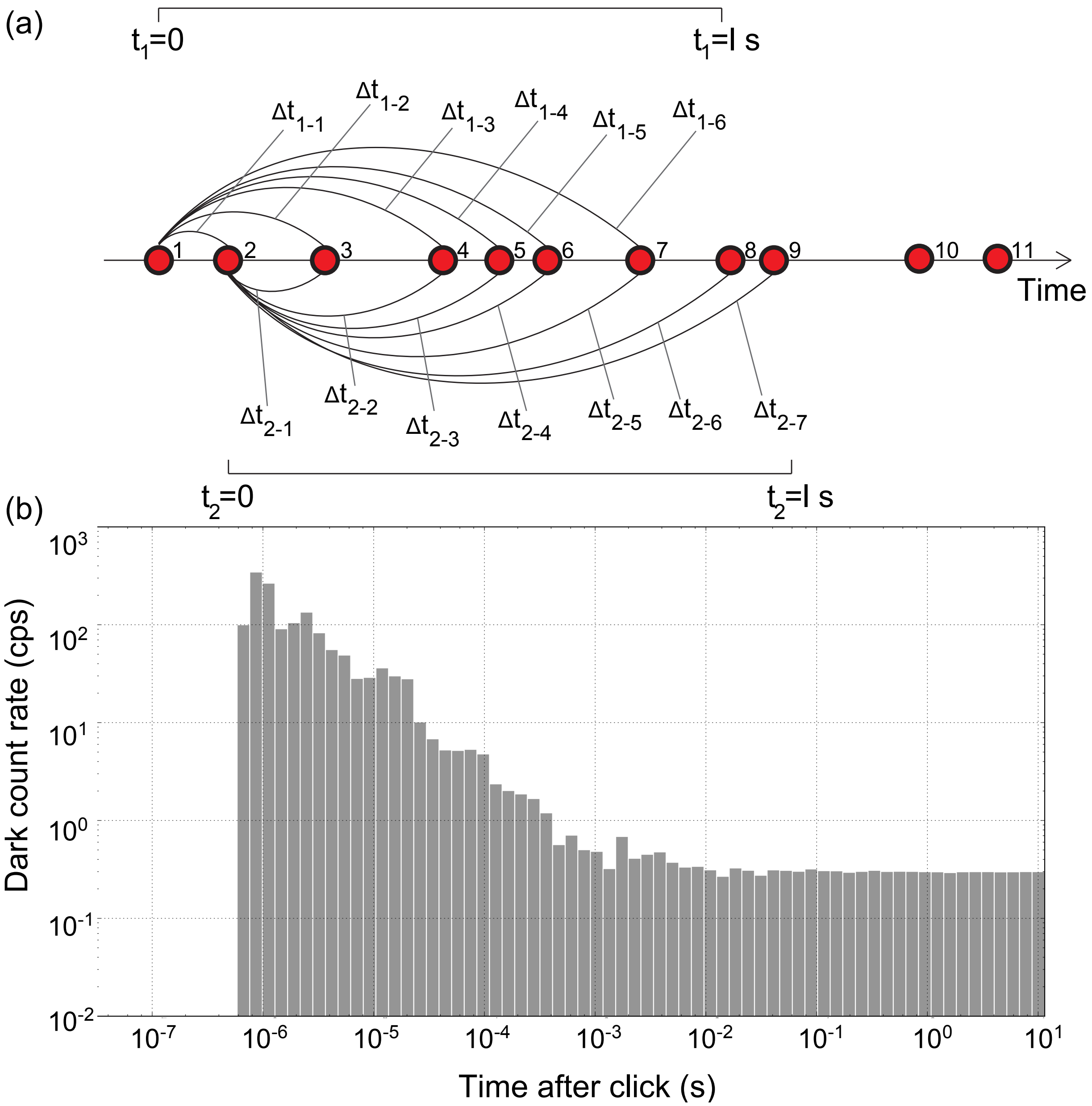


Figure 5.3: Improved long-time afterpulsing analysis

Analysis scheme (a) and resulting histogram (b) with exponentially increasing bins. This histogram uses the same data as Fig. 5.2 (114109 counts, C30902SH APD at −100 °C, at 14 V overvoltage.) The afterpulsing peak of the histogram has the higher resolution which allows to see its features, e.g. step-wise structure in this example. The "tail" of the histogram does not decline here because in this analysis it does not reflect the Poisson distribution of the dark counts but shows the averaged level of dark counts.

from the end of the dead time until about the peak value of the count rate (about 0.3 μs). The plot levels off on the right to the DCR. The afterpulsing probability is calculated as the area of the histogram above DCR level.

Life time constants of trapped carriers can be found by fitting the decaying slope of the peak [107] a sum of exponents:

$$P(t) = D + A_1 \cdot e^{-t/\tau_1} + A_2 \cdot e^{-t/\tau_2} + ..., \tag{5.1}$$

where $P(t)$ is a carrier emission probability, D is DCR due to thermally generated carriers, A_1, A_2, ... are amplitudes of the different exponential components. Our software implemented fitting for up to four exponential components. Only lifetimes longer than the detector dead time (about 0.8 μs) for our passive quenching circuit can be determined; also, this fitting procedure applicable only when the secondary afterpulses (afterpulses caused by afterpulses) are negligible. For Si-SPADs that we used our method for, afterpulses are less than 1%, then second order afterpulses are insignificant.

We implemented a Python code for analyzing afterpulsing and calculate the trap's life times, see Appendix A.

Summarizing, we have developed a new advanced method of analysis for long time afterpulses, allowing calculating afterpulsing probability including secondary afterpulses and higher orders of afterpulses. Our algorithm was developed for dark count analysis, but with minor adjustments it was implemented for analysis of data collected from an APD illuminated with weak periodic light pulses [108].

Chapter 6

Building a super low noise SPD

6.1 Motivation

A necessity of a secure communications, that will be able to withstand hacking attacks from quantum computers, leads to fast development of quantum cryptography [7, 11, 109–112]. Quantum key distribution (QKD) is now the most commercialized area of quantum communications. There are several companies (e.g., ID Quantique (Switzerland)) on the market selling QKD systems, which are ready for use by customers with high-demand of security, e.g., banking, medicine or government and military. A very important direction for the development of QKD is its expansion to global scale and the creation of world-wide QKD network [31, 56, 113–115]. A lot of work has already been done to reach the longest distances over the ground for free-space quantum communications, e.g., [33, 93, 116, 117].

The main challenge of the long-distance free-space quantum communication is the high photon losses in the channel, caused mostly by absorption, diffraction and turbulence in the air [56, 118]. To minimize absorption losses, while still using very well performing Silicon simple photon detectors, a wavelength around a low-loss window at around 800 nm is often chosen. Diffraction losses can be minimized only by increasing sizes of sending and receiving telescopes, however the atmospheric turbulence puts a limit on this improvement. Turbulence losses are unpredictable and depend on weather conditions. Other photon losses happen in sending and receiving apparatus, and single-photon detectors are essential part of it. The suitable detectors for long-distance free-space quantum communications must demonstrate high detection efficiency, low detection timing jitter, low dark count rate (DCR) and low afterpulsing probability. E.g., targeted parameters for a potential SPDs for a quantum satellite were the following: DCR below 200 cps, quantum detection efficiency at least 45%, timing jitter about 250 ps, afterpulsing below 1% for 500 ns. From a number of potential candidates, silicon avalanche photodiodes (APDs) and photomultiplier tubes (PMTs) are the most suitable. However PMTs have lower detection efficiency at the required 800 nm, whereas APDs have a long history of use in quantum communications thanks to their advantages: larger photosensitive area of 500 μm, low DCR (typical 100 cps), high detection efficiency, compact package, low timing-jitter of 0.5 ns FWHM, and low cost. Low DCR and high detection efficiency are crucial for performance of quantum free-space ground-to-ground communications. Cooling of APDs can be used to decrease DCR [77].

While cooling causes increase of afterpulsing, it can be a useful tool for implementing APD-based SPDs for satellite-based quantum communications [119, 120].

We have built and tested a Si-APD detector, demonstrating very good parameters, suitable for long-distance free-space quantum communication experiments. We can compare performance of our new detector with the most advanced commercially available models, e.g., ID Quantique ID100VIS and ID120VIS [121, 122]. ID100VIS demonstrates outstanding performance, and the similar level of DCR as our home-built detector, however it has 100 times smaller sensitive area, and lower detection efficiency (maximum 35% at 500 nm). ID120VIS has the same size of sensitive area as our SPD, and demonstrates a high detection efficiency, but its DCR is 200 cps, through DCR of our SPD is a few cps. We built our SPD using of-the-shelf APD (Excelitas, C30902SH) with 500 μm diameter photosensitive area. Our new detector has a compact package (see Fig. 6.1 a and b), and is able to cool down an APD down to −100 °C, utilizing a 5-stage thermoelectric cooler. Due to that low cooling our detector demonstrated very low DCR, down to few cps. The detector package was vacuumed, to improve thermal insulation and prevent condensation. We measured dark count rate, photon detection efficiency, jitter and afterpulsing as functions of temperature and APD bias voltage.

For afterpulses analysis we developed a new calculation method, elaborated especially for long time afterpulses, which appear in APDs at low temperatures and feature high probabilities and longer lifetimes of traps. It represented in Chapter 5.

6.2 Detectors design

6.2.1 Mechanical and thermal design

Our present detector model is an improved version of the previous home-built SPD [77], which was able to cool down to around −65 to −80 °C, and demonstrated DCR of about 20 cps, which made it possible to use them in a long-distance free-space experiment [33]. In our present work we attempted to create an APD based SPD able to cool down below −100 °C in a relatively compact and low cost package, and investigate behavior of APDs at such low temperatures.

The photo of the detector is represented in the Fig. 6.1. Aluminum box is closed tightly with a lid sealed with a rubber O-ring, and a vacuum lubricant is used for better insulation. A five-stage TEC (Osterm PE5-195-1420-2040) was used to cool down an APD placed in a holder on the top of TEC. The holder is made of Kovar to prevent destruction caused by difference in thermal expansion coefficients between TEC ceramics and the holder material. To achieve temperatures as low as about −100 °C the package is under vacuum to prevent convection between cold and hot side of the TEC stages and with the outside walls. The vacuum also prevents condensation. A vacuum turbo pump was constantly active during the SPD operation, providing a vacuum level of 10^{-5} Torr. We noticed that 10^{-3} Torr already reduces convection sufficient to reach the thermal performance at maximum vaccum level within 1 °C. The temperature of the APD is measured by a platinum sensor RTD-100, epoxied in the holder base, and connected via 4-wire scheme to eliminate errors caused by wire lengths differences. All electrical connections to the cold plate were soldered via 50 μm diameter annealed Pt wires, to reduce heat conduction. The hot side of the TEC was cooled down with +14 °C water, provided by ThermoTek T255P closed-loop chiller. Temperature controller for the TEC was custom made in our lab, but instruments with similar parameters are available commercially. At the lowest achieved temperature of −104 °C the TEC, at the ambient temperature of about +20 °C, was running at its highest settings of 13 V and 3 A, consuming 39 W of electrical power.

6.2.2 Electronics

Our new electronics design is based on the previous version, used in Ref. [77]. In our new electronics schematic we attempted to minimize timing jitter, used a faster

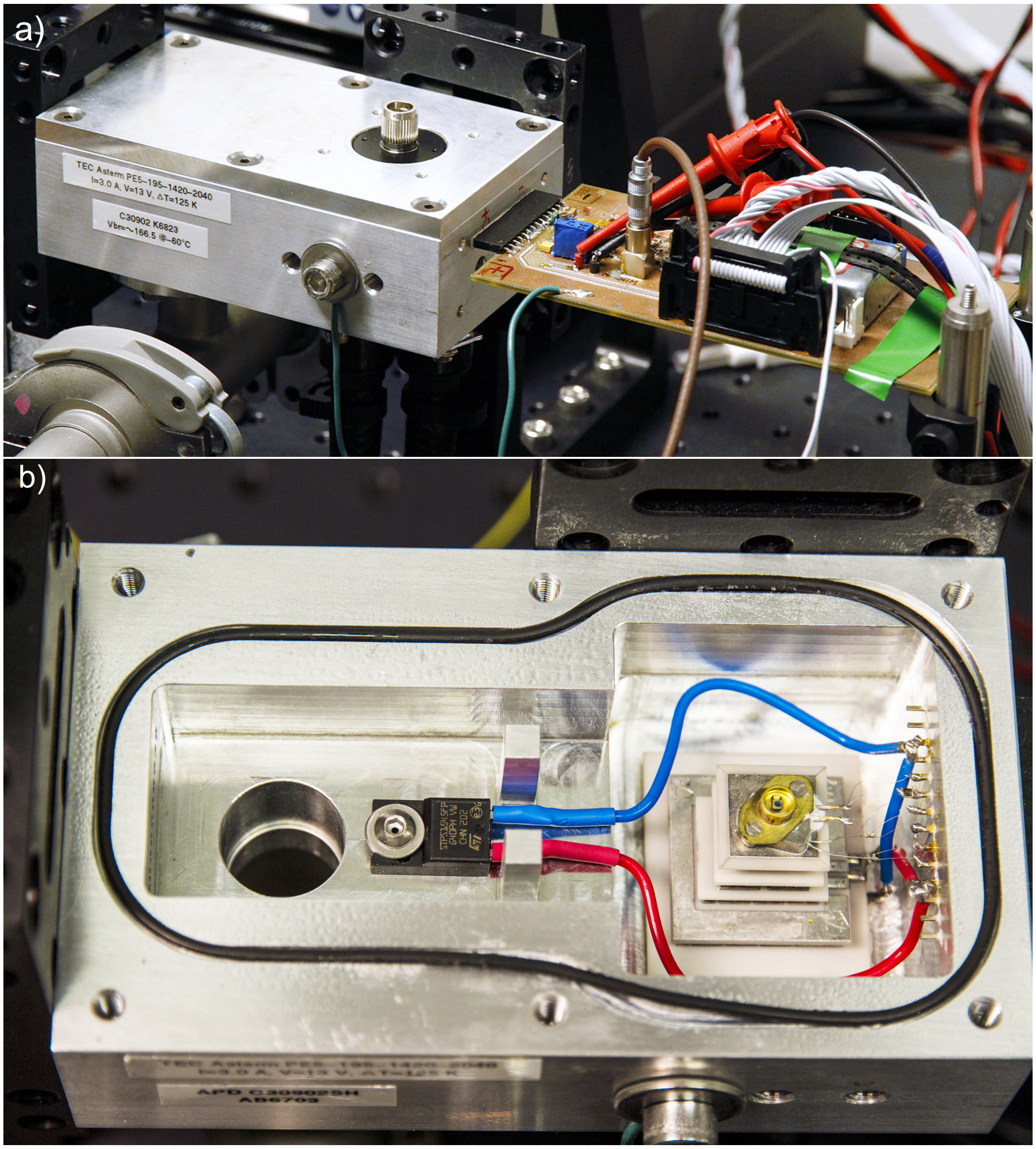
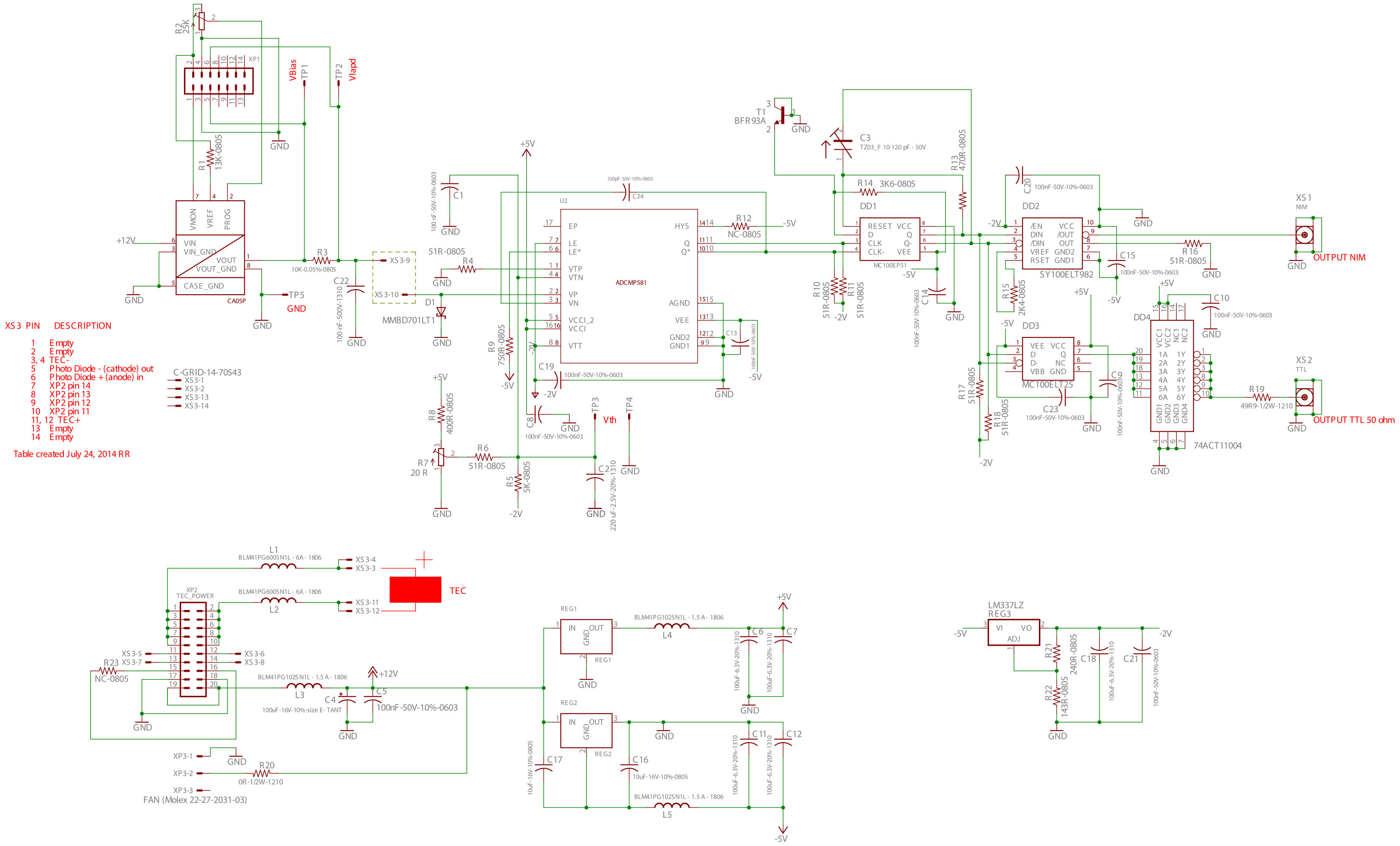


Figure 6.1: Photo of the detector.
a) The main metal container houses the detector which is under vacuum. A metal shield normally covers the electronic board, but was removed for the photo. b) The detector package is open. An APD is mounted in the holder on the top of the TEC. A thermal paste is applied to improve cooling of the APD. The APD and thermal sensor are connected by Platinum wires to the fee-through pins. The quench resistor is soldered directly to the fee-through pin. A Schottky diode is inserted in the TEC line to prevent a damage from an occasional switched polarity.

comparator ADCMP581 with variable threshold voltage. Also, in the new scheme we located TEC controller and signal detection and processing circuits on different boards in order to avoid electrical cross-talk interference, that we observed sometimes with our previous scheme. The electronics schematic is shown in the Figure 7.4 and electronics board shown in the Figure 6.3. As in the previous scheme, we implemented a simple but reliable passive quenching scheme with quenching resistance of 403 kΩ. It's core part is similar to one described in Ref. [74] as a passive quenching circuit with current-mode output. Its maximum detection rate of 0.2–0.4 Mcps is lower compared to active quenching circuits, but sufficient for applications with low signal rate, e.g., long distance free-space quantum communications that require very low dark counts level. The long dead time (>1 µs) is not a problem for the low-signal-rate application, and furthermore, it suppresses afterpulses. All measurement results presented in this paper were done with the optimum threshold setting for our comparator at 150 mV. The detection scheme has transistor-transistor logic (TTL) and nuclear instrumental mode (NIM) outputs.

A $0 - 500\,\mathrm{V}$ high voltage bias supply (EMCO CA05P) was used in our scheme. We implemented a possibility of remote diagnostic and control of the detector parameters, for future use of the SPD in various experiments.

In the Fig. 6.1 a metal shield is removed to show the electronic board. However the detector cannot be used without a proper shielding because of interference with outer sources, e.g., mobile phones.



XS3 PIN	DESCRIPTION
1	Empty
2	Empty
3, 4	TEC-
5	Photo Diode - (cathode) out
6	Photo Diode + (anode) in
7	XP2 pin 14
8	XP2 pin 13
9	XP2 pin 12
10	XP2 pin 11
11, 12	TEC+
13	Empty
14	Empty

Table created July 24, 2014 RR

Figure 6.2: Detector electronics scheme

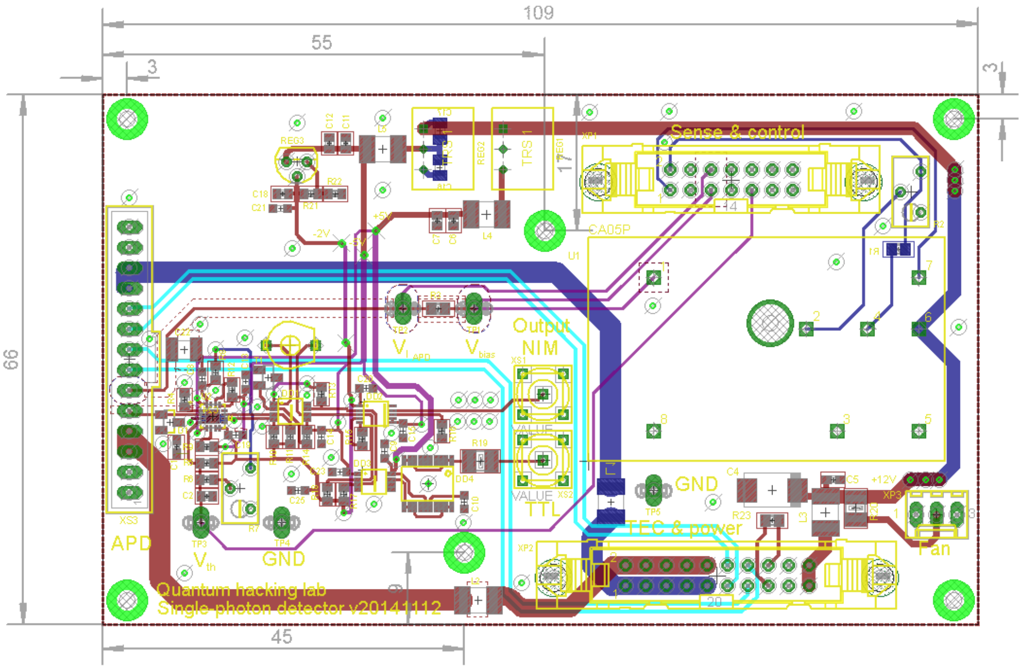


Figure 6.3: Detector electronics board layout

6.3 SPD characterization procedure

For characterization of our detector we used a scheme shown in the Figure 6.4. First, the APD's breakdown voltage was determined, then DCR was measured with a detector lid on and the laser off. Then, the detection jitter, detection efficiency and afterpulsing probability were measured.

Breakdown voltage was determined by extrapolation method [123]. Bias voltage of an APD was initially set to approximately $20 - 30\,\mathrm{V}$ above breakdown, and gradually decreased. Then corresponding avalanche amplitudes were recorded for each bias voltage. About 10 points were measured until the bias voltage was very close to the breakdown. The results were plotted on a chart of avalanche amplitude vs. bias voltage. Then, the breakdown voltage was determined as an intersection point of an extrapolated linear part of the resulting function with the bias voltage axes. This method allows to determine breakdown voltage with better than $\pm 0.5\,\mathrm{V}$ precision.

Dark count rate. False counts produced by an APD in absence of light are called dark counts and caused by intrinsic processes in APD [74, 91, 124]. The largest contribution for dark counts is caused by thermal excitation, when a thermally excited carrier triggers an avalanche. Those dark counts decrease exponentially with temperature [77], about 50% every 8 degrees. Another effect contributing to the

DCR are tunneling and afterpulsing [74, 91, 124]. Another a minor contribution can come from blackbody radiation, when photons from the detector package are getting detected.

In order to ensure complete blocking of surrounding photons during the DCR measurements, our detector was kept with its lid on, and the room lights were turned off. The photon counts were averaged over 100 s using a counter (Stanford Research Systems SR620) to minimize uncertainty due to counting statistics.

We estimated the expected contribution to the DCR caused by blackbody radiation from the detector lid located about 10 mm from APD's sensitive area and kept at room temperature of 293 K. The thermal energy radiated by a blackbody radiator per second per unit area is given by the Stefan-Boltzmann Law:

$$\frac{P}{A} = \sigma T^4 [j/m^2 s], \tag{6.1}$$

where P is the radiated power, A is radiating area and σ is Stefan-Boltzmann constant and equals to $5.67 \cdot 10^{-8}\ Wm^{-2}K^{-4}$. The spectral range of our APD is 400..900 nm and the area of the lid contributing into the blackbody radiation is $A = \pi d^2/4 = 19.6 \cdot 10^{-8}\,\mathrm{m}^2$. Distribution of the radiated power over wavelength range is given by Planck radiation formula:

$$\langle E \rangle = \frac{h\nu}{e^{h\nu/kT} - 1} \tag{6.2}$$

Finding the power radiated within a given wavelength range requires integration over the range. Using an online calculator utilizing the numerical approximation [125], the power radiated in the 400..900 nm interval equals to $P = 0.377 \cdot 10^{-23}$ W. To estimate the upper bound for the number of the radiated photons, we assume that all emitted photons are at 900 nm, then $h\nu = 1.38eV = 1.602 \cdot 10^{-19} Ws$. Then, number of photons $N_{ph} = P/h\nu = 0.377 \cdot 10^{-23} W/1.602 \cdot 10^{-19} Ws = 0.235 \cdot 10^{-4}/s = 0.085/hour$. Thus, the area of the lid of the same size as APD's photosensitive area contributes negligibly, less than 1 photon per hour.

Detection efficiency was measured using a 808 nm pulsed laser (Figure 6.4) pulsing at the repetition frequency of 30 kHz, then the laser pulses were attenuated down to a well characterized optical power of 0.0139 pW, which corresponds to 56500 photons per second, using neutral density filters and digital attenuators calibrated at 808 nm. Detection efficiency was calculated as a ratio of detected N_{det} to expected N_{sent} photons:

$$\eta = \frac{N_{\mathrm{det}} - \mathrm{DCR}}{N_{\mathrm{sent}}}, \tag{6.3}$$

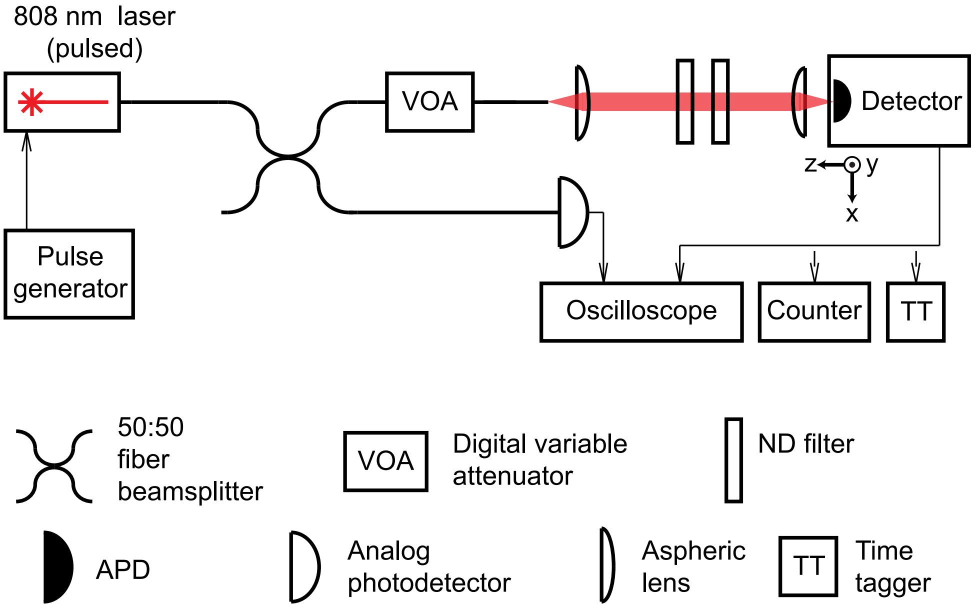


Figure 6.4: Characterization scheme
For DCR and detection efficiency measurements the output of the SPD is connected to the counter. For afterpulsing analysis the SPD output is connected to a time stamp unit (time tagger (TT)). For breakdown voltage and timing jitter measurements the SPD is connected to the oscilloscope. Two axis translation stage allows to scan photosensitive area of the SPD.

where N_{sent} is determined as

$$N_{\text{sent}} = \frac{P\lambda}{hc}, \tag{6.4}$$

where P is power of the laser measured by a power meter before calibrated attenuators and calculated to the detector point, λ is wavelength, h is Planck's constant, and c is the speed of light. Measurement error of this type of measurement is significant [77], and estimated to be ±10%.

Afterpulsing probability was calculated from recorded 10^6 dark counts using TT, with resolution 128 ps. Then the obtained data were processed according to our method described in Chapter 5. The longest necessary data acquisition time was 5.5 days at $-100\,^{\circ}$C.

Detection timing jitter was measured using an oscilloscope (4 GHz bandwidth LeCroy 640Zi) in a histogram mode. Bright laser pulses from 808 nm laser (see Fig. 6.4) were divided into two arms; one connected through a linear photodetector to the oscilloscope and the second part of the beam attenuated below single photon level and focused to 25 µm spot at the SPD photosensitive area. The APD's avalanche signals were connected to another oscilloscope's input. Then we built a histogram of time delays between the laser pulses and the SPD output over 10^6 samples, and determine timing jitter of the SPD as a full width at half maximum (FWHM) of histogram. An example of the resulting histograms is shown in insets in the Fig. 6.6.

Using two axis translation stage we tested dependance of timing jitter on the position of the focused beam at the APD's sensitive area.

6.4 Results

A sample APD C30902SH (Excelitas) was cooled down and fully characterized at several temperatures over the range of −100 °C to 0 °C range, biased at 14 V above its breakdown voltage. DCR was measured at 7, 14, 28 and 40 V above breakdown voltage in temperature range from −104 to −30 °C. The timing jitter of APD was measured at −60 to −30 °C and at several bias voltages.

The breakdown voltage [Fig. 6.5(a)] increases with temperature about linearly with a coefficient 0.8 $\mathrm{V}^\circ\mathrm{C}^{-1}$. This is a typical behavior of Si APDs [126], which as we show here extends down to −104 °C.

The DCR as a function of temperature is shown in Fig. 6.5(b). The lowest achieved DCR of 0.3 ± 0.05 counts per second (cps) was observed for the APD biased 14 V and cooled down to −100 °C. There was a discrepancy between DCR measurements done at different times. The four curves in Fig. 6.5(b) with dots were measured at one time, and the curve with diamonds for 14 V over breakdown voltage, was measured several months later during collecting data for afterpulsing analysis. Down to −70 °C the curves match perfectly, but then one curve levels off whereas the other continues linearly. It could be due to a poor black-out. Another possible explanation could be a "memory effect": after a strong illumination an APD has a higher DCR for a long time up to 24 hours [127, 128].

To verify experimentally the contribution of black body radiation to our DCR measurement, we performed DCR measurement with the detector lid cooled down below zero, and compared it with measurement when the lid was at room temperature. No notable change in DCR was registered.

Detection efficiency varies in the range 48 to 53 % (Fig. 6.5(c), decreasing slightly at higher temperatures, likely because of higher DCR.

We measured the detection timing jitter of C30902SH depending on its bias voltage, temperature, comparator level and position of the beam at the photosensitive area.

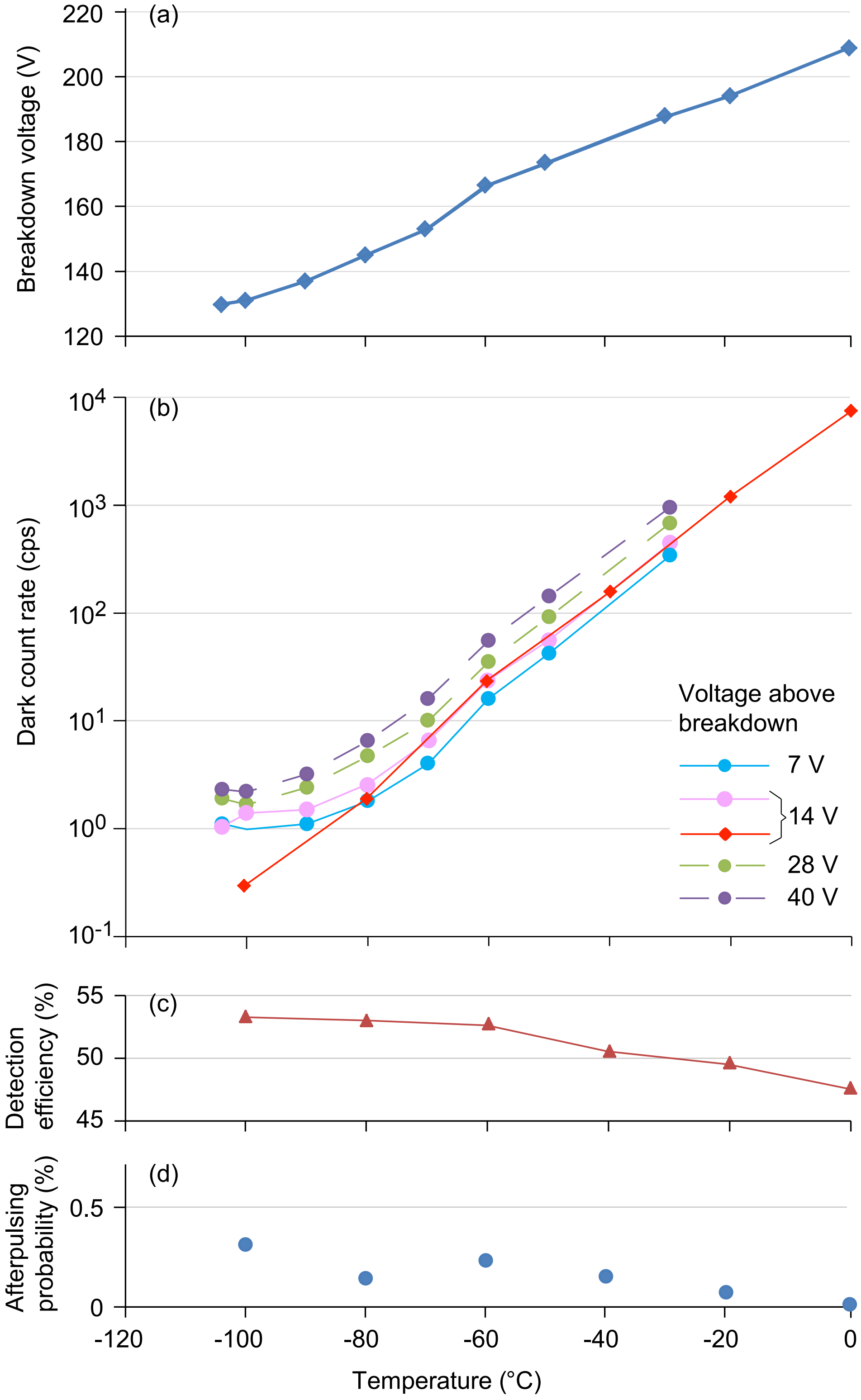


Figure 6.5: Detector characteristics
(a) APD breakdown voltage, (b) DCR, (c) detection efficiency, (d) afterpulsing probability of C30902SH. The latter two were measured at 14 V over breakdown voltage.

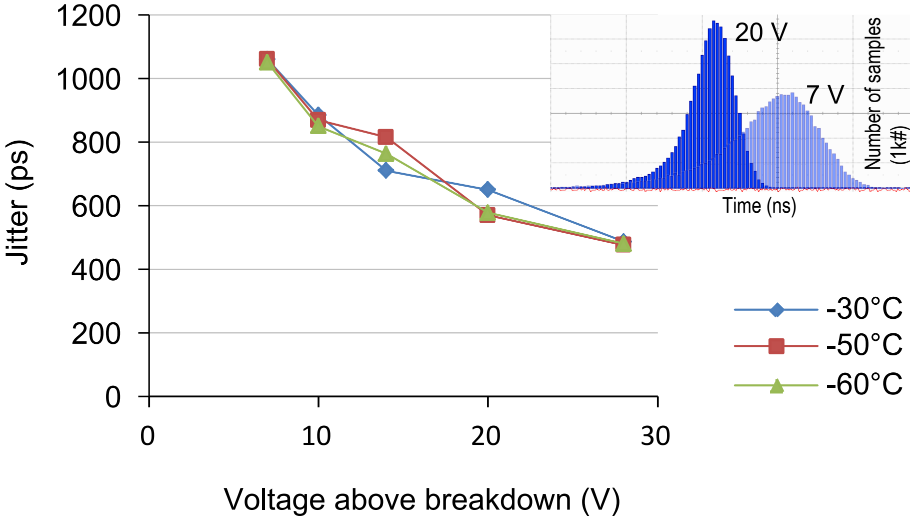


Figure 6.6: Detection timing jitter

Detection timing jitter as a function of bias voltage was measured for C30902SH at three different temperatures: −30, −50, −60 °C. As applied voltage increases, the jitter decreases, see an example of two histograms in the **inset**, measured on 10^5 samples at the following conditions: −50 °C, comparator threshold set at 100 mV, bias voltage 7 and 20 V above breakdown. The timing jitter values were measured at FWHM (full width at half-maximum) is 1220 and 640 ps.

Timing jitter decreases with rise of APD's bias voltage in the same way for all three measured temperatures, see Fig. 6.6. This happens due to increase of avalanche propagation speed [71–74, 123, 129, 130]. Examples of jitter distribution at two different bias voltages are shown in inset in Fig. 6.6.

Also we have checked timing jitter dependence on position of an incident light at the sensitive area of the APD. As expected [124, 131], the time of an avalanche propagation in the detector area depends on the position of the initial seed. The measurement was done at −50 °C, at five different bias voltages, same as in Fig. 6.6. The beam was focused to the spot of 25 μm in diameter. The results demonstrate notably lower jitter at the center with up to 250 ps difference comparing to the edge's measurements. Distance between center and the edge was 25 μm. The data represented in Fig. 6.6 were measured with the beam focused at the center of APD's sensitive area.

Decrease of the comparator threshold voltage in the avalanche registration scheme leads to a decrease of timing jitter. Stronger avalanches progress faster and have higher coefficient for their rising slopes, therefore they cross the comparator's threshold earlier, and will be registered first. Smaller avalanches have less steep rising slop and will hit the comparator threshold level with some delay comparing to big avalanches. To minimize this time delay, it is beneficial to lower the comparator threshold voltage. However, the lowest practical limit for this comparator level by line noises and cross talks was 23 mV.

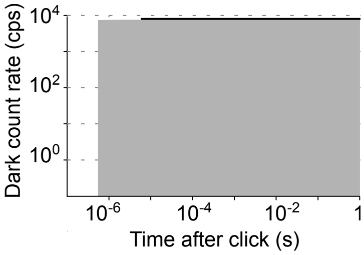
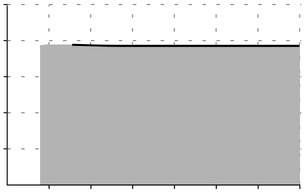
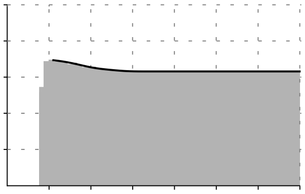
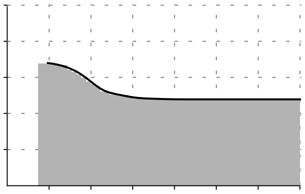
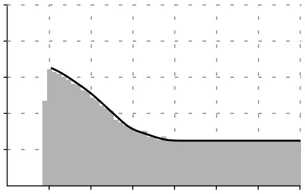
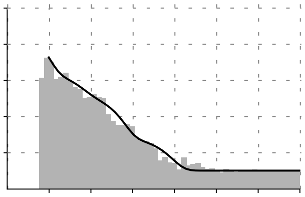
We calculated afterpulsing probability for C30902SH APD using our method described in the previous chapter. The resulting temperature dependence is shown in Fig. 6.5(d). Afterpulsing notably increases with cooling, because the life time of carrier traps increases, but does not exceed 1% at the lowest tested temperature of −100 °C.

Results of our attempted calculation of trap lifetimes are presented in Table 6.1. The decay slope at −20 °C was approximated with one exponent, at −40 and −60 °C with three exponents, at −80 and −100 °C with four exponents. The estimated trap lifetimes are between 1.37 μs and 482 μs. The fitting starts from the bin next after the maximum bin. Using the fitting with a sum of exponents, we reach a good fitting for curves from −20 °C to −80 °C, whereas for −100 °C, where we used a sum of five exponents, fitting is not so perfect, but possibly it could do better with more exponents. The data at −100 °C is also somewhat noisy, owing to the very low DCR and limited time of measurement (only 5.5 days).

Unfortunately we only had time to fully characterize our detector with only one sample of Si APD (Excelitas C30902SH). Another sample of the Excelitas, C30902SH was tested for DCR at temperatures down to −90 °C and demonstrated the similar level of DCR (0.58 cps at −91 °C).

We remark that the methodology introduced in this Article was also used to characterize many more APD samples exposed to space radiation, as described in the Chapter 8. That testing included multiple samples of three different Si-APD models: Excelitas C30921SH and SLiK, and Laser Components SAP500S2. The afterpulse characterization methodology has also been further refined in Ref. [108], periodic weak laser pulses were applied to the APD at repetition rate $1/l$. This increases the count rate without affecting the afterpulse distribution, and allows to collect data faster at low temperatures.

Table 6.1: Time constants with their amplitudes and corresponding afterpulsing histograms at six temperatures. $\boldsymbol{D}$ denotes thermally generated (constant) dark count level. The fit given by τ_i, A_i is plotted as solid lines.

$\boldsymbol{T}$	$\boldsymbol{\tau}$	$\boldsymbol{A}$	**Histogram**
(°C)	**(s)**	**(cps)**	
0	0	0	
	$\boldsymbol{D}$	7603	
-20	$1.10 \cdot 10^{-5}$	60	
	$\boldsymbol{D}$	1212	
-40	$3.73 \cdot 10^{-6}$	108	
	$1.72 \cdot 10^{-5}$	49	
	$1.90 \cdot 10^{-4}$	5	
	$\boldsymbol{D}$	155	
-60	$5.36 \cdot 10^{-6}$	233	
	$3.94 \cdot 10^{-5}$	18.5	
	$1.84 \cdot 10^{-4}$	3	
	$\boldsymbol{D}$	24	
-80	$1.37 \cdot 10^{-6}$	133	
	$6.13 \cdot 10^{-6}$	61	
	$2.44 \cdot 10^{-5}$	22	
	$2.06 \cdot 10^{-4}$	2.5	
	$\boldsymbol{D}$	1.9	
-100	$3.6 \cdot 10^{-7}$	3446	
	$3.4 \cdot 10^{-6}$	123	
	$2.75 \cdot 10^{-5}$	37	
	$4.82 \cdot 10^{-4}$	2.3	
	$\boldsymbol{D}$	0.3	

6.5 Discussion and conclusion

We built and characterized a custom compact SPD based on a Si-APD which has very low noise, due to cooling of −100 °C. All main parameters of our SPD are in a good range for use in long distance quantum communication experiments: the DCR below 1 cps, afterpulsing at the lowest temperature does not exceed 0.5%, detection efficiency about 50%, detection timing jitter changes between 500 and 1050 ps, depending on bias voltage of the APD. Using SPDs with such parameters could be beneficial for experiments of quantum communications over high-loss channels. Afterpulses can be further reduced by discarding in post-processing, depending on application requirements.

To determine afterpulsing probability, we have developed a new advanced method of analysis of afterpulses over a large time-scale of 1 second. This method allows calculating afterpulses probability including secondary afterpulses (caused by afterpulses) and higher orders of afterpulses, and easily determining a level of dark counts without afterpulses contribution. Our algorithm can be adapted with minor adjustments for analysis of data collected from an APD illuminated with weak periodic light pulses [108]. Furthermore, we implemented a curve fitting procedure to our data to calculate lifetime constants for carrier traps, and their corresponding amplitudes.

The results of the present research have been used for planning detector design for a future space mission [132] and for finding a way of mitigating radiation damage in APDs [108, 120].

A possible next step is to collect higher number of data points at −100 °C and resolve the shape of the afterpulsing probability decay at that temperature. Possibly, it will provide additional information about lifetimes of traps. The afterpulsing analysis algorithm can be improved to minimize dependence on bin size parameters, and optimize calculation process. Also, it would be interesting to test our new detector with APDs from other manufactures, e.g., Laser Components.

Chapter 7

Detector prototype for Airborne demonstration of QKD receiver payload

7.1 Experiment motivation and description

To extend distances for quantum communications, including QKD, up to global scale, satellite based quantum stations need to be developed. We built an SPD prototype of the receiver payload as a form-fit-function model of a satellite suitable system, which was part of the payload prototype used for an airborne demonstration of QKD [132], where QKD was established between a transmitting stationary ground station and a quantum receiver placed on board of a flying airplane. The successful demonstration of QKD over 3-10 km distance was an important step towards implementing a satellite-ground QKD.

Commercially available APDs did not fulfill special requirements for the nano satellite QKD receiver. The QKD receiver prototype was custom built according to requirements for space qualified satellite payload. Many components used in the detector prototype are of space grade, and other easily replaced by their close models with space grade. Requirements on satellite receiver payload for thermal, vacuum and power management were elaborated and implemented.

The QKD source was a high speed polarization source based on described in Ref. [99] and implementing BB84 protocol with decoy states ([17, 114]). The source created weak coherent pulses at 785 nm. Signal and decoy levels were generated with electro-optical intensity modulator. Mean photon numbers for outgoing pulses were $\mu \approx 0.5$ and $\nu \approx 0.1$ for signal and decoy pulses.

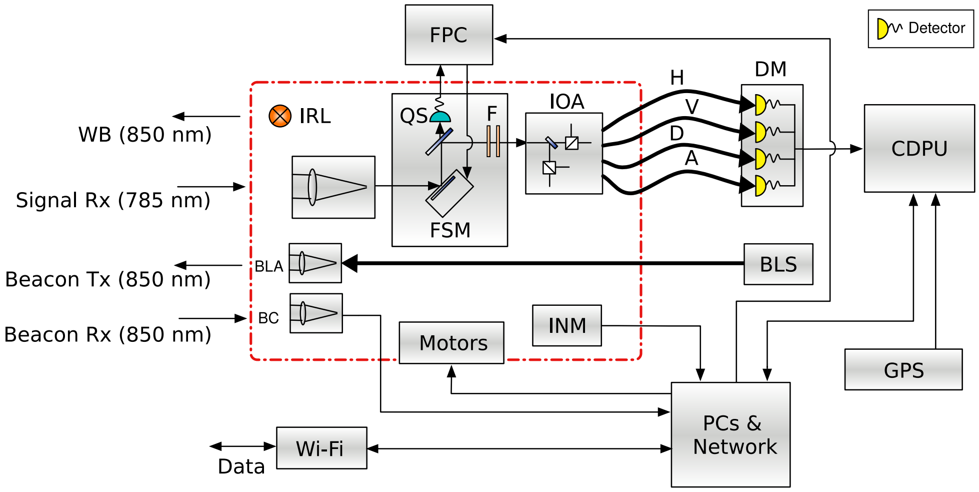


Figure 7.1: Schematic diagram of the receiver apparatus
Acronyms are as follows: F, band-pass filters; FSM, fast-steering mirror; QS, quad cell photosensor; FPC, fine pointing controller; IOA, integrated optical assembly (developed by INO); DM, detector module; FPU, fine-pointing unit; WB, wide-field beacon (produced by the IRL); CDPU, control and data processing unit . Other acronyms and details given in the text. The red border indicates components that are mounted on the motors. (*Re-printed from* [132].)

Four polarizations for BB84 protocol (vertical, horizontal, diagonal and anti-diagonal) were created using two electro-optical phase modulators in a balanced Mach-Zehnder interferometer. The intensity and polarization were randomized over 1000 pulse sequence. Though its insecurity for real QKD implementation, it was sufficient for our demonstration experiment. The quantum signals were transmitted trough a 12-cm aperture refractive telescope.

In the experiment we used fine- and coarse-pointing systems ([133, 134]) at a wavelength of 850 nm to set up and maintain a link between ground and the moving aircraft.

In the Fig. 7.1 a scheme for the receiver apparatus shown. The 10-cm aperture refractive telescope collects the quantum and beakon signals. First signals go through a fine-pointing unit (FPU), that was developed by commercial companies (Institute National d'Optique (INO) and Neptec Design Group). The FPU separates quantum and beakon signals, directing the beakon signal to the fine-pointing apparatus, providing position feedback, and the quantum signal to a spatial-mode filter (50 μm pinhole) and two spectral filters of 785 nm wavelength. Then the quantum signal passes through polarization analyzer contained in the integrated optical assembly (IOA). Four outputs of the IOA corresponding to four polarization states (V, H, D,

A) coupled to fibers connected to four SPDs inside the detector module (DM). Detection signals from SPDs were time tagged with resolution of 78 ps. The rest of the receiver-side QKD protocol was executed in the CDPU using the Linux operating system, implementing data storage, communication and processing operations.

7.2 1-channel prototype SPD

At the first stage of our project, we designed, built and characterized 1-channel Si-APD based SPD. In the Fig. 7.2 it is shown mounted on a characterization setup. For the 1-channel prototype we used Excelitas SLiK APD, window type.

The bracket (Fig. 7.3) was machined of aluminum alloy, anodized and served to hold the SLiK Si-APD and electronics board, and dissipate heat from the SLiK's in-built TEC. Electronic scheme for the prototype developed at IQC is shown in Fig. 7.4. It is a passive quenching scheme, featuring a possibility for a remote control via CPU. Bias voltage and temperature (thermistor reading) of the APD, voltage and current of TEC and comparator threshold were controlled. Time tagging was realized on FPGA.

This first 1-channel prototype was tested for breakdown voltage, DCR and efficiency at temperatures between +20 and −20 °C) and at several different bias voltages. Detection timing jitter was measured only at −20 °C, because that temperature looked the most suitable for our prospective use of the SPD, providing DCR below 200 cps. The characterization setup and procedure were similar to those used for characterization of Low temperature super low-noise in-lab built SPD (Ch. 4). Results of the characterization can be seen in the Figs. 7.5 and 7.6. The lowest DCR was expectantly observed at the lowest tested temperature of −20 °C and was 158 cps. At 28 V above breakdown voltage the detection efficiency was maximum and measured 53 %. Timing jitter at those conditions was 210 ps.

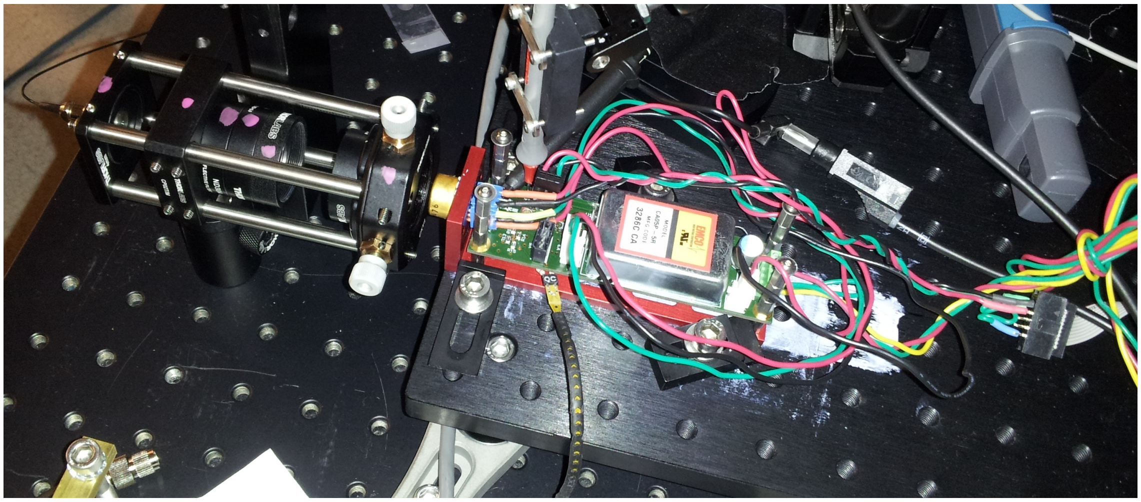


Figure 7.2: 1-channel SPD mounted in a characterization setup

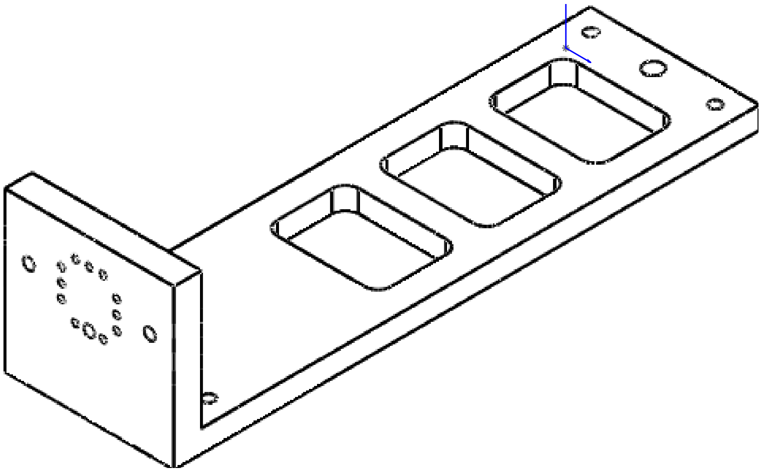


Figure 7.3: Bracket for 1-channel prototype

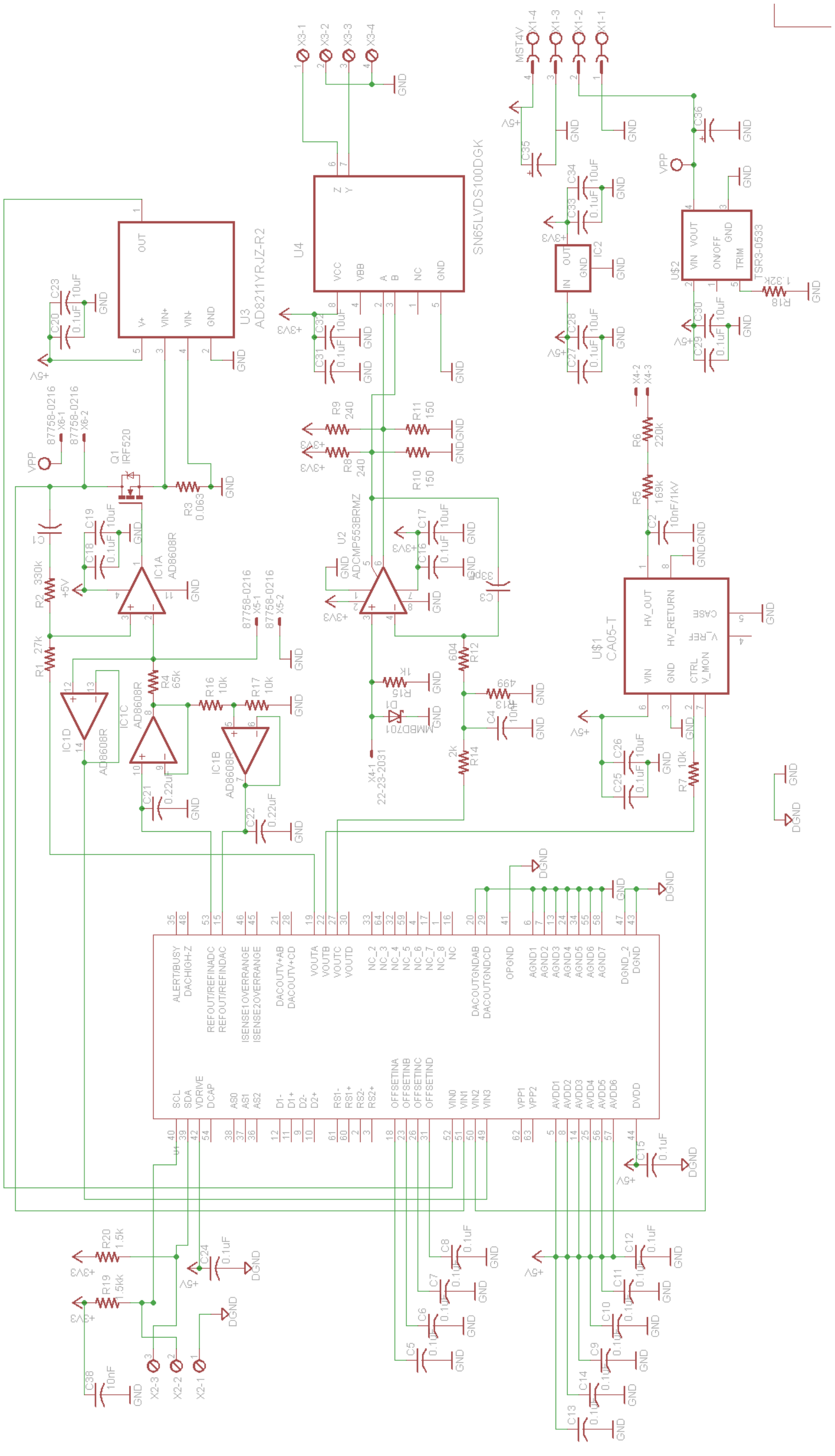


Figure 7.4: Electronics scheme for 1-channel

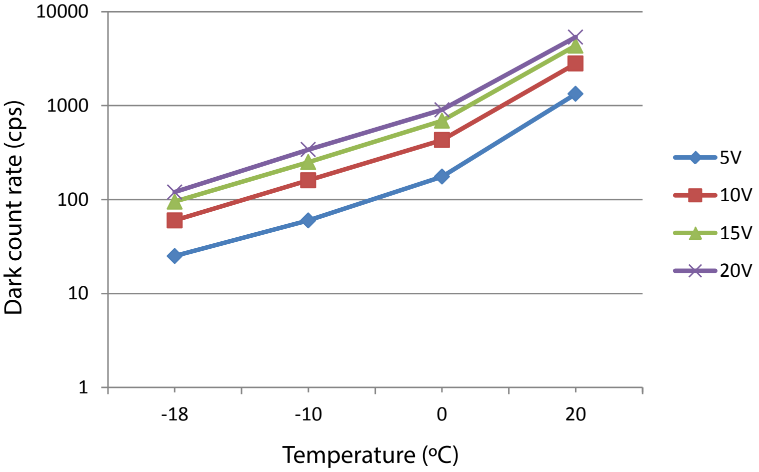
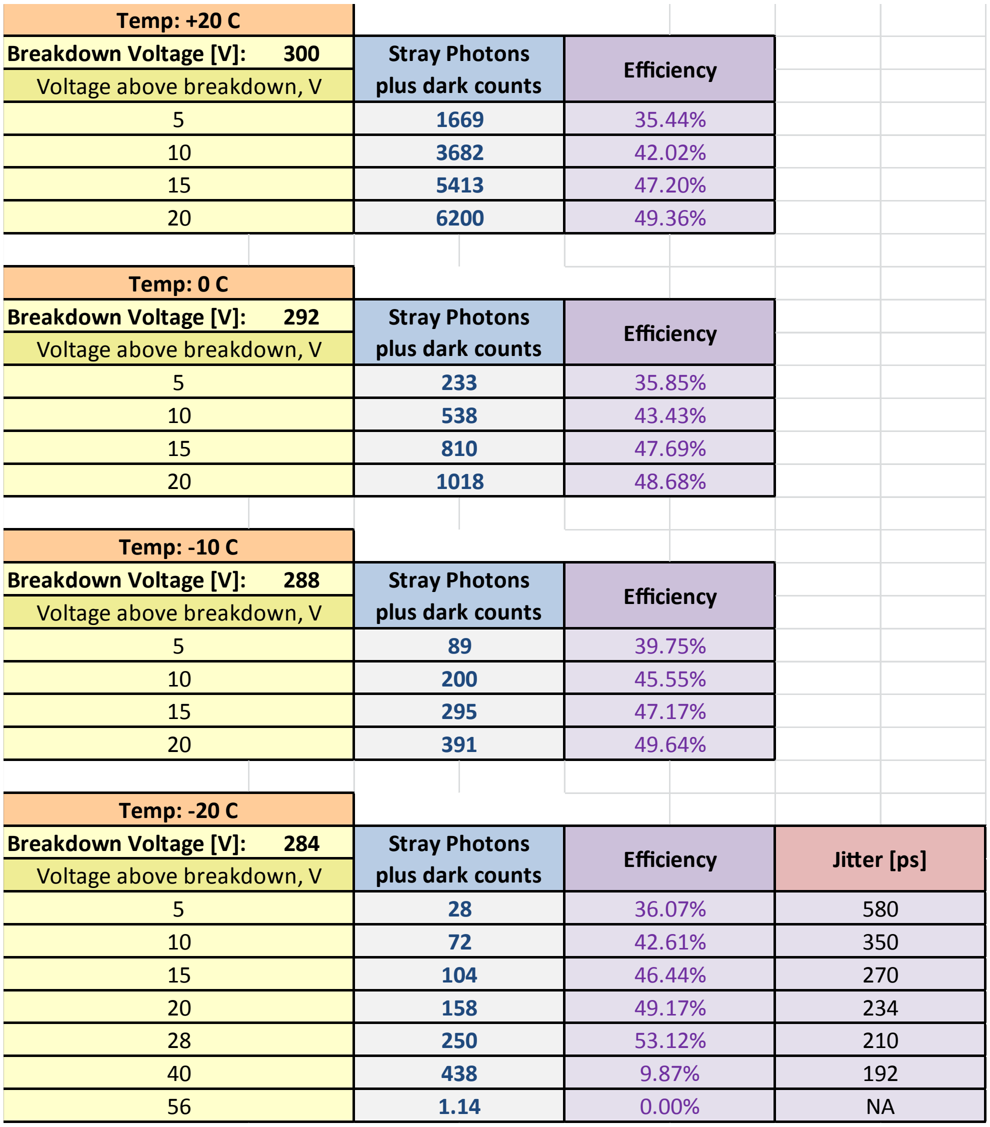


Figure 7.5: DCR of the 1-channel prototype SPD



Temp: +20 C		
Breakdown Voltage [V]: 300	Stray Photons plus dark counts	Efficiency
Voltage above breakdown, V		
5	1669	35.44%
10	3682	42.02%
15	5413	47.20%
20	6200	49.36%

Temp: 0 C		
Breakdown Voltage [V]: 292	Stray Photons plus dark counts	Efficiency
Voltage above breakdown, V		
5	233	35.85%
10	538	43.43%
15	810	47.69%
20	1018	48.68%

Temp: -10 C		
Breakdown Voltage [V]: 288	Stray Photons plus dark counts	Efficiency
Voltage above breakdown, V		
5	89	39.75%
10	200	45.55%
15	295	47.17%
20	391	49.64%

Temp: -20 C			
Breakdown Voltage [V]: 284	Stray Photons plus dark counts	Efficiency	Jitter [ps]
Voltage above breakdown, V			
5	28	36.07%	580
10	72	42.61%	350
15	104	46.44%	270
20	158	49.17%	234
28	250	53.12%	210
40	438	9.87%	192
56	1.14	0.00%	NA

Figure 7.6: Characterization results of the 1-channel prototype SPD
DCR and detection efficiency was measured at four temperatures (+20, 0, -10, −20 °C) and four bias voltages (5, 10, 15 and 20 V above breakdown voltage) to determine the most beneficial regime for the satellite SPD prototype. At −20 °C also the detection timing jitter was measured, and added three bias voltages: 28, 40 and 56 V.

7.3 4-channel prototype SPD

Based on the obtained results with our 1-channel prototype we designed and build the 4-channel prototype (Fig. 7.7). Also Excelitas Si-SLiK fiber-coupled APDs were used. The electronics boards were independant for each channel, and the scheme was the same as designed for 1-channel SPD (Fig. 7.4).

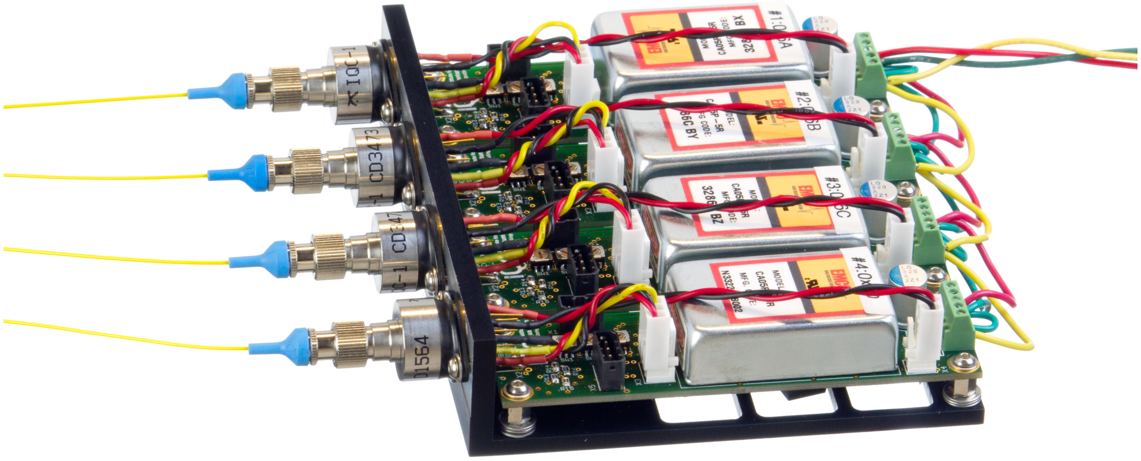


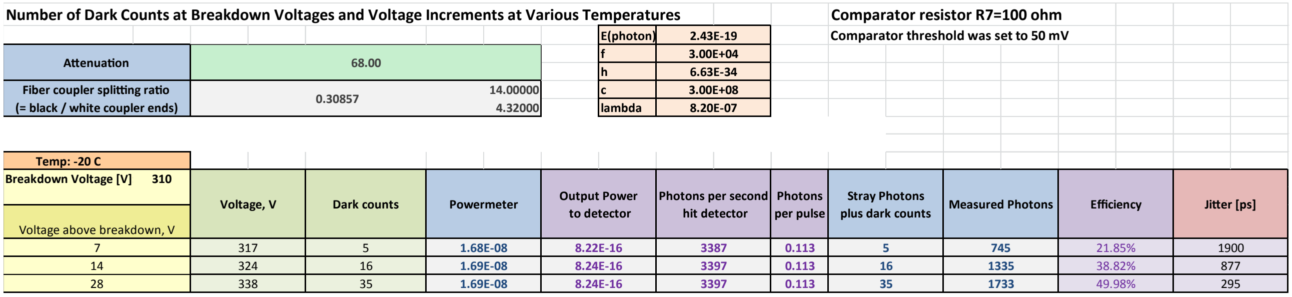
Figure 7.7: 4-channel prototype detectors module. Side view
The size of the DM is 30 × 127 × 143 mm, and weight is 516 g. It consumes 2.3 W of electrical power, while cooling APDs down to −20 °C. *(photo © Vadim Makarov)*

Four channels were characterized one by one.

Results for breakdown voltages at four temperatures are shown in the Fig. 7.9.

DCRs were measured over 100 s and then averaged to minimize uncertainty, results are shown in the Fig. 7.10. All four SPDs demonstrated low DCR at −20 °C. Even at 28 V above breakdown, the DCR is 35 cps and less.

In the Fig. 7.8 an example of a characterization log for the channel A at −20 °C



Number of Dark Counts at Breakdown Voltages and Voltage Increments at Various Temperatures

Comparator resistor R7=100 ohm

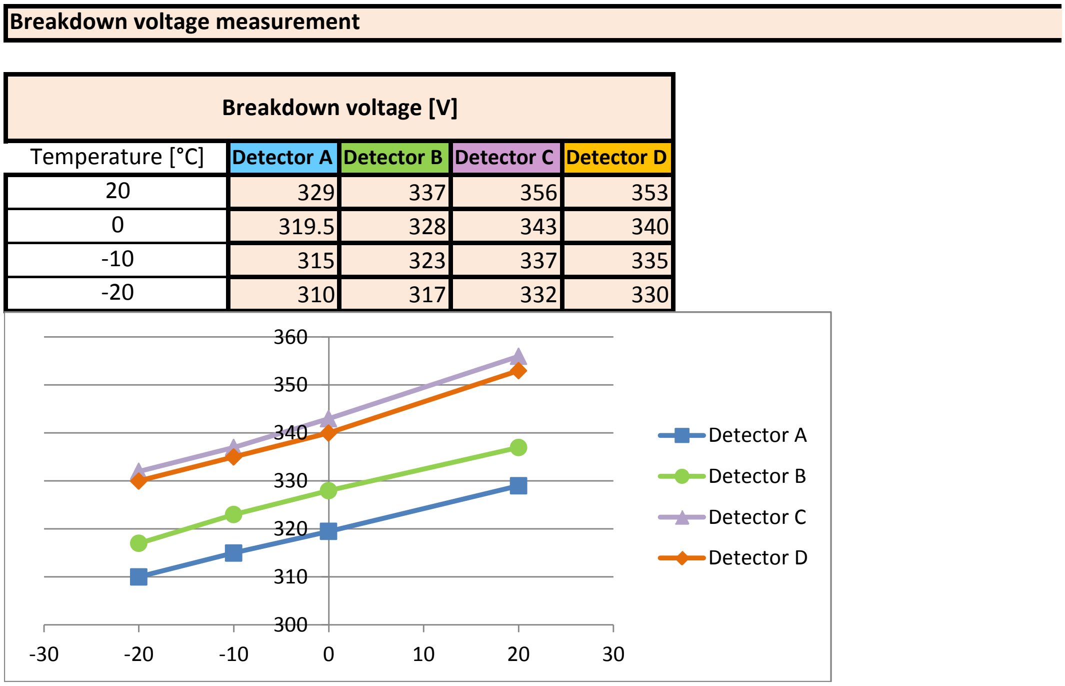
Comparator threshold was set to 50 mV

Attenuation	68.00	
Fiber coupler splitting ratio (= black / white coupler ends)	0.30857	14.00000 4.32000

E(photon)	2.43E-19
f	3.00E+04
h	6.63E-34
c	3.00E+08
lambda	8.20E-07

Temp: -20 C Breakdown Voltage [V] 310 Voltage above breakdown, V	Voltage, V	Dark counts	Powermeter	Output Power to detector	Photons per second hit detector	Photons per pulse	Stray Photons plus dark counts	Measured Photons	Efficiency	Jitter [ps]
7	317	5	1.68E-08	8.22E-16	3387	0.113	5	745	21.85%	1900
14	324	16	1.69E-08	8.24E-16	3397	0.113	16	1335	38.82%	877
28	338	35	1.69E-08	8.24E-16	3397	0.113	35	1733	49.98%	295

Figure 7.8: Characterization of the 4-channel prototype channel A



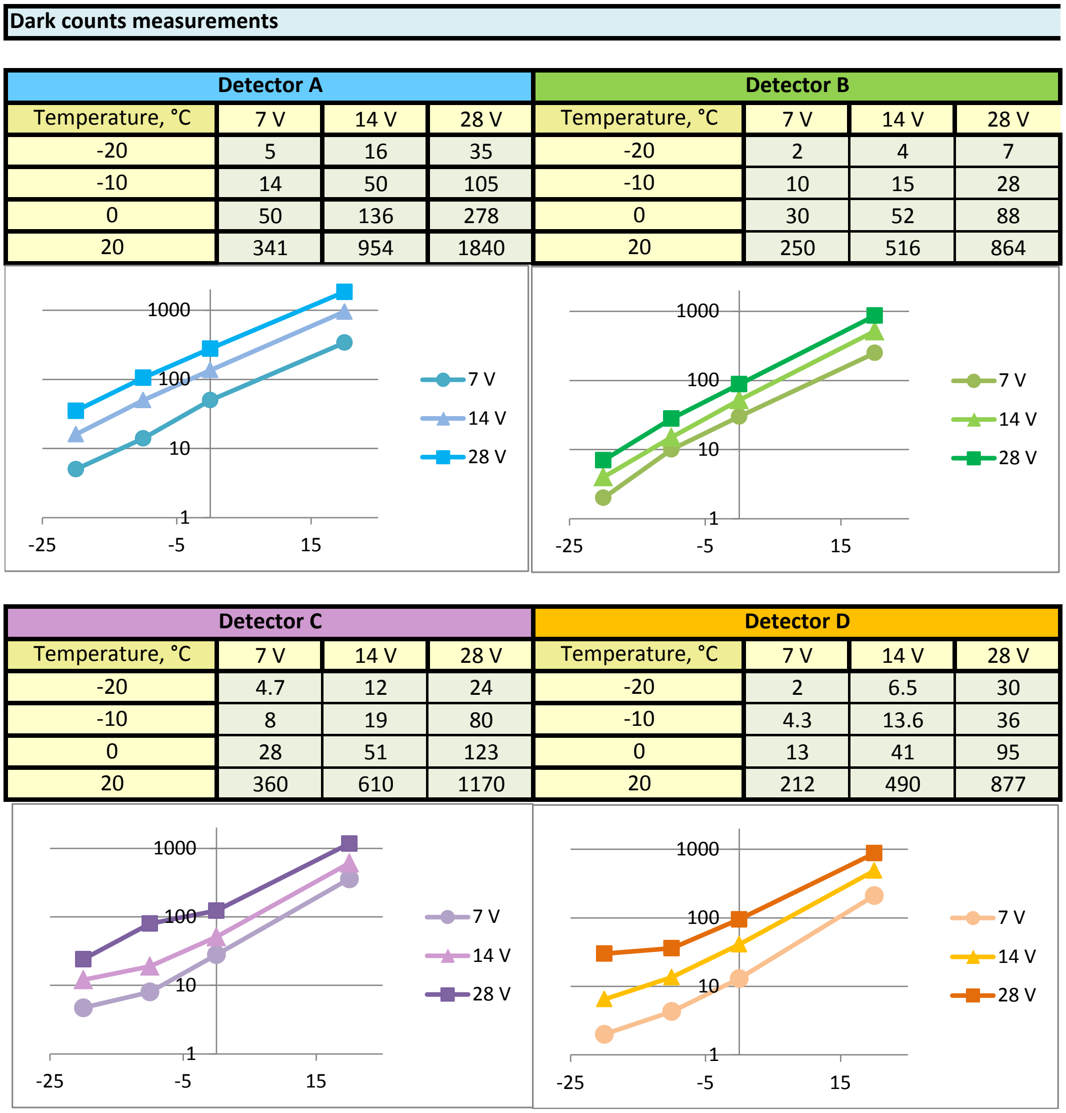
Breakdown voltage measurement

Breakdown voltage [V]				
Temperature [°C]	Detector A	Detector B	Detector C	Detector D
20	329	337	356	353
0	319.5	328	343	340
-10	315	323	337	335
-20	310	317	332	330

Figure 7.9: Characterization. Breakdown voltage measurement

is demonstrated. The detection efficiency was measured by calibration method, described in details in Chapter 4. Laser pulses at 820 nm were generated with frequency 30 kHz, attenuated by variable digital attenuator and ND filters by 68 dB and detected by an SPD under test. The optical average power of the laser was measured by a power meter connected to one arm of a fiber coupler, installed immediately at the laser output. Then, detection efficiency was calculated as (detected photons)/(sent photons). Results for detection efficiency measurement are shown in the Fig. 7.11. The highest efficiency of 49.6–51% was observed at 28 V above breakdown voltage.

The detection timing jitter was measured as time delay between laser pulse and an SPD output, and statistic was collected over about 500,000 pulses, the results histogrammed, and the timing jitter determined as full width of the half maximum (FWHM) of the histogram. Results are shown in the Fig. 7.11.



Dark counts measurements

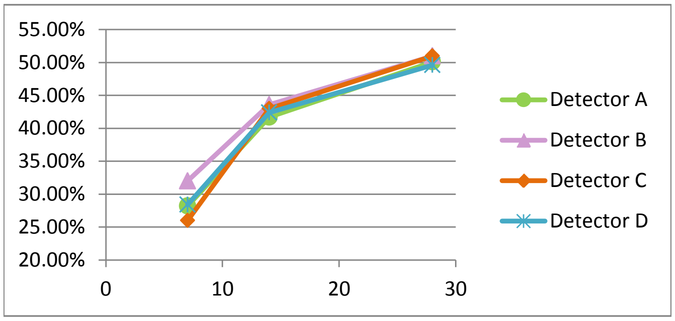
Detector A				Detector B			
Temperature, °C	7 V	14 V	28 V	Temperature, °C	7 V	14 V	28 V
-20	5	16	35	-20	2	4	7
-10	14	50	105	-10	10	15	28
0	50	136	278	0	30	52	88
20	341	954	1840	20	250	516	864

Detector C				Detector D			
Temperature, °C	7 V	14 V	28 V	Temperature, °C	7 V	14 V	28 V
-20	4.7	12	24	-20	2	6.5	30
-10	8	19	80	-10	4.3	13.6	36
0	28	51	123	0	13	41	95
20	360	610	1170	20	212	490	877

Figure 7.10: Characterization. DCR measurement

Efficiency measurement

Efficiency [%]				
Overvoltage [V]	Detector A	Detector B	Detector C	Detector D
7	28.20%	32.00%	26.00%	28.40%
14	41.70%	43.60%	43.00%	42.40%
28	50.10%	51.00%	51.00%	49.60%



Jitter measurement

Jitter [ps]				
Overvoltage [V]	Detector A	Detector B	Detector C	Detector D
7	1900	1030	1670	1300
14	877	460	600	537
28	295	295	320	325

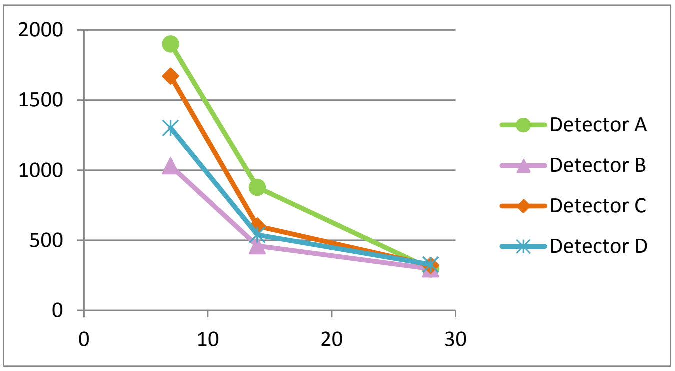
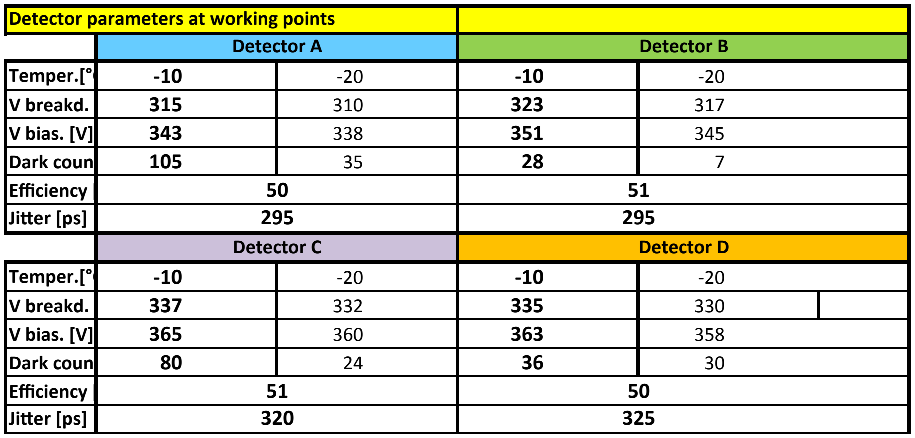


Figure 7.11: Characterization. Efficiency and jitter measurement

7.4 Discussion and conclusion

We have built and characterized the four channel SPD prototype with Excelitas SLiK Si-APDs.

Based on the results of the characterization of the four-channel prototype, the optimal working points were determined as shown in Fig. 7.12.



Detector parameters at working points				
	Detector A		Detector B	
Temper.[°	-10	-20	-10	-20
V breakd.	315	310	323	317
V bias. [V]	343	338	351	345
Dark coun	105	35	28	7
Efficiency	50		51	
Jitter [ps]	295		295	
	Detector C		Detector D	
Temper.[°	-10	-20	-10	-20
V breakd.	337	332	335	330
V bias. [V]	365	360	363	358
Dark coun	80	24	36	30
Efficiency	51		50	
Jitter [ps]	320		325	

Figure 7.12: Parameters of detectors for the optimal working points

Our SPD prototype was mounted on an aircraft in flight and successfully used in the Airborne demonstration of QKD receiver payload experiment [132]. Using BB84 decoy-state protocol, the QKD was established between the stationary ground station and the moving receiver over optical links of 3–10 km, resulting in generating secure key up to 868 kb in length. Different pass configurations were tested, simulating possible satellite trajectories.

Apparatus used in the experiment either are already suitable for satellite use, or have a clear path-to-flight. Some components need to be replaced with radiation hard versions. APDs in the satellite receiver module will develop high dark counts under space radiation, that will aggravate their performance, as will be studied extensively in the next chapter. However, mitigating radiation damage with cooling and thermal [120] or laser annealing [108] can keep detectors parameters acceptable for QKD. A space-suitable DM prototype is under development.

Our experiment proved feasibility of QKD with a quantum receiver placed on a flying aircraft and the whole receiver prototype has a clear path-to-flight. Therefore, a feasibility and convenience of up-link approach with its opportunity to interchange quantum sources has been demonstrated.

Chapter 8

Radiation test and mitigating radiation damage

8.1 Radiation test motivation

Single-photon detectors (SPDs) have been utilized in a number of space applications, including laser ranging (LIDAR) for atmospheric and topology measurements of the Earth [135, 136], elementary particle scintillation detectors [137], and precise laser time transfer [138]. SPDs will also be necessary to support quantum communication applications [31, 56, 57, 111, 113, 139], where high detection efficiency, low timing jitter, low dark count rate (DCR) and low afterpulsing probability are key parameters for achieving successful, high-fidelity transmissions [56, 133]. Photomultiplier tubes (PMTs) and silicon avalanche photodiodes (APDs) are two types of SPDs that generally have good performance for this application, whereas superconducting nanowire detectors may offer better performance, in some respects, at the cost of being significantly less practical, requiring cryogenic cooling [59].

For optical transmissions through the atmosphere, a low-loss window exists at around 800 nm wavelength [56]. PMTs have reduced detection efficiencies for wavelengths longer than 650 nm, but silicon-based APDs have high detection efficiency in that region, low timing jitter, low DCR, and low afterpulsing, making them a prime candidate technology for quantum communication applications. However, incident radiation significantly increases the DCR of APDs [119, 140–143], which can quickly turn an APD unsuitable for quantum communications on a space platform.

Successful ground-to-satellite quantum communication requires each detector's DCR to be kept below about 200 counts per second (cps) [56]. Previous use of silicon APD technology (specifically, Excelitas SLiK devices) for photon detection on a satellite showed an increase in dark count rates by ∼30 cps for each day in orbit [136], which would make them unusable for quantum communications in merely a few weeks. Other ground-based radiation tests of APDs also demonstrated DCRs of thousands cps [119, 140–143], which is too high for quantum communications.

Recently reported tests attempted mitigation by cooling to temperatures as low as −20 °C to overcome the increased DCR [119]. It is known that the DCR of non-irradiated APDs can be reduced by deeper cooling, decreasing the rate of thermally induced spontaneous avalanches [77], but at the same time cooling increases the lifetimes of trapped carriers that contribute to afterpulsing, which may interfere with quantum communication [77, 120]. Thermal annealing was also found to reduce the DCR after irradiation [119, 141, 143]. However, no previously reported tests have applied deep cooling to radiation damaged APDs, nor have any demonstrated a sufficiently low DCR required for quantum communications, specifically quantum key distribution (QKD), or verified other detector parameters throughout a reasonable lifetime (e.g., 1 year for an initial demonstrator mission) of a quantum receiver satellite.

Here we experimentally show that the effects of radiation doses approximately equivalent to as much as 2 years in low-Earth orbit are successfully mitigated by cooling and thermal annealing, allowing APDs to be used in a quantum satellite. We have tested three APD device models—Excelitas C30921SH and Laser Components SAP500S2 (each with sensitive areas 500 µm in diameter), and Excelitas SLiK (with sensitive area 180 µm in diameter)—and one PMT device model—Hamamatsu H7422P-40. All samples survived irradiation and remained functional photon detectors, with the only significant effect being the increase of the DCR in all APD samples. Breakdown voltage, afterpulsing, detection efficiency and timing jitter of the irradiated APDs were characterized and shown to be in the range acceptable for quantum communications. PMTs were also tested for dark counts, timing jitter, afterpulsing and detection efficiency.

8.2 Radiation test: chosen orbit, radiation doses, tested samples

SPDs in low-Earth orbit experience space radiation primarily in the form of protons, electrons and heavy ions, resulting in two types of permanent damage in the semiconductor material: displacement and ionization damage [144–146]. APDs are less sensitive to ionization damage; e.g., Ref. [119] demonstrated that after 1-year equivalent ionization damage (in a 800 km equatorial orbit) Si APDs increased DCRs up to 2 times. However, displacement damage causes new defects in the semiconductor lattice of the active area, significantly affecting the DCR; e.g., in Ref. [119] DCR of APD irradiated by protons increased by one to two orders of magnitude (limited by a saturated passive quenching window comparator).

Dark current in APDs originates from two main components: surface currents, which are unaffected by gain, and bulk leakage current which passes through the avalanche region and is therefore gain multiplied. Bulk dark current generation is linked directly to non-ionizing energy loss in a variety of silicon semiconductors [147]. Ionization damage is mainly associated with surface oxide interface dark current, and was not directly considered in this study. Afterpulsing is caused by delayed emission of trapped charge from bulk defects, in a thermally activated process (analogous to charge transfer efficiency losses in charge-coupled devices).

Proton displacement damage arises due to structural displacements in the silicon crystal caused by elastic collisions, and inelastic spallation reactions. The distribution of energies of trapped protons in low-Earth orbit environment, transported through 10 mm of aluminum shielding (equivalent to the shielding provided by the satellite structure), possesses a broad peak in the range of 50 to 75 MeV. Here the ratio between elastic and inelastic energy loss ranges from 1.7 to 1.2, whereas at 100 MeV the ratio is roughly 1.0. Following a commonly accepted silicon damage deposition model [148], we calculated the monochromatic proton fluence that produces the same average specific non-ionizing energy loss in silicon.

Due to this difference in the energy distribution ratio, the physical range of damage fragments through the sensitive microvolume of the detector will also be different, because inelastic reactions result in a much greater variance in the range of fragments in the silicon, compared to elastic damage which is uniformly distributed throughout. (That is, the damage energy equilibrium may not be established until several micrometers below the Si surface from the direction of incident proton flux.) This would result in under-dosing of the first few micrometers near the surface of the APD—at 100 MeV, damage equilibrium is not reached until about 3 to 5 μm beneath the surface [148]. However, Ref. [149], which shows the internal structure of different types of APD, suggests that the important amplification region is typically tens of micrometers below the surface, where these small damage energy distribution differences will not be a major factor.

Following Ref. [56], we chose a polar orbit at 600 km altitude, providing global coverage, and is representative for our anticipated quantum satellite. With a hypothetical shielding of 10-mm-thick aluminum around the detectors, which is an approximate equivalent to the shielding provided by a satellite structure, the predicted radiation doses were calculated using the SPENVIS radiation modeling tool for durations of 0.6, 6, 12, and 24 months. The radiation doses were determined to be equivalent to 100 MeV proton fluences of 10^8, 10^9, 2×10^9, and 4×10^9 cm^{-2}, respectively.

We tested a total of 32 APD devices and 4 PMT devices. These samples were divided among nine groups (see Table 8.1). We applied each of the four fluences to the first four groups with the devices switched off. For the fifth group, APD bias voltage was applied during irradiation at the highest fluence (24 month equivalent) to examine whether bias voltage affects the extent of damage caused by irradiation. The last group of samples was kept as a control group, being stored and transported alongside the other five groups, but without undergoing irradiation. The irradiation was done at the Tri-University Meson Facility (TRIUMF) at the University of British Columbia using a 106 MeV proton beam, which was slightly higher energy than the nominal 100 MeV.

Table 8.1: Tested devices and radiation doses

Nine groups of tested samples and their corresponding nominal radiation fluences, equivalent to in-orbit exposures over 0.6, 6, 12, and 24 months with protons at 100 MeV. Each APD in group 5 was biased during irradiation at 20 V above its breakdown voltage. Group 9 was not irradiated, and kept as a control.

Group	**Device type and quantity**	**Fluence @ 100 MeV, protons/cm^2**
1	SLiK – 2 pcs SAP500S2 – 2 pcs	10^8
2	SLiK – 2 pcs SAP500S2 – 2 pcs	10^9
3	SLiK – 2 pcs SAP500S2 – 2 pcs C30921SH – 2 pcs	2×10^9
4	SLiK – 2 pcs SAP500S2 – 2 pcs C30921SH – 2 pcs	4×10^9
5	SLiK – 2 pcs SAP500S2 – 2 pcs C30921SH – 2 pcs	4×10^9 (biased)
6	H7422-40 – 1 pc	10^9
7	H7422-40 – 1 pc	2×10^9
8	H7422-40 – 1 pc	4×10^9
9	SLiK – 2 pcs SAP500S2 – 2 pcs C30921SH – 2 pcs H7422-40 – 1 pc	0

8.3 Characterization setup

For each group, each APD sample was assembled on an aluminum plate, with a PCB attached from the back (see Fig. 8.1). A thermistor was attached to each plate to observe the local temperature. During irradiation, five groups of APDs and three PMTs were attached to a single aluminum frame (Fig. 8.2) connected to an electrical ground. To suppress spontaneous thermal annealing of radiation damage during the irradiation process, the frame was cooled to ≈0 °C with chilled antifreeze pumped through copper tubes epoxied to the frame. This cooling also allowed us to conduct some testing of the APDs in situ, and observe the changing dark count rate during the irradiation process for group 5. (Without cooling, APD DCRs after irradiation could not be measured at room temperature, as our devices would be saturated.)

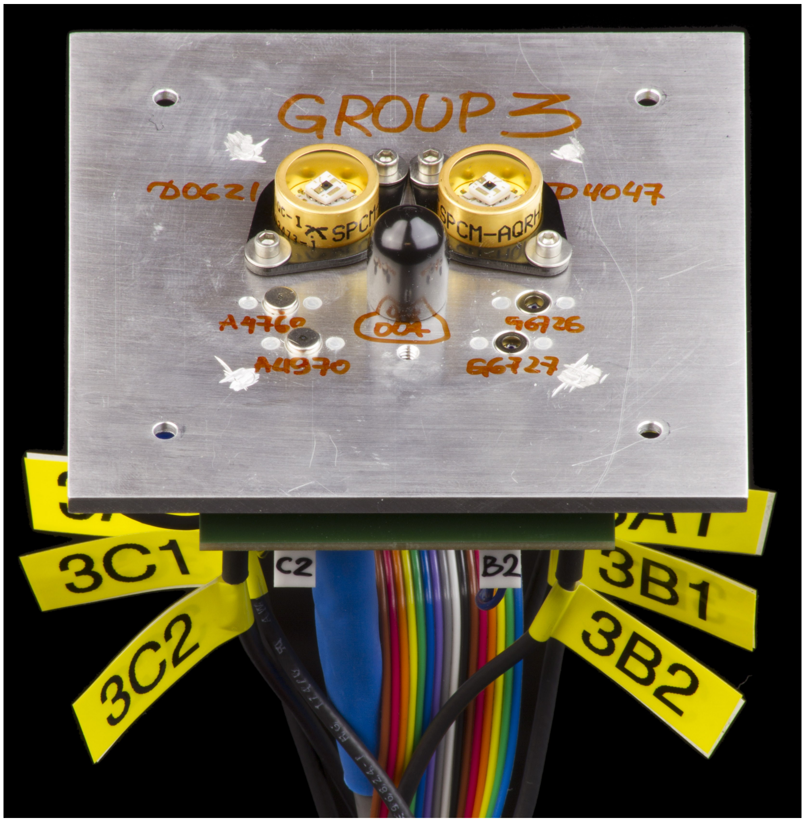


Figure 8.1: One group of tested APDs.

One group of APDs, consisting of two SLiK devices (top), two C30921SH devices (bottom left), and two SAP500S2 devices (bottom right). (The device under the black cap, center, is not discussed in this paper.) The detectors are connected to a PCB with 6 passive quenching circuits, attached to the back of the plate. Bias voltage supply and signal cables can be seen exiting from behind (far bottom).

For each of our APDs we used a passive quenching circuit with quenching resistance of 403 kΩ, similar to that described in Ref. [74] as a passive quenching circuit with current-mode output. This type of quenching circuit is appropriate for a quantum receiver satellite because of its simplicity and robustness, protecting against excessive current due to, e.g., bright illumination or charged particles, or accidental high voltage spikes. Its maximum detection rate of 0.2–0.4 Mcps is lower compared to active quenching circuits, but sufficient for the detection rates expected in near-term QKD applications [56]. Conveniently, the long (>1 μs) dead-time of this circuit suppresses afterpulsing, even at low temperatures. Circuits for all APDs in a group were mounted on the same circuit board, outputting avalanche pulses through coaxial signal cables connected to each detector's cathode.

The breakdown voltage of each detector was found by gradually increasing the applied bias voltage until pulses due to dark counts began to appear in the trace of an oscilloscope. The oscilloscope was also used to observe the shape of the pulse at the nominal operating condition of 20 V excess bias. To determine detection performance properties, avalanche pulses were collected from each device, discriminated at 50 mV threshold and time-tagged with a resolution of 156.25 ps, while applied bias voltages and thermal parameters were simultaneously recorded at 10 Hz.

For measuring timing response properties and detection efficiency, each APD group was illuminated with a pulsing 780 nm reference laser emerging from a single-mode fiber. An optical test rig (see Fig. 8.3) was assembled that held the optical fiber and a lens in place at ≈20 cm distance from the detector group plate. The attenuation and divergence of the laser beam was chosen such that less than one photon per pulse would be incident on each detector. The optical test rig was placed in a cold freezer (Fig. 8.4) to perform low-temperature tests down to −86 °C. The DCRs of the samples were measured either in the optical test rig with reference laser turned off, or while on the main aluminum frame within a light-tight enclosure. DCRs were averaged over several minutes (up to 15) of collected data to minimize uncertainty. Afterpulsing probability was calculated from DCR measurement data using an improved afterpulsing analysis [150]. For timing jitter and efficiency measurements, counts were collected for 15 minutes or until about 10^6 detection events were registered (whichever came first).

All PMT measurements were taken while operating at −5 °C (one of the pre-set working temperatures of the in-built cooler). The measurements of DCR and afterpulsing were done similarly as for APDs. For timing jitter and detection efficiency, we used a pulsed reference laser at 690 nm wavelength, with an Excelitas SLiK acting as a calibrated reference to determine the absolute efficiency.

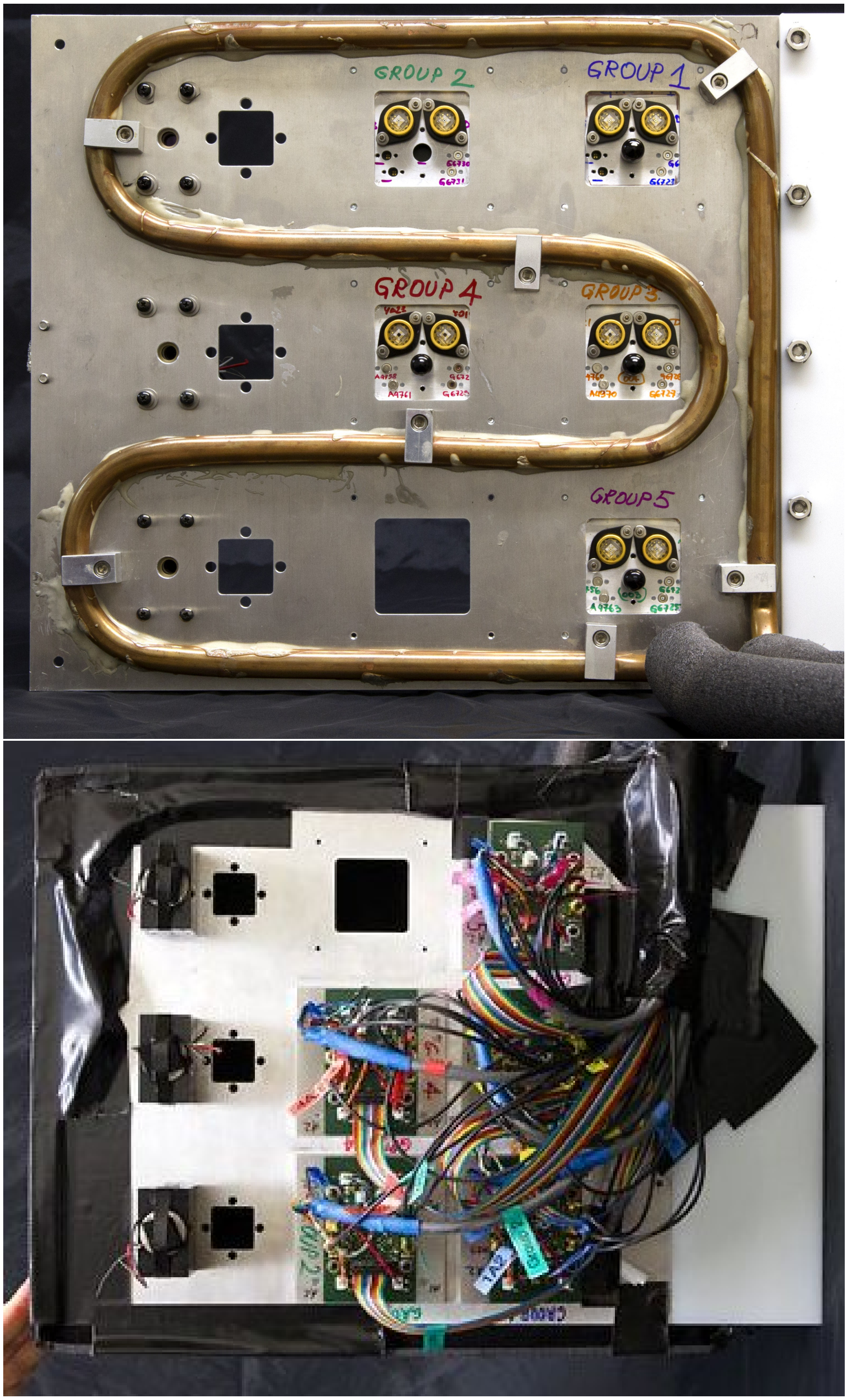


Figure 8.2: The main aluminum frame with all detectors groups installed

Upper figure, front view. 5 APD (right and middle column) and 3 PMT (leftmost column) groups—mounted prior to irradiation. Chilled antifreeze flowing through the copper tubing keeps the frame at 0 °C. A dry, insulating light-tight box (not shown) was placed around the frame. Lower figure, back view with cables attached.

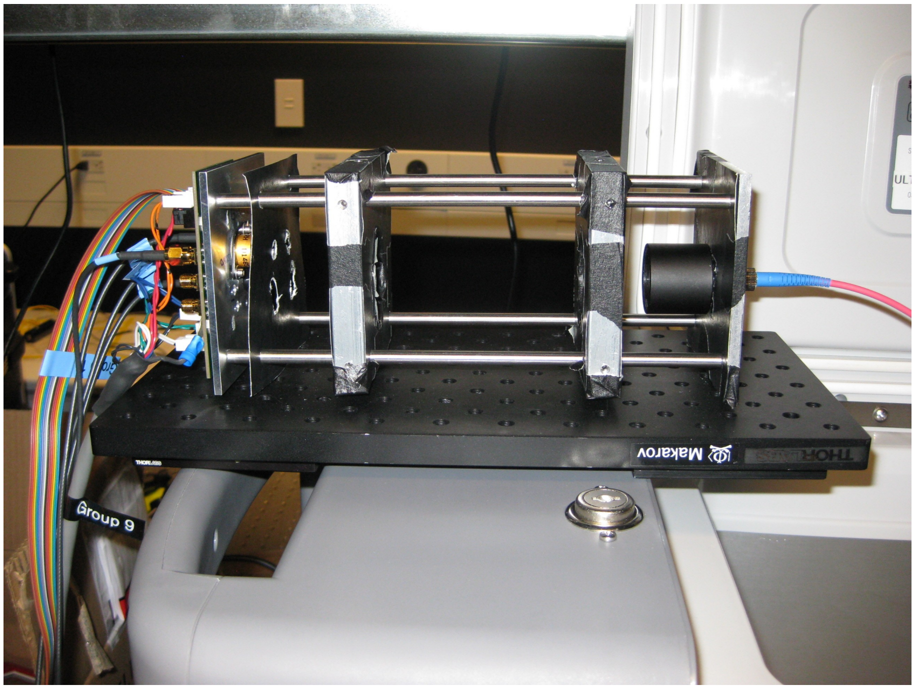


Figure 8.3: Assembly for the APDs characterization.

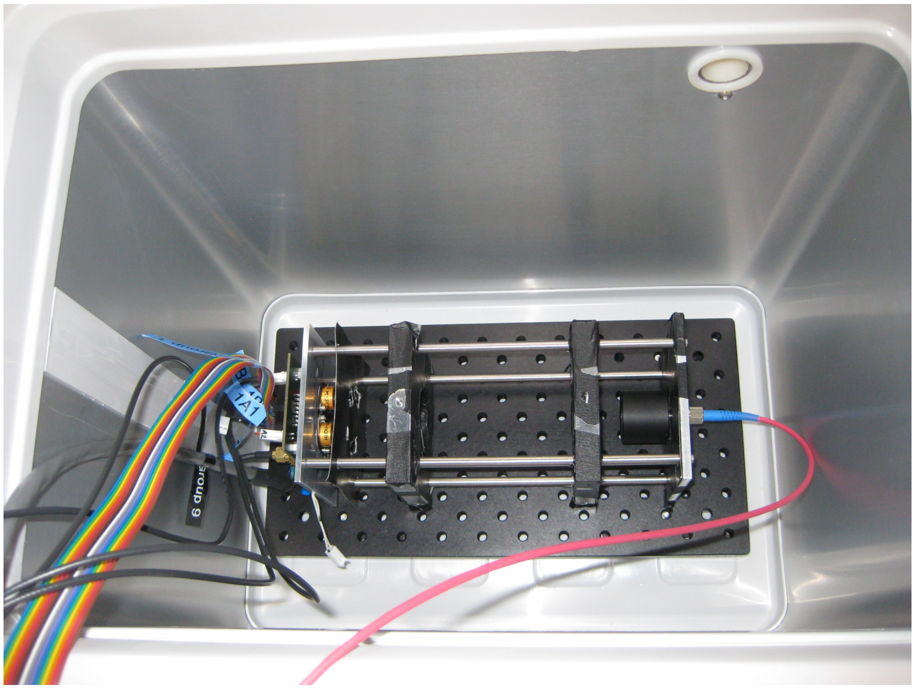


Figure 8.4: Optical rig with APD group 1 installed is placed in the freezer.

8.4 Test schedule

Prior to irradiation, we measured the breakdown voltage, DCR, efficiency, timing jitter and afterpulsing probability of all APD samples at −20 °C. Group 4 and the control group were also characterized at lower temperatures. PMTs were tested for DCR, efficiency, timing jitter and afterpulsing probability.

At TRIUMF on June 12-13, 2014, each APD group (apart from the control) was in turn characterized for breakdown and DCR, then irradiated for a duration corresponding to the desired fluence for that group (actual applied fluences were within 1% of desired, except for group 1 which received 4% greater fluence). Immediately after irradiation the APDs were re-characterized for breakdown and DCR. These pre- and post-irradiation characterizations were performed in situ, at 0 °C, to minimize the influence of spontaneous thermal annealing. Uniquely, group 5, which received the same fluence as group 4, was held biased with its DCR recorded during the irradiation. Each PMT group was irradiated to the desired fluence, but no PMT measurements were taken in situ.

After irradiation, the APD and PMT samples were packed in a thermally isolated box filled with dry ice for transportation. This box provided temperatures no higher than −12 °C during the 48 hour transit. Following this, the samples were kept in a freezer at about −20 °C between tests. All APD samples were re-tested at 0 °C for breakdown voltage and DCR upon arriving from the radiation facility, with no significant changes observed. PMTs were recharacterized at −5 °C.

All APD samples were then characterized (breakdown, DCR, efficiency, jitter, and afterpulsing probability) at temperatures ranging from −20 °C to −86 °C, allowing us to assess the effectiveness of cooling to mitigate damage due to irradiation. Finally, we performed thermal annealing on some groups at varying hot temperatures and durations, with further characterization at selected stages and cold temperatures.

8.5 Effects of radiation damage

All irradiated APDs exhibited a significant increase in their DCRs, illustrated in Fig. 8.5 for −86 °C operating temperature, consistent with previous studies [119, 140, 141]. The DCR increase in each device followed the radiation dose applied, conditional that operating temperatures were kept sufficiently low—at high temperatures, the device count rates saturated. At high doses and standard operating temperatures,

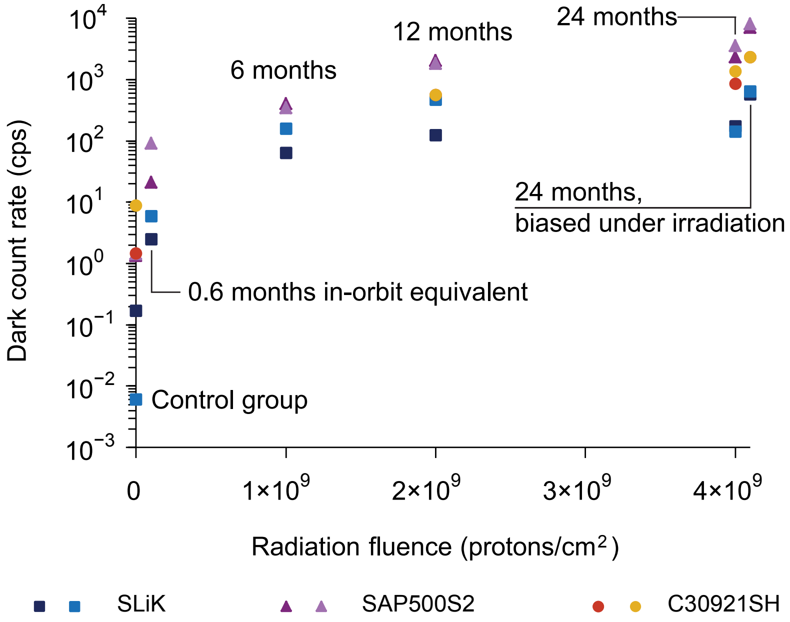


Figure 8.5: DCR of APDs as function of radiation dose

Measurement was taken at −86 °C operation with APDs biased 20 V above their breakdown voltages. In every case, radiation damage caused a DCR increase. The APDs biased during irradiation developed a noticeably higher dark count rate.

the DCRs of all devices would prevent successful quantum communications—for example, Excelitas SLiK devices (overall the best performing devices) operating at −20 °C exhibit DCRs of the order of 10^5 cps.

No significant changes in breakdown voltages, pulse shapes or efficiency owing to irradiation were observed. The timing jitter of detection pulses when operating at low temperatures did not change for SLiK and SAP500S2 samples, and increased by 100 ps for C30921SH (see Fig. 8.6). However, the timing jitter when operating at higher temperatures appeared to increase for all the irradiated APDs—for example, within group 4 at −20 °C operation, jitter increased for SLiKs by up to 80 ps, for SAP500S2 by up to 300 ps, and for C30921SH by up to 250 ps. This increased timing jitter is likely due to the operation of the passive quenching mechanism at a high count rate: in this condition, avalanches often trigger before the APD voltage has fully recovered, leading to effectively lower bias voltages, which are known to have higher jitter [74], for these events. Furthermore, the variation in effective bias voltages between events leads to variable current rise-times at the discriminator, and thus time-tagged events with delays dependent on the stochastic arrival of adjacent avalanches. We remark that lower jitter values than those observed in our experiment

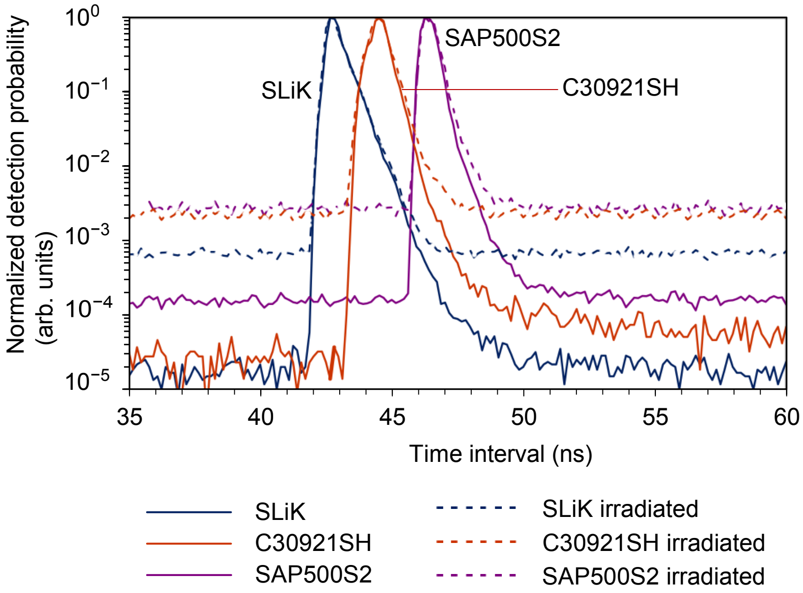


Figure 8.6: Timing response histogram of APDs from group 4, before and after proton irradiation

Normalized timing response histogram for representative APDs from group 4 was measured before and after irradiation at −60 °C using a pulsed laser. The time intervals were measured from a laser pulse to the APD's output pulse caused by a photon from the same laser pulse. The full width half maximum (FWHM) of the histogram determines an APD's timing jitter. Before irradiation the timing jitter was ≈ 600 ps for SLiK, ≈ 550 ps for C30921SH, and ≈ 700 ps for SAP500S2. Changes in the baseline count probabilities are due to the changes in DCRs. At full width half maximum there is no noticeable change in the timing response of SLiKs and SAP500S2 before and after irradiation, and a moderate increase of 100 ps was observed for C30921SH. Measured timing jitter includes timing jitter of the laser and time tagger.

can be obtained by optimizing detector electronics [132, 151].

The probability of afterpulses increased for SLiK and C30921SH samples after irradiation (Fig. 8.7), likely due to an increased number of defects in the semiconductor crystal structure. For SAP500S2, the afterpulsing results did not show a consistent trend. Note that the afterpulsing probabilities for all SAP500S2 devices, including those in the control group, were remarkably high at lower temperatures, reaching 30%. A longer dead-time than that provided by our circuit is clearly needed for correct operation of SAP500S2 [152].

APDs biased during the irradiation (group 5) developed higher DCRs than those that received the same fluence while unbiased (group 4). This result may be an important factor when planning an operational schedule for devices in an orbiting satellite—

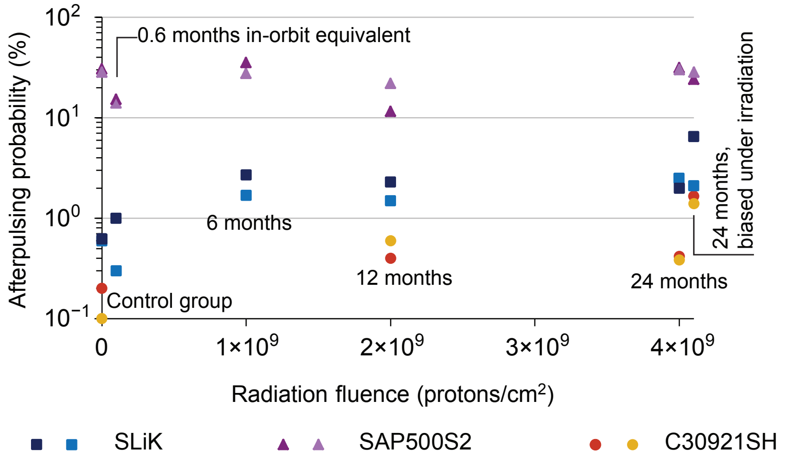


Figure 8.7: Afterpulsing probability as function of radiation dose

Afterpulsing probability, measured at −86 °C, which increased for SLiK and C30921SH devices during the first 6 to 12 month equivalent radiation dose. SAP500S2 results are high and inconsistent with respect to the applied radiation.

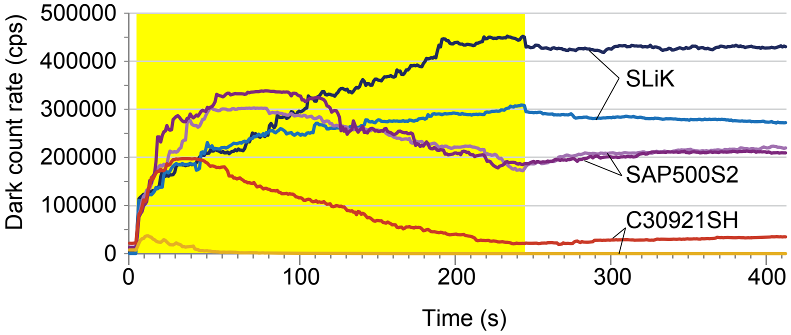


Figure 8.8: DCR of APDs biased during irradiation

The highlighted portion represents the period of irradiation. While the irradiation is on, the DCR of each APD increases until saturation in the passive quenching circuit, after which saturation causes an apparent (not real) decrease in the DCRs. After irradiation ceased, actual DCRs slightly improved due to spontaneous annealing, leading to an apparent DCR rise in the over-saturated samples.

Table 8.2: PMTs' characteristics before and after irradiation

Four tested PMTs, their corresponding nominal fluences, equivalent to in-orbit exposures over 6, 12, and 24 months, their DCRs, afterpulsing probabilities, and jitters before and after radiation, and their detection efficiency. PMTs were not powered during the radiation. The PMT from group 9 was not irradiated, and kept as a control.

Group	Fluence @100 MeV, protons/ cm^2	Before irradiation			After irradiation			
		DCR, cps	Afterpulsing, %	Jitter, ps	DCR, cps	Afterpulsing, %	Jitter, ps	Efficiency, %
6	10^9	6.25	3.4	600	399	1.1	660	23
7	2×10^9	14.4	13.8	550	592	0.76	640	23
8	4×10^9	7	166	600	10	45	400	21
9	0	5	0.22	590	0.5	0.22	590	20

for example, it may be preferable that the detectors are off while crossing regions with higher radiation levels, such as the South Atlantic Anomaly [153]. Fig. 8.8 demonstrates the dynamic change of DCRs of the APDs during irradiation. Note that all devices eventually exhibit over-saturation behavior [154] during the in-situ test.

Table 8.2 shows the measured properties of the PMTs. In general, DCRs increased noticeably and exceeded the 200 cps desired for QKD. Anomalously, however, the PMT under the highest fluence experienced a DCR increase of merely 43%. Given that this sample also exhibited 166% afterpulsing probability prior to irradiation (and 45% afterwards), it seems that the device may be defective and its properties unrepresentative. (Although, owing to a lack of time, the PMTs were not aged prior to the experiment, as is recommended by Hamamatsu. This resulted in generally elevated afterpulsing probabilities before irradiation.) DCRs as presented in Table 8.2 were measured at 19 days after irradiation. A second DCR measurement was also performed 27 days after irradiation, where it was observed to have decreased by 10 to 25% since the first measurement, possibly due to self-annealing, despite the PMTs being kept in a freezer at −20°C.

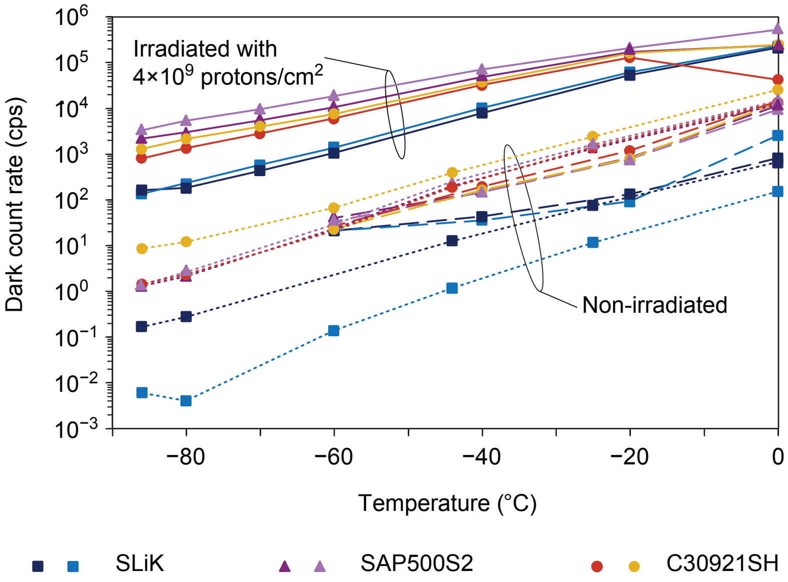


Figure 8.9: Cooling effect on DCRs before and after irradiation

Cooling effect on DCRs of group 4 (24 month equivalent dose). Pre-irradiation data are connected with dashed lines, post-irradiation with solid lines, and the control group with dotted lines. DCRs decrease with temperature exponentially for irradiated and non-irradiated samples.

8.6 Mitigation of radiation damage in APDs

8.6.1 Cooling

Measurements of the detection properties of the samples reveal that radiation-induced DCRs decrease with temperature exponentially for all irradiated APDs, following the same trend as for non-radiated APDs. For SLiKs from group 4, irradiated with a 24-month-in-orbit equivalent dose, DCR dropped to 200 cps at about −80 °C (see Fig. 8.9). The drop of DCR with temperature followed an exponential gradient of about factor 2 per 8 °C, which is the same factor as for non-irradiated samples. The breakdown voltage, efficiency, and timing jitter demonstrated no significant change, though the afterpulsing probability increased significantly as lower temperatures prolonged the release of trapped carriers [155]. The maximum afterpulsing probabilities in group 4 measured at −86 °C are 2.7% for SLiKs, 31% for SAP500S2, and 1.7% for C30921S2.

Although afterpulsing is higher, we can conclude that, given sufficient cooling, SLiK SPDs can serve well for quantum protocols even after 24 months in orbit. Notably, the required temperatures are significantly above those typically reached by cryogenic coolers, and though the cooling necessary might represent a significant power demand on a small satellite system, it is nevertheless achievable. In a larger satellite or an orbital station it could be easily implemented, e.g., by using solid-state thermoelectic coolers (TECs).

8.6.2 Thermal annealing

We applied thermal annealing to all our irradiated APD samples except those in group 2 (which were set aside for laser annealing tests taking place separately [108]). Samples were left at room temperature (+20°C) and in a hot-air-flow oven at +50, +80 and +100 ± 1.5 °C for various lengths of time. After a week of annealing at room temperature there was an observed decrease of DCR, down to a factor relative to pre-annealing rates as low as 0.57 for SAP500S2 samples, and 0.71 for SLiK samples. While interesting, this rate of improvement is almost certainly too slow to be useful on a satellite platform.

For thermal annealing at higher temperatures we built a convection oven, implementing a hot-air gun as a heater, see the Fig. 8.10. The stability of the temperature in the oven was ±0.5 °C.

All oven-annealed APDs demonstrated more significant decreases of DCRs, with the most improvement achieving a factor 0.15 times the original pre-annealing DCR for a SLiK APD from group 3 annealed at +50, +80 and +100 °C (see Fig. 8.11)—almost a full order of magnitude DCR improvement. SAP500S2 samples saw factors as low as 0.28, and C30921SH as low as 0.3, compared to pre-annealing DCRs, both from group 4 annealed at +80 and +100 °C (see Fig. 8.12).

Instead of the oven, we utilized in-built TECs for annealing of SLiKs from group 3 at +100 °C, as this approach has the potential to simplify annealing within orbit conditions. To achieve +100 °C at the sensitive area while the package is at room temperature, a SLiK's TEC consumes 0.41 W of electrical power. The total annealing time with TECs was 8 h. One of the SLiKs demonstrated steady improvement of the dark count rate during that time, though the second SLiK showed some degradation after 4 h of annealing (Fig. 8.11).

Breakdown voltage, detection efficiency, afterpulsing and timing response jitter of all APDs demonstrated no notable change after thermal annealing.

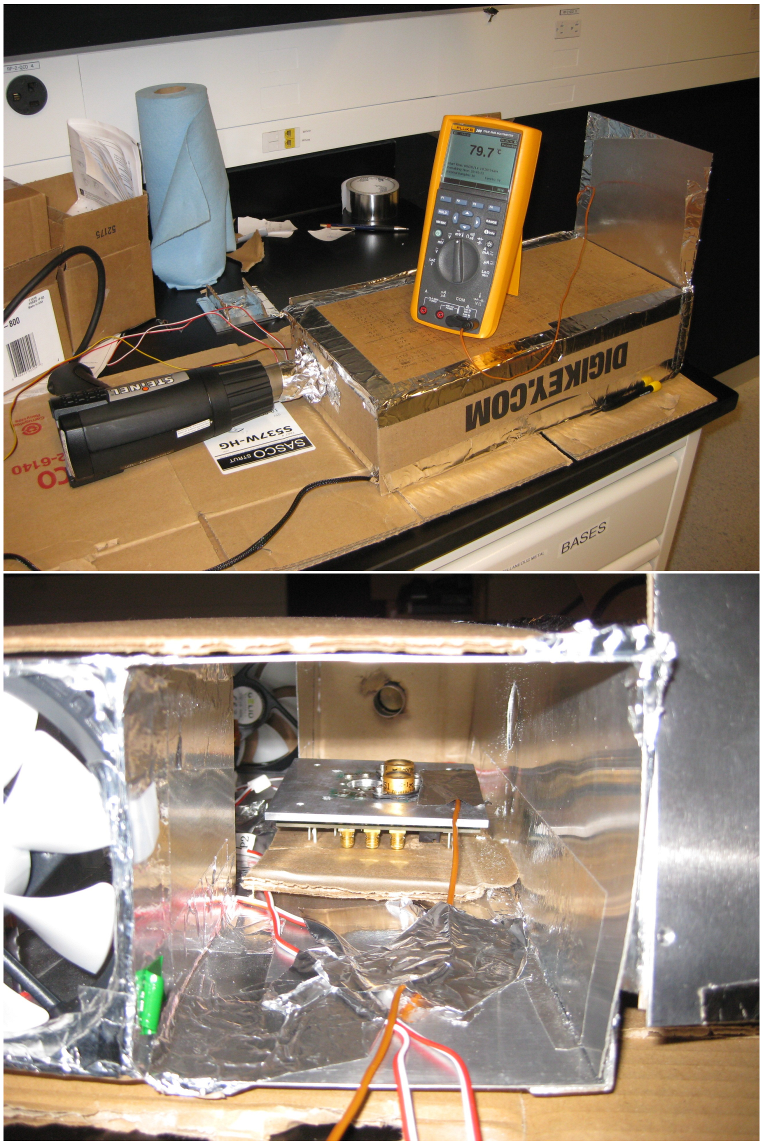


Figure 8.10: Setup for thermal annealing of a group of APDs

Upper figure, our convection oven; lower figure, an APD group placed inside the oven, thermocouple sensor attached to the aluminum group plate.

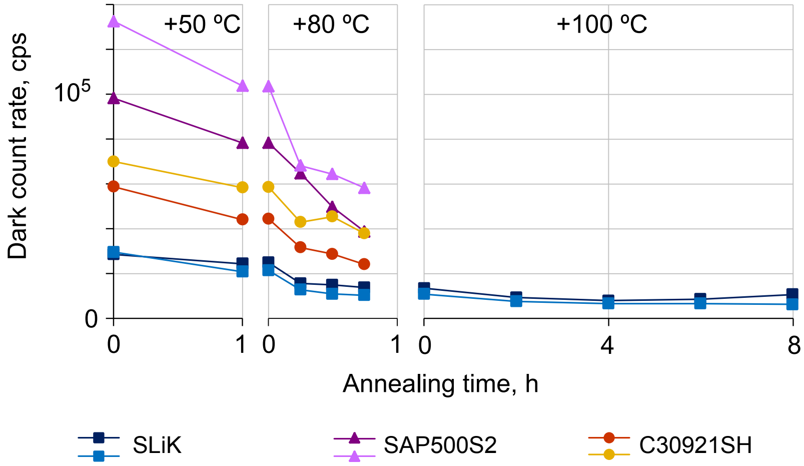


Figure 8.11: Thermal annealing of APDs from group 3

DCRs measured at −20 °C after annealing of APDs from group 3 at +50 °C over 1 h, at +80 °C over 45 min, and for SLiK samples after further annealing at +100 °C over 8 h. DCRs of all APDs decrease significantly during 45 minutes of +80 °C annealing, and continue to decrease for a SLiK during +100 °C annealing, through the DCR of one of the two SLiKs increased during last 4 hours.

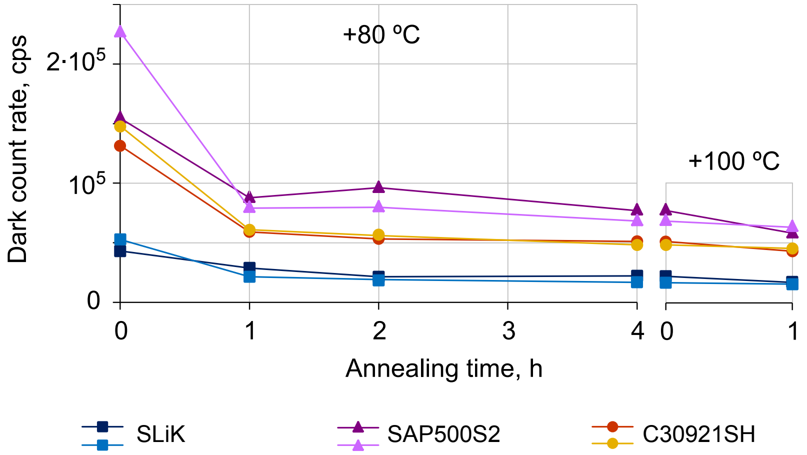


Figure 8.12: Thermal annealing of APDs from group 4

DCRs measured at −20 °C after annealing of APDs from group 4 at +80 °C over 4 h, followed by annealing at +100 °C over 1 h. The most significant decrease of DCRs for all APDs occurred during the first hour of +80 °C annealing, but DCRs still continued to improve with additional annealing.

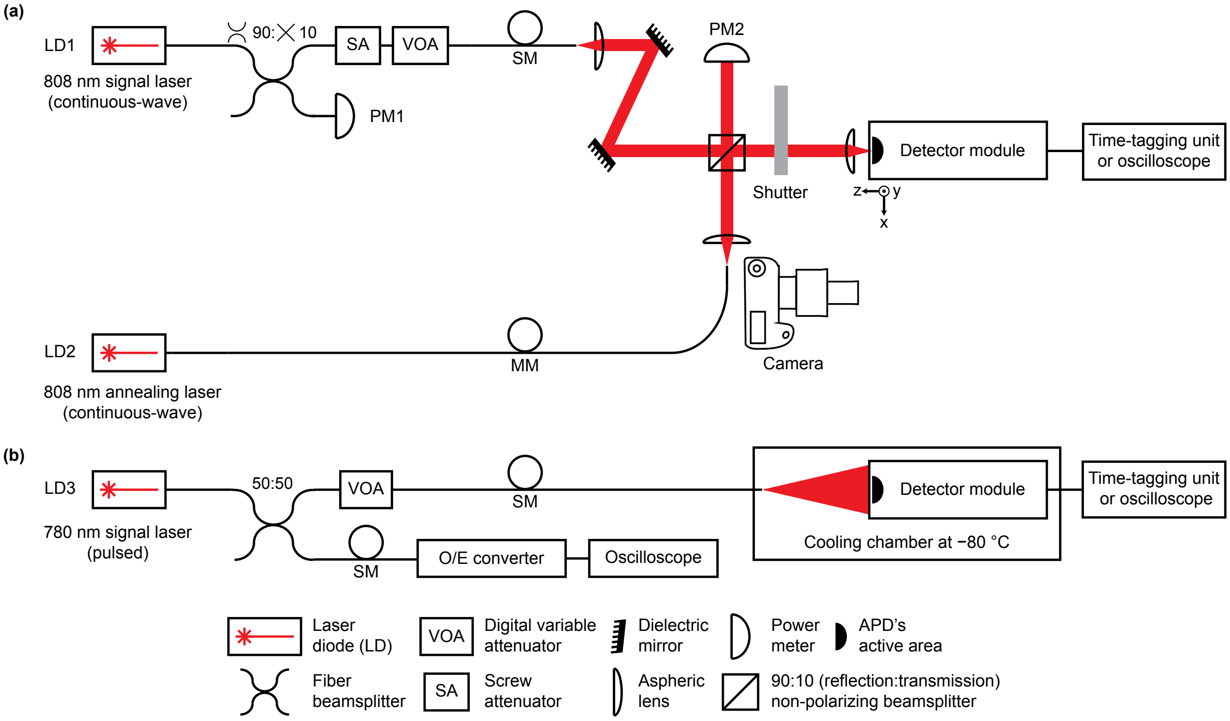


Figure 8.13: Experimental setup.

(a) Setup for laser annealing and characterization at room temperature. (b) Setup for characterization at −80 °C. SM: single-mode optic fiber; MM: multi-mode optic fiber; O/E: optical-to-electrical. (Figure is re-printed from [108]).

8.6.3 Laser annealing

It was shown in [156] that laser annealing can decrease DCR of non-irradiated APDs by up to 5.4 times.

We performed laser annealing (the project was led by Jin Gyu Lim) on nine irradiated APDs (see Table 8.3) and demonstrated a significant improvement in DCRs for all samples [108]. Our experiment demonstrated an advantage of laser annealing over thermal annealing of APDs for reducing DCR, also we obtained a good results of the laser annealing of thermally pre-annealed APDs, as their DCRs was reduced farther more.

Experimental setup for laser annealing and characterization of tested samples is shown in Fig. 8.13. The samples under test were placed in the module, that was moved between annealing and characterization setups for characterization after each step of annealing. The laser annealing setup shown in Fig. 8.13(a) is an updated version of the setup used in [156]. APD samples were inserted in a detector group

Table 8.3: Summary of detector samples, applied radiation, previous thermal annealing, and measured results of laser annealing. (*Table is re-printed from* [108].)

Sample ID	106 MeV proton fluence (cm^{-2})	Equivalent time in 600 km polar orbit (months)	Thermal annealing procedure	Dark count rate at -80 °C				Annealing power (W)	V_{excess} (V)
				Before (Hz)	Lowest after (Hz)	Highest reduction factor	Typical for pre-radiation (Hz)		
C30902SH-1	10^9	6	None	347	2.3	150	~ 5	0.8	14
C30902SH-2	10^9	6	None	363	2.64	137		1.5	14
SLiK-1	10^8	0.6	2 h @ +100 °C	6.71	0.16	41.7	< 1	1.4	14
SLiK-2	10^8	0.6	2 h @ +100 °C	2.19	0.42	5.3		0.8	14
SLiK-3	4×10^9	24	4 h @ +80 °C, 2 h @ +100 °C	43.1	2.09	21		1.4	14
SLiK-4	10^9	6	None	192	8.3	23		1.0	20
SLiK-5	4×10^9	24 (applied bias voltage)	3 h @ +80 °C, 2 h @ +100 °C	447	58	7.7		1.0	20
SAP500S2-1	4×10^9	24	4 h @ +80 °C, 2 h @ +100 °C	1579	2.08	758	~ 2	1.4	20
SAP500S2-2	10^8	0.6	2 h @ +100 °C	213	1.66	128		1.6	20

plate used for radiation experiment (see Fig. 8.1), which could be moved between the laser annealing and characterization setups. Two 808 n lasers LD1 (signaling) and LD2 (annealing) are overlapped in a purpose, that two lasers beams would be focused at the same spot. Then we could adjust position of a tested APD, checking it with the low power laser LD1, and the high-power laser beam from LD2 will be focused at the same point on the APD's active area. LD1 also served for measuring SLiKs' photon detection efficiency, done in-situ. The detector module is mounted on an XYZ translation stage, which can move between the laser annealing setup and a camera. The free-space part of the setup is black-outed.

For APDs' characterization we measured DCR, relative changes in photon efficiency, afterpulsing probability and timing jitter. For afterpulsing analysis we used the method described in Chapter 4. As all the irradiated APDs demonstrated so high DCR that their electronic circuits were saturated, we characterized them at −80 °C, see our characterization setup in Fig. 8.13(b). SLiKs have an in-built thermoelectric cooler (TEC) and a thermistor, thus they could be characterized in our laser-annealing setup at −30 °C as well. All APDs were characterized at 20 V above breakdown, as other characterizations in the radiation test were done. For characterization we used a 780 nm laser LD3. Single photon detection efficiency was measured in a relative way, similarly to described in Section 8.3 and other characterization parameters were also measured similarly to Section 8.3.

Laser annealing was done in a step-wise manner: 60 s of annealing was followed by 60 s of cooling down at room temperature before characterization. Two APDs SLik-4 and SLiK-5 were annealed by a single laser shot of 1 W power, to test if the step-wise process was different from a single annealing event.

The main result of laser annealing was a dramatic decrease of DCR, see results represented in the Table 8.3. The maximum DCR decrease for SLiKs was from 5.3 to 41.7 times at −80 °C. SliKs annealed by one-shot laser power demonstrated similar results as SLiKs annealed with the step-wise method. For C30902SH the maximum DCR reduction was from 137 to 150 times at −80 °C. Also, there was no difference in effects observed between a single laser shot and step-wise annealing methods. For SAP500S2 the maximum DCR reduction was 128 and 758 times.

For detailed results of APDs characterization see [108]. In summary, detection efficiency did not change notably for SLiKs and C30921SHs, but changed depending on annealing laser power for SAP500S2s. Note that SAP500S2 found to withstand much less laser power before destruction. Afterpulsing increased after laser annealing in SLiKs and C30921SH samples, through decreased in SAP500S2. But the last ones showed a very high afterpulsing at −80 °C even before irradiation, and after laser annealing their afterpulsing was of orders of magnitudes higher than for SLiKs and C30921SHs.

8.7 Discussion and conclusion

We have conducted radiation tests of 32 APD (Excelitas and Laser Components) and 4 PMT (Hamamatsu) SPD devices, with radiation levels equivalent to lifetimes in low-Earth 600 km polar orbit of 0.6 months, 6 months, 12 months and 24 months. Our performance characterization measurements showed a significant increase in DCRs for all APD devices, while there was no measurable radiation-induced degradation in the photon detection efficiency and timing jitter, and only a small increase in the afterpulsing probability.

All APD samples demonstrated a significant increase in DCR due to radiation exposure, increasing the DCR by many orders of magnitude, well above the maximum 200 cps or so required for quantum communications tasks. Subsequently, we have experimentally demonstrated that radiation damage can be successfully mitigated by sufficient cooling. For Excelitas SLiK devices, cooling to −86 °C was sufficient to restore the DCR to below the 200 cps level that would make quantum communications possible, even after 24-month-equivalent radiation dose.

Further DCR reduction (while preserving other performance properties) was obtained through thermal annealing. APD devices were heated at +50 to +100 °C over a few hours, in the best case resulting in a DCR only 0.15 times that prior to annealing. It is worth noting that this approach can reduce the amount of cooling power required to reach the targeted low DCR—e.g., following annealing, the SLiK APDs could achieve the target DCR of 200 cps at about −70 °C, 16 °C higher than prior to annealing. Thermal annealing at +80 to +100 °C seems to be the most effective, but some additional tests are required to optimize the thermal annealing for radiation damaged APDs.

Results from the PMT samples indicated a small (but still noticable) degradation in DCR and almost no degradation in any other measured property (efficiency, timing jitter, and afterpulsing probability) after applied radiation. This makes them a tantalizing candidate, particularly for optical inter-satellite communication applications. However, as their peak efficiency is at wavelengths where atmospheric losses are higher, they remain less interesting for ground–satellite links.

We note that, while thermal annealing is effective at reducing DCRs of APDs, the coarse method of oven-heating devices can be time and energy consuming. Alternative, more directed approaches such as laser annealing [108] could be beneficial under a limited power budget of a satellite platform.

Our measurements correspond to the case where an APD is embedded on an orbiting satellite for up to two years prior to thermal or laser annealing being applied. In a real satellite mission, either of annealing methods could be applied intermittently and at regular intervals through a mission's lifetime. We speculate that doing so could repair some of the radiation-induced damage soon after it is created, thereby keeping the DCR low, delaying the necessity of deeper cooling, and extending detector lifetimes. Implementing thermal or laser annealing and cooling on APDs can extend their lifetime up to 10 years, until performance of QKD protocol will be lowered down to zero key rate. Experimental tests of the effect of multiple irradiation and annealing cycles shall be performed in the near future.

Chapter 9

Conclusion and outlook

Long distance quantum communications and a global quantum network are getting priority projects in many countries around the world. The quantum network can be used for QKD to provide unconditional level of security. Many researches has been done on the way of improving security of QKD implementations and increasing distances of quantum communications. My thesis contributes to this research by covering novel and unexplored regimes relevant to commercial QKD on one hand, and the development of a satellite based QKD system on the other hand.

My first project was participation in a security test of Clavis2 QKD system [89]. Though the result of our experiment demonstrated security of the Clavis2 system against a straightforward Trojan-horse attack thanks to afterpulsing effect in APDs, it led to a following research [84] demonstrated that at the wavelength of 1924 nm the attack can be successful and some countermeasures have to be realized in the system.

In the later projects during my thesis I placed my efforts mostly on the development of SPDs suitable for long distance quantum communications or over high loss channels. One of the projects described in this thesis was dedicated to quantum teleportation through 144 km free-space channel [33], that was a big achievement at that time. My contribution to the project was building SPDs with unique parameters, very low DCR combined with compact size and relatively low price, that made our detectors excellent candidates for that project.

Long distance quantum communications proved feasibility of ground-to-satellite quantum communications, because the losses of an on-ground long distance quantum channel are similar or even higher than of a ground-to-LEO satellite link [56]. Global satellite based quantum network is economically more beneficial than a fiber-based ground quantum network, since it does not need so many trusted-nod stations requiring service and protection for security. The first quantum satellites are already launched by China [37–39] and Singapore [157, 158], and a first satellite based quantum network was demonstrated with the Chinese satellite [52]. A Canadian quantum satellite mission (Canada's Quantum Encryption and Science Satellite (QEYSSat)) is planned launching in approximately 2020, and preparation work is in progress. That satellite will have less functionality than Chinese Micius mission, however it will be less complex system with smaller mass of 60–80 kg compared to the reported 635 kg for Micius.

Two of my later projects were specifically about building and testing SPDs for long distance quantum communications in space. One was a four-channel prototype for Canadian quantum satellite, it was implemented in the Air-borne experiment [132] (the project in frame of preparation for QEYSSat) of a demonstration of QKD between a ground station and a flying Aircraft. The four-channel detector prototype developed for this project has very light weight and long life time in radiation environment. Our detector prototype worked flawlessly during the experiment and the next generation prototype is already under development in IQC. The second project was about building an improved version of SPDs used in the teleportation experiment, with very low noise, that could be used in future experiments with free space long distance quantum communications.

To meet very special requirements to be space qualified, SPDs must pass an evaluation including tests for their mechanical hardness and thermo-vacuum construction, and radiation test. My last project was about the radiation testing of APDs and PMTs potentially suitable for QEYSSat, and finding possible methods for mitigating radiation damage to extend life time of the detectors in space and therefore, life time of the mission. I was able to show that thermal annealing, cooling, and laser annealing were all very effective in decreasing DCR of irradiated APDs. Comparing to other recent projects about APDs radiation tests and mitigating radiation damage [159] in our experiment we implemented deeper cooling decreasing DCR of APDs down to pre-radiation level, and implemented laser annealing that was not used before for this purpose. Interesting to note that radiation increased afterpulsing rate of the irradiated APDs, the effect has not being described previously. Now our group is working on implementing laser annealing in the quantum satellite prototype in frame of other projects towards Canadian quantum satellite.

References

[1] Frank Miller. Telegraphic code to insure privacy and secrecy in the transmission of telegrams. *C. M. Cornwell*, 1882.

[2] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.*, 45:109–115, 1926.

[3] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:656–715, 1949.

[4] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[5] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3):172–198, Mar 1927.

[6] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

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

[8] Wolfgang Tittel, Gregoire Ribordy, and Nicolas Gisin. Quantum cryptography. *Physics World*, 11(3):41–5, 1998.

[9] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3–28, 1992.

[10] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, 2000.

[11] A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[12] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869, 1995.

[13] Norbert Ltkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1), 2002.

[14] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, 2003.

[15] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92(5):057901, 2004.

[16] X.-B. Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A*, 72(1):012322, 2005.

[17] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, 2005.

[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, 2002.

[19] Hai-Qiang Ma, Jian-Ling Zhao, and Ling-An Wu. Quantum key distribution based on phase encoding and polarization measurement. *Opt. Lett.*, 32(6):698–700, Mar 2007.

[20] kyo Inoue, Yuuki Iwai, Tatsuya Kukita, and Toshimori Honjo. Differential-quadrature-phase-shift (dqps) quantum key distribution. *Lasers and Electro-Optics, Conference on Quantum electronics and Laser Science Conference. CLEO/QELS 2009*, Dec 2009.

[21] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.*, 82:2594–2597, Mar 1999.

[22] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Phys. Rev. A*, 66:062304, Dec 2002.

[23] Mario Martinelli. Time reversal for the polarization state in optical systems. *Journal of Modern Optics*, 39(3):451–455, 1992.

[24] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "Plug and play" systems for quantum cryptography. *Appl. Phys. Lett.*, 70(7):793–795, 1997.

[25] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel. Interferometry with Faraday mirrors for quantum cryptography. *Electron. Lett.*, 33(7):586–588, 1997.

[26] Bell L. S. On the einstein podolsky rosen paradox. *Physics*, 1:195–200, 1964.

[27] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[28] C. H. Bennett. Quantum cryptography using any 2 nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992.

[29] C. H. Bennett and D. P DiVincenzo. Quantum information and computation. *Nature*, 404:247–255, 2000.

[30] Guido Berlín, Gilles Brassard, Félix Bussières, and Nicolas Godbout. Fair loss-tolerant quantum coin flipping. *Phys. Rev. A*, 80:062321, 2009.

[31] C Bonato, A Tomaello, V Da Deppo, G Naletto, and P Villoresi. Feasibility of satellite quantum key distribution. *New J. Phys.*, 11(4):045017, 2009.

[32] Guido Berlín, Gilles Brassard, Félix Bussières, Nicolas Godbout, Joshua A. Slater, and Wolfgang Tittel. Experimental loss-tolerant quantum coin flipping. *Nat. Commun.*, 2:561, 2011.

[33] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, Vadim Makarov, Thomas Jennewein, Rupert Ursin, and Anton Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489:269, 2012.

[34] Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, and Eleni Diamanti. Experimental plug and play quantum coin flipping. *Nat. Commun.*, 5:3717, 2014.

[35] Hoi-Kwong Lo, Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nat. Photon.*, 8:595–604, 2014.

[36] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X*, 6:011024, Mar 2016.

[37] 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, Kui-Xing Yang, Xuan Han, Yong-Qiang Yao, Ji Li, Hai-Yan Wu, Song Wan, Lei Liu, Ding-Quan Liu, Yao-Wu Kuang, Zhi-Ping He, Peng Shang, Cheng Guo, Ru-Hua Zheng, Kai Tian, Zhen-Cai Zhu, Nai-Le Liu, Chao-Yang Lu, Rong Shu, Yu-Ao Chen, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key teleportation. *Nature*, 549:70–73, 2017.

[38] 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, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549:43–47, 2017.

[39] 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, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[40] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.

[41] R. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[42] Matteo Mariantoni, H. Wang, T. Yamamoto, M. Neeley, Radoslaw C. Bialczak, Y. Chen, M. Lenander, Erik Lucero, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, Y. Yin, J. Zhao, A. N. Korotkov, A. N. Cleland, and John M. Martinis. Implementing the quantum von neumann architecture with superconducting circuits. *Science*, 334(6052):61–65, 2011.

[43] Nicola Jones. Computing: The quantum company. *Nature*, 498:61–65, 2013.

[44] Simon J. Devitt. Performing quantum computing experiments in the cloud. *Phys. Rev. A*, 94:032329, Sep 2016.

[45] Rafael N. Alexander, Pei Wang, Niranjan Sridhar, Moran Chen, Olivier Pfister, and Nicolas C. Menicucci. One-way quantum computing with arbitrarily large time-frequency continuous-variable cluster states from a single optical parametric oscillator. *Phys. Rev. A*, 94:032327, Sep 2016.

[46] Adrian Hutter and Daniel Loss. Quantum computing with parafermions. *Phys. Rev. B*, 93:125105, Mar 2016.

[47] S. and Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe. Demonstration of a small programmable quantum computer with atomic qubits. *Nature*, 536:63–66, 2016.

[48] M Saffman. Quantum computing with atomic qubits and rydberg interactions: progress and challenges. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 49(20):202001, 2016.

[49] M. Hebenstreit, D. Alsina, J. I. Latorre, and B. Kraus. Compressed quantum computation using a remote five-qubit quantum computer. *Phys. Rev. A*, 95:052339, May 2017.

[50] S. Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Four Estate, London, 1999.

[51] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549:188–194, 2017.

[52] Binglin Chen. China completes first part of a 'quantum internet'. *Physics World*, 30(1):10, 2017.

[53] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics*, 1(6):343–348, 2007.

[54] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016.

[55] Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, Xin-Dong Cai, Ping Xu, Ge-Sheng Pan, Jian-Jun Jia, Yong-Mei Huang, Hao Yin, Jian-Yu Wang, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature.*, 488:185–188, 2010.

[56] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New J. Phys.*, 15:023006, 2013.

[57] E. Gibney. Chinese satellite is one giant step for the quantum internet. *Nature*, 535:478–479, 2016.

[58] E. Gibney. Europes billion-euro quantum project takes shape. *Nature*, 545, 2017.

[59] R. H. Hadfield. Single-photon detectors for optical quantum information applications. *Nat. Photonics*, 3:696–705, 2009.

[60] E. E. Wollman, V. B. Verma, A. D. Beyer, R. M. Briggs, B. Korzh, J. P. Allmaras, F. Marsili, A. E. Lita, R. P. Mirin, S. W. Nam, and M. D. Shaw. Uv superconducting nanowire single-photon detectors with high efficiency, low noise, and 4 k operating temperature. *Opt. Express*, 25(22):26792–26801, Oct 2017.

[61] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93% system efficiency. *Nat. Photonics*, 7:210, 2013.

[62] Iman Esmaeil Zadeh, Johannes W. N. Los, Ronan B. M. 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.

[63] Visible Single-Photon Detector, https://marketing.idquantique.com/acton/attachment/11868/f-0236/1/-/-/-/-/ID100_Brochure.pdf, cited 17 Nobember 2017.

[64] ID230 Infrared Single-Photon Detector, https://marketing.idquantique.com/acton/attachment/11868/f-0234/1/-/-/-/-/ID230_Brochure.pdf, cited 17 Nobember 2017.

[65] Viacheslav Burenkov, He Xu, Bing Qi, Robert H. Hadfield, and Hoi-Kwong Lo. Investigations of afterpulsing and detection efficiency recovery in superconducting nanowire single-photon detectors. *Journal of Applied Physics*, 113(21):213102, 2013.

[66] K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren. Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. *Opt. Express*, 14(2):527–534, 2006.

[67] D. Rosenberg, A. J. Kerman, R. J. Molnar, and E. A. Dauler. High-speed and high-efficiency superconducting nanowire single photon detector array. *Opt. Express*, 21(2):1440–1447, Jan 2013.

[68] Varun B. Verma, Boris Korzh, Felix Bussieres, Robert D. Horansky, Shellee D. Dyer, Adriana E. Lita, Igor Vayshenker, Francesco Marsili, Matthew D. Shaw, Hugo Zbinden, Richard P. Mirin, and Sae Woo Nam. High-efficiency superconducting nanowire single-photon detectors fabricated from mosi thin-films. *Opt. Express*, 23, Dec 2015.

[69] G. A. Morton. Photomultipliersfor scintillation counting. *RCA Rev.*, 10:525–553, 1949.

[70] H. Kume, K. Koyama, A. Nakatsugawa, S. Suzuki, and D. Fatlowitz. Ultrafast microchannel plate photomultipliers. *Appl. Opt.*, 27:1170–1178, 1988.

[71] S. Cova, G. Ripamonti, and A. Lacaita. Avalanche semiconductor detector for single optical photons with a time resolution of 60 ps. *Nucl. Instrum. Methods A*, 253:482–487, 1987.

[72] S. Cova, A. Lacaita, M. Ghioni, and G. Ripamonti. 20-ps timing resolution with single-photon avalanche diodes. *Rev. Sci. Instrum.*, 60:1104, 1989.

[73] A. Lacaita, M. Ghioni, F. Zappa, G. Ripamonti, and S. Cova. Recent advances in the detection of optical photons with silicon photodiodes. *Nucl. Instrum. Methods A*, 326:290–294, 1993.

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

[75] Sergio Cova, Antonio Longoni, Alessandra Andreoni, and Rinaldo Cubeddu. A semiconductor detector for measuring ultraweak fluorescence decays with 70 ps fwhm resolution. *IEEE, J. of Quatum Electr.*, QE-19:630, 1983.

[76] S. Cova, A. Longoni, and A. Andreoni. Towards picosecond resolution with single-photon avalanche diodes. *Rev. Sci. Instrum.*, 52:408–412, 1981.

[77] Y.-S. Kim, Y.-C. Jeong, S. Sauge, V. Makarov, and Y.-H. Kim. Ultra-low noise single-photon detector based on si avalanche photodiode. *Rev. Sci. Instrum.*, 82:093110, 2011.

[78] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.*, 11(6):065001, 2009.

[79] L. Lydersen and J. Skaar. Security of quantum key distribution with bit and basis dependent detector flaws. *Quant. Inf. Comp.*, 10:60–76, 2010.

[80] H.-W. Li, Z.-Q. Yin, S. Wang, W.-S. Bao, G.-C. Guo, and Z.-F. Han. Security of quantum key distribution with state-dependent imperfections. *Quant. Inf. Comp.*, 11:0937–0947, 2011.

[81] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. After-gate attack on a quantum cryptosystem. *New J. Phys.*, 13:013043, 2011.

[82] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.*, 107:110501, 2011.

[83] Mu-Sheng Jiang, Shi-Hai Sun, Chun-Yan Li, and Lin-Mei Liang. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys. Rev. A*, 86:032310, 2012.

[84] Shihan Sajeed, Carter Minshull, Nitin Jain, and Vadim Makarov. Invisible trojan-horse attack. *Sci. Rep.*, 7:8403, 2017.

[85] A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *J. Mod. Opt.*, 48(13):2023–2038, 2001.

[86] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73(2):022320, 2006.

[87] C. Branciard, N. Gisin, B. Kraus, and V. Scarani. Security of two quantum cryptography protocols using the same four qubit states. *Phys. Rev. A*, 72(3):032301, 2005.

[88] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74(2):022313, 2006. erratum ibid. **78**, 019905 (2008).

[89] Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.*, 16:123030, 2014.

[90] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, 4:41–41, 2002.

[91] R. H. Haitz. Mechanisms contributing to the noise pulse rate of avalanche diodes. *J. Appl. Phys.*, 36:3123–3131, 1965.

[92] Olivier Landry, J. A. W. van Houwelingen, Alexios Beveratos, Hugo Zbinden, and Nicolas Gisin. Quantum teleportation over the swisscom telecommunication network. *J. Opt. Soc. Am. B*, 24(2):398–403, 2007.

[93] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek,

B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nat. Phys.*, 3(7):481–486, 2007.

[94] Thomas Scheidl, Rupert Ursin, Johannes Kofler, Sven Ramelow, Xiao-Song Ma, Thomas Herbst, Lothar Ratschbacher, Alessandro Fedrizzi, Nathan K. Langford, Thomas Jennewein, and Anton Zeilinger. Violation of local realism with freedom of choice.

[95] Xian-Min Jin, Ji-Gang Ren, Bin Yang, Zhen-Huan Yi, Fei Zhou, Xiao-Fan Xu, Shao-Kai Wang, Dong Yang, Yuan-Feng Hu, Shuo Jiang, Tao Yang, Hao Yin, Kai Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Experimental free-space quantum teleportation. *Nat. Photon.*, 4(46):376–381, 2010.

[96] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical bell-state analyzer. *Applied Physics B*, 72(1):67–71, Jan 2001.

[97] Yoon-Ho Kim, Sergei P. Kulik, Maria V. Chekhova, Warren P. Grice, and Yanhua Shih. Experimental entanglement concentration and universal bell-state synthesizer. *Phys. Rev. A*, 67:010301, Jan 2003.

[98] H. S. Poh, J. Lim, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. Eliminating spectral distinguishability in ultrafast spontaneous parametric down-conversion. *Phys. Rev. A*, 80:043815, 2009.

[99] 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. *J. Lightwave Technol.*, 31(9):1399–1408, May 2013.

[100] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.*, 89(10):101122, 2006.

[101] Thomas Scheidl, Rupert Ursin, Alessandro Fedrizzi, Sven Ramelow, Xiao-Song Ma, Thomas Herbst, Robert Prevedel, Lothar Ratschbacher, Johannes Kofler, Thomas Jennewein, and Anton Zeilinger. Feasibility of 300km quantum key distribution with entangled states. *New Journal of Physics*, 11(8):085002, 2009.

[102] Xiao song Ma, Sebastian Kropatschek, William Naylor, Thomas Scheidl, Johannes Kofler, Thomas Herbst, Anton Zeilinger, and Rupert Ursin. Experimental quantum teleportation over a high-loss free-space channel. *Opt. Express*, 20(21):23126–23137, Oct 2012.

[103] A. Yoshizawa, R. Kaji, and H. Tsuchida. Quantum efficiency evaluation method for gated-mode single-photon detector. *Electron. Lett.*, 38(23):1468–1469, 2002.

[104] A. C. Giudice, M. Ghioni, S. Cova, and F. Zappa. A process and deep level evaluation tool: afterpulsing in avalanche junctions. In *European Solid-State Device Research, 2003. ESSDERC '03. 33rd Conference, Estoril, Portugal*, pages 347–350, 2003.

[105] Mark A. Itzler, Xudong Jiang, and Mark Entwistle. Power law temporal dependence of ingaas/inp spad afterpulsing. *J. Mod. Opt.*, 59:1472, 2012.

[106] G. Humer, M. Peev, C. Schaeff, S. Ramelow, M. Stipčević, and R. Ursin. A simple and robust method for estimating afterpulsing in single photon detectors. *J. Lightwave Technol.*, 33(14):3098–3107, 2015.

[107] S. Cova, A. Lacaita, and G. Ripamonti. Trapping phenomena in avalanche photodiodes on nanosecond scale. *IEEE Electron Device Lett.*, 12(12):685–687, 1991.

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

[109] G. Gilbert and M. Hamrick. Practical quantum cryptography: A comprehensive analysis (part one). Tech. rep. mtr00w0000052, The MITRE Corporation, 2000.

[110] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Daylight quantum key distribution over 1.6 km. *Phys. Rev. Lett.*, 84:5652–5655, Jun 2000.

[111] J. G. Rarity, P. C. M. Owens, and P. R. Tapster. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.*, 4, 2002.

[112] J. E. Nordholt, Richard J. Hughes, George L. Morgan, C. Glen Peterson, and Christopher C. Wipf. Present and future free-space quantum key distribution.

In *Proc. of SPIE on Free-Space Laser Communication Technologies*, volume 4635, pages 116–126, 2002.

[113] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lütkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, Weinfurter, H., Zukowski, M., and Zeilinger, A. Space-quest, experiments with quantum entanglement in space. *Europhys. News*, 40(3):26–29, 2009.

[114] 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. *Phys. Rev. A*, 84:062326, Dec 2011.

[115] B. L. Higgins, J.-P. Bourgoin, N. Gigov, E. Meyer-Scott, Z. Yan, and T. Jennewein. Detailed performance analysis of the proposed qeyssat quantum receiver satellite. In *Conf. on Lasers and Electro-Optics JW4A.118*, 2012.

[116] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283, 1998.

[117] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.*, 4:43, 2002.

[118] C Erven, B Heim, E Meyer-Scott, J P Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New J. Phys.*, 14(12):123018, 2012.

[119] Yue Chuan Tan, Rakhitha Chandrasekara, Cliff Cheng, and Alexander Ling. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *Opt. Express*, 21:16946, 2013.

[120] E. Anisimova, D. Nikulov, S. S. Hu, M. Bourgon, R. Ursin, T. Jennewein, and V. Makarov. Low-noise single-photon detectors for long-distance free-space quantum communication. in preparation; preliminary results presented

at QCrypt 2015 in Tokyo, Japan and Single Photon Workshop 2015 in Geneva, Switzerland.

[121] http://www.idquantique.com/photon-counting/photon-counting-modules/id100/, cited 18 September 2017. ID100VIS data sheet.

[122] http://www.idquantique.com/photon-counting/photon-counting-modules/id120/, cited 18 September 2017. ID120VIS data sheet.

[123] R. H. Haitz. Model for the electrical behavior of a microplasma. *J. Appl. Phys.*, 35:1370–1376, 1964.

[124] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *J. Mod. Opt.*, 51(9):1267–1288, 2004.

[125] Radiated power from blackbody, http://hyperphysics.phy-astr.gsu.edu/hbase/quantum/radfrac.html, visited 29 Nobember 2017.

[126] the origin of this effect is that at higher temperature, larger semiconductor lattice vibrations lead to higher nonelastic collision probability with carriers [160]. The carriers that collide with the lattice more often need higher electric field to gain sufficient energy for ionization (to generate more carriers and sustain avalanche). This leads to higher breakdown voltage [91, 123, 124].

[127] http://www.excelitas.com/downloads/DTS_C30902_C30921.pdf, cited 19 September 2017. C309XX-SH data sheet.

[128] http://www.excelitas.com/Downloads/DTS_SPCM-AQRH.pdf, cited September 2017. SPCM-AQRH data sheet.

[129] A. Lacaita, M. Ghioni, F. Zappa, G. Ripamonti, and S. Cova. Photon-assisted avalanche spreading in reach-through photodiodes. *Appl. Phys. Lett.*, 62:606, 1993.

[130] A. Spinelli and A. L. Lacaita. Physics and numerical simulation of single photon avalanche diodes. *IEEE Trans. Electron Devices*, 44(11):1931–1943, 1997.

[131] A. Lacaita, S. Cova, A. Spinelli, and F. Zappa. Observation of avalanche propagation by multiplication assisted diffusion in p-n junctions. *Appl. Phys. Lett.*, 57:489–491, 1990.

[132] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein. Airborne demonstration of a quantum key distribution receiver payload. Quantum Sci. Technol. (in press).

[133] 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. *Phys. Rev. A*, 92:052339, 2015.

[134] Pugh C. J. et al. A fine pointing system suitable for quantum communications on a satellite. *In preparation.*

[135] B. E. Schutz, H. J. Zwally, C. A. Shuman, D. Hancock, and J. P. DiMarzio. Overview of the ICESat mission. *Geophys. Rev. Lett.*, 32:L21S01, November 2005.

[136] 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. *J. Mod. Optic*, 51:1333, 2004.

[137] P. Lecoq. *Scintillation Detectors for Charged Particles and Photons*, pages 45–71. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[138] Ivan Prochazka and Fumin Yang. Photon counting module for laser time transfer via earth orbiting satellite. *J. Mod. Optic*, 56(2-3):253–260, 2009.

[139] S. K. Joshi, J. Pienaar, T. C. Ralph, L. Cacciapuoti, W. McCutcheon, J. Rarity, D. Giggenbach, V. Makarov, I. Fuentes, T. Scheidl, E. Beckert, M. Bourennane, D. E. Bruschi, A. Cabello, J. Capmany, J. A. Carrasco, A. Carrasco-Casado, E. Diamanti, M. Dušek, D. Elser, A. Gulinatti, R. H. Hadfield, T. Jennewein, R. Kaltenbaek, M. A. Krainak, H.-K. Lo, Ch. Marquardt, P. Mataloni, G. Milburn, M. Peev, A. Poppe, V. Pruneri, R. Renner, C. Salomon, J. Skaar,

N. Solomos, M. Stipčević, J. P. Torres, M. Toyoshima, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, A. Zeilinger, M. Żukowski, and R. Ursin. Space QUEST mission proposal: experimentally testing decoherence due to gravity.

[140] Xiaoli Sun, Daniel Reusser, Henri Dautet, and James B. Abshire. Measurement of proton radiation damage to Si avalanche photodiodes. *IEEE Trans. Electron. Devices*, 44:2160, 1997.

[141] Xiaoli Sun and Henri Dautet. Proton radiation damage of Si APD single photon counters. In *Proc. of IEEE Radiation Effects Data Workshop 2001*, page 146, 2001.

[142] M. Marisaldi, P. Maccagnani, F. Moscatelli, C. Labanti, F. Fuschino, M. Prest, A. Berra, D. Bolognini, M. Ghioni, I. Rech, A. Gulinatti, A. Giudice, G. Simmerle, D. Rubini, A. Candelori, and S. Mattiazzo. Single photon avalanche diodes for space applications. In *Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC), 2011 IEEE*, pages 129–134, 2011.

[143] Francesco Moscatelli, Martino Marisaldi, Piera Maccagnani, Claudio Labanti, Fabio Fuschino, Michela Prest, Alessandro Berra, Davide Bolognini, Massimo Ghioni, Ivan Rech, Angelo Gulinatti, Andrea Giudice, Georg Simmerle, Andrea Candelori, Serena Mattiazzo, Xiaoli Sun, John F. Cavanaugh, and Danilo Rubini. Radiation tests of single photon avalanche diode for space applications. *Nucl. Instr. and Meth., A*, 711:65 – 72, 2013.

[144] George C Messenger and Milton S Ash. The effects of radiation on electronic systems, 1986.

[145] J.R. Srour and J.M. McGarrity. Radiation effects on microelectronics in space. *Proc. IEEE*, 76:11, 1988.

[146] A. H. Johnston. Radiation damage of electronic and optoelectronic devices in space. In *The 4th Int. Workshop on Radiation Effects on Semiconductor Devices for Space Application*, 2000.

[147] J. R. Srour and D. H. Lo. Universal damage factor for radiation-induced dark current in silicon devices. *IEEE Trans. Nucl. Sci.*, 47(6):2451–2459, 2000.

[148] C. J. Dale, L. Chen, P. J. McNulty, P. W. Marshall, and E. A. Burke. A comparison of monte carlo and analytic treatments of displacement damage in si microvolumes. *IEEE Trans. Nucl. Sci.*, 41(6):1974–1983, 1994.

[149] Heidi N. Becker, Tetsuo F. Miyahira, and Allan H. Johnston. The influence of structural characteristics on the response of silicon avalanche photodiodes to proton irradiation. *IEEE Trans. Nucl. Sci.*, 50(6):1974–1981, 2003.

[150] E. Anisimova, D. Nikulov, S. S. Hu, M. Bourgon, R. Ursin, T. Jennewein, and V. Makarov. Low-noise single-photon detector for long-distance free-space quantum communication. in preparation.

[151] Excelitas SPCM-AQRH-TR timing resolution optimised single photon counting module, http://www.excelitas.com/Downloads/DTS_SPCM-AQRH-TR.pdf, visited 15 May 2017.

[152] M. Stipčević, D. Wang, and R. Ursin. Characterization of a commercially available large area, high detection efficiency single-photon avalanche diode. *J. Lightwave Technol.*, 31(23):3591–3596, 2013.

[153] R. K. Schaefer, L. J. Paxton, C. Selby, B. Ogorzalek, G. Romeo, B. Wolven, and S.-Y. Hsieh. Observation and modeling of the South Atlantic Anomaly in low Earth orbit using photometric instrument data. *Space Weather*, 14(5):330–342, 2016.

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

[155] Alexei Trifonov, Darius Subacius, Audrius Berzanskis, and Anton Zavriyev. Single photon counting at telecom wavelength and quantum key distribution. *J. Mod. Opt.*, 51(9-10):1399, 2004.

[156] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M. Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov. Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.*, 112:070503, Feb 2014.

[157] Cliff Cheng, Rakhitha Chandrasekara, Yue Chuan Tan, and Alexander Ling. Space-qualified nanosatellite electronics platform for photon pair experiments. *J. of Lightwave Techn.*, 33:4799–4804, 2015.

[158] 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. *Phys. Rev. Appl.*, 5:054022, 2016.

[159] Yue Chuan Tan, Rakhitha Chandrasekara, Cliff Cheng, and Alexander Ling. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *Opt. Express*, 21:16946–16954, 2015.

[160] S. M. Sze and K. K. Ng. *Physics of semiconductor devices*. Wiley-Interscience, 2007.

Appendix A

Software for calculations of afterpulsing and traps life times

Our software for afterpulsing calculation and lifetime traps curve fitting was written in Python programming language. It consists of three parts: defaults.py, gui.py, functions.py.

A.1 defaults.py

```
# default conditions
a = 1.1
endtime = 1.0
start = 78.125*10**-12
numofdata = 1000000
maxbins = int(math.ceil(math.log(endtime/start)/math.log(a)))
resolution = 78.125*10**-12
```

A.2 functions.py

```
import csv
import math
import numpy as np
import os
import sys

import default as df

intpersec = 1 / df.resolution

# get intial conditions from filename
def extract (filename):
    noext = filename.split(".")[0]
    nopath = noext.split("/")[-1]
    conditions = nopath.split("_")
    others = []
    for i in range(len(conditions)):
        if i > 3:
            others.append(conditions[i])
        elif conditions[i][0].isalpha():
            model = conditions[i]
        elif conditions[i][-1] == ("C" or "c"):
            temp = conditions[i]
        elif conditions [i][-2] == "m":
            thres = conditions[i]
        elif conditions [i][-1] == ("V" or "v"):
            over = conditions[i]
    return noext, nopath, model, temp, over, thres

# reads file and stores data from second column into array
def parsedata (filename, number=0):
    num = 0
    data = []
    file = open(filename, 'r')
    for line in file:
        if number == 0:
            if not line.strip():
                continue
            else:
                data.append(float(line.split()[1]))
        elif num < number:
            if not line.strip():
                continue
            else:
                try:
                    # print "  first part %i %f", num, ...
                        line.split()[1]
                    data.append(float(line.split()[1]))
                except IndexError as ie:
                    print num, line.split()[1]
            num += 1
    file.close()
    return data

# finds the value to stop taking differences; makes sure last ...
   value is last difference in time interval (last first count)
def last (data, endtime):
    sums = 0
    num = 1
    last = len(data) - 1
    while sums < (endtime * intpersec):
        sums = data[last] - data[last - num]
        num += 1
    return last - num + 1

# get a from specified number of bins and maxbins from a
def geta(maxbins, start, endtime):
    return round(math.e**(math.log(endtime/start)/maxbins), 2)

def getmaxbins(a, start, endtime):
    return int(math.ceil(math.log(endtime/start)/math.log(a)))

# create bins actual values
def bins (maxbins, start, a):
    binslist = [0]
    for i in range(maxbins+1):
        binslist.append(start*a**i)
    return binslist

def binnum (num, start, a):
    if num == 0:
        number = 0
    elif math.floor(math.log(num/start)/math.log(a)) < 0:
        number = 0
    else:
        number = int(math.floor(math.log(num/start)/math.log(a))) ...
           + 1
    return number

# create new array of differences in each bin
def differences (lastnum, maxbins, data, start, a, endtime):
    num = 0
    difflist = [0] * (maxbins + 1)
    errors = []
    for i in range(lastnum+1):
        if (lastnum - i) % 1000 == 0:
            print lastnum - i
        j = 1
        while True:
            diff = data[i+j] - data[i]

            if diff < (5 * 10 ** -7)  * intpersec:
                print "diff error", i
                errors.append("%f, %f, %e" % (i, (i+j), (diff * ...
                    df.resolution)))
                j+=1
                continue

            if diff < (endtime * intpersec):
                num += 1
                try:
                    difflist[binnum(diff * df.resolution, start, ...
                       a)] += 1
                except ValueError, e:
                    #print "ValueError: %s, %i, %i, %f" % ...
                       (str(e), i, i+j, diff)
                    #print "Errors in Data File"
                    #return
                    #j += 1
                    break
                j += 1
            else:
                break
    return difflist, errors, num

# normalization of data
def norm (lastnum, maxbins, data, bins):
    normed = [0] * (maxbins+1)
    for num in range (0, maxbins+1):
        if data[num] == 0:
            normed[num] = 0
        else:
            normed[num] = data[num]/((bins[num+1] - bins[num]) * ...
               (lastnum + 1))
    return normed

```

```
# finding true dark counts using d as guideline for difference to ...
    stop
def dark(data, d, maxbins):
    num = 0
    sums = data[maxbins-1]
    for x in range(maxbins-2, 0, -1):
        diff = data[x] - data[x+1]
        if abs(diff) ≤ d:
            num += 1
            sums += data[x]
        else:
            num += 1
            break
    if num == 0:
        return 0
    else:
        return sums / num

# finding afterpulse probability
def area(dark, data, bins, maxbins):
    sums = 0
    sumsarray=[]
    array = []
    for x in range(maxbins+1):
        array.append(data[x] - dark)
    length = len(array)
    start = next(i for i in range(length) if (array[i] > 0))
    try:
        end = next(i for i in range(start+1, length) if ...
            (array[i+1] ≤ 0 and array[i+2] ≤ 0 and array[i+3] ≤ 0 ...
            and array[i+4] ≤ 0))
    except IndexError:
        #end = next(i for i in range(start+1, length) if ...
            (array[i+1] ≤ 0 and array[i+2] ≤ 0 and array[i+3] ≤ 0))
        end = next(i for i in range(start+1, length) if ...
            (array[i+1] ≤ 0 and array[i+2] ≤ 0))
    for y in range(start, end+1):
        sums += array[y] * (bins[y+1] - bins[y])
        sumsarray.append(sums)
    return sums, sumsarray, array

# taking logs of data
def log (data, maxbins):
    logged = [0] * (maxbins+1)
    for num in range(len(data)):
        if data[num] == 0:
            data[num] = 0
        else:
            logged[num] = math.log10(data[num])
            #print logged[num]
    return logged

# finding right x—axis labels; meaningful times: nanosecond, ...
   microsecond, millisecond, (0.5, 1, 10, 100), second, (1,2,3,4,5)
def time(timesinsec, start, a):
    num = []
    for x in timesinsec:
        if x == 0:
            num.append(0)
        else:
            num.append(math.log(x/start)/math.log(a) + 1)
    return num

# check if directory exists, if not then create
def makedirec(newdirec):
    if not os.path.exists(newdirec):
        os.makedirs(newdirec)

# write data to files
def writeto (filename, data):
    file = open(filename, "w")
    num = 1
    if data == []:
        file.write("No Errors")
    for x in data:
        file.write(str(num) + "\t" + str(x) + "\n")
        num += 1
    file.close()

def wwithnames (filename, data):
    file = open(filename, "w")
    for name in data.keys():
        if isinstance(data[name], dict):
            for d in data[name].keys():
                file.write(str(d) + "\t\t" + str(data[name][d]) + ...
                   "\n")
        elif isinstance(data[name], list):
            num = 1
            if data[name] == []:
                file.write(str(name) + "\t\t" + "None" + "\n")
            for x in data[name]:
                if num == 1:
                    file.write(str(name) + "\t\t" + str(num) + ...
                        "\t" + str(x) + "\n")
                else:
                    file.write("\t\t" + str(num) + "\t" + str(x) ...
                        + "\n")
                num += 1
        elif isinstance(data[name], np.ndarray):
            num = 0
            for x in data[name]:
                alphabet = "bcfghijklmn"
                if num == 0:
                    file.write(str(name) + "\t" + ...
                        str(alphabet[num]) + "\t" + str(x) + "\n")
                else:
                    file.write("\t\t" + str(alphabet[num]) + "\t" ...
                        + str(x) + "\n")
                num += 1
        else:
            file.write(str(name) + "\t\t" + str(data[name]) + "\n")
    file.close()

# writing data to table in csv format; if table exists then ...
   append, if not then create with headers
def writetable(rowdata, headers, path):
    if not os.path.isfile(path + "table.csv"):
        table  = open(path + "table.csv", "ab")
        writer = csv.writer(table)
        writer.writerow(headers)
        writer.writerow(rowdata)
        table.close()
    else:
        table  = open(path + "table.csv", "ab")
        writer = csv.writer(table)
        writer.writerow(rowdata)
        table.close()

# define functions to fit the data with; 1 - 5 exponents
def f1(x, start, a, d, b, c):
    return b * np.exp(-c * start *  a**x) + d

```

```
def f2(x, start, a, d, b, c, f, g):
    return b * np.exp(-c * start * a**x) + f * np.exp(-g * start ...
        * a**x) + d

def f3(x, start, a, d, b, c, f, g, h, i):
    return b * np.exp(-c * start * a**x) + f * np.exp(-g * start ...
        * a**x) + h * np.exp(-i * start * a**x) + d

def f4(x, start, a, d, b, c, f, g, h, i, j, k):
    return b * np.exp(-c * start * a**x) + f * np.exp(-g * start ...
        * a**x) + h * np.exp(-i * start * a**x) + j * np.exp(-k * ...
        start * a**x) + d

def f5(x, start, a, d, b, c, f, g, h, i, j, k, l, m):
    return b * np.exp(-c * start * a**x) + f * np.exp(-g * start ...
        * a**x) + h * np.exp(-i * start * a**x) + j * np.exp(-k * ...
        start * a**x) + l * np.exp(-m * start * a**x) + d
```

A.3 gui.py

```
import matplotlib
import math
matplotlib.use("TkAgg")
import matplotlib.pyplot as plt
from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg, ...
    NavigationToolbar2TkAgg
import numpy as np
import os
from scipy.optimize import curve_fit
import sys
import Tkinter as tk
import ttk
import tkFileDialog as filedialog

import default as df
import functions as fn

import logging

class printTerm(logging.Handler):
    def __init__(self, display):
        logging.Handler.__init__(self)
        self.display = display

    def write(self, s):
        self.display.configure(state=tk.NORMAL)
        self.display.insert("end", s)
        self.display.yview_pickplace("end")
        self.display.configure(state=tk.DISABLED)
        self.display.see(tk.END)
        self.display.update_idletasks()

class Program(ttk.Frame):

    def __init__(self, parent):
        self.myParent = parent
        self.myContainer = ttk.Frame(parent)

        self.myContainer.rowconfigure(0, weight=1)
        self.myContainer.rowconfigure(1, weight=1)
        self.myContainer.rowconfigure(2, weight=1)
        self.myContainer.rowconfigure(3, weight=1)
        self.myContainer.columnconfigure(1, weight=1)
        self.myContainer.pack(expand="yes", fill="both")

        self.fullfile = None
        self.conditions = None
        self.prgrun = False
        self.curverun = False
        self.plotcurve = False

        self.createWidgets()

    def createWidgets(self):
        self.createFile()
        self.createTerminal()
        self.createOptions()
        self.createGraphs()

    def createFile(self):
        files = ttk.Frame(self.myContainer)
        files.columnconfigure(1, weight=1)
        label = ttk.Label(files, text="Select a file to open:")
        entry = ttk.Entry(files)
        button = ttk.Button(files, text="Browse...", ...
           command=lambda e=entry : self.fileDialog(e))
        button2 = ttk.Button(files, text="Start", command=lambda ...
           : self.startInitial())

        label.grid(row=0, column=0)
        entry.grid(row=0, column=1, sticky="ew")
        button.grid(row=0, column=2)
        button2.grid(row=0, column=3)
        files.grid(sticky="ew")

    def fileDialog(self, entry):
        opts = {"initialfile": entry.get(),
                "filetypes": (("Text files", ".txt"),
                              ("All files", ".*"),)}
        opts["title"] = "Select a file to open..."
        self.fullfile = filedialog.askopenfilename(**opts)
        if self.fullfile:
            entry.delete(0, "end")
            entry.insert("end", self.fullfile)
        self.conditions = None
        self.md.delete(0, "end")
        self.ov.delete(0, "end")
        self.thr.delete(0, "end")
        self.tem.delete(0, "end")
        self.ad.delete(0, "end")
        self.startd.delete(0, "end")
        self.endd.delete(0, "end")
        self.maxd.delete(0, "end")
        self.numd.delete(0, "end")

    def startInitial(self):
        if self.fullfile:
            print "Starting Program ..."
            self.conditions = fn.extract(self.fullfile)
            self.path = os.path.dirname(self.fullfile) + os.sep
            self.filename = self.conditions[0]
            self.name = self.conditions[1]
            self.reset()
            print "File Opened"

    def createTerminal(self):
        disp = ttk.Labelframe(self.myContainer, text="Display")
        disp.grid(row=2, column=0, sticky="nsew")

        self.term = tk.Text(disp)
        self.term.pack(fill="both", expand="yes")
        sys.stdout = printTerm(self.term)
        sys.stderr = printTerm(self.term)

    def createOptions(self):
        opts = ttk.Labelframe(self.myContainer, text="Options")
        opts.grid(row=1, column=0, sticky="nsew")

        self.note = ttk.Notebook(opts)
        self.optsConditions()
        self.optsSave()
        self.optsCurve()
        self.note.pack(expand="yes", fill="both")

    def optsConditions(self):
        self.pg1 = ttk.Frame(self.note)
        self.note.add(self.pg1, text="Conditions")
        self.pg1.rowconfigure(0, weight=1)
        self.pg1.rowconfigure(1, weight=1)
        self.pg1.columnconfigure(0, weight=1)
        self.pg1.columnconfigure(1, weight=1)

        detector = ttk.Labelframe(self.pg1, text="Detector")
        detector.grid(columnspan=2, sticky="nsew")
        detector.rowconfigure(0, weight=1)
        detector.rowconfigure(1, weight=1)
        detector.columnconfigure(1, weight=1)
        detector.columnconfigure(3, weight=1)

        lbl1 = ttk.Label(detector, text="Model:")
        self.md = ttk.Entry(detector)
        lbl2 = ttk.Label(detector, text="Over Voltage:")
        self.ov = ttk.Entry(detector)
        lbl3 = ttk.Label(detector, text="Threshold:")
        self.thr = ttk.Entry(detector)
        lbl4 = ttk.Label(detector, text="Temperature:")
        self.tem = ttk.Entry(detector)
        lbl1.grid(row=0, column=0)
        self.md.grid(row=0, column=1, sticky="ew")
        lbl2.grid(row=1, column=0)
        self.ov.grid(row=1, column=1, sticky="ew")
        lbl3.grid(row=1, column=2)
        self.thr.grid(row=1, column=3, sticky="ew")
        lbl4.grid(row=0, column=2)
        self.tem.grid(row=0, column=3, sticky="ew")

        initial = ttk.Labelframe(self.pg1, text="Data")
        initial.grid(columnspan=2, sticky="nsew")
        initial.rowconfigure(0, weight=1)
        initial.rowconfigure(1, weight=1)
        initial.rowconfigure(2, weight=1)
        initial.columnconfigure(1, weight=1)
        initial.columnconfigure(3, weight=1)

        lbl5 = ttk.Label(initial, text="a:")
        self.ad = ttk.Entry(initial)
        self.ad.bind("<FocusOut>", lambda event: self.changeMax())
        lbl6 = ttk.Label(initial, text="Starting Bin Size:")
        self.startd = ttk.Entry(initial)
        self.startd.bind("<FocusOut>", lambda event : ...
            self.changeMax())
        lbl7 = ttk.Label(initial, text="Maximum Bins:")
        self.maxd = ttk.Entry(initial)
        self.maxd.bind("<FocusOut>", lambda event : self.changeA())
        lbl8 = ttk.Label(initial, text="Endtime:")
        self.endd = ttk.Entry(initial)
        self.endd.bind("<FocusOut>", lambda event : self.changeMax())
        lbl9 = ttk.Label(initial, text="Number of Data Points:")
        self.numd = ttk.Entry(initial)
        lbl5.grid(row=0, column=0)
        self.ad.grid(row=0, column=1, sticky="ew")
        lbl6.grid(row=1, column=0)
        self.startd.grid(row=1, column=1, sticky="ew")
        lbl7.grid(row=0, column=2)
        self.maxd.grid(row=0, column=3, sticky="ew")
        lbl8.grid(row=1, column=2)
        self.endd.grid(row=1, column=3, sticky="ew")
        lbl9.grid(row=2, column=0)
        self.numd.grid(row=2, column=1, sticky="ew")

        button = ttk.Button(self.pg1, text="Reset to Default", ...
            command=lambda : self.reset())
        button.grid(row=2, column=0, sticky="ew")
        button2 = ttk.Button(self.pg1, text="Run", command=lambda ...
            : self.runprg())
        button2.grid(row=2, column=1, sticky="ew")
```

```

    def changeMax(self):
        if self.conditions:
            newa = float(self.ad.get())
            self.maxd.delete(0, "end")
            self.maxd.insert("end", fn.getmaxbins(newa, ...
               float(self.startd.get()), float(self.endd.get())))

    def changeA(self):
        if self.conditions:
            newm = int(self.maxd.get())
            self.ad.delete(0, "end")
            self.ad.insert("end", fn.geta(newm, ...
               float(self.startd.get()), float(self.endd.get())))

    def reset(self):
        if self.conditions:
            self.md.delete(0, "end")
            self.md.insert("end", self.conditions[2])
            self.ov.delete(0, "end")
            self.ov.insert("end", self.conditions[4])
            self.thr.delete(0, "end")
            self.thr.insert("end", self.conditions[5])
            self.tem.delete(0, "end")
            self.tem.insert("end", self.conditions[3])
            self.ad.delete(0, "end")
            self.ad.insert("end", df.a)
            self.startd.delete(0, "end")
            self.startd.insert("end", df.start)
            self.endd.delete(0, "end")
            self.endd.insert("end", df.endtime)
            self.maxd.delete(0, "end")
            self.maxd.insert("end", df.maxbins)
            self.numd.delete(0, "end")
            self.numd.insert("end", df.numofdata)

    def runprg(self):
        if self.conditions:
            print "Running Program ..."

            self.model = self.md.get()
            self.over = self.ov.get()
            self.thres = self.thr.get()
            self.temp = self.tem.get()
            self.a = float(self.ad.get())
            self.start = float(self.startd.get())
            self.endtime = float(self.endd.get())
            self.maxbins = int(self.maxd.get())
            self.numofdata = int(self.numd.get())
            print "...%i", self.numofdata
            self.actualdata = fn.parsedata(self.fullfile, ...
               self.numofdata)
            self.lastnum = fn.last(self.actualdata, self.endtime)
            self.overalltime = ...
               (self.actualdata[len(self.actualdata)-1] - ...
               self.actualdata[0]) * df.resolution
            self.avgdcs = len(self.actualdata) / self.overalltime
            self.binedges = fn.bins(self.maxbins, self.start, self.a)

            self.differenced = fn.differences(self.lastnum, ...
               self.maxbins, self.actualdata, self.start, ...
               self.a, self.endtime)
            self.diffdata = self.differenced[0]
            self.errors = self.differenced[1]
            self.numberofalldiffs = self.differenced[2]
            self.normed = fn.norm(self.lastnum, self.maxbins, ...
               self.diffdata, self.binedges)
            self.logged = fn.log(self.normed, self.maxbins)

            self.dc = fn.dark(self.normed, 5, self.maxbins)
            self.darkcount = (self.normed[-2] + self.normed[-3] + ...
               self.normed[-4]) / 3
            self.af = fn.area(self.darkcount, self.normed, ...
               self.binedges, self.maxbins)
            self.afarea = self.af[0]
            self.afsums = self.af[1]
            self.afarray = self.af[2]
            self.afpercent = self.afarea * 100

            self.rowdata = [self.name, self.model, self.temp, ...
               self.over, self.thres, self.avgdcs, ...
               self.darkcount, self.afpercent, self.maxbins, ...
               self.a, self.numofdata, self.overalltime, ...
               self.endtime, self.numberofalldiffs, self.lastnum]
            self.headers = ["Filename", "Model", "Temperature", ...
               "Over Voltage", "Comparator Threshold", "Average ...
               Dark Counts", "Real Dark Counts", "Afterpulse ...
               Percentage", "Number of Bins", "a", "Length of ...
```

```
               Data Used", "Overall Time", "Endtime", "Number of ...
               Differences", "Last Number"]
            fn.writetable(self.rowdata, self.headers, self.path)

            self.x = ...
               np.array(range(self.maxbins+1)[self.normed.index(max(self.normed))
            self.y = ...
               np.array(self.normed[self.normed.index(max(self.normed)):len(self.

            print "Done Processing"
            print "Dark Count: %s" % self.darkcount
            print "Afterpulse Percentage: %s" % self.afpercent
            self.drawGraphs()
            self.prgrun = True

    def optsSave(self):
        self.pg2 = ttk.Frame(self.note)
        self.note.add(self.pg2, text="Save Files")
        for row in range(1, 7):
            self.pg2.rowconfigure(row, weight=2)
        self.pg2.rowconfigure(0, weight=1)
        self.pg2.columnconfigure(0, weight = 1)
        self.pg2.columnconfigure(1, weight = 1)
        self.pg2.columnconfigure(2, weight = 1)

        title = ttk.Label(self.pg2, text="Select Data to Save")
        saveas = ttk.Label(self.pg2, text="Save File As")
        title.grid(row=0, column=0, sticky="ew")
        saveas.grid(row=0, column=1, sticky="ew")

        self.var1 = tk.IntVar()
        self.var2 = tk.IntVar()
        self.var3 = tk.IntVar()
        self.var4 = tk.IntVar()
        self.var5 = tk.IntVar()
        self.var6 = tk.IntVar()
        self.button1 = ttk.Checkbutton(self.pg2, ...
           text="Conditions", variable = self.var1, ...
           command=lambda num=1: self.showName(num))
        self.button2 = ttk.Checkbutton(self.pg2, ...
           text="Differenced", variable = self.var2, ...
           command=lambda num=2: self.showName(num))
        self.button3 = ttk.Checkbutton(self.pg2, ...
           text="Normalized", variable = self.var3, ...
           command=lambda num=3: self.showName(num))
        self.button4 = ttk.Checkbutton(self.pg2, text="Logged", ...
           variable = self.var4, command=lambda num=4: ...
           self.showName(num))
        self.button5 = ttk.Checkbutton(self.pg2, text="Errors", ...
           variable = self.var5, command=lambda num=5: ...
           self.showName(num))
        self.button6 = ttk.Checkbutton(self.pg2, ...
           text="All—in—One", variable = self.var6, ...
           command=lambda num=6: self.showName(num))
        self.button1.grid(row=1, column=0, sticky="ew")
        self.button2.grid(row=4, column=0, sticky="ew")
        self.button3.grid(row=2, column=0, sticky="ew")
        self.button4.grid(row=5, column=0, sticky="ew")
        self.button5.grid(row=3, column=0, sticky="ew")
        self.button6.grid(row=6, column=0, sticky="ew")

        self.entry1 = ttk.Entry(self.pg2)
        self.entry2 = ttk.Entry(self.pg2)
        self.entry3 = ttk.Entry(self.pg2)
        self.entry4 = ttk.Entry(self.pg2)
        self.entry5 = ttk.Entry(self.pg2)
        self.entry6 = ttk.Entry(self.pg2)
        self.entry1.grid(row=1, column=1, sticky="ew")
        self.entry2.grid(row=4, column=1, sticky="ew")
        self.entry3.grid(row=2, column=1, sticky="ew")
        self.entry4.grid(row=5, column=1, sticky="ew")
        self.entry5.grid(row=3, column=1, sticky="ew")
        self.entry6.grid(row=6, column=1, sticky="ew")

        self.res = ttk.Button(self.pg2, text="Reset to Default ...
           Names", command = lambda : self.resetName())
        self.res.grid(row=3, column=2, sticky="ew")
        self.save = ttk.Button(self.pg2, text="Save Files", ...
           command = lambda : self.saveFiles())
        self.save.grid(row=4, column=2, sticky="ew")

    def showName(self, num):
        if self.conditions:
            self.resetName()

    def resetName(self):
        if self.conditions:
            if self.var1.get():
                self.entry1.delete(0, "end")
                self.entry1.insert("end", self.name + "_" + ...
                    str(self.a) + "_conds.txt")
            else:
                self.entry1.delete(0, "end")
            if self.var2.get():
                self.entry2.delete(0, "end")
                self.entry2.insert("end", self.name + "_" + ...
                    str(self.a) + "_diffdata.txt")
            else:
                self.entry2.delete(0, "end")
            if self.var3.get():
                self.entry3.delete(0, "end")
                self.entry3.insert("end", self.name + "_" + ...
                    str(self.a) + "_normed.txt")
            else:
                self.entry3.delete(0, "end")
            if self.var4.get():
                self.entry4.delete(0, "end")
                self.entry4.insert("end", self.name + "_" + ...
                    str(self.a) + "_logged.txt")
            else:
                self.entry4.delete(0, "end")
            if self.var5.get():
                self.entry5.delete(0, "end")
                self.entry5.insert("end", self.name + "_" + ...
                    str(self.a) + "_errors.txt")
            else:
                self.entry5.delete(0, "end")
            if self.var6.get():
                self.entry6.delete(0, "end")
                self.entry6.insert("end", self.name + "_" + ...
                    str(self.a) + "_all.txt")
            else:
                self.entry6.delete(0, "end")

        if self.prgrun:
            if self.var7.get():
                self.entry7.delete(0, "end")
                self.entry7.insert("end", "1")
            else:
                self.entry7.delete(0, "end")
            if self.var8.get():
                self.entry8.delete(0, "end")
                self.entry8.insert("end", "1")
            else:
                self.entry8.delete(0, "end")
            if self.var9.get():
                self.entry9.delete(0, "end")
                self.entry9.insert("end", "1")
            else:
                self.entry9.delete(0, "end")
            if self.var10.get():
                self.entry10.delete(0, "end")
                self.entry10.insert("end", "1")
            else:
                self.entry10.delete(0, "end")
            if self.var11.get():
                self.entry11.delete(0, "end")
                self.entry11.insert("end", "1")
            else:
                self.entry11.delete(0, "end")


    def saveFiles(self):
        if self.prgrun:
            print "Saving Files ..."
            newdirec = self.filename + "_" + str(self.a)
            fn.makedirec(newdirec)
            if self.entry1.get()[-4:] != ".txt":
                new1 = newdirec + os.sep + self.entry1.get() + ".txt"
            else:
                new1 = newdirec + os.sep + self.entry1.get()
            if self.entry2.get()[-4:] != ".txt":
                new2 = newdirec + os.sep + self.entry2.get() + ".txt"
            else:
                new2 = newdirec + os.sep + self.entry2.get()
            if self.entry3.get()[-4:] != ".txt":
                new3 = newdirec + os.sep + self.entry3.get() + ".txt"
            else:
                new3 = newdirec + os.sep + self.entry3.get()
            if self.entry4.get()[-4:] != ".txt":
                new4 = newdirec + os.sep + self.entry4.get() + ".txt"
            else:
                new4 = newdirec + os.sep + self.entry4.get()
            if self.entry5.get()[-4:] != ".txt":
                new5 = newdirec + os.sep + self.entry5.get() + ".txt"
            else:
                new5 = newdirec + os.sep + self.entry5.get()
            if self.entry6.get()[-4:] != ".txt":
                new6 = newdirec + os.sep + self.entry6.get() + ".txt"
            else:
                new6 = newdirec + os.sep + self.entry6.get()

            allconds = {"filename": self.name,"model": ...
               self.model, "temp": self.temp, "over": self.over, ...
               "threshold": self.thres, "a": self.a, "start": ...
               self.start, "endtime": self.endtime, "maxbins": ...
               self.maxbins, "numberofdata": self.numofdata}
            allinone = {"conditions": allconds, "diffdata": ...
               self.diffdata, "normed": self.normed, "logged": ...
               self.logged, "errors": self.errors}

            if self.var1.get():
                fn.wwithnames(new1, allconds)
            if self.var2.get():
                fn.writeto(new2, self.diffdata)
            if self.var3.get():
                fn.writeto(new3, self.normed)
            if self.var4.get():
                fn.writeto(new4, self.logged)
            if self.var5.get():
                fn.writeto(new5, self.errors)
            if self.var6.get():
                fn.wwithnames(new6, allinone)

            print "Files Saved"

    def optsCurve(self):
        self.pg4 = ttk.Frame(self.note)
        self.note.add(self.pg4, text="Curve Fitting")

        for row in range(1, 6):
            self.pg4.rowconfigure(row, weight=2)
        self.pg4.rowconfigure(0, weight=1)
        self.pg4.columnconfigure(0, weight = 1)
        self.pg4.columnconfigure(1, weight = 1)
        self.pg4.columnconfigure(2, weight = 1)
        self.pg4.columnconfigure(3, weight = 1)
        self.pg4.columnconfigure(4, weight = 1)

        title = ttk.Label(self.pg4, text="Number of e")
        params = ttk.Label(self.pg4, text="Initial Parameter (a ...
           power of 10 i.e. 10000)")
        colour = ttk.Label(self.pg4, text="Line Colour")
        title.grid(row=0, column=0, sticky="ew")
        params.grid(row=0, column=1, sticky="ew")
        colour.grid(row=0, column=2, sticky="ew")

        self.var7 = tk.IntVar()
        self.var8 = tk.IntVar()
        self.var9 = tk.IntVar()
        self.var10 = tk.IntVar()
        self.var11 = tk.IntVar()
        self.button7 = ttk.Checkbutton(self.pg4, text="1", ...
           variable = self.var7, command = lambda num=7: ...
           self.showName(num))
        self.button8 = ttk.Checkbutton(self.pg4, text="2", ...
           variable = self.var8, command = lambda num=8: ...
           self.showName(num))
        self.button9 = ttk.Checkbutton(self.pg4, text="3", ...
           variable = self.var9, command = lambda num=9: ...
           self.showName(num))
        self.button10 = ttk.Checkbutton(self.pg4, text="4", ...
           variable = self.var10, command = lambda num=10: ...
           self.showName(num))
        self.button11 = ttk.Checkbutton(self.pg4, text="5", ...
           variable = self.var11, command = lambda num=11: ...
           self.showName(num))
        self.button7.grid(row=1, column=0, sticky="ew")
        self.button8.grid(row=2, column=0, sticky="ew")
        self.button9.grid(row=3, column=0, sticky="ew")
        self.button10.grid(row=4, column=0, sticky="ew")
        self.button11.grid(row=5, column=0, sticky="ew")

        self.entry7 = ttk.Entry(self.pg4)
        self.entry8 = ttk.Entry(self.pg4)
        self.entry9 = ttk.Entry(self.pg4)
        self.entry10 = ttk.Entry(self.pg4)
        self.entry11 = ttk.Entry(self.pg4)
        self.entry7.grid(row=1, column=1, sticky="ew")
        self.entry8.grid(row=2, column=1, sticky="ew")
        self.entry9.grid(row=3, column=1, sticky="ew")
        self.entry10.grid(row=4, column=1, sticky="ew")
        self.entry11.grid(row=5, column=1, sticky="ew")

        label1 = ttk.Label(self.pg4, text="Blue")
        label1.grid(row=1, column=2, sticky="ew")
        label2 = ttk.Label(self.pg4, text="Red")
        label2.grid(row=2, column=2, sticky="ew")
        label3 = ttk.Label(self.pg4, text="Yellow")
        label3.grid(row=3, column=2, sticky="ew")
        label4 = ttk.Label(self.pg4, text="Cyan")
        label4.grid(row=4, column=2, sticky="ew")
        label5 = ttk.Label(self.pg4, text="Magenta")
        label5.grid(row=5, column=2, sticky="ew")

        self.plot = ttk.Button(self.pg4, text="Plot Curve Fits", ...
           command = lambda : self.plotCurve())
        self.plot.grid(row=2, column=3, sticky="ew")
        self.save1 = ttk.Button(self.pg4, text="Save Graph", ...
           command = lambda : self.saveGraph())
        self.save1.grid(row=3, column=3, sticky="ew")
        self.save2 = ttk.Button(self.pg4, text="Save Params", ...
           command = lambda : self.saveParams())
        self.save2.grid(row=4, column=3, sticky="ew")
        self.entry12 = ttk.Entry(self.pg4)
        self.entry13 = ttk.Entry(self.pg4)
        self.entry12.grid(row=3, column=4, sticky="ew")
        self.entry13.grid(row=4, column=4, sticky="ew")
        label6 = ttk.Label(self.pg4, text="File Names")
        label6.grid(row=0, column=4, sticky="ew")

    def f1(self, x, b, c):
        return b * np.exp(-c * self.start *  self.a**x) + ...
           self.darkcount

    def f2(self, x, b, c, f, g):
        return b * np.exp(-c * self.start * self.a**x) + f * ...
           np.exp(-g * self.start * self.a**x) + self.darkcount

    def f3(self, x, b, c, f, g, h, i):
        return b * np.exp(-c * self.start * self.a**x) + f * ...
           np.exp(-g * self.start * self.a**x) + h * np.exp(-i * ...
           self.start * self.a**x) + self.darkcount

    def f4(self, x, b, c, f, g, h, i, j, k):
        return b * np.exp(-c * self.start * self.a**x) + f * ...
           np.exp(-g * self.start * self.a**x) + h * np.exp(-i * ...
           self.start * self.a**x) + j * np.exp(-k * self.start ...
           * self.a**x) + self.darkcount

    def f5(self, x, b, c, f, g, h, i, j, k, l, m):
        return b * np.exp(-c * self.start * self.a**x) + f * ...
           np.exp(-g * self.start * self.a**x) + h * np.exp(-i * ...
           self.start * self.a**x) + j * np.exp(-k * self.start ...
           * self.a**x) + l * np.exp(-m * self.start * ...
           self.a**x) + self.darkcount

    def f6(self, x, b, c, f, g, h, i, j, k, l, m, n, o):
        return  self.f5(x, b, c, f, g, h, i, j, k, l, m)+ n * ...
           np.exp(-o * self.start * self.a**x)

    def plotCurve(self):
        if self.prgrun:
            self.params1 = []
            self.params2 = []
            self.params3 = []
            self.params4 = []
            self.params5 = []
            self.params6 = []

            if self.var7.get():
                print "Curve fitting 1 ..."
                try:
                    p1 = int(self.entry7.get())
                    self.params1, covariance1 = ...
                       curve_fit(self.f1, self.x, self.y, p0=[1, ...
                       p1])
                    print self.params1
                except RuntimeError:
                    print "Fitting Error: Please change Initial ...
                       Parameters and try again"
                    return
            if self.var8.get():
                print "Curve fitting 2 ..."
                try:
                    p2 = int(self.entry8.get())
                    self.params2, covariance2 = ...
                       curve_fit(self.f2, self.x, self.y, ...
                       p0=[1,p2,1,p2])
                    print self.params2
                except RuntimeError:
```

```
                print "Fitting Error: Please change Initial ...
                    Parameters and try again"
                return
        if self.var9.get():
            print "Curve fitting 3 ..."
            try:
                p3 = int(self.entry9.get())
                self.params3, covariance3 = ...
                    curve_fit(self.f3, self.x, self.y, ...
                    p0=[1,p3,1,p3,1,p3])
                print self.params3
            except RuntimeError:
                print "Fitting Error: Please change Initial ...
                    Parameters and try again"
                return
        if self.var10.get():
            print "Curve fitting 4 ..."
            try:
                #p4 = int(self.entry10.get())
                #self.params4, covariance4 = ...
                    curve_fit(self.f4, self.x, self.y, ...
                    p0=[1,p4,1,p4,1,p4,1,p4])
                self.params4, covariance4 = ...
                    curve_fit(self.f4, self.x, self.y, ...
                    maxfev=50000)
                print self.params4
            #except RuntimeError:
            except Exception as err:
                print type(err)
                print err.args
                print err
                print "Fitting Error: Please change Initial ...
                    Parameters and try again"
                return
        if self.var11.get():
            print "Curve fitting 5 ..."
            try:
                #p5 = int(self.entry11.get())
                #self.params5, covariance5 = ...
                    curve_fit(self.f5, self.x, self.y, ...
                    p0=[1,p5,1,p5,1,p5,1,p5,1,p5])
                #self.params5, covariance5 = ...
                    curve_fit(self.f5, self.x, self.y, ...
                    p0=[1,p5,1,p5,1,p5,1,p5,1,p5])
                #p0=[30, 30000, 0, 0, 350, 1700000, 400, ...
                   1700000, 100, 300000]
                self.params5, covariance5 = ...
                   curve_fit(self.f5, self.x, self.y, ...
                   maxfev=50000)
                #self.params6, covariance6 = ...
                   curve_fit(self.f6, self.x, self.y, ...
                   maxfev=50000)
                print self.params5
                #print self.params6
            #except RuntimeError:
            except Exception as err:
                print err
                print "Fitting Error: Please change Initial ...
                   Parameters and try again"
                return
        print "Plotting Curve Fitted Graph ..."

        if self.plotcurve:
            self.gphf3.destroy()

        #timesinsec = [0, 10**-9, 10**-8, 10**-7, 10**-6, ...
           10**-5, 10**-4, 10**-3, 10**-2, 10**-1, 0, 0.5, 1,2]
        timesinsec = [0, 10**-9, 10**-8, 10**-7, 10**-6, ...
           10**-5, 10**-4, 10**-3, 10**-2, 10**-1, 1, 10**1]
        times = [0, '1 ns', '10 ns', '100 ns', r'$10^{-6}$', ...
           r'$10^{-5}$',r'$10^{-4}$',r'$10^{-3}$',r'$10^{-2}$',r'$10^{-1}$',
           r'$10^{0}$']
        numfortime = fn.time(timesinsec, self.start, self.a)
        checked = False

        self.gphf3 = ttk.Frame(self.gph3)
        self.gphf3.pack(fill="both", expand="yes")
        self.fig3 = plt.figure()
        plt.bar(range(self.maxbins+1), self.normed, log=True, ...
           width=1, color='0.5', edgecolor='w')
        plt.xticks(numfortime, times)
        plt.ylabel("Dark count probability $s^{-1}$")
        plt.xlabel("Time after click")
        plt.grid(axis="both")
        #self.params5i = [  7.70588954e+04,   8.38545084e+05, ...
             8.37291039e+04,   9.26471484e+05, \
        #                1.3 * 1.80974878e+00,  0.9 * ...
           1.72225219e+03,  -1.59868460e+05, 8.81143768e+05, ...
```

```
            1 * 3.84207195e+01, 3.49983366e+04]
        if self.var7.get():
            plt.plot(self.x, self.f1(self.x, *self.params1), ...
               'b', linewidth=1.5)
            checked = True
        if self.var8.get():
            plt.plot(self.x, self.f2(self.x, *self.params2), ...
               'r', linewidth=1.5)
            checked = True
        if self.var9.get():
            plt.plot(self.x, self.f3(self.x, *self.params3), ...
               'y', linewidth=1.5)
            checked = True
        if self.var10.get():
            plt.plot(self.x, self.f4(self.x, *self.params4), ...
               'c', linewidth=1.5)
            checked = True
        if self.var11.get():
            plt.plot(self.x, self.f5(self.x, *self.params5), ...
               'm', linewidth=1.5)
            #plt.plot(self.x, self.f6(self.x, *self.params6), ...
               'g', linewidth=1.5)
            #plt.plot(self.x, self.f5(self.x, ...
               *self.params5i), 'p', linewidth=1.5)
            checked = True
        self.canvas3 = FigureCanvasTkAgg(self.fig3, self.gphf3)
        self.canvas3.show()
        self.canvas3.get_tk_widget().pack(fill="both", ...
           expand="yes")
        toolbar = NavigationToolbar2TkAgg(self.canvas3, ...
           self.gphf3)
        toolbar.update()
        self.canvas3._tkcanvas.pack(fill="both", expand="yes")

        newfilename = self.name + "_" + str(self.a) + "_" + ...
           "CurveFitted"

        if checked:
            self.entry12.delete(0, "end")
            self.entry12.insert("end", newfilename + ".pdf")
            self.entry13.delete(0, "end")
            self.entry13.insert("end", newfilename + ...
               "Params.txt")

        self.plotcurve = True
        print "Done Plotting"

def saveGraph(self):
    if self.plotcurve:
        timesinsec = [0, 10**-9, 10**-8, 10**-7, 0.5*10**-6, ...
           10**-6, 10**-5, 10**-4, 10**-3, 10**-2, ...
           10**-1,0.5, 1, 2]
        times = [0, '1 ns', '10 ns', '100 ns', ...
           r'$\frac{1}{2}$ $\mu$s', r'1 $\mu$s', r'10 ...
           $\mu$s',r'100 $\mu$s',r'$\frac{1}{1000}$ ...
           s',r'$\frac{1}{100}$ s',r'$\frac{1}{10}$ s', ...
           r'$\frac{1}{2}$ s', 1, 2]
        numfortime = fn.time(timesinsec, self.start, self.a)

        newdirec = self.filename + "_" + str(self.a)
        fn.makedirec(newdirec)
        if self.entry12.get()[-4:] != ".pdf":
            newfilename = newdirec + os.sep + ...
               self.entry12.get() + ".pdf"
        else:
            newfilename = newdirec + os.sep + self.entry12.get()

        plt.figure(figsize=(18,9))
        plt.bar(range(self.maxbins+1), self.normed, width=1, ...
           color='0.5', edgecolor='w')
        plt.xticks(numfortime, times)
        plt.grid(axis="both")
        if self.var7.get():
            plt.plot(self.x, self.f1(self.x, *self.params1), ...
               'b', linewidth=1.5)
        if self.var8.get():
            plt.plot(self.x, self.f2(self.x, *self.params2), ...
               'r', linewidth=1.5)
        if self.var9.get():
            plt.plot(self.x, self.f3(self.x, *self.params3), ...
               'y', linewidth=1.5)
        if self.var10.get():
            plt.plot(self.x, self.f4(self.x, *self.params4), ...
               'c', linewidth=1.5)
        if self.var11.get():
            plt.plot(self.x, self.f5(self.x, *self.params5), ...
               'm', linewidth=1.5)


        plt.savefig(newfilename)
        print "Graph Saved"

def saveParams(self):
    if self.plotcurve:
        newdirec = self.filename + "_" + str(self.a)
        fn.makedirec(newdirec)
        if self.entry13.get()[-4:] != ".txt":
            newfilename = newdirec + os.sep + ...
               self.entry13.get() + ".txt"
        else:
            newfilename = newdirec + os.sep + self.entry13.get()
        params = {"1 Exponent": self.params1, "2 Exponents": ...
           self.params2, "3 Exponents": self.params3, "4 ...
           Exponents": self.params4, "5 Exponents": ...
           self.params5}
        fn.wwithnames(newfilename, params)
        print "Params Saved"

def createGraphs(self):
    gphs = ttk.Labelframe(self.myContainer, text="Graphs")
    gphs.grid(row=0, column=1, rowspan=3, sticky="nsew")

    self.gphNote = ttk.Notebook(gphs)
    self.gphNorm()
    self.gphLog()
    self.gphCurve()
    self.gphNote.pack(expand="yes", fill="both")

def gphNorm(self):
    self.gph1 = ttk.Frame(self.gphNote)
    self.gphNote.add(self.gph1, text="Normed")

def gphLog(self):
    self.gph2 = ttk.Frame(self.gphNote)
    self.gphNote.add(self.gph2, text="Logged")

def gphCurve(self):
    self.gph3 = ttk.Frame(self.gphNote)
    self.gphNote.add(self.gph3, text="Curve Fitted")

def drawGraphs(self):
    if self.prgrun:
        self.gphf1.destroy()
        self.gphf2.destroy()

    print "Drawing Graphs ..."
    #timesinsec = [0, 10**-9, 10**-8, 10**-7, 10**-6, 10**-5, ...
       10**-4, 10**-3, 10**-2, 10**-1,0.5, 1, 2]
    timesinsec = [10**-9, 10**-8, 10**-7, 10**-6, 10**-5, ...
       10**-4, 10**-3, 10**-2, 10**-1, 1]
    #times = [0, '$10^{-9}$', '10 ns', '100 ns', r'1 $\mu$s', ...
       r'10 $\mu$s',r'100 $\mu$s',r'$\frac{1}{1000}$ ...
       s',r'$\frac{1}{100}$ s',r'$\frac{1}{10}$ s', ...
       r'$\frac{1}{2}$ s', 1, 2]
    times = ['$10^{-9}$', '$10^{-8}$', '$10^{-7}$', ...
       r'$10^{-6}$', ...
       r'$10^{-5}$',r'$10^{-4}$',r'$10^{-3}$',r'$10^{-2}$',r'$10^{-1}$', ...
       '$10^0$']
    numfortime = fn.time(timesinsec, self.start, self.a)

    self.gphf1 = ttk.Frame(self.gph1)
    self.gphf1.pack(fill="both", expand="yes")
    self.fig1 = plt.figure()
    plt.bar(range(self.maxbins+1), self.normed, width=1, ...
       color='0.5', edgecolor='w')
    plt.xticks(numfortime, times)
    plt.grid(axis="both")
    self.canvas1 = FigureCanvasTkAgg(self.fig1, self.gphf1)
    self.canvas1.show()
    self.canvas1.get_tk_widget().pack(fill="both", expand="yes")
    toolbar = NavigationToolbar2TkAgg(self.canvas1, self.gphf1)
    toolbar.update()
    self.canvas1._tkcanvas.pack(fill="both", expand="yes")

    self.gphf2 = ttk.Frame(self.gph2)
    self.gphf2.pack(fill="both", expand="yes")
    self.fig2 = plt.figure()
    plt.ylim(10**(-2), 10**4)
    print self.maxbins
    plt.bar(range(self.maxbins+1), self.normed, log=True, ...
       width=1, color='0.5', edgecolor='w')
    plt.xticks(numfortime, times)
    #plt.xlim(10**(-9), 10**0)
    #plt.xscale('log')
    plt.grid(axis="both")
    plt.ylabel("Dark count probability $s^{-1}$")
    plt.xlabel("Time after click")
    self.canvas2 = FigureCanvasTkAgg(self.fig2, self.gphf2)
    self.canvas2.show()
    self.canvas2.get_tk_widget().pack(fill="both", expand="yes")
    toolbar2 = NavigationToolbar2TkAgg(self.canvas2, self.gphf2)
    toolbar2.update()
    self.canvas2._tkcanvas.pack(fill="both", expand="yes")
    print "Done Plotting"
    print "Saving Graphs"

    timesinsec1 = [0, 10**-9, 10**-8, 10**-7, 0.5*10**-6, ...
       10**-6, 10**-5, 10**-4, 10**-3, 10**-2, 10**-1,0.5, ...
       1, 2]
    times1 = [0, '1 ns', '10 ns', '100 ns', r'$\frac{1}{2}$ ...
       $\mu$s', r'1 $\mu$s', r'10 $\mu$s',r'100 ...
       $\mu$s',r'$\frac{1}{1000}$ s',r'$\frac{1}{100}$ ...
       s',r'$\frac{1}{10}$ s', r'$\frac{1}{2}$ s', 1, 2]
    numfortime1 = fn.time(timesinsec1, self.start, self.a)

    newdirec = self.filename + "_" + str(self.a)
    fn.makedirec(newdirec)
    newfilename = newdirec + os.sep + self.name + "_" + ...
       str(self.a)

    plt.figure(figsize=(18,9))
    plt.bar(range(self.maxbins+1), self.normed, width=1, ...
       color='0.5', edgecolor='w')
    plt.xticks(numfortime1, times1)
    plt.grid(axis="both")
    plt.savefig(newfilename + ".pdf")

    plt.figure(figsize=(18,9))
    plt.bar(range(self.maxbins+1), self.logged, width=1, ...
       color='0.5', edgecolor='w')
    plt.xticks(numfortime1, times1)
    plt.grid(axis='both')
    plt.savefig(newfilename + "_logged.pdf")

    print "Graphs Saved"


root = tk.Tk()
program = Program(root)
root.mainloop()
```